LICENSE INFORMATION

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

**Preface**  
About this guide .................................. 7  
Audience .................................. 7  
Conventions .................................. 7  
Find product documentation .............................. 8

### 1 Introduction

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive protection</td>
<td>9</td>
</tr>
<tr>
<td>What is McAfee Drive Encryption</td>
<td>9</td>
</tr>
<tr>
<td>How McAfee Drive Encryption works</td>
<td>10</td>
</tr>
<tr>
<td>Product components</td>
<td>10</td>
</tr>
<tr>
<td>Features</td>
<td>11</td>
</tr>
<tr>
<td>Opal self-encrypting drives</td>
<td>12</td>
</tr>
<tr>
<td>Trusted Platform Module</td>
<td>13</td>
</tr>
<tr>
<td>Requirements</td>
<td>15</td>
</tr>
<tr>
<td>Testing for client system requirements</td>
<td>16</td>
</tr>
</tbody>
</table>

### 2 Quick Start Guide

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation prerequisites</td>
<td>18</td>
</tr>
</tbody>
</table>

### 3 Installing Drive Encryption

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the Drive Encryption software</td>
<td>19</td>
</tr>
<tr>
<td>Overview of the installation process</td>
<td>19</td>
</tr>
<tr>
<td>Install the Drive Encryption and Help extensions</td>
<td>20</td>
</tr>
<tr>
<td>Check in the Drive Encryption software packages</td>
<td>21</td>
</tr>
<tr>
<td>Register Microsoft Active Directory</td>
<td>21</td>
</tr>
<tr>
<td>Deploy Drive Encryption to the client system</td>
<td>22</td>
</tr>
<tr>
<td>Drive Encryption activation sequence</td>
<td>26</td>
</tr>
<tr>
<td>Send an agent wake-up call</td>
<td>28</td>
</tr>
<tr>
<td>Install Drive Encryption using a third-party tool</td>
<td>29</td>
</tr>
<tr>
<td>Add users to a system</td>
<td>29</td>
</tr>
<tr>
<td>Assign a policy to users</td>
<td>30</td>
</tr>
<tr>
<td>Configure UBP enforcement</td>
<td>31</td>
</tr>
<tr>
<td>Assign a policy to a system</td>
<td>31</td>
</tr>
<tr>
<td>Enforce Drive Encryption policies on a system</td>
<td>32</td>
</tr>
<tr>
<td>Edit the client tasks</td>
<td>33</td>
</tr>
<tr>
<td>Requirements testing on client systems</td>
<td>33</td>
</tr>
<tr>
<td>Upgrading from EEPC 7.0.x and Drive Encryption 7.1.x to Drive Encryption 7.2</td>
<td>37</td>
</tr>
<tr>
<td>Upgrade to Drive Encryption 7.2</td>
<td>37</td>
</tr>
<tr>
<td>Upgrade systems with TPM autoboot policy enabled</td>
<td>39</td>
</tr>
<tr>
<td>User experience summary</td>
<td>40</td>
</tr>
<tr>
<td>Upgrade checklist</td>
<td>40</td>
</tr>
<tr>
<td>Uninstalling the Drive Encryption client</td>
<td>41</td>
</tr>
<tr>
<td>Disable the Drive Encryption client</td>
<td>41</td>
</tr>
<tr>
<td>Remove Drive Encryption from the client system</td>
<td>42</td>
</tr>
</tbody>
</table>
Remove the Drive Encryption extensions ............................................. 42
Remove the Drive Encryption software packages ............................... 43
Manually uninstall Drive Encryption from the client system .................. 43

4 Drive Encryption offline activation ............................................. 45
How offline activation works ......................................................... 45
Create and download the McAfee Agent installation package .............. 46
Extracting the MSI packages (Agent and PC) .................................. 47
Download and extract the EpeOaGenXML.exe file .............................. 47
Extract and download the Key Server Public Key ............................. 47
Create the user configuration file .................................................... 48
Creating the offline activation package ............................................ 48
Optional offline activation features .................................................. 49
Generate the offline activation package ............................................. 49
Performing offline activation .......................................................... 50
Install the McAfee Agent package .................................................. 51
Install the Agent and PC software packages ..................................... 51
Install the offline activation package and activate Drive Encryption ..... 52
Log on to the client system ......................................................... 52
Perform recovery tasks using DETech ........................................... 53
Machine Key Management ......................................................... 54

5 Managing Drive Encryption policies .......................................... 57
Policy categories ............................................................................. 57
Product Settings policy ................................................................. 58
User-based policy settings ............................................................ 74
Server policy settings ................................................................. 79
Create a policy from the Policy Catalog ......................................... 80
Edit Drive Encryption policy settings from the Policy Catalog .......... 81
Assign a policy to a system group .................................................... 81
Enforce Drive Encryption policies on a system group ....................... 81

6 Managing Drive Encryption users ............................................. 83
Manage the users assigned to a system .......................................... 83
Add group users ........................................................................... 84
Users ......................................................................................... 84
Add local domain users ............................................................... 84
User management through User Directory ...................................... 86
Manage Organizational Units from the User Directory page ........... 86
Manage Users from the User Directory page .................................. 86
Edit user inheritance ..................................................................... 87
How Drive Encryption controls the Windows logon mechanism ......... 87
Enable Single-Sign-On (SSO) on a system ..................................... 88
Synchronize the Drive Encryption password with the Windows password 88
Configure password content rules ................................................ 89
Manage a disabled user in Microsoft Active Directory or User Directory 90
Managing the blacklist rule with the ALDU function ........................... 90
Add an ALDU blacklist policy ....................................................... 91
Configure global user information ................................................. 92
Manage logon hours ................................................................... 92
Define Drive Encryption permission sets for McAfee ePO users ......... 93
How disabling/deleting a user in Active Directory affects the Drive Encryption user ... 93

7 Managing client computers ..................................................... 95
Add a system to an existing system group ...................................... 95
Move systems between groups ..................................................... 96
Select the disks for encryption .................................................. 96
Enable or disable automatic booting ............................................. 97
Enable or disable temporary automatic booting .......................... 98
Set the priority of encryption providers .................................... 99
Maintain a list of incompatible products ..................................... 99
Enable accessibility (USB audio devices) in the Pre-Boot environment .................................................. 100
Allow user to reset self-recovery answers ................................... 101
Manage the default and customized themes .............................. 102
Assign a customized theme to a system .................................... 102
Manage simple words ............................................................... 103
Drive Encryption system recovery ........................................... 104
Managing servers and client systems — general recommendations .................................................. 106
Configure role-based access control for managing Drive Encryption .................................................. 106

8 McAfee Drive Encryption out-of-band management ....................... 109
The DEDeep extension .............................................................. 109
Enable the out-of-band feature .................................................. 110
Configure the out-of-band remediation functionality ..................... 110
Configure the out-of-band unlock PBA feature ............................. 111
Configure the out-of-band management feature .......................... 113
Checklist for using Intel® AMT and Drive Encryption ...................... 114

9 Configuring and managing tokens and readers ......................... 115
Modify the token type associated with a system or group .................. 115
Using a Stored Value token in Drive Encryption ........................... 116
   Associate a Stored Value token with a system or group ................ 116
   Using Single-Sign-On (SSO) .................................................. 117
Using a PKI token in Drive Encryption ....................................... 117
   Associate a PKI token with a system or group .......................... 117
   Using Single-Sign-On (SSO) .................................................. 117
Using a Self-Initializing token in Drive Encryption ....................... 117
   Associate a Self-Initializing token with a system or group ............ 118
   Using Single-Sign-On (SSO) .................................................. 118
Setup scenarios for the Read Username from Smartcard feature ............ 118
   Setting up your environment using the Subject field .................... 119
   Setting up your environment using the Subject Alternative Name - Other Name field .............. 119
Using a Biometric token in Drive Encryption .................................. 120
   Use a UPEK Biometric token in Drive Encryption ....................... 120
   Use a Validity Biometric token in Drive Encryption ...................... 121

10 Managing Drive Encryption reports ...................................... 123
Queries as dashboard monitors ................................................ 123
Create Drive Encryption custom queries .................................... 124
View the standard Drive Encryption reports ............................... 124
Drive Encryption client events ................................................ 126
Create the Drive Encryption dashboard ..................................... 129
View the Drive Encryption dashboard ....................................... 129
Report the encrypted and decrypted systems .............................. 130

11 Recovering users and systems .............................................. 131
Enable or disable the self-recovery functionality .......................... 131
Perform self-recovery on the client computer ............................. 132
Enable or disable the administrator recovery functionality ............. 133
Perform administrator recovery on the client system ..................... 133
Generate the response code for the administrator recovery .............. 134
Smartphone recovery .............................................................. 134
Preface

This guide provides the information you need to configure, use, and maintain 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.

Conventions

This guide uses these typographical conventions and icons.

- **Italic**
  - Title of a book, chapter, or topic; a new term; emphasis

- **Bold**
  - Text that is emphasized

- **Monospace**
  - Commands and other text that the user types; a code sample; a displayed message

- **Narrow Bold**
  - 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:**
  - Extra information to emphasize a point, remind the reader of something, or provide an alternative method

- **Tip:**
  - Best practice information

- **Caution:**
  - Important 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® Drive Encryption delivers powerful encryption that protects data from unauthorized access, loss, and exposure. With data breaches on the rise, it is important to protect information assets and comply with privacy regulations.

Contents
- Comprehensive protection
- What is McAfee Drive Encryption
- How McAfee Drive Encryption works
- Product components
- Features
- Requirements
- Testing for client system requirements

Comprehensive protection

The McAfee Drive Encryption suite provides multiple layers of defense against data loss with several integrated modules that address specific areas of risk. The suite provides protection for individual computers and roaming laptops with Basic Input Output System (BIOS) and Unified Extensible Firmware Interface (UEFI).

This release supports UEFI-based tablets, using a McAfee ePO Tablet Test tool to verify if the pre-boot environment will respond to the touch interface on your tablet. For more information about this tool, see this KnowledgeBase article KB78050.

What is McAfee Drive Encryption

McAfee Drive Encryption is a strong cryptographic utility for denying unauthorized access to data stored on any system or disk when it is not in use.

It prevents the loss of sensitive data, especially from lost or stolen equipment. It protects the data with access control using Pre-Boot Authentication and a powerful encryption engine.

To log on to a system, the user must first authenticate through the pre-boot environment. On successful authentication, the client system’s operating system loads and gives access to normal system operation.

McAfee Drive Encryption made up of the encryption software installed on client systems and the managing component on the servers. It is deployed and managed through McAfee® ePolicy Orchestrator® (McAfee® ePO®) using policies. A policy is a set of rules that determines how McAfee Drive Encryption software functions on the user’s computer.

The disk encryption process is completely transparent to the user and has little impact on the computer's performance.
How McAfee Drive Encryption works

McAfee Drive Encryption protects the data on a system by taking control of the hard disk or self-encrypting drive (Opal) from the operating system. When used with self-encrypting drives, Drive Encryption manages the disk authentication keys; with non-self-encrypting drives. The Drive Encryption driver encrypts all data written to the disk and decrypts the data read off the disk.

For more information about Opal, see Opal self-encrypting drives.

The McAfee Drive Encryption software is installed on the client system. After the installation is complete, and depending on the Drive Encryption policy assigned to the client system, the client system starts to activate Drive Encryption.

Encryption begins only upon successful activation. During the activation process, the system synchronizes with McAfee ePO and acquires user data, token data, and Pre-Boot theme data. Pre-Boot Authentication does not appear if the system is restarted during the activation process.

The system can also be activated without synchronizing with the McAfee ePO server when performing the Offline Activation process.

Drive Encryption takes control of the disk only after the activation process is successfully completed. It then begins to enforce the encryption policy. After successful activation and system restart, the user authenticates and logs on through the Pre-Boot environment, which then loads the operating system.

Product components

Each McAfee Drive Encryption component or feature plays a part in protecting your systems.

**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. The McAfee ePO console:

- Allows you to manage McAfee Drive Encryption policies on the client computer
- Allows you to deploy and manage McAfee Drive Encryption products
- Provides comprehensive reporting and product deployment capabilities; all through a single point of control

This guide does not provide detailed information about installing or using the McAfee ePO software. See the product documentation for your version of McAfee ePO.

**Policies**

McAfee Drive Encryption is managed through McAfee ePO using a combination of user-based policies and product settings policies. The McAfee ePO console allows you to enforce policies across groups of computers or on a single computer. Any new policy enforcement through McAfee ePO overrides the existing policy that is already set on the individual systems. For information about policies and how they are enforced, see the product documentation for your version of McAfee ePO.

**Product extensions and packages**

The Drive Encryption extension installed in McAfee ePO defines the encryption algorithm for the client system. The Drive Encryption software packages checked in to McAfee ePO defines the actual Drive Encryption software that is installed on the client system.
Drive Encryption Admin

The Drive Encryption administration system called Drive Encryption Admin defines the generic Drive Encryption settings for product settings policies, user-based policies, local domain user settings, and user server settings.

LDAP server

Drive Encryption acquires users through the Microsoft Active Directory (AD) or through the McAfee ePO User Directory. You must have a registered LDAP server or have installed User Directory in order to use Policy Assignment Rules to enable dynamically assigned permission sets, and to enable manual and automatic user account creation.

Drive Encryption can also acquire users through standalone user management using the User Directory feature, which removes the dependency on LDAP server. For more information, see the User management through User Directory section.

How does LDAP Sync work

In Active Directory, it is possible to create a group structure where a group contains several other groups. With LDAP Sync, all the groups can be synchronized recursively.

Consider the following AD structure, where:

- Group A contains Group B and Group C
- Group B contains Group D

If EEAdmin registers for Group A to perform recursive sync, the users of Group B, Group D, and Group C are synchronized recursively.

Client system components

For McAfee ePO to communicate with a client system, the client system is configured with these components:

- Windows operating system
- McAfee® Agent for Windows

The McAfee ePO server can be configured to deploy McAfee Agent, Drive Encryption Agent, and the Drive Encryption product to client system using McAfee ePO client tasks.

For more details and procedures, see the product documentation for your version of McAfee ePO.

Features

These features of Drive Encryption are important for your organization’s system security and protection.

- **Centralized management** — Drive Encryption integrates fully into McAfee ePO, leveraging the McAfee ePO infrastructure for automated security reporting, monitoring, deployment, and policy administration.

- **Transparent encryption** — Drive Encryption enables transparent encryption without hindering users or system performance.

- **Access control** — Drive Encryption enforces strong access control with Pre-Boot Authentication.
• **Remote management capability** — Drive Encryption supports Intel® Active Management Technology (Intel® AMT) for remotely managing and securing systems in conjunction with McAfee® ePO Deep Command.

• **Recovery** — The recovery feature allows the end user to perform emergency recovery when the system fails to reboot or its Pre-Boot File System (PBFS) is corrupt.

• **Support for self-encrypting drives** — The combination of Drive Encryption and McAfee ePO enables centralized management of self-encrypting drives that conform to the Opal standard from Trusted Computing Group (TCG), including locking and unlocking, reporting, recovery, policy enforcement, and user management. For details, see [Opal self-encrypting drives](Opal self-encrypting drives).

• **Trusted Platform Module (TPM)** — Drive Encryption supports TPM 2.0 on Windows 8 and above UEFI systems in order to provide platform authentication without the need for Pre-Boot Authentication (PBA).

## Opal self-encrypting drives

Opal drives are self-contained, standalone hard disk drives (HDDs) that conform to the TCG Opal standard. Drive Encryption provides a management tool for Opal drives.

### Background

An Opal drive is always encrypted by the onboard crypto processor; however, it might or might not be locked. Although the Opal drives handle all of the encryption, the unlock keys need to be managed by Drive Encryption. If an Opal drive is not managed, it behaves and responds like a non-Opal HDD.

### Management of Opal drives

The combination of Drive Encryption and McAfee ePO for Opal provides these features:

- Centralized management
- Reporting and recovery functionality
- Secure Pre-Boot Authentication that unlocks the Opal drive
- Efficient user management
- Continuous policy enforcement

In some cases, Drive Encryption installed systems might fail to lock OPAL disks during reboot. Subsequent policy enforcement might fail until a full power-cycle is performed.

### Recovery

Importantly, the overall experience for administrators and users in installing and using Drive Encryption is the same, whether the target system has an Opal drive or a non-Opal HDD. The installation of the product extension, deployment of the software packages, policy definition and enforcement, recovery, and the method of management are the same for systems with Opal and non-Opal HDDs. You can apply the same policy to Opal and non-Opal systems, and the client system will choose the appropriate encryption provider for the system, giving Drive Encryption a powerful, seamless and transparent approach to managing Opal and non-Opal systems in the same environment.

To activate a system using Opal encryption, Windows 7 SP1 or later is required. On systems with Opal drives where the operating system is Windows 7 RTW or earlier, software encryption is used.

Opal activation might occasionally fail because certain Microsoft APIs used in the activation process fail. If this occurs, the activation will restart at the next ASCI.
Important note about reimagining Opal drives

When any OPAL system activated using OPAL encryption is reimaged and restarted without removing Drive Encryption prior to reimaging, the user will be locked out of the system. This happens because:

- The pre-boot remains active, but the authentication screen is not displayed, and the user is locked out, even though, you have reimaged the disk
- The Pre-Boot File System (PBFS) is destroyed during the imaging process, thereby user data is not available to authenticate.

Compatible systems

Opal self-encrypting drives are supported on:

- Systems that boot using BIOS in AHCI mode
- Systems that boot using UEFI only where the UEFI protocol `EFI_STORAGE_SECURITY_COMMAND_PROTOCOL` is present on the system. This protocol is only guaranteed to be present if the system is Windows 8 logo compliant and the system was shipped from the manufacturer fitted with an Opal self-encrypting drive.

This release provides support for Opal Compatibility tool that tests the Opal drive on your systems to verify if it is compatible to use the Opal features. For more information about this tool, see this KnowledgeBase article KB76182.

Opal self-encrypting drives might not be supported on UEFI systems if the system is not Windows 8, Windows 8.1, or Windows 10 compliant, or if the system did not ship from the manufacturer fitted with an Opal self-encrypting drive. A UEFI security protocol that is required for Opal management is only mandatory on Windows 8 logo-compliant systems where an Opal self-encrypting drive is fitted at the time of shipping. Systems shipped without self-encrypting drives might not include the required security protocol. Without the security protocol, Opal management is not possible, since Drive Encryption cannot communicate with the security features of the drive in the pre-boot environment.

This does not affect support for Opal drives under BIOS.

Trusted Platform Module

Trusted Platform Module (TPM) 2.0 provides platform authentication support for Windows 8 and above UEFI systems, without the need for Pre-Boot Authentication (PBA).

TPM is a platform that allows encryption to occur using keys within the TPM. TPM is also implemented in firmware for tablets.

Drive Encryption supports TPM 2.0 on Windows 8 and above UEFI systems for the TPM autoboot and cold-boot protection features.

Use of TPM for automatic booting

The existing automatic booting feature creates a copy of the system’s encryption key as a plain-text file in the Pre-Boot File System. With the TPM autoboot feature, Drive Encryption uses TPM to encrypt this file.

The file can only be decrypted on the system that encrypted it and only if the boot path is unmodified from when it was encrypted. This makes sure that only the specific TPM can decrypt the file, and moreover (like SecureBoot) ensures that malware has not changed the boot path. A combination of TPM encryption and boot path measurements allow the user to securely bypass Pre-Boot Authentication (PBA) through to Windows logon, where user authentication occurs.

Any software update that changes the boot path, like a Microsoft update to the UEFI bootloader will result in pre-boot being displayed since the boot path has changed, and therefore the disk encryption key cannot be unsealed.
Protection of systems in Windows lock, log off, and standby states

In a world where more and more systems stay switched on but in low-power states (Always-On Always-Connect - AOAC), Drive Encryption 7.2.0 provides an additional level of protection for these systems, and extended the protection to protect systems where the user has locked the screen or logged off.

Drive Encryption currently protects systems that are certified for Connected Standby.

How does cold-boot protection work

The AOAC model requires systems to be in low power states to enable the system to receive push-notifications from a server, or to periodically wake to pull data from servers whilst the system "sleeps". Since this process must happen automatically and without user intervention, user authentication is not possible and therefore the disk encryption key must be kept in RAM, so that the disk can be accessed during the wake period. This allows applications and services to access the hard disk even when the user is not physically with the system.

Hence the system is vulnerable to cold-boot and other sophisticated RAM-based attacks.

To help defend against this problem, Drive Encryption has implemented a new security mode called Elevated Secure Crypt using the AES256-CBC encryption algorithm. This feature is only available when using software encryption; it is not available if you are using Opal drives.

How does Elevated Security Crypt mode work

The Drive Encryption driver now operates in two modes, Standard Crypt mode or Elevated Security Crypt mode. When a Windows user is logged on to the system, the encryption driver operates in the Standard Crypt mode. When the user puts the system to Standby state, locks the screen, or logs off from Windows, the encryption driver switches to the Elevated Security Crypt mode, and the encryption key is removed from DRAM and stored elsewhere in a location that is available for use in the Elevated Security Crypt AES algorithm.

The Drive Encryption driver is therefore able to continue to access the hard disk, allowing applications and services to continue to function; since the key is no longer in DRAM, the system is harder to attack.

Make sure to note that policy enforcement from McAfee ePO to the client systems is disabled when the system is in Elevated Security Crypt mode.

Until the user resumes from Standby and (importantly) authenticates through to Windows, or whilst the system sits at the Windows login or screen lock screens, the encryption driver remains in Elevated Security Crypt mode. Once the user has authenticated back into Windows, the encryption driver transfers the key back into DRAM, effectively switching back into the Standard Crypt mode.

When the system is on Elevated Security Crypt mode, there is an impact on the system's performance. However, since the system gets into the Elevated Security Crypt mode only during Windows log off, lock, standby states, or during authentication, it will not be noticed when the user is logged on to the system, as the system switches to Standard Crypt mode.

The two crypt modes work in conjunction with TPM-based autoboot:

- If TPM is used to autoboot the system, the Elevated Security Crypt mode is used throughout the boot process until a Windows user has authenticated when Standard Crypt mode is used.
Requirements

Make sure that your server and client systems meet these pre-requisites before installing Drive Encryption.

Table 1-1  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</td>
<td>• <strong>CPU</strong>: Pentium III 1 GHz or higher</td>
</tr>
<tr>
<td></td>
<td>• <strong>RAM</strong>: 512 MB minimum (1 GB recommended)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hard Disk</strong>: 200 MB minimum free disk space</td>
</tr>
</tbody>
</table>

For requirements on Intel® AMT systems, see the product documentation for McAfee ePO Deep Command.

Table 1-2  Software requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO</td>
<td>5.1.x and 5.3.x</td>
</tr>
<tr>
<td>Drive Encryption</td>
<td>Extensions:</td>
</tr>
<tr>
<td></td>
<td>• EEAdmin.zip</td>
</tr>
<tr>
<td></td>
<td>• EEPC.zip</td>
</tr>
<tr>
<td></td>
<td>• help_de_720.zip</td>
</tr>
<tr>
<td></td>
<td>• EEGO.zip</td>
</tr>
<tr>
<td></td>
<td>• EEDeep.zip</td>
</tr>
<tr>
<td></td>
<td>Before installing this extension, you must install the McAfee ePO Deep Command extension.</td>
</tr>
<tr>
<td></td>
<td>• UserDirectory.zip</td>
</tr>
<tr>
<td></td>
<td>Software packages:</td>
</tr>
<tr>
<td></td>
<td>• MfeEEPC.zip</td>
</tr>
<tr>
<td></td>
<td>• MfeEEAgent.zip</td>
</tr>
<tr>
<td>Microsoft Windows Installer 3.0</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Distributable package (for McAfee ePO)</td>
<td></td>
</tr>
<tr>
<td>Microsoft .NET Framework 2.0</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Distributable package (for McAfee ePO)</td>
<td></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 1-3  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</td>
<td>For the latest information on supported platforms, environments, and operating systems, see KB79422.</td>
</tr>
<tr>
<td></td>
<td>For the latest information about Windows 10 compatibility with McAfee products, see KB84419.</td>
</tr>
</tbody>
</table>

Testing for client system requirements

Client systems must meet the requirements for Drive Encryption before the product can be installed.

The Pre-Boot Smart Check can be used with the Drive Encryption GO (DEGO) 7.2.0 utility to help with initial deployments. DEGO performs checks and validation in the operating system, and the Pre-Boot Smart Check performs checks/validations outside of the operating system. The combined usage of these tools provides the highest confidence of a successful deployment.

For more information, see Requirements testing for client systems.
This section depicts the quick start diagram and specifies the prerequisite checklist to quickly assist you to understand the process of McAfee Drive Encryption installation.

**Quick Start Diagram for MDE Installation**

**Step 1** Ensure that the client systems are managed by the supported McAfee ePO server and the supported version of McAfee Agent is installed on these clients. For the latest information on supported platforms, environments, and operating systems, see KB79423.

**Step 2** Install the MDE extensions into McAfee ePO.

**Step 3** Check in the MDE software packages into McAfee ePO.

**Step 4** Register an AD server on McAfee ePO.

**Step 5** Assign users to the client system.

**Step 6** Create product setting policy or edit default policy and assign it to a system or a group of systems.

**Step 7** Create user based policy or edit default policy and assign it to a user or a group of users on a system.

**Step 8** Create the client tasks and deploy EEAgent and EEPC packages sequentially to the client and restart the client only when prompted after deploying the EEPC package.

You should now be able to see the Encryption icon | McAfee Drive Encryption System Status option on the menu bar that is present on the desktop of the client.

**NOTE:** While modifying the default product setting policy or creating the new product setting policy, the administrator must select any one of the disk encryption options other than **None**, by navigating to Encryption tab | Encrypt. The default option **None** does not initiate the encryption.

**NOTE:** The Drive Encryption system status changes from **Inactive** to **Active** only after adding the user and enforcing the policies correctly.
Installation prerequisites

Before installing Drive Encryption, ensure that the following relevant pre-requisites are satisfied.

Table 2-1  Prerequisite checklist

<table>
<thead>
<tr>
<th>List</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure the target client system(s) meets the system requirements as detailed in KB79422.</td>
<td>[]</td>
</tr>
<tr>
<td>Check the latest version of hardware compatibility XML file attached to KB81900 to make sure you have the latest version.</td>
<td>[]</td>
</tr>
<tr>
<td>Deploy McAfee Agent for Windows on the client system.</td>
<td>[]</td>
</tr>
<tr>
<td>Install the EEADMIN.ZIP and EEPC.ZIP extensions into the McAfee ePO server.</td>
<td>[]</td>
</tr>
<tr>
<td>The EEADMIN.ZIP extension is a prerequisite for the EEPC.ZIP extension.</td>
<td>[]</td>
</tr>
<tr>
<td>Check in the MfeEEAgent.ZIP and MfeEEPC.ZIP software packages into the McAfee ePO server.</td>
<td>[]</td>
</tr>
<tr>
<td>Register an Active Directory server on the McAfee ePO server.</td>
<td>[]</td>
</tr>
<tr>
<td>Create the client tasks and deploy the Endpoint Encryption Agent for Windows and Endpoint Encryption for PC packages sequentially to the client system, then restart the client only when prompted.</td>
<td>[]</td>
</tr>
<tr>
<td>You should now be able to see the McAfee Drive Encryption System Status on the McAfee Agent menu bar under Quick Settings</td>
<td>[]</td>
</tr>
<tr>
<td></td>
<td>Show Drive Encryption Status on the client system. Also, you will find the system state as Inactive.</td>
</tr>
<tr>
<td>Add users to the client system from the McAfee ePO server and send an Agent wake-up call.</td>
<td>[]</td>
</tr>
<tr>
<td>Create product setting policy or edit the default policy and assign it to a system or a group of systems. While modifying the default policy or creating the new policy, ensure to select any one of the disk encryption options other than None, by navigating to Encryption</td>
<td>[]</td>
</tr>
<tr>
<td></td>
<td>Encrypt. The default option None does not initiate encryption.</td>
</tr>
<tr>
<td>Send an Agent wake-up call. It is a good practice to select the Force complete policy and task update option while sending this Agent wake-up call. You will now find that the encryption is initiated on the client system.</td>
<td>[]</td>
</tr>
<tr>
<td>Verify the McAfee Drive Encryption System Status by clicking Encryption</td>
<td>[]</td>
</tr>
<tr>
<td></td>
<td>McAfee Drive Encryption System Status on the menu bar that is available on the desktop of the client.</td>
</tr>
</tbody>
</table>
Installing Drive Encryption

This chapter describes the process of installing, upgrading, and uninstalling the Drive Encryption software.

This release supports upgrading EEPC 7.0.x and Drive Encryption 7.1.x systems to Drive Encryption 7.2. For more information about upgrading EEPC 7.0.x and Drive Encryption 7.1.x systems to Drive Encryption 7.2, see the Upgrade section of this document.

Contents

- Installing the Drive Encryption software
- Upgrading from EEPC 7.0.x and Drive Encryption 7.1.x to Drive Encryption 7.2
- Uninstalling the Drive Encryption client

Installing the Drive Encryption software

The Drive Encryption extensions and software packages must be installed and checked in to the McAfee ePO server before you can deploy the software to the clients and configure the policies.

In this guide:

- EEPC 7.0.x refers to EEPC 7.0 or later
- Drive Encryption 7.1.x refers to Drive Encryption 7.1 or later

Make sure that you remove any competitor’s encryption products from your system. Do not install any other encryption products after installing McAfee Drive Encryption.

Overview of the installation process

The Drive Encryption client software is deployed from the McAfee ePO server and installed on the client system through the McAfee Agent.

The client system requires a restart to complete the installation. After the restart, the client communicates with the McAfee ePO server, pulls down the assigned Drive Encryption policies and the assigned users, and activates the system according to the defined policies. Drive Encryption creates the Pre-Boot File System (PBFS) on the client system at the time of activation, then proceeds to encrypt the disks according to specified policies. The assigned users can be initialized through the Pre-Boot screen after the restart.

The installation and deployment process is the same for both Drive Encryption software and Opal encrypted drives. The overall Drive Encryption installation and deployment process is made up of the following stages.

This assumes that the user has already installed McAfee ePO and has the McAfee Agent installed on various clients, which successfully communicate with the McAfee ePO server.
1 Install the EEAdmin.zip, EEPC.zip, help_de_720.zip, EEGO.zip, EEDeep.zip, and UserDirectory .zip extensions into McAfee ePO.

EEDeep.zip is an optional extension and can be installed only if you want to use McAfee ePO Deep Command with Drive Encryption.

2 Check in the Drive Encryption software packages (MfeEEPC.zip and MfeEEAgent.zip) to the McAfee ePO server.

3 Configure the registered server (Microsoft Active Directory).

You can also create and manage users using User Directory to remove the dependency on the LDAP server.

4 Deploy the Drive Encryption software packages to the client systems.

5 Restart the client system. The Quick Settings | Show Drive Encryption Status option appears in McAfee Agent on the client's system tray.

6 Add users to the system or a group of systems in the Encryption Users page of McAfee ePO.

7 Create a custom product settings policy or edit the default policy, then assign it to the system or a group of systems by using the standard McAfee ePO policy assignment capabilities.

8 Create a custom user-based policy or edit the default policy, then assign it to a user or a group of users on a system. Configure UBP enforcement if you are using Policy Assignment Rules.

The Show Drive Encryption Status changes from Inactive to Active only after adding at least one user and enforcing the policies correctly.

9 Verify the Drive Encryption System Status by right-clicking McAfee Agent on the client's system tray, then clicking Quick Settings | Show Drive Encryption Status.

### Install the Drive Encryption and Help extensions
You can view and configure the policies and settings of Drive Encryption by installing the product and Help extensions into the repository on the McAfee ePO server.

**Before you begin**
You must have administrator rights to perform this task.


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

1 Click Menu | Software | Extensions | Install Extension to open the Install Extension dialog box.

2 For each extension that you want to install:
   a Browse to and select the extension file, then click OK.

   The Install Extension page displays the extension name and version details.

   b Click OK.
Check in the Drive Encryption software packages
The software package must be checked in to the Master Repository so that you can deploy the software to
the client system. You must check in the MfeEEPC.zip and MfeEEAgent.zip packages.

Before you begin
- You must have administrator rights to perform this task.
- Make sure that there are no pull or replication tasks running.

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

1. Click Menu | Software | Master Repository, then click Actions | Check In Package to open the Check In Package wizard.
2. From the Package type list, select Product or Update (.zip), then browse and select the MfeEEPC.zip package file.
3. For each package that you want to check in:
   a. Browse to and select the package file, then click Next.
   b. On the Package Options page, click Save.

The checked-in packages appear under the respective branches in the Master Repository.

Register Microsoft Active Directory
If you are sourcing Drive Encryption users from Active Directory, it is necessary to register Microsoft Active Directory with McAfee ePO before you can create Drive Encryption users. Make sure to note that you can also create users using the User Directory feature, which removes the dependency on LDAP server.

Before you begin
You must have administrator rights to modify the server settings, permission sets, users, and registered servers.

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

1. Click Menu | Configuration | Registered Servers, then click New Server to open the Registered Server Builder wizard.
2. From the Server type drop-down list on the Description page, select LDAP Server, specify a unique user-friendly name and any details, then click Next.
3. On the Details page:
   a. Select Active Directory from LDAP server type, then enter the Domain name or the Server name.
      
      Use a DNS-style domain name, and make sure that McAfee ePO is configured with appropriate DNS settings and can resolve the DNS-style domain name of the Active Directory. The server name is the name or IP address of the system where the Microsoft Active Directory is present.
   b. Enter the user name for Active Directory accounts in this format: domain\Username.
Deploy Drive Encryption to the client system

The McAfee ePO repository infrastructure allows you to deploy the Drive Encryption product to your managed systems from a central location. Once you have checked in the software package, use this Product Deployment client task to install the product on managed systems.

Before you begin
- You must have administrator rights to perform this task.
- To check the requirements and compatibility of the client system, you need to deploy DEGO 7.2.0 to the client system. For details, see Drive Encryption GO.

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

1. Click Menu | Software | Product Deployment.
2. Select New Deployment to start a new project.
3. Type a name and description for this deployment. This name appears on the Product Deployment page after you save the deployment.
4. Choose the type of deployment:
   - Continuous — Uses your System Tree groups or tags to configure the systems receiving the deployment. This feature allows these systems to change over time as they are added or removed from the groups or tags
   - Fixed — Uses a fixed (defined) set of systems to receive the deployment. System selection is done using your System Tree or the output of Managed Systems Queries

5. To automatically update your products, make sure that the Auto Update checkbox is selected.
   - If the checkbox is deselected, products are still updated with the latest patches, hotfixes, and content packages, but major and minor releases are ignored.

During a new deployment, the McAfee Agent checks for new updates, hotfixes, and content packages of all installed products on the client. See the McAfee Agent documentation for details.

6. To specify which software to deploy, select the McAfee Drive Encryption 7.2 product from the Package list.
   - Click + to add the McAfee Drive Encryption Agent for Windows 7.2 and McAfee Drive Encryption for Windows 7.2 packages

7. From the Actions list, select Install.
8. Under Select the systems, click Select Systems.
The System Selection dialog box is a filter that allows you to select groups in your System Tree using these tabs:

- **System Tree** — Select System Tree groups or subgroups and their associated systems.
- **Tags** — Select tag groups or tag subgroups and their associated systems.
- **Selected Systems** — Displays the total selections you made in each tab, creating the target systems for your deployment.

For example, if your System Tree contains Group A, which includes both servers and workstations, you can target the entire group. You can also target only the servers or only the workstations (if they are tagged correctly), or a subset of either system type in Group A.

If needed, configure the following:

- **Run at every policy enforcement (Windows only)**
- **Allow end users to postpone this deployment (Windows only)**
- **Maximum number of postponements allowed**
- **Option to postpone expires after**
- **Display this text**

Under **Select a start time**, select a schedule for your deployment:

- **Run Immediately** — Starts the deployment task during the next ASCI.
- **Once or Daily** — Opens the scheduler so you can configure the start date, time, and randomization.

Click **Save** at the top of the page. The **Product Deployment** page opens with your new project added to the list of deployments.

After you create a deployment project, a client task is automatically created with the deployment settings.

**Basic preparations and recommendations**

Follow these recommendations to make sure that your data is protected during and after the encryption process.

**Back up the system before you encrypt it, and perform regular backups**

As with any roll out and deployment, it is good practice to back up the system before installing Drive Encryption to ensure data is not lost in the unlikely event that a problem occurs. The DETech recovery tools can also be used to decrypt and recover any unbootable disks. Refer to the **DETech User Guide** for more information.

When upgrading Drive Encryption, the Mfeepehost service must not be stopped manually or by third-party software because this can cause problems. In addition, during an upgrade, the system must be kept powered on until the software (both Host and Encryption Provider portions) completes installing.

**CHKDSK /r Clean up the disk before you encrypt it**

Hard disks that are damaged, or have a high number of undiscovered bad sectors, might fail during the full disk encryption process. Run a **CHKDSK /r** command prior to installing Drive Encryption to make sure the disk is healthy. Optionally, run the OEM diagnostic tools to make sure that all other hardware components are working correctly.
Understand the supported tokens/readers for Drive Encryption

Make sure that the supported reader drivers are installed in your client system before trying to install Drive Encryption. Make sure to obtain the correct drivers from the manufacturers' web sites and review their release notes to avoid any known issues with the tokens or readers. The supported tokens and readers are listed in these KB articles:

- Supported Readers used for authentication in Drive Encryption 7.x: https://kc.mcafee.com/corporate/index?page=content&id=KB79788
- Supported Tokens used for authentication in Drive Encryption 7.x: https://kc.mcafee.com/corporate/index?page=content&id=KB79787

Maintain separate test and production clients

Enterprise administrators are advised to maintain separate test and production environments. Modification to the production server should be limited. Use the test system to test software updates, driver updates, and Windows Service Packs prior to updating the production systems.

Build and test recovery tools

The administrator needs to be aware that there will be changes to the normal client boot process due to installing Drive Encryption. Administrators are advised to:

- Create and test the customized DETech WinPE V3 or V4 (for UEFI systems) Disk with Drive Encryption drivers installed.
- Create and test an DETech Standalone Boot disk.

Register on a smartphone

We recommend that you download and install the McAfee Endpoint Assistant app on your Android or IOS smartphone so that you can scan the QR code and initiate self-recovery without the need to contact your administrator for assistance.

On the client system, the first time you logon, a QR code is displayed. Scanning the QR code with your mobile device saves it to the device and establishes trust between the client system and the device. Later, if needed, you can initiate recovery by clicking Smart Phone Recovery and using the QR code at Pre-Boot Authentication.

We recommend that you scan the QR code using a mobile device with a high-level processing capacity.

The McAfee Endpoint Assistant app can be used on mobile devices running on these platforms:
- iOS — OS 6.1, iOS 7.x
- Android — 3.0.x (Honeycomb) and above on select platforms

You can download the McAfee Endpoint Assistant app from the Google Play Store and Apple Play Store.

For more details, see Smartphone recovery in the McAfee Drive Encryption Product Guide.

Run a pilot test of software compatibility

We recommend that you run a pilot test of Drive Encryption on a client system. This will make sure that Drive Encryption is not in conflict with any encryption software on the client computers before rolling out to a large number of clients. DEGO can be a valuable tool to detect the presence of third-party encryption software that might prevent activation or create further issues with Drive Encryption.

This is particularly useful in environments that use a standardized client image.
Administrators should also run performance testing during the pilot test.

McAfee professionals did not come across any performance-related issues with Drive Encryption during our own testing, however, this might vary depending upon the processor, memory, and drivers.

**Do a phased deployment**

For an efficient deployment, perform phased deployment in order to scale the deployment process. Create deployment tasks and deploy Drive Encryption to systems arranged in groups or batches in the System Tree. You can also base it on a specific tag in ePolicy Orchestrator.

**Add a user to the client system**

You should add at least one user to the client system for Drive Encryption to activate on the client.

**Perform disk recovery on decrypted disks**

Wherever possible, as a best practice, if you need to perform any disk recovery activities on a disk protected with Drive Encryption, we recommend that you first decrypt the disk. For more information about decrypting the Drive Encryption installed system, see *McAfee Drive Encryption 7.2.0 Product Guide* and the DETech User Guide.

**Automatic Repair should be disabled for Windows 8 and above systems**

Automatic Repair of an encrypted disk for Windows 8 and above systems might destroy the encrypted operating system files without any notification and cause permanent boot problems. However, previous versions of Windows display a confirmation message before starting the repair. Windows 8 launches into Automatic Repair immediately if a problem is detected, leaving little scope to prevent destruction of encrypted data.

To disable Automatic Repair, run this command from an administrative command prompt:

```
bcde
d /set {current} recoveryenabled No
```

**Educate your client users about Password/Token/PIN secrecy**

Educate your client users to understand that they are responsible for the security of their password, PIN, or token details. Encourage them to change their password, or request a new PIN, if they feel that it might have been compromised.

**Make sure password strength is sufficient**

Make sure that your password policy is strong enough for your requirements.

**Create client deployment task**

We recommend that you create a new system group in ePolicy Orchestrator for Drive Encryption deployment. Name it Drive Encryption Test Systems or Drive Encryption Production Systems, respectively, for example.

Do not create the deployment task at the My Organization level of the System Tree. Select a group in the System Tree, go to the Client Tasks tab and create the deployment task.
Importing systems from Active Directory to ePolicy Orchestrator

McAfee ePO provides an AD Synchronization/NT domain task to synchronize ePolicy Orchestrator with the configured Active Directory. This option allows you to map the ePolicy Orchestrator System Tree structure with a registered Active Directory. Using this option, you can import and effectively manage large numbers of systems in ePolicy Orchestrator.

This option works only with Active Directory.

For detailed procedures on how to import systems from Active Directory to ePolicy Orchestrator, refer to the product documentation for your version of McAfee ePO.

Order of the Drive Encryption Agent and Drive Encryption deployment

It is not mandatory to have two different tasks for the product deployment, however the deployment order is critical. The DEAgent package must be deployed before the Drive Encryption package.

We recommend that you create a single task to deploy both packages, provided that it deploys the DEAgent package first, then the Drive Encryption package.

If you configure the task to deploy the Drive Encryption package followed by the DEAgent package, the client system restarts in the middle as required, and the DEAgent is never deployed.

You can also create two separate tasks to deploy the packages, providing you wait for the first deployment (DEAgent) to complete before deploying the second package. You can also verify the completion of the DEAgent deployment, before deploying the Drive Encryption package, by creating and executing a customized query from the McAfee ePO server. If the Drive Encryption package is deployed first, you can run the DEAgent task and deploy it later. For more about custom queries, see Create Drive Encryption custom queries in the Drive Encryption Product Guide.

End user experience

The deployment task pushes both the Drive Encryption Agent and the Drive Encryption components to the selected systems. The installation is silent, however, the user is prompted to restart the client when the Drive Encryption component install is complete. It is important that the user restarts the client PC when prompted. If this does not happen, Drive Encryption does not activate.

Drive Encryption activation sequence

When the DEAgent and Drive Encryption packages are successfully deployed, the user is prompted to restart the system.

The restart is essential for activation of Drive Encryption on the client to proceed. The restart can be canceled, however; Drive Encryption will not become active on the client until the restart has occurred. In addition, hibernation and the use of new USB devices will be impaired until a restart is issued.

Drive Encryption Status

System restarts as initiated. You don’t yet see the PBA page as the Drive Encryption software is not yet active on the client. However, you should now be able to see the new option:

- Quick Settings | Show Drive Encryption Status in McAfee Agent System Tray on the client system (DE: Windows)

DEAgent synchronization with the McAfee ePO server

The status in the Show Drive Encryption Status window is Inactive until DEAgent synchronizes with the McAfee ePO server and gets all the users assigned to it. This is referred to as an ASCI event.
It can be manually triggered on the client by opening the McAfee Agent Status Monitor, then clicking Collect and Send Props. It can also be triggered from the McAfee ePO server by an agent wake-up call, otherwise, you need to wait for the scheduled agent-server communication interval to occur (the default is 60 minutes). After two agent-server communication intervals, Drive Encryption activation begins. The activation process requires a number of McAfee ePO events to be sent, and this can take some minutes to occur. Once the client-server communication has completed, the Drive Encryption Status switches to Active and encryption starts based on the policy defined.

When Drive Encryption activation is complete, it should be restarted once before hibernation takes place. For this reason, we recommend that hibernation be disabled from the Control Panel on Windows clients.

User intervention during encryption

The user can continue to work on the client system as normal even during encryption. Once the entire disk is encrypted, the technology is completely transparent to the end user.

When the system is restarted and Drive Encryption is first activated, the user should log on with the username that matches the user attribute set in the LdapSync: Sync across users from LDAP task and the default password of 12345 (this is the McAfee default password which can be changed in the User Based Policy) in the PBA page. The user is then prompted to change this password and enroll for self-recovery based on the policy set.

If you want the system to automatically capture the user’s credentials without making them use a default password on PBA, enable the Do not prompt for default password option under User Based Policies | Password.

We recommend that you change the default password and enforce policies with stronger passwords.

PBA

PBA

Single Sign On (SSO)

The Drive Encryption client system then boots to Windows. This first boot establishes SSO (if it has been enabled). On future restarts, the user needs to log in to PBA only. Once authenticated, SSO automatically logs on to Windows.

In short, the SSO option facilitates the user with the single authentication to the Operating System even when PBA is enabled. Though it requires an extra step, disabling SSO is the more secure configuration.

When the Must match username option is enabled, both the Drive Encryption user name and the Windows user name should match for SSO to work, regardless of which domain the user is part of. This user can even be a local user.

When the Synchronize Drive Encryption password with Windows option is enabled, the Drive Encryption password is reset to the Windows password. However, be aware that if the Password history option is enabled or Password content rules are set, and the Drive Encryption password is same as the Windows password, then synchronization does not occur.

On changing the Drive Encryption password, the synchronization is reset. Synchronization of the password occurs only when there is a change in the Windows password.
Activate Drive Encryption using Add local domain users

Using the Add local domain users option, you can activate Drive Encryption on the client systems without manually adding users in ePolicy Orchestrator.

This option provides automatic user assignment, eliminating the need for administrators to manually assign users to client systems in the McAfee ePO console. The recommended best practice is to manually assign at least one user to all systems to ensure successful Drive Encryption activation even if the Add local domain user option fails to function as configured. However, if this option is configured correctly, it will not fail. A general recommendation is to manually add a group of support users to all systems, then activate Drive Encryption using the Add local domain users option. You can remove these users at a later stage after completing the deployment.

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

Task
1. Configure the Product Settings Policy with the Add local domain users option enabled.
2. Log on to the client system. After the agent to server communication interval, the Add local domain users feature adds the previously/currently logged on domain users to the client system.
3. Drive Encryption is activated in the client system during the next ASCI. You can now restart the client to log on using the PBA page.

Send an agent wake-up call

The client computer gets the policy update whenever it connects to the McAfee ePO server during the next agent-server communication interval (ASCI). The policy update can be scheduled or forced. The agent wake-up call option forces the policy update to the client system. For information on adding a new system, see the product documentation for your version of McAfee ePO.

Before you begin

You must have administrator rights to perform this task.

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

1. Click Menu | Systems | System Tree, then select a system or a group of systems from the System Tree.
2. Select the System Names of that group.
3. Click Actions | Agents | Wake Up Agents.
4. Select a Wake-up call type and a Randomization period (0–60 minutes) within which the systems respond to the wake-up call sent by ePolicy Orchestrator.
5. Select Get full product properties for the agents to send complete properties instead of sending only the properties that have changed since the last agent-to-server communication.
6. Select Force complete policy and task update for the agent to send the complete policy and task update.
7. Click OK.

To view the status of the agent wake-up call, navigate to Menu | Automation | Server Task Log.
Install Drive Encryption using a third-party tool

Although McAfee ePO has all the required features for deploying Drive Encryption, you might need to use a third-party tool to deploy the product.

Before you begin
Make sure that the following software is installed:
• McAfee ePO
• McAfee Agent
• Drive Encryption 7.2 extensions on McAfee ePO
Make sure that your LDAP server is registered in McAfee ePO.

These files must be installed (two different versions of each file, per operating system type).
• Agent installer files: MfeEEAgent32.msi or MfeEEAgent64.msi
• Plug-in installer files: MfeEEPc32.msi or MfeEEPc64.msi

For more information about enabling the logs when installing Drive Encryption through msi, see KB86190.

Task
1 Determine whether your client system is running a 32-bit or a 64-bit version of the Windows operating system.
2 Log on to the client using an administrator account with sufficient rights for installing the software.
3 Copy the agent and plug-in installer files for your operating system to a temporary location on the client system.
4 Install the agent: double-click the agent installer file for your operating system.
5 Install the plug-in: double-click the plug-in installer file for your operating system.
6 Restart the client system to complete the installation.

After restarting the client system, you need to add users and configure the required encryption policies on McAfee ePO. Once the encryption policy is configured, encryption begins after the next agent-server communication.

Add users to a system

Use the ePolicy Orchestrator server to add the Drive Encryption users to the client system. The Drive Encryption software can be activated on a client system only after adding a user and enforcing the required encryption policies correctly.

Before you begin
You must have administrator rights to perform this task.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Data Protection | Encryption Users to open the My Organization page.

2. From the System Tree pane, select a group or system.

   To add users to a particular system, select the required system from the System tab on the My Organization pane.

3. Click Actions | Drive Encryption | Add Users to open the Add Drive Encryption Users page.

4. To add users, click + in the Users field, browse to the users' list, select the users, then click OK.

5. To add groups, click + in the From the groups field, browse to the user group's list, select the groups, then click OK.

6. To add an organizational unit, click + in the From the organizational units field, browse to the organizational unit list, select the unit, then click OK.

7. On the Add Drive Encryption Users page, click OK.

You can now accommodate large number of users in pre-boot. The maximum number of users that you can now accommodate is 5000 to the previous 250. However, McAfee recommends minimizing the number of users assigned for better performance.

Assign a policy to users
Configure and assign the policies to the users, and specify which users or groups of users are allowed to use the policies by setting the Policy Assignment Rules. The allowed users get their required User-Based Policies.

Before you begin
You must have administrator rights to perform this task.

You can also apply a Policy Assignment Rule to all policies from My Default policies.

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


2. Click Actions | New Assignment Rule. The Policy Assignment Builder wizard opens to the Details page.

3. Enter the name and description, then click Next.

4. In the Rule Type field, select User Based.

5. Click Next to open the Assigned Policies page.

6. Click Add Policy, then define these options:
   - From the Product drop-down list, select Drive Encryption 7.2.
   - From the Category drop-down list, select User Based Policies.
   - From the Policy drop-down list, select My Default.

7. Click Next to open the Selection Criteria page.
8 In the Comparison field, select either System is in group or subgroup or System is in group.

In the Value field, the My Organization group is selected by default.

9 Click Next to open the Summary page, then click Save.

The policy is assigned to the selected users.

Configure UBP enforcement

By default, all users inherit the default User-Based Policy assigned to a system, and are prevented from using Policy Assignment Rules. This inheritance allows maximum system scalability.

To allow a user to use a non-default UBP, you must enable the Configure UBP enforcement option for that user. This option allows Policy Assignment Rules to select a specific non-default user-based policy for the user. If not enabled, Policy Assignment Rules are not performed and the user inherits the default user-based policy.

Drive Encryption requires that you specify which groups of users can use the Policy Assignment Rules. The allowed users get their required user-based policy. Users who are not allowed to use the Policy Assignment Rules inherit the default user-based policy assigned to the system.

Task

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

1 Click Menu | Reporting | Queries & Reports, then from Shared Groups in the Groups pane, select Drive Encryption. The standard DE query list appears.

2 Run the DE: Users query to list all Drive Encryption users.

3 Select at least one user from the list to enforce the policy.

4 Click Actions | Drive Encryption | Configure UBP enforcement.

5 Select Enable or Disable, then click OK to configure the UBP enforcement state.

At each ASCI, McAfee ePO makes sure that all relevant user-based policies are deployed to each client in addition to the user-based policy for the logged-on user configured with UBP enforcement.

When Enable is selected, Policy Assignment Rules are enabled for the selected users, and a specific UBP is assigned to the user according to the rule defined. Policy Assignment Rules are enabled for the selected users only if a rule has been set for those users.

Assign a policy to a system

You can assign the required policy in the Policy Catalog to any system or system group. Assignment allows you to define policy settings once for a specific need, then apply the policy to multiple locations.

Before you begin

You must have administrator rights to perform this task.

When you assign a new policy to a particular group, all child groups and systems that are set to inherit the policy from this assignment point are assigned that policy.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Systems | System Tree, then select a group of systems from the System Tree. The systems within this group (but not its subgroups) appear in the details pane.

2. Select the target system, then click Actions | Agent | Modify Policies on a Single System. The Policy Assignment page for that system appears.

3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption are listed with the system’s assigned policy.

4. Select the Product Settings policy category, then click Edit Assignments.

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

6. From the Assigned policy drop-down list, select the Product Setting policy.
From this location, you can edit the selected policy or create a new policy.

7. Select whether to lock policy inheritance so that any systems that inherit this policy can’t have another one assigned in its place.

8. When modifying the default policy or creating the new policy, select any disk encryption option except None, by navigating to Encryption (tab) | Encrypt. The default option None does not initiate the encryption, but does enable the Pre-Boot Authentication.

   Make sure that you select the correct encryption provider and set the priority, as appropriate. For systems with Opal drives, only the All disks and Boot disk only encryption options are supported. Also, for systems with Opal TCG complaint drives, set the highest priority to use Opal in the organization.

9. Click Save.

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

Before you begin
You must have administrator rights to perform this task.

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

1. Click Menu | Systems | System Tree | Systems tab, then from the System Tree, select the group where the system belongs. The systems within this group appear in the details pane.

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

3. Select Drive Encryption 7.2, then click Enforcing next to Enforcement status.

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

5. 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 Drive Encryption 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.
Edit the client tasks

The McAfee ePO server allows you to create, edit, and schedule client tasks that run on managed systems.

**Before you begin**
You must have administrator rights to perform this task.

You can define tasks for the entire System Tree, for a specific group, or for an individual system. Like policy settings, client tasks are inherited from parent groups in the System Tree.

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

Task

1. Click Menu | Policy | Client Task Catalog, then select McAfee Agent for the product and Product Deployment for the task type.
2. Click the task to edit it in the Client Task Builder wizard.
3. Edit the task settings as needed, then click Save.

For more information on how to perform this task, see the product documentation for your version of McAfee ePO.

The managed systems receive these changes during the next agent-server communication.

Requirements testing on client systems

Drive Encryption requirements must be met before the product can be installed on a client system. The DEGO and Pre-Boot Smart Check tools verify that these prerequisites are met.

Drive Encryption GO

McAfee® provides the Drive Encryption GO (DEGO) 7.2 utility for system administrators to determine which systems are compatible for installing and activating Drive Encryption.

DEGO runs a set of compatibility tests on a client system, then creates a report through the McAfee ePO console that summarizes the readiness of the managed systems.

The Drive Encryption system policy can be configured to prevent activation of encryption on client systems that fail DEGO testing.

DEGO tests validate the compatibility of the client system.

DEGO runs these tests:

- Incompatible product detection — Checks for SafeBoot, HP ProtectTools 2009, Bitlocker, PointSec, Truecrypt, GuardianEdge, Symantec Drive Encryption, SafeGuardEasy, and PGP Whole Disk Encryption.

- Smart Controller predictive failure — Reports if the S.M.A.R.T. controller indicates an imminent failure.
• Disk Status — For BIOS-based systems, reports if the disk (MBR and partition structure) is suitable to install Drive Encryption.

DEGO is not supported for Unified Extensible Firmware Interface (UEFI) systems.

• Datachannel communication status — Reports the success or failure of the Datachannel communication from the client to the McAfee ePO server.

• Datachannel communication delay — Tests the delay (in milliseconds) of the communication between the McAfee ePO server and the client.

If any of these requirements are not valid and the Drive Encryption system policy is configured to abandon activation if the DEGO tests fail, Drive Encryption activation fails.

DEGO can detect a series of circumstances that might impact the rollout of Drive Encryption. However, DEGO is not a substitute for due diligence testing prior to rollout.

**Install and deploy DEGO**

Installing DEGO and deploying it on client systems enables automatic requirements testing.

**Before you begin**

Make sure that DEGO is installed on the McAfee ePO server, and that McAfee Agent is installed on all relevant client systems and can communicate with McAfee ePO.

**Task**

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

1. Install the EEGO.zip extension in McAfee ePO.
2. Check in the EEGOPackage.zip software package in McAfee ePO.
3. Use a product deployment task to deploy DEGO to the client system.
4. Enforce DEGO policies on the client system.

After restarting, the client system communicates with the McAfee ePO server and pulls down the assigned Drive Encryption GO policy. It then runs the tests and reports the system diagnostic information according to the defined policies.

If you select Only activate if health check (Drive Encryption : Go) passes and then uninstall DEGO from the client, it is not possible to deselect this option. As a result, Drive Encryption fails to activate.

The status of DEGO client systems can be monitored through various chart representations available in McAfee ePO reports.

**Pre-Boot Smart Check**

The Pre-Boot Smart Check performs various tests to ensure that the Drive Encryption pre-boot environment can work successfully on a device.

It tests the areas that have been identified as causing incompatibility issues in the past.

The flow for this process is made up of these stages:

• System receives the system policy with Pre-Boot Smart Check enabled.

• System activates with default Pre-Boot configuration, but encryption does not commence.

• System forces a restart to occur.
• User must log on through Pre-Boot.
• If Windows logon is successfully achieved, encryption commences.
• If there is a compatibility issue on the platform, the system does not reach Windows.
  • The user must hard-boot the system.
  • Pre-Boot starts in a different Pre-Boot configuration.
• User must log on through Pre-Boot.

Repeat this until all Pre-Boot configurations are exhausted.

• If no Pre-Boot configuration successfully boots Windows, Drive Encryption is removed from the system the next time Windows restarts.
• If a device fails the Pre-Boot Smart Check, it does not activate Drive Encryption. You can view the audit log to get the latest information on the check's progress from the last time the device synchronized with McAfee ePO.

Enable the Pre-Boot Smart Check feature
Enable this feature to perform the hardware compatibility check before Drive Encryption activation and encryption.

Before you begin
You must have administrator rights to perform this task.

When you enable this feature, it modifies the Drive Encryption activation sequence and creates a pre-activation stage. During this stage, a series of hardware compatibility checks are performed prior to actual activation and subsequent encryption to successfully activate Drive Encryption on platforms where BIOS issues might exist.

This feature is available only for BIOS systems using PC software encryption. It is not available for UEFI or Opal systems.

The client system might need to be restarted several times before the Smart Check is complete. If the boot sequence appears to freeze, make sure to power cycle the system and try again. It might take up to 8 restarts before all configuration options have been exhausted and for Drive Encryption to be deactivated.

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

1 Click Menu | Systems | System Tree, then select a group from the System Tree.
2 Select at least one system, then click Actions | Agent | Modify Policies on a Single System. The Policy Assignment page for that system appears.
3 From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption are listed with the system’s assigned policy.
4 Select the Product Settings policy category, then click Edit Assignments to open the Product Settings page.
5 If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6 Select the policy from the Assigned policy drop-down list, then click Edit Policy to open the Policy Settings page.

From this location, you can edit the selected policy or create a new policy.
In the Encryption Providers tab, select Enable Pre-Boot Smart Check to update this policy on the client systems.

This feature is applicable only for BIOS-based systems using PC software encryption.

After you select this option, the Force system restart once activation completes option is selected automatically.

Click Save.

After the policy is applied to the client systems, Drive Encryption activation starts and completes after a period of time. Drive Encryption is not in Active state now. The user is notified that the system is about to restart. A few moments later, the system restarts automatically.

After the client system restarts, authenticate to the PBA.

If the system is successfully booted into Windows, the Drive Encryption status switches to Active and Drive Encryption is activated successfully.

If the system is not able to boot into Windows (or the PBA cannot run) due to hardware compatibility issues, the user must manually power off the system and try again. Several restarts are required before smart-check fails and boots into Windows. On each retry, the PBA configures a different set of compatibility configurations to work around any issues on the client system to boot into Windows. After all configurations are attempted, the client system bypasses the PBA and boots directly into Windows. The client system then deactivates and records the failure by sending an audit message to McAfee ePO. The PBA is removed and Drive Encryption activation fails.

Update the hardware compatibility list on McAfee ePO and client systems

To update the hardware compatibility list on McAfee ePO and client systems, you need to perform the following steps:

**Task**

1. Download the latest HWDefaultProductDetections.zip from KB81900.

2. Extract the contents of the file, then import the HWDefaultProductDetections.xml file into McAfee ePO:
   a. Click Menu | Server Settings.
   b. Under Setting Categories, select Drive Encryption, then in the right pane click Manage Hardware Compatibility Settings.
   c. On the new page, click Actions | Import hardware compatibility settings.
   d. On the new page, click Choose File and navigate the file to McAfee ePO.
   e. After the file is selected, click OK to upload the file to McAfee ePO.
3 Perform the appropriate action(s) below depending on the status of your client:

- If the client system successfully activated and encrypted with the installed / upgraded Drive Encryption client build, then:
  1. Create a DETech recover disk. For more information, see the *McAfee Drive Encryption 7.2.0 DETech User Guide*. For details, see KB24871.
  2. Perform an Emergency Boot on the client as per the *McAfee Drive Encryption 7.2.0 DETech User Guide*.
  3. Allow enough time for a full communication interval between the client and the McAfee ePO server to take place before rebooting.

- If the client has activated but is not yet encrypted, deactivate and reactivate the software.

- If the client does not have Drive Encryption installed, no action is required. Install the software as normal.

For a list of systems and the appropriate Drive Encryption build that is required to align with the hardware compatibility list, see KB81900.

Earlier versions of `HWDefaultProductDetections.xml` are not compatible with later versions of Drive Encryption. Best practice is to install the latest patch and hotfix as specified in KB81900.

### Upgrading from EEPC 7.0.x and Drive Encryption 7.1.x to Drive Encryption 7.2

The primary goal of upgrading is to update the product components while maintaining all of the existing encryption, policies, users, authentication details, Single Sign On (SSO) details, audit, and tokens.

If you are using EEPC 7.0.x, you must upgrade the extensions to EEPC 7.0 Patch 4 before initiating the upgrade process to Drive Encryption 7.2.

If you are using Drive Encryption 7.1.x, you can directly upgrade to Drive Encryption 7.2. For more information, see the *Installing Drive Encryption* section.

### Upgrade to Drive Encryption 7.2

Perform these tasks to upgrade the clients from EEPC 7.0.x to Drive Encryption 7.2.

1. Upgrade the EEPC 7.0.x EEAdmin extension to EEPC 7.0 Patch 4, which is included in the Drive Encryption 7.2 package.

2. Upgrade McAfee ePO to minimum supported versions or later (McAfee ePO 5.1.x and 5.3.x).

3. Run the user data upgrade task

4. Upgrade to Drive Encryption 7.2

It is critical that you follow the below mentioned steps precisely in order to successfully upgrade the system.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Put the McAfee ePO server down, back up the SQL server and McAfee ePO server, then put the McAfee ePO server up in order to backup your McAfee ePO database. For more information about backing up your McAfee ePO database, see the product documentation for your version of McAfee ePO.

2 Install the EEAdmin.zip extension for EEPC 7.0 Patch 4.
   You must use the EEPC 7.0 Patch 4 system for user data upgrade even if all the encryption users and legacy EEPC extensions are deleted from McAfee ePO.

3 Upgrade McAfee ePO to minimum supported versions or later (McAfee ePO 5.1.x and 5.3.x).
   For more information about upgrading to McAfee ePO (5.1.x and 5.3.x), see the product documentation for your version of McAfee ePO.

4 Allow any LDAP Sync task that is running to complete, and then disable all EEPC LDAP Sync task and LDAP Sync:Sync Across Users from LDAP task.
   Make sure to note that the EEPC LDAP Sync task should have been manually created before.

5 Click Menu | Automation | Server Tasks to open the Server Tasks page.

6 Select the EE : User Data Upgrade task, then click Edit under Actions to upgrade the user data from EEPC 7.0 Patch 4 to Drive Encryption 7.2 format.
   If you enable this option without a valid registered server in McAfee ePO, an error message “Failed to determine the attributes to sync for at least one archetype” appears.

7 On the Description pane, type the Notes and enable the Schedule status, if you wish to run this task automatically in a scheduled manner, then click Next.

8 On the Actions pane, enable the checkbox to accept the terms and conditions, then click Next.
   If you have more than one LDAP servers registered, and the EEPC attributes are not configured to be the same across all servers, this checkbox will be disabled.
   In order to proceed with the upgrade process, the attributes must match across all registered servers. If you have to modify the configuration of any server attributes to achieve this, make sure that you run all EEPC LDAPSync task(s) related to the modified server configuration and wait for an ASCI to make sure that all systems have been updated before running the data upgrade task.

9 On the Schedule pane, if you have enabled Schedule status, select the Schedule type, Start date, End date, and Schedule options appropriately, then click Next.

10 On the Summary pane, verify the selections that you have made, then click Save.

11 Run the EE : User Data Upgrade task.
   On the Server Task Log page (Menu | Automation | Server Task Log), you can view the progress of this task.
   If the task fails, check the logs and address all issues, and run the task until it succeeds.
   Make sure to note that you cannot perform any other task until the EE : User Data Upgrade task is completed.
12 Install the Drive Encryption 7.2 extensions to the McAfee ePO system.

13 Check in the Drive Encryption 7.2 Agent and PC software packages to the McAfee ePO system.

14 Re-enable the LDAP Sync:Sync Across Users from LDAP task.

15 Run the LDAP Sync:Sync Across Users from LDAP task manually.

16 Deploy the Drive Encryption 7.2 software packages to the client system.

17 Restart the client system after the deployment task is completed.

After restarting the client system, the new files and drivers are in place. The Drive Encryption 7.2 encryption status dialog box shows the status as Active throughout the upgrade process.

**Upgrade systems with TPM autoboot policy enabled**

On upgrading the client to Drive Encryption 7.2.0, the user will be prompted to authenticate in preboot due to boot measurement changes caused by the upgrade process. Without intervention, the Help Desk calls may be generated as users attempt to log back onto their systems after the upgrade, as TPM autoboot users may not know their preboot usernames or passwords, or no users may be assigned to the system.

Intel Security recommends that McAfee ePO administrators take proactive actions to mitigate the potential problem using one of the following approaches:

**Method 1** — Enable normal autoboot through policy before sending the upgrade task to systems that are running with TPM autoboot policy enabled. The normal autoboot policy can be disabled/revoked by the McAfee ePO administrator after the systems report a successful upgrade to Drive Encryption 7.2.0.

**Method 2** — Enable temporary autoboot for two restarts prior to upgrading systems that are running with TPM autoboot policy enabled. This will ensure that new boot measurements are made following the upgrade, and that preboot will not be displayed.

**Task**

1 Enable temporary autoboot through policy.

2 Enable temporary autoboot on each TPM autoboot endpoint with "--number-of-reboots 2" on an active 7.1.x client.

   Temporary autoboot is now successfully set.

   ![Info](image)

   It is recommended that 2 instances of temporary autoboot are set to allow the boot code to be synced.

3 Deploy Drive Encryption 7.2.0 EEAgent and EEPC.

4 Restart the client when prompted. (This will use insecure temporary autoboot.)

5 On the next restart of the client, the temporary autoboot will again be exercised.

6 For any subsequent restarts, secure TPM autoboot will be reinstated.

   ![Warning](image)

   Whilst temporary autoboot is enabled, the system is not secure.
**User experience summary**

This table summarizes the user experience during the client upgrade from EEPC 7.0.x or Drive Encryption 7.1.x to Drive Encryption 7.2.

<table>
<thead>
<tr>
<th>EEPC 7.0.x</th>
<th>Drive Encryption 7.1.x</th>
<th>Pre-Boot</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade EEAdmin extension to EEPC 7.0 Patch 4</td>
<td>N/A</td>
<td>EEPC 7.0.x or Drive Encryption 7.1.x</td>
<td>The client system remains unchanged.</td>
</tr>
<tr>
<td>Upgrade McAfee ePO to 4.6.7 or 5.1</td>
<td>N/A</td>
<td>EEPC 7.0.x or Drive Encryption 7.1.x</td>
<td>The client system remains unchanged.</td>
</tr>
<tr>
<td>Disable sync tasks, then run the EE : User Data Upgrade task</td>
<td>N/A</td>
<td>EEPC 7.0.x or Drive Encryption 7.1.x</td>
<td>The client system remains unchanged.</td>
</tr>
<tr>
<td>Upgrade all extensions to Drive Encryption 7.2, then re-enable sync tasks</td>
<td>Upgrade all extensions to Drive Encryption 7.2, then re-enable sync tasks</td>
<td>EEPC 7.0.x or Drive Encryption 7.1.x</td>
<td>The client system remains unchanged.</td>
</tr>
<tr>
<td>Drive Encryption 7.2 client deployment</td>
<td>Drive Encryption 7.2 client deployment</td>
<td>EEPC 7.0.x or Drive Encryption 7.1.x</td>
<td>The Drive Encryption 7.2 deployment forces the restart of the client system.</td>
</tr>
</tbody>
</table>
| After deployment and restarts | After deployment and restarts | Drive Encryption 7.2 | • The Drive Encryption 7.2 system status remains as Active throughout the upgrade process.  
• The user credentials for both PBA and Windows logons are the same as EEPC 7.0.x or Drive Encryption 7.1.x for Drive Encryption 7.2.  
• SSO to Windows continues to function as it did before the upgrade. |

**Upgrade checklist**

To upgrade from EEPC 7.0.x to Drive Encryption 7.2, make sure to run through this checklist to complete the upgrade process.

It is critical that you follow the below mentioned steps precisely in order to successfully upgrade the system.

<table>
<thead>
<tr>
<th>List</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Put the McAfee ePO server down</td>
<td>[ ]</td>
</tr>
<tr>
<td>Back up the SQLServer</td>
<td>[ ]</td>
</tr>
<tr>
<td>Back up the McAfee ePO server</td>
<td>[ ]</td>
</tr>
<tr>
<td>Put the McAfee ePO server up</td>
<td>[ ]</td>
</tr>
<tr>
<td>Install the 7.0 Patch 4 EEAdmin extension</td>
<td>[ ]</td>
</tr>
<tr>
<td>List</td>
<td>Check</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Upgrade McAfee ePO to minimum supported versions or later (McAfee ePO 5.1.x and 5.3.x)</td>
<td>[ ]</td>
</tr>
<tr>
<td>Disable the EEPC LDAP Sync task and LDAP Sync:Sync Across Users from LDAP task</td>
<td>[ ]</td>
</tr>
<tr>
<td>Run the EE : User Data Upgrade task</td>
<td>[ ]</td>
</tr>
<tr>
<td>Install the Drive Encryption extensions</td>
<td>[ ]</td>
</tr>
<tr>
<td>Check in the Drive Encryption 7.2 software packages</td>
<td>[ ]</td>
</tr>
<tr>
<td>Re-enable the LDAP Sync:Sync Across Users from LDAP task</td>
<td>[ ]</td>
</tr>
<tr>
<td>Run the LDAP Sync:Sync Across Users from LDAP task</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

**Uninstalling the Drive Encryption client**

To uninstall Drive Encryption from the client, the encryption policy must be disabled in order to decrypt the client system, and then software packages can be removed. Here are some important steps involved in removing the software.

1. Disable the Drive Encryption product setting policy.
2. Make sure that the Drive Encryption System Status is **Inactive**.
3. Uninstall Drive Encryption from the client system.

**Disable the Drive Encryption client**

Modify the Drive Encryption product setting policy on the McAfee ePO console to deactivate the Drive Encryption client.

**Before you begin**

You must have administrator rights to perform this task.

**Task**

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

1. Click **Menu | Systems | System Tree | Systems**, then select a group from the **System Tree**.
2. Select a system, then click **Actions | Agent | Modify Policies on a Single System**.
3. From the **Product** drop-down list, select **Drive Encryption 7.2**. The policy categories under **Drive Encryption** are listed with the system’s assigned policy.
4. Select the **Product Setting** policy category, then click **Edit Assignments**.
5. If the policy is inherited, select **Break inheritance and assign the policy and settings below next to Inherit from**.
6. 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.
7. Select whether to lock policy inheritance. Any systems that inherit this policy can’t have another one assigned in its place.
8. On the **General tab**, deselect **Enable policy**.

**On Opal systems, make sure that you select the correct encryption provider and set the priority, as appropriate, so that the policy enforcement occurs correctly.**
9. Click **Save** on the **Policy Settings** page, then click **Save** on the **Product Settings** page.

10. Send an agent wake-up call.

On disabling the product setting policy, all the encrypted drives are decrypted, and the Drive Encryption status becomes **inactive**. This can take a few hours depending on the number and size of the encrypted drives. However, client systems with Opal drives become **inactive** very quickly.

### Remove Drive Encryption from the client system

The McAfee ePO repository infrastructure allows you to remove the Drive Encryption product from your managed systems from a central location. To remove the software package from the client system, use this Product Deployment client task.

**Before you begin**

- You must have administrator rights to perform this task.
- Make sure that you remove Drive Encryption from the client system before removing the product extensions from McAfee ePO.

**Task**

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

1. Click **Menu | Systems | System Tree**.

2. Select one or more systems on which to run the task.

3. Click **Actions | Agent | Run Client Task Now**.

4. Select the **Product** as *McAfee Drive Encryption 7.2* and the **Task Type** as *Uninstall*.

5. Click the existing **Task Name** that you want to uninstall, then click **Run Task Now**.

6. Click **Save**.

The Running Client Task Status page appears, and displays the state of all running tasks. When the tasks are complete, the results can be viewed in the **Audit Log** and **Server Task Log**.

### Remove the Drive Encryption extensions

To uninstall the Drive Encryption extensions, remove the *EEAdmin.zip*, *EEPC.zip*, *help_de_720.zip*, *EEGO.zip*, *EEDeep.zip*, and *UserDirectory.zip* extensions from the McAfee ePO server.

**Before you begin**

- You must have administrator rights to perform this task.
- Make sure that you deactivate the Drive Encryption Agent before removing the Drive Encryption extension from McAfee ePO.
- Because Drive Encryption is managed by a single McAfee ePO server, you can remove the DEAdmin extension only when McAfee ePO management is not required for both products.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Software | Extensions, then select Drive Encryption. The Extension page appears with the extension name and version details.

2. Click Remove.

3. When prompted for confirmation, click OK to remove the extension.

Remove the Drive Encryption software packages
When you deactivate and remove the Drive Encryption software from the client system, you need to remove the Drive Encryption software packages (MfeEEPC.zip and MfeEEAgent.zip) from the McAfee ePO server.

Before you begin
- You must have administrator rights to perform this task.
- Make sure that you deactivate the Drive Encryption client before removing the Drive Encryption software package from McAfee ePO.

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

1. Click Menu | Software | Master Repository. The Packages in Master Repository page lists the software packages and their details.

2. Click Delete next to the Drive Encryption software packages.

3. Click OK.

Manually uninstall Drive Encryption from the client system
Although McAfee ePO has all the required features for removing the product from the client system, you can also manually uninstall Drive Encryption from the client system.

Before you begin
- You must have administrator rights to perform this task.
- Make sure that you deactivate the Drive Encryption client before initiating the manual removal process.

Task
1. After deactivating the Drive Encryption Agent, on the client system, browse to these registry values and double-click the Uninstall command. The Edit String dialog box appears.
   - For DE Agent on 32-bit system: HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Application Plugins\EEADMIN_1000.
   - For Drive Encryption on 32-bit system: HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates \ePolicy Orchestrator\Application Plugins\EEPC.
• For DE Agent on 64-bit system: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Application Plugins\EEADMIN_1000.

• For Drive Encryption on 64-bit system: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \Network Associates\ePolicy Orchestrator\Application Plugins\EEPC.

2 Copy the Value data from the Edit String dialog box, paste and run it on the command prompt. You can retain the /q command to run a silent removal and to avoid restarting the system after uninstalling the Drive Encryption product.

   The uninstall option switch /q might not work for Windows Vista and Windows 7, where User Access Control (UAC) is set to protect.
Drive Encryption offline activation

Activating Drive Encryption on the client system is the most important phase in the Drive Encryption installation process. The activation process enables the client system to receive the required policies and user assignments from the McAfee ePO server for the first time. The Offline Activation feature allows you to activate Drive Encryption on a client system without connecting to the McAfee ePO server.

Contents
- How offline activation works
- Creating the offline activation package
- Performing offline activation
- Perform recovery tasks using DETech
- Machine Key Management

How offline activation works

To activate Drive Encryption on a system that has no network connectivity or no connection to McAfee ePO, you can create an offline activation package on the McAfee ePO server and later distribute it to the required client system. This package contains the initial set of policies and a list of offline users.

Once the Drive Encryption software is installed successfully using the MSI packages (Agent and PC packages), you must run the offline activation tool to apply and enforce your selected policies and to add user accounts. When the system is active, encryption commences. If autoboot is not enabled, you might be required to authenticate on the Pre-Boot Authentication page using the offline user account specified as part of the offline install.

These offline users are not part of the Active Directory.

During the activation process, the disk encryption key is written to a user-specified location in an encrypted form. This key is useful in recovery scenarios where the disk encryption key is manually sent to the McAfee ePO server for decryption.

To perform a check on requirements and compatibility of the client system, you must install DEGO 7.2.0 or above to the client system. For more information, see Requirements testing for client systems.

DEGO can't communicate the results to McAfee ePO, however the logging can be used to determine any compatibility issues before offline activation.

What happens when an offline activated system connects to McAfee ePO

Assuming that the offline activation was performed for provisioning purposes, the system connects to McAfee ePO. Upon successful communication with McAfee ePO, the client moves into an online mode. Online mode is a normal connection between the McAfee Agent and McAfee ePO. It discards the offline
policy that was enforced at activation. In its place, it receives the real policy from McAfee ePO and the list of assigned users as in a normal activation, and saves its encryption key in McAfee ePO. You could view it as a second, but automatic, activation.

Create and download the McAfee Agent installation package
The McAfee Agent extension must be installed on the McAfee ePO server before the agent is installed on any target systems.

Before you begin
- Make sure that you have created a temporary folder on the McAfee ePO system, to save the files required for offline activation.
- You must have administrator rights to perform this task.

We recommend that you refer to the McAfee ePO documentation to verify that you are using the most current package and extension.

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

1. Download the agent extension, ePOAgentMeta.zip, and the agent package, MA460Win.zip, to the system containing the McAfee ePO server.

2. Install the agent extension.
   a. Click Menu | Software | Extensions, then click Install Extensions.
   b. Browse to the location containing ePOAgentMeta.zip, select it and click OK. The Install Extensions summary page appears.
   c. Click OK to complete the installation of the extension.

3. Check in the agent package to one of the repository branches, Current (default), Previous, or Evaluation.

4. Create an installation package:
   a. Click Menu | Systems | System Tree, click System Tree Actions, then select New Systems from the drop-down menu.
   b. Select Create and download agent installation package.
   c. Select the Agent version for Windows.
   d. Deselect Embed Credentials in Package.
      
      If deselected, you receive the default package. If selected, you can specify required credentials.
   e. Click OK. The Download file dialog box opens.
   f. Select FramePkg.exe and save it to the temporary folder.
Extracting the MSI packages (Agent and PC)

There are two files required to install Drive Encryption on the client systems, and two versions of each file, according to operating system type.

You can extract these files from the Drive Encryption product build:

- Agent installer files: MfeEEAgent32.msi or MfeEEAgent64.msi
- PC Plug-in installer files: MfeEEPc32.msi or MfeEEPc64.msi

These files are available in MfeEEAgent.zip and MfeEEPC.zip under McAfeeEE720\EE Software Packages\Endpoint Encryption Host 7.2 and McAfeeEE720\EE Software Packages\Endpoint Encryption 7.2 folders, respectively, in the product build.

Download and extract the EpeOaGenXML.exe file

Use the EpeOaGenXML.exe file as an input to create the offline activation package. Extract this file from the Drive Encryption build that you downloaded from the download site.

Before you begin

Make sure that you have access to the latest Drive Encryption build.

Task

1. Download the latest Drive Encryption build to a temporary location on the target system.
2. Extract the EpeOaGenXML.exe file from the product build to the temporary folder on the target system. The EpeOaGenXML.exe file is available at McAfeeDE710\Drive Encryption Misc\Drive Encryption Admin tools.

Extract and download the Key Server Public Key

The Key Server Public Key, located in the McAfee ePO Default Product Policy, is required for generating the offline activation package. It is used to encrypt the disk encryption key on the client system during activation.

Before you begin

You must have administrator rights to perform this task.

To obtain the Key Server Public key, download the default product policy from the McAfee ePO server.

Task

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

1. Click Menu | Policy | Policy Catalog.
2. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption displays the system's assigned policy.
3. Select the Product Settings policy category, then click Export from the My Default policy row.
4. Click the link to open the file, or right-click the link to download and save the file to the same location as the EpeOaGenXML.exe file.

When saving the download file, change the file name from My_Default.xml to ePO_policy.xml.
Create the user configuration file

You must have at least one user account within the offline activation package to activate Drive Encryption offline on a client system that is not connected to McAfee ePO. You must add these users to a user configuration file, then use that file when creating the offline package.

**Before you begin**
- Make sure that you have the list of user names to be added to the user configuration file.
- Make sure that you have the required token details.

When using the Offline Activation process, the offline user can be set up as a password user or token user. For a token user, only SI tokens are supported, as standard PKI tokens need to sync back with McAfee ePO to be authenticated.

**Task**

1. Open a text file and add the Drive Encryption users that you need to add to the client system. Name the file, as appropriate (for example: UserList.txt).

2. Save the text file to a temporary location on the target system. The format of each user being added is `name: token`, where:
   - **Name**— The Drive Encryption user name that you need to add to the client system and that will be used for Drive Encryption logon. Make sure that you add a colon (:) after the user name.
   - **Token**— The token type you need to assign to that user.

   In the user configuration file, you can have any number of blank spaces between names and tokens.

Five token types are supported:
- Password
- Four Self-Initiating (SI) token types (Gemalto, ActivID, PIV, and CAC)

   The token type is case-sensitive.

Remember:
- If your SI token is configured using the Gemalto .NET PKI Smart Card token type, use the Gemalto tag.
- If your SI token is configured using the ActivIdentity/CAC PKI Smart Card token type, use the ActivID tag.
- If your SI token is configured using the PIV PKI Smart Card token type, use the PIV tag.
- If your SI token is configured using the Common Access Card PKI Smart Card " token type, use the CAC tag.

Creating the offline activation package

The offline activation package is used for activating Drive Encryption on a client system that is not connected to the McAfee ePO server.

These files are required to create the offline activation package:
You must extract and export the Key Server Public Key from the McAfee ePO server, then manually create the user configuration file.

**Optional offline activation features**

Drive Encryption includes two optional offline activation features, **Skip Unused Sectors** and **Disable Power Fail Recovery**.

**Skip Unused Sectors**

You can use the **Skip Unused Sectors** during offline activation to make sure that only sectors that contain data (as displayed in the Windows file system) are encrypted during the initial encryption of the disk.

> The **Skip Unused Sectors** feature is also known as **Windows: Encrypt only used sectors**.

Sectors that are marked as empty are included within the encrypted volume, but their contents are not read, encrypted, or written back to the disk. This significantly reduce the time required to initially encrypt a volume, particularly if the volume contains only a small amount of data.

It is important to note that:

- Sectors that are marked as empty might have previously contained sensitive data. For example, if the user deletes a document on the disk, Windows marks the sectors containing the document data as empty but does not erase the contents. If **Skip Unused Sectors** is used, the deleted document contents are left unencrypted on the disk until the "empty" sector containing the data is reused for another file.

- Following activation, when data is written to a sector that the Windows file system had flagged as empty during the offline activation process, the data written is encrypted in the normal manner.

**Disable Power Fail Recovery**

During initial encryption of the disk, Drive Encryption detects data corruption due to power failures and corrects these errors automatically when power is restored. **Disable Power Fail Recovery** is used to disable the power failure tests.

> The **Disable Power Fail Recovery** feature is also known as **Windows: Accelerated initial encryption**.

This feature slightly reduces the time required to perform the initial encryption of the disk at the expense of a risk of data corruption, if the system that is encrypted is powered-off unexpectedly. This option is in effect only during the initial encryption phase and does not affect the performance or functionality of the system when initial encryption is complete.

**Generate the offline activation package**

Using EpeOaGenXML.exe and the user configuration file, you can create the offline activation package with default policy settings that you export from the McAfee ePO server.

**Before you begin**

- Make sure that you have copied the required input files (EpeOaGenXML.exe, Userlist.txt) to the McAfee ePO system.
- You must have administrator rights to perform this task.
**Task**

1. Open the command prompt, then navigate to the folder that contains the EpeOaGenXML.exe and Userlist.txt files.

2. Type `EpeOaGenXML.exe --help` to display the list of policy configuration options available with Drive Encryption 7.2.0.

3. Generate the offline activation package using the command:

   ```
   EpeOaGenXML.exe --option arg
   ```

   where: `--option arg` specifies the required setting for any of the policy configurations. For example, `--PbfsSize 60 --BackupMachineKey false --Sso true`

   If you don’t specify any input for `arg` on the command line, the default policy configuration is used to generate the offline activation package. However, you can also modify the default policy configuration options by specifying the required settings on the command line.

4. To generate the offline activation package using the default policy settings and the Userlist.txt file, run the command:

   ```
   EpeOaGenXML.exe --user-file UserList.txt.
   ```

   If the user configuration file is in a different location than EpeOaGenXML.exe, specify its full path. If there are blank spaces in the path, make sure that you type the path within the double quotes. For example, `EpeOaGenXML.exe --user-file "c:\documents and settings\user\my documents \UserList.txt"`.

5. To generate the offline activation package with non-default policy settings and the Userlist.txt file, run the command:

   ```
   EpeOaGenXML.exe --user-file UserList.txt --PbfsSize 60 --BackupMachineKey false --Sso true --SkipUnused true --Disable PF true
   ```

   If you enabled the `SkipUnused` option, enter `Yes` in response to the message: By using this feature you accept the risk associated with not encrypting unused sectors with respect to (deleted) sensitive data leakage.

   If the package is generated successfully, no feedback or error message appears. The offline activation package (ESOfflineActivateCmd.XML and OfflineActivation.exe) is created in the folder where the EpeOaGenXML.exe file is located.

   - **ESOfflineActivateCmd.XML**— Lists all the users you added, the policy settings, and all the policy configuration options. If you modified any of the policy configuration options while running the EpeOaGenXML.exe file, that change also appears in the XML file.
   - **OfflineActivation.exe** — This is the actual offline activation package to be used to activate Drive Encryption on the client system that is not connected to a network or McAfee ePO.

---

**Performing offline activation**

The purpose of creating the offline activation package is to install and activate Drive Encryption offline on a client system that is not connected to a network or to the McAfee ePO server.

After creating and downloading all required packages and MSIs, you must them to the client system and run them one at a time to install and activate the Drive Encryption software on the system.
Before you perform offline activation on the client system:

- Make sure that your client system is not connected to network and not managed by the McAfee ePO server.
- Make sure that your client system has an administrator account with sufficient rights for installing and activating the Drive Encryption software.
- Make sure that you have copied these files to a temporary location on the client system:
  - OfflineActivation.exe
  - McAfee Agent installation package (FramePkg.exe)
  - MfeEEAgentXX.msi and MfeEEPcXX.msi, where XX=32-bit or XX=64-bit

**Install the McAfee Agent package**

Use this method to install the software on systems manually. You can install the agent on the system, or distribute the FramePkg.exe installer to users to install the agent themselves.

**Before you begin**

You must have administrator rights to perform this task.

If you want users (who have local administrator rights) to install the agent on their own systems, distribute the agent installation package file to them. You can attach it to an email message, copy it to media, or save it to a shared network folder.

**Task**

1. Distribute the agent installation package to the target system.
2. Double-click FramePkg.exe and wait a few moments while the agent is installed.

**Install the Agent and PC software packages**

The Agent and PC software packages include the files you must install on the client system.

**Before you begin**

Make sure that your client system has an administrator account with sufficient rights for installing and activating the Drive Encryption software.

These files must be installed (two different versions of each file, per operating system type):

- Agent installer files: MfeEEAgent32.msi or MfeEEAgent64.msi
- Plug-in installer files: MfeEEPc32.msi or MfeEEPc64.msi

**Task**

1. Determine whether your client computer is running a 32-bit or a 64-bit version of Windows.
2. Log on to the target computer using an administrator account with sufficient rights for installing the software.
3. Copy the agent and plug-in installer files for your operating system, to a temporary location on the client system.
4. Install the agent: double-click the agent installer file for your operating system.
5. Verify the installation by right-clicking **McAfee Agent System Tray** on the client system, then clicking **About**. The **McAfee Drive Encryption Agent** and version number are listed.
6 Install the plug-in: double-click the plug-in installer file for your operating system.

7 Restart the client system to complete the installation of Drive Encryption.

8 Verify the Drive Encryption System Status by right-clicking McAfee Agent System Tray on the client system, then clicking Quick Settings | Show Drive Encryption Status.

Install the offline activation package and activate Drive Encryption

To activate Drive Encryption offline, you must install the offline package that has the users list, policy settings, and policy configuration options. Copy and run the OfflineActivation.exe package on the client system to activate Drive Encryption offline.

**Before you begin**

Make sure that your client system has an administrator account with sufficient rights for installing and activating the Drive Encryption software.

**Task**

1 Run the OfflineActivation.exe file from the temporary location. A command prompt window displays this message: Activating Drive Encryption, please wait... message. The command prompt window disappears after adding the users and activating Drive Encryption.

2 Verify the Drive Encryption System Status by right-clicking McAfee Agent System Tray on the client system, then clicking Quick Settings | Show Drive Encryption Status.

The activation process might take up to 3 minutes.

The Drive Encryption System State should be Active, and after a short while the Volume Status should change to Decrypted. The message Activation has completed successfully also appears on the Drive Encryption System Status window.

Log on to the client system

When the client system is restarted and Drive Encryption is first activated, the user should log on with the user name that matches the user account defined in the user configuration file.

**Task**

1 Restart the client system after installing and activating Drive Encryption. The Pre-Boot Authentication page appears, prompting for a user name.

2 In the user name field, type the user name that was defined in the user configuration file.

The user account can be a password user or a user associated with a supported token type. When you are logging on for the first time, initialize the user with the default password of 12345 on the Pre-Boot Authentication page. The user is then prompted to change this password and enroll for self-recovery.
After initializing your token, the self-recovery enrollment dialog box appears. The default self-recovery setting for Offline Activation is configured to prompt for these recovery questions:

- What is your favorite color?
- What is your pet's name?
- What is your favorite musician?

Once recovery enrollment is complete, the client system boots to Windows.

**Perform recovery tasks using DETech**

Every Drive Encryption client system that is activated using the offline activation package has a machine key, which is encrypted with the Key Server Public Key from the McAfee ePO server.

**Before you begin**

- You must be a McAfee ePO administrator to decrypt the machine key in the recovery information file, because the decryption requires access to the private key from the McAfee ePO server.
- The encrypted machine key is stored in a recovery information file (.xml) on the client system. Any user trying to enable the recovery procedures on the client system needs to first get the decrypted machine key from the McAfee ePO server.

**Task**

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

1. Insert any removable media, such as a USB drive, into the client system that was activated using the offline activation package.

2. Copy the DERecovery.xml file from the default location (C:\) to the removable media.

   The default location can be changed when creating the offline activation package from the command prompt. You can specify the \-Recovery arg to define a different file name and location. For example, an external drive or USB drive.

3. Copy the recovery information file (DERecovery.xml) to a temporary location on the McAfee ePO system.

4. On the McAfee ePO server, click Menu | Systems | System Tree, then select the System Tree tab.

5. Click Actions | Drive Encryption | Decrypt Offline recovery file.

6. Browse and select the recovery information file to be decrypted, then click OK. The Export recovery information page with the Export information (.xml) file appears.

7. Right-click the .xml file and save it to the removable media.

8. Restart the unrecoverable system using the DETech (Standalone) boot disk to load the McAfee DETech interface.

9. Click Actions | Enable USB. DETech can now access the USB drive, which has the recovery information file.

11 Enter the daily Authorization/Access Code, then click OK. When the correct authorization code for the day is entered, the Authorization status changes to Authorized.

12 Click File under Authentication, browse and select the Recovery Information File (.xml) from the USB drive, then click OK.

The Authentication status changes to Authenticated with File. You can now perform any recovery task using the procedures given in the McAfee DETech User Guide.

---

**Machine Key Management**

The purpose of encrypting the client's data is to control access to the data by controlling access to the encryption keys. It is important that keys are not accessible to users.

The key that encrypts the hard disk sectors needs to be protected. These keys are referred to as Machine Keys. Each system has its own unique Machine Key. The Machine Key is stored in the McAfee ePO database to be used for client recovery when required.


**Machine Key re-use**

The Machine Key re-use option is used to activate the system with the existing key on the McAfee ePO server. This option is highly useful when a boot disk gets corrupted and the user cannot access the system. Other disks on the corrupted system can be recovered by activating it with the same key from McAfee ePO.

The Machine Key re-use feature is not applicable for self-encrypting (Opal) drive systems.

**What happens to Machine Keys when a Drive Encryption active system is re-imaged?**

All existing system data is lost, therefore the Machine Key is lost when a Drive Encryption active system is re-imaged.

**What happens to the Machine Key when you delete a Drive Encryption active system from McAfee ePO?**

The Machine Key remains in the McAfee ePO database; however, the key association with the client system is lost when the client system is deleted from McAfee ePO. When the client system reports back to McAfee ePO during the next ASCI, it appears as a new node. A new node does not have any users assigned to the client system. The administrator must therefore assign users to allow logon, or enable the Add local domain user option in the Product Setting Policy. The administrator must also configure the required policies in McAfee ePO.
The next data channel communication after adding the users and configuring the policies makes sure that:

- The Machine Key is re-associated with the client system and the recovery key is available. When the associated Machine Key is not present with the new node, McAfee ePO sends a Machine Key request. If the user is logged on to the client system, an agent-to-server communication between the client and the McAfee ePO server ensures the Machine Key is updated in McAfee ePO and the users are updated on the client. Thereafter, the Machine Key is available and admin recovery and policy enforcement work.

- The users are assigned to the client system. Therefore, these users can straightaway log on to the client system.

Although Drive Encryption 7.2 increases the number of users that pre-boot can support to 1000s rather than 100s, we recommend minimizing the number of users assigned per node. Firstly, best security practice aims to limit the number of users that can access a system to the smallest group of users. Secondly, assigning large numbers of users to each node might affect the overall scalability of the entire system and reduce the maximum number of nodes that can be supported by Drive Encryption.

What happens to Machine Keys when transferring a client system from one McAfee ePO server to another?

The Machine Key remains in the McAfee ePO database, however, the key association with the client system is lost when the client system is transferred from another McAfee ePO server.

When a transferred client system reports back to McAfee ePO during the next ASCI, it appears as a new node and therefore has no users assigned to it. The administrator must assign users to allow logon at PBA, assign users to the McAfee ePO branch where the systems are added (by default LOST&FOUND), and enable the Add local domain user option in the Product Setting Policy. The administrator must also configure the required policies in McAfee ePO.

To transfer all systems between McAfee ePO servers, the best process is to follow the McAfee ePO Disaster Recovery process. For more information, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB66616.

The next data channel communication after adding the users and configuring the policies ensures:

- The Machine Key is re-associated with the client system and the recovery key is available. When the associated Machine Key is not present with the new node, McAfee ePO sends a Machine Key request. If the user is logged on to the client system, an agent to server communication between the client and the McAfee ePO server ensures the Machine Key is updated in McAfee ePO and the users are updated on the client. Thereafter, the Machine Key will be available and admin recovery and policy enforcement will work.

- The users are assigned to the client system and can log on to the client system.

What happens to Machine Keys when moving systems from one branch to another in McAfee ePO?

The LeafNode is not deleted from McAfee ePO database when a system is moved from one branch to another in McAfee ePO, hence the Machine Key is available for the particular client system.

How to destroy the recovery information for a Drive Encryption installed system

When you want to secure-erase the drives in your Drive Encryption installed system, remove all users from the system (including those inherited from parent branches in the system tree). This makes the disks inaccessible through normal authentication as there are no longer any users assigned to the system. You must then destroy the recovery information for the system using the option Menu | Systems
You must also disable the Add local domain user option in the Product Setting Policy. This means that the system can never be recovered.
Managing Drive Encryption from a single location is achieved by integrating the Drive Encryption software into ePolicy Orchestrator. This management is accomplished through the combination of product policies.

Are you configuring policies for the first time?

When configuring policies for the first time:

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

Contents

- Policy categories
- Create a policy from the Policy Catalog
- Edit Drive Encryption policy settings from the Policy Catalog
- Assign a policy to a system group
- Enforce Drive Encryption policies on a system group

Policy categories

Policy settings for Drive Encryption are grouped by category. Each policy category refers to a specific subset of policy settings.

On the Policy Catalog page, policies appear under Drive Encryption and the individual policies appear under a specific category.

- Product settings
- User-based settings
- Server settings

When you open or edit an existing policy or create a new policy under Drive Encryption, the policy settings are organized in a series of tabs.
# Product Settings policy

The Product Settings policy options are organized into these tabs: General, Encryption, Log On, Recovery, Boot Options, Theme, Out-of-Band, Encryption Providers, and Companion Devices.

## Table 5-1 General tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable policy</td>
<td>Enables the set policies on the client computers.</td>
</tr>
<tr>
<td></td>
<td>• Only activate if health check (Drive Encryption: Go) passes — Select this option to activate Drive Encryption on client systems only when the Drive Encryption: GO health check passes.</td>
</tr>
<tr>
<td></td>
<td>You can enable this option only if the DEGO extension 7.x or higher is installed in McAfee ePO.</td>
</tr>
<tr>
<td>Logging level</td>
<td>Allows the administrator to set a different logging level for each client computer that has the specific policy setting assigned.</td>
</tr>
<tr>
<td></td>
<td>To overwrite the logging level defined in McAfee ePO, the LoggingLevelOverride registry key needs to be set on the client system.</td>
</tr>
<tr>
<td></td>
<td>• None — Does not create any log for the client system managed by McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>• Error — Logs only error messages.</td>
</tr>
<tr>
<td></td>
<td>• Error and Warnings — Logs the error and warning messages.</td>
</tr>
<tr>
<td></td>
<td>• Error, Warnings, and Informational — Logs the error and warning messages with more descriptions.</td>
</tr>
<tr>
<td></td>
<td>• Error, Warnings, Informational and Debug — Logs the error, warning, and debug messages.</td>
</tr>
<tr>
<td>Harden against cold boot attacks</td>
<td>Allows you to use the Elevated Security Crypt mode to help protect against cold-boot and other RAM-based attacks, when:</td>
</tr>
<tr>
<td>when</td>
<td>• The system is locked.</td>
</tr>
<tr>
<td></td>
<td>• The user is logged off.</td>
</tr>
<tr>
<td></td>
<td>• The system is in standby.</td>
</tr>
<tr>
<td></td>
<td>• Always (On systems that support Intel SGX)</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Protection of systems in Windows lock, log off, and standby states section.</td>
</tr>
<tr>
<td>Expire users who do not login</td>
<td>Allows the administrator to control and manage the users who have not logged on to the client system. This option forces the user account, which is not initialized, to expire after a number of hours as set in the policy.</td>
</tr>
<tr>
<td>Allow users to create endpoint info file</td>
<td>Allows the user to collect client system details such as the list of assigned users, policy settings, recovery, and Drive Encryption status. After enabling this option, the Save Machine info button appears in:</td>
</tr>
<tr>
<td></td>
<td>• Windows — McAfee Agent Tray</td>
</tr>
<tr>
<td></td>
<td>You can click this button and save the text file for later reference.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encrypt</td>
<td>Allows you to select the required encryption type and to set the encryption priority.</td>
</tr>
</tbody>
</table>

**Encryption type**

- **None** — Does not encrypt any disk.
- **All disks** — Encrypts all disks in a system.
- **Boot disk only** — Encrypts only the boot disk.
- **Selected partitions** — Allows you to select the required partitions of the client system and select them to be encrypted. You can select the required partitions by specifying the Windows drive letters/volume names. Partition level encryption is not applicable to client systems using OPAL encryption.

> Do not assign a drive letter to the Windows 7 hidden system partition on your client system. Doing so prevents activation of the Drive Encryption software on the client system.

This table also lists the available encryption providers (PC Software and PC Opal) available. You can change and set the encryption priority by moving the encryption provider rows up and down, as appropriate.

By default, software encryption is used on both Opal and non-Opal systems in this version of Drive Encryption. To ensure that Opal technology is chosen in preference to software encryption, we recommend that you always set Opal as the default encryption provider, by moving it to the top of the list on the Encryption Providers page. This ensures that Opal locking will be used on Opal drives.

> Make sure that you select the required encryption type, as appropriate. Policy enforcement might fail on client systems if you select an unsupported encryption type.

- **All disks except boot disk** — Encrypts all disks except the boot disk (not recommended)

The Encryption type options None, All disks except boot disk, and Selected partitions are not applicable to self-encrypting drives in Opal mode.
Table 5-3 Log On (Drive Encryption) tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic booting</td>
<td>When enabled, the client system boots automatically without prompting for a Pre-Boot Authentication. The expiration date for auto-booting can also be set. If required, the user can select the UTC time standard option.</td>
</tr>
<tr>
<td></td>
<td>If you enable this option without requiring the use of TPM for automatic booting, the Drive Encryption product does not protect the data on the drive when it is not in use.</td>
</tr>
<tr>
<td></td>
<td>• Disable and restart system after 3 (1-10) failed logons or unlocks (Windows only, Vista onwards) — This feature is an enhancement of the primary Enable automatic booting feature. Select this option to disable the autoboot after a specific number (defaulted to 3 or specify from 1-10) of failed Windows logons.</td>
</tr>
<tr>
<td></td>
<td>On the Windows authentication screen, if the user fails to authenticate the defined number of times, a message appears indicating that the maximum number of failed operating system logons was reached, and that Pre-Boot Authentication is enabled on the machine. Upon clicking OK, the client system restarts and PBA screen appears. Once the user authenticates through PBA and Windows successfully, autoboot is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Use of TPM for automatic booting — Select one of these options:</td>
</tr>
<tr>
<td></td>
<td>• Never — The encryption key is written to a plain-text file, which is unencrypted. The system is not secure.</td>
</tr>
<tr>
<td></td>
<td>• If available — If the TPM is available, the encryption key is written to a plain-text file, which is encrypted. The system is secure. If the TPM is not available, the encryption key is written to a plain-text file, which is unencrypted. The system is not secure.</td>
</tr>
<tr>
<td></td>
<td>• Required (Note: if TPM is not available on the system, automatic booting will not be enabled) — If the required TPM is available, the encryption key is written to a plain-text file, which is encrypted. The system is secure. If the required TPM is not available, automatic booting will not be enabled and the user will see the PBA screen to authenticate. The system is secure.</td>
</tr>
<tr>
<td></td>
<td>This option is applicable only for systems installed with Drive Encryption 7.2.0. If you apply a policy to the earlier versions of Drive Encryption 7.2.0 with automatic booting enabled and use of TPM set to 'Required', it will leave the client system in an unprotected state since autoboot will be enabled with no protection of the disk encryption key.</td>
</tr>
<tr>
<td>Allow temporary automatic booting</td>
<td>Allows you to turn (on or off) the PBA screen, with a client-side utility. This eliminates the need to modify the policy in McAfee ePO, and fully automates patching and other client management scenarios.</td>
</tr>
<tr>
<td>Pre-boot power management:</td>
<td>The client system will shut down automatically after the set time at pre-boot.</td>
</tr>
<tr>
<td>Automatically shutdown pre-boot</td>
<td></td>
</tr>
<tr>
<td>after a period of inactivity: 1-60</td>
<td></td>
</tr>
<tr>
<td>minutes</td>
<td></td>
</tr>
<tr>
<td>Log on message</td>
<td>Type a message that appears to the client user.</td>
</tr>
<tr>
<td>Do not display previous user name</td>
<td>Prevents the client system from automatically displaying the user name of the last logged on user on all Drive Encryption logon dialog boxes.</td>
</tr>
<tr>
<td>at log on</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-3 Log On (Drive Encryption) tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Enable on screen keyboard             | Enables the Pre-Boot On-Screen Keyboard (OSK) and the associated Wacom serial pen driver. When this option is enabled, the pen driver finds supported pen hardware (Panasonic CF-H1 and Samsung Slate 7) and displays the OSK.  

- **Always display on screen keyboard** — Forces the Pre-Boot to always display a clickable on-screen keyboard, whether the pen driver finds suitable hardware or not.  

- **Enable on screen keyboard** is turned on, if there is a serial digitizer device for which we have support on BIOS systems, then the OSK is displayed. Otherwise, on both BIOS and UEFI systems, if there is a requirement to display the OSK, then you must also select the option **Always display on screen keyboard**. This forces the OSK to be displayed without looking for any serial digitizer devices under BIOS.  

- **Add local domain users (and tag with 'EE:ALDU')** — Selecting this option does not add any local domain users to the client system.  

- **Add all previous and current local domain users of the system** — Domain users who have previously and are currently logged on to the system can authenticate through the Pre-Boot, even if the administrator has not explicitly assigned the user to the client system.  

- **Only add currently logged on local domain user(s); activation is dependent on a successful user assignment** — Only the domain users who are logged on to the current Windows session are added to the system and hence Drive Encryption is activated, even if the administrator has not explicitly assigned the user to the client system.  

  If you select this option, at least one user should be added to the client system for a successful Drive Encryption activation on the client. The activation doesn’t happen until a user logs on to Windows.  

| Enable accessibility                  | Select this option to sound a beep as a signal when the user moves the focus from one field to the next using mouse or keyboard in the Pre-Boot environment. This option is helpful to visually challenged users.  

- The USB audio functionality allows visually impaired users to hear an audio signal (spoken word) as guidance when the user moves the cursor from one field to the next in the Pre-Boot environment. The USB speakers and headphones can be used to listen to the audio signal.  

  For more details, see Enable Accessibility (USB audio devices) in the Pre-Boot environment.  

| Disable pre-boot authentication when not synchronized | Blocks a user from logging on to PBA in the client system, if the client system is not synchronized with the McAfee ePO server for the set number of days.  

- The user is blocked from logging on to PBA, and can then request the administrator to perform Administrator Recovery to unlock the client system. This allows the client system to boot and communicate with the McAfee ePO server.  

  The client system continues to block the user from logging on to the system until synchronization with McAfee ePO. |
### Table 5-3 Log On (Drive Encryption) tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read username from smartcard</td>
<td>Automatically retrieves the available user information on the client system from the inserted smartcard; hence the Authentication window does not prompt for a user name. The user can then authenticate by typing the correct PIN. You need to enable the matching rules that are required for matching smartcard user principle name (UPN) names with Drive Encryption user names.</td>
</tr>
<tr>
<td></td>
<td>• Disable pre-boot authentication when not synchronized Match certificate user name field up to @ sign — Matches the certificate user name up to the @ sign of the user name. For example, if the UPN is <a href="mailto:SomeUser@SomeDomain.com">SomeUser@SomeDomain.com</a> and the Drive Encryption user name is SomeUser, a match is found.</td>
</tr>
<tr>
<td></td>
<td>• Hide user name during authentication — The Drive Encryption user name does not appear in the Authentication window.</td>
</tr>
<tr>
<td></td>
<td>This feature is supported on the Gemalto.Net V2+ tokens, and PIV and CAC tokens.</td>
</tr>
<tr>
<td>Lock workstation when inactive: After x number of minutes</td>
<td>The client system is locked automatically when it is inactive for the set time.</td>
</tr>
</tbody>
</table>

### Table 5-4 Log On (Windows) tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>V7.2 Onwards</td>
<td>Third-party credential providers:</td>
</tr>
<tr>
<td></td>
<td>• Allow integrated third-party credential providers to override the Drive Encryption credential provider — Enable this option to make sure that the Drive Encryption credential provider does not load and allow a compatible third-party credential provider to override the existing credential provider.</td>
</tr>
<tr>
<td></td>
<td>Single sign-on (SSO):</td>
</tr>
<tr>
<td></td>
<td>• Provide a single sign-on experience for Drive Encryption users (SSO) — Enable this option to allow the user to log on to the system with a single authentication process. It allows automatic logon to the operating system once the user authenticates through the Pre-Boot Authentication page.</td>
</tr>
<tr>
<td></td>
<td>• Allow the capturing of smart card PINs for SSO replay — Enable this option to allow Drive Encryption to capture the smart card PIN for SSO.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Password synchronization</strong>:</td>
<td></td>
</tr>
<tr>
<td>• Update the Drive Encryption user password to match the Windows user password (during Windows logon, or password changes)</td>
<td>Enable this option to synchronize the Drive Encryption password to match the Windows password when the Windows password is changed on the client system. For example, if users change their password on the client, the Drive Encryption password is also changed to the same value.</td>
</tr>
<tr>
<td>• Ignore Drive Encryption password rules and history when updating the Drive Encryption password</td>
<td>Enabling this option allows you to ignore Drive Encryption password rules and history when synchronizing the Drive Encryption password. <strong>This may result in a reduction of password strength for Drive Encryption users.</strong></td>
</tr>
<tr>
<td>• Periodically check domain credentials for changes and ask the user to re-capture the Drive Encryption password if required</td>
<td>Enabling this option allows you to periodically check the domain credentials for any changes and also inform the user to re-capture the Drive Encryption password, if required. <strong>This will result in an increased load on the domain server that manages the endpoint.</strong></td>
</tr>
<tr>
<td>• Polling interval (minutes) <strong>(5-480)</strong></td>
<td>Enter the time in minutes within the set limit to periodically check the domain credentials for any changes.</td>
</tr>
<tr>
<td><strong>Preboot user options</strong></td>
<td></td>
</tr>
<tr>
<td>• Allow user to cancel SSO and password synchronization</td>
<td>Enable this option to allow the user to cancel SSO and password synchronization.</td>
</tr>
<tr>
<td><strong>Windows username matching</strong></td>
<td></td>
</tr>
<tr>
<td>• The Windows username must match the username of the Drive Encryption user before capturing SSO or synchronizing passwords</td>
<td>Ensures the SSO details are captured only when the user's Drive Encryption and Windows user names match. This ensures that the SSO data captured is replayed for the user for which it was captured.</td>
</tr>
<tr>
<td><strong>Credential provider bitmap</strong></td>
<td></td>
</tr>
<tr>
<td>• Do not display McAfee shield on Windows logon tiles</td>
<td>Enabling this option allows you to hide the McAfee shield on Windows logon tiles.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pre V7.2</td>
<td>Enable SSO — Select this option to enable Single Sign On.</td>
</tr>
<tr>
<td></td>
<td>• Must match user name — Ensures the SSO details are captured only when the user’s Drive Encryption and Windows user names match. This ensures that the SSO data captured is replayed for the user for which it was captured. When you select the Enable SSO option, the Must match user name option is also enabled by default.</td>
</tr>
<tr>
<td></td>
<td>• Using smart card PIN — Allows Drive Encryption to capture the smart card PIN for SSO.</td>
</tr>
<tr>
<td></td>
<td>• Synchronize Drive Encryption password with Windows — The Drive Encryption password synchronizes to match the Windows password when the Windows password is changed on the client system. For example, if users change their password on the client, the Drive Encryption password is also changed to the same value.</td>
</tr>
<tr>
<td></td>
<td>• Allow user to cancel SSO — Allows the user to cancel the SSO to Windows in Pre-Boot. When this option is enabled, the user has an additional checkbox at the bottom of the Pre-Boot logon dialog box.</td>
</tr>
<tr>
<td></td>
<td>Make sure to note that SSO now works with Drive Encryption 7.2.0 when the client system resumes from hibernation or when booting the system using Windows 8 fast boot.</td>
</tr>
<tr>
<td>Require Drive Encryption logon (only supported on V6 clients) — This requires you to mandatorily log on to PBA for EEPC 6.x.x systems, thereby disabling the SSO functionality.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Require log on when token is removed — This requires you to mandatorily log on when the token is removed.</td>
</tr>
<tr>
<td></td>
<td>This option is available for selection only if the Require Drive Encryption logon (only supported on V6 clients) option is enabled.</td>
</tr>
</tbody>
</table>
Table 5-5  Recovery tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>The Recovery option is enabled by default. This activates the Administrator Recovery option in the client system.</td>
</tr>
<tr>
<td>Administrator</td>
<td>• <strong>Key size</strong> — The recovery key size options. The recovery Response Code size depends on this recovery key size. This does not affect the size of the challenge code.</td>
</tr>
<tr>
<td>recovery</td>
<td>• <strong>Low</strong> — A recovery key size that creates a short Response Code for the recovery.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong> — A recovery key size that creates a medium size Response Code for the recovery.</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong> — A recovery key size that creates a lengthy Response Code for the recovery.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Full</strong> — A recovery key size that creates a Response Code, with the maximum number of characters, for the recovery.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Message</strong> — Displays a text message when you select Recovery. This can include information such as your help desk contact details.</td>
</tr>
<tr>
<td>Self-recovery</td>
<td><strong>Allow users to re-enroll self-recovery information at PBA</strong> — Allows the client user’s self-recovery details can be reset. The user must then re-enroll their self-recovery details with new self-recovery answers.</td>
</tr>
<tr>
<td></td>
<td>Before resetting the self-recovery questions on the client system, make sure that you have enabled the Enable Self Recovery option under User Based Policy</td>
</tr>
<tr>
<td></td>
<td>When this option is enabled, the Pre-Boot Authentication (user name) screen includes the Reset self-recovery option. On selecting Reset self-recovery, the user is prompted for a password, then self-recovery enrollment.</td>
</tr>
<tr>
<td></td>
<td>Only initialized users can reset their self-recovery details.</td>
</tr>
</tbody>
</table>

Table 5-6  Boot Options tab (Windows only)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Boot Manager</td>
<td>Activates the built-in pre-boot partition manager. This allows you to select the primary partition on the hard disk that you want to boot. Naming of the partition is also possible with the boot manager. The timeout for the booting to start can also be set.</td>
</tr>
<tr>
<td>Always enable</td>
<td>Forces the Drive Encryption Pre-Boot code to always initialize the USB stack. USB audio functionality allows the visually impaired users to listen to an audio signal (spoken word) as a guidance when the user moves the cursor from one field to the next, in the Pre-Boot environment. The USB speakers and headphones can be used to listen to the audio signal.</td>
</tr>
<tr>
<td>pre-boot USB support</td>
<td>You will notice an improper synchronization of the mouse cursor and the stylus on USB connected Wacom pen digitizers. To avoid this, make sure to enable this option.</td>
</tr>
<tr>
<td></td>
<td>For more details, see Enable Accessibility (USB audio devices) in the Pre-Boot environment.</td>
</tr>
<tr>
<td>Enable pre-boot</td>
<td>If selected, the policy enables pre-boot PCMCIA support.</td>
</tr>
<tr>
<td>PCMCIA support</td>
<td>Graphics mode</td>
</tr>
<tr>
<td></td>
<td>Allows you to select the screen resolution for a system or a system group. The default option is Automatic.</td>
</tr>
</tbody>
</table>
### Table 5-7  Theme tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select theme</td>
<td>Contains the options for selecting a theme.</td>
</tr>
<tr>
<td>Preview</td>
<td>Displays the preview of the selected theme. The preview is not available for shared policies from another McAfee ePO.</td>
</tr>
</tbody>
</table>

### Table 5-8  Out-of-Band tab (Windows only)

<table>
<thead>
<tr>
<th>Drive Encryption: Out Of Band Management Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable at PBA</td>
<td>Enables the Drive Encryption out-of-band management features through policies and then perform actions on Intel® AMT provisioned client systems. You can select this option only if you installed the Drive Encryption: Out Of Band Management extension in McAfee ePO.</td>
</tr>
</tbody>
</table>

### Table 5-9  Encryption Providers tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC Software</td>
<td>• Use compatible MBR — Causes Drive Encryption to boot a built-in fixed MBR instead of the original MBR that was on the system after pre-boot logon. It is used to avoid problems with some systems that had other software that runs from the MBR and no longer work if Drive Encryption is installed.</td>
</tr>
<tr>
<td></td>
<td>• Fix OS boot record sides — Some boot records report an incorrect number of sides. Selecting this option fixes this on the client system. This is available only when you install the Drive Encryption extension.</td>
</tr>
<tr>
<td></td>
<td>• Use windows system drive as boot disk — Maintains the compatibility with some systems where the disk 0 is not the boot disk. Selecting this option forces the users product to assume that the boot disk is the one that contains the Windows directory but not disk 0.</td>
</tr>
<tr>
<td></td>
<td>• Enable Pre-Boot Smart Check (BIOS based systems only) — Modifies the Drive Encryption activation sequence and creates a pre-activation stage, where hardware compatibility checks are performed prior to actual activation and subsequent encryption.</td>
</tr>
<tr>
<td></td>
<td>• Force system restart once activation completes — This option is selected by default when you select Enable Pre-Boot Smart Check (BIOS based systems only) to restart your system after activation.</td>
</tr>
<tr>
<td>Opal</td>
<td>Require all disks to be Opal — Requires all the drives in your client system to be Opal drives for the PC Opal encryption provider to be activated.</td>
</tr>
</tbody>
</table>

### Table 5-10  Companion Devices tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Companion Device Support</td>
<td>Enable this option to allow the user to perform system recovery through smartphone.</td>
</tr>
<tr>
<td></td>
<td>The Companion Device application is now known as McAfee Endpoint Assistant.</td>
</tr>
</tbody>
</table>
**Recommended Product Settings policy**

The Product Settings policy controls the behavior of the Drive Encryption client. For example, it contains the options for enabling encryption, enabling automatic booting, and controlling the theme for the pre-boot environment.

You can configure the Product Settings policy by navigating through Menu | Policy | Policy Catalog, then selecting Drive Encryption 7.2 from the Product drop-down list. Select Product Settings from the Category drop-down list, locate the My Default policy, then click Edit Settings. For more information about individual policy settings, see the McAfee Drive Encryption 7.2.0 Product Guide.

The Product Settings policy options are organized into a series of tabs.

### Table 5-11 General tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Policy</td>
<td>Leave this option checked (enabled). This policy should be enabled to activate Drive Encryption on the client system. This option needs to be disabled to uninstall Drive Encryption from the client.</td>
</tr>
<tr>
<td></td>
<td>The Only activate if Health Check (Drive Encryption GO) check passes option is applicable only if the DEGO extension is installed in McAfee ePO.</td>
</tr>
<tr>
<td>Logging Level</td>
<td>Set the required logging level.</td>
</tr>
<tr>
<td></td>
<td>To overwrite the logging level defined in ePolicy Orchestrator, the LoggingLevelOverride registry key needs to be set on the client system.</td>
</tr>
<tr>
<td></td>
<td>• None — Does not create any log for the client system managed by McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>• Error — Logs only error messages.</td>
</tr>
<tr>
<td></td>
<td>• Error and Warnings — Logs the error and warning messages.</td>
</tr>
<tr>
<td></td>
<td>• Error, Warnings, and Informational — Logs the error and warning messages with more descriptions.</td>
</tr>
<tr>
<td></td>
<td>• Error, Warnings, Informational and Debug — Logs the error, warning, and debug messages. We recommend that you enable this option only when you require extended logging for troubleshooting purposes. Try not to enable this option for standard usage because it might impact the performance.</td>
</tr>
<tr>
<td>Harden against cold boot attacks when</td>
<td>Allows you to use the Elevated Security Crypt mode to help protect against cold-boot and other RAM-based attacks, when:</td>
</tr>
<tr>
<td></td>
<td>• The system is locked — The encryption driver switches to the Elevated Security Crypt mode when the user locks the screen.</td>
</tr>
<tr>
<td></td>
<td>• The user is logged off — The encryption driver switches to the Elevated Security Crypt mode when the user logs off.</td>
</tr>
<tr>
<td></td>
<td>• The system is in standby — The encryption driver switches to the Elevated Security Crypt mode when the system in standby</td>
</tr>
<tr>
<td></td>
<td>For more information, see Protection of systems in Windows lock, log off, and standby states in the McAfee Drive Encryption 7.2.0 Product Guide.</td>
</tr>
</tbody>
</table>
Table 5-11 General tab (continued)

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expire users who do not login</td>
<td>Leave this option checked (enabled). This option allows the administrator to control and manage the users who have not logged on to the client system. This option forces the user account, which is not initialized, to expire after a number of hours as set in the policy. This feature allows you to control access to client systems by preventing unauthorized access using uninitialized user accounts.</td>
</tr>
</tbody>
</table>
| Allow users to create endpoint info file | Leave this option checked (enabled). This option allows the user to collect client system details such as the list of assigned users, policy settings, recovery, and Drive Encryption status.  
After enabling this option, a Save Machine info button appears in Windows, under McAfee Agent Tray | Quick Settings | Show Drive Encryption Status. You can click this button and save the text file for later reference. |

Table 5-12 Encryption tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt</td>
<td>Allows you to select the required encryption type and to set the encryption priority.</td>
</tr>
</tbody>
</table>
| Encryption type         | All Disks is the recommended option (the None option does not initiate the encryption).  
The All disks except boot disk option, which encrypts all disks except the boot disk, is not a recommended option.  
The None, All disks except boot disk, and Selected partitions options are not applicable for self-encrypting drives in Opal mode. |
| Selected Partitions     | Allows you to select the required partitions of the client system to be encrypted. You can select the required partitions by specifying the Windows drive letters or volume names.  
Partition level encryption is not applicable to client systems using Opal encryption. If the selected partitions include both Opal and non-Opal hard drives, both will be software-encrypted.  
Do not assign a drive letter to the Windows 7 hidden system partition on your client system. Assigning the drive letter prevents activation of Drive Encryption software on the client system.  
This table also lists the available encryption providers (PC Software and PC Opal) available. You can change and set the encryption priority by moving the encryption provider rows up and down, as appropriate.  
By default, software encryption is used on both Opal and non-Opal systems in this version of Drive Encryption. To ensure that Opal technology is chosen in preference to software encryption, we recommend that you always set Opal as the default encryption provider, by moving it to the top of the list on the Encryption Providers page. This ensures that Opal locking will be used on Opal drives.  
Make sure that you select the required encryption type, as appropriate. Policy enforcement might fail on client systems if you select an unsupported encryption type. |
### Table 5-13 Log On (Drive Encryption) tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable automatic booting</strong></td>
<td>Leave this option unchecked (disabled). If you enable this feature, the client system does not have the PBA. This is normally referred to as Autoboot mode. Nonetheless, enabling this option can be helpful when you need to manage the autobooting scenarios. There are multiple scenarios where this option can be enabled or disabled. For instance, to minimize the end user impact during rollout, or to allow patches to be installed and the reboots to take place without end user intervention during patch cycles. It is the responsibility of the administrator to decide on when to enable or disable this option.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable and restart system after 3 (1-10) failed logons or unlocks (Windows only, Vista onwards)</strong> — We recommend that you enable this option if you enabled the <em>Enable automatic booting</em> option. This option disables the system autoboot after a specific number of failed Windows logons.</td>
</tr>
<tr>
<td></td>
<td>If you enable this option, the Drive Encryption software does not protect the data on the drive when it is not in use.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Do not display previous user name at log on</strong> — Leave this option checked (enabled). This option prevents the client system from displaying the user name of the last logged on user automatically on all Drive Encryption logon dialog boxes.</td>
</tr>
<tr>
<td></td>
<td><strong>Enable on screen keyboard</strong> — Leave this option checked (enabled), especially for tablets or on-screen mouse device systems. This option enables the Pre-Boot On-Screen Keyboard (OSK) and the associated Wacom serial pen driver. When this option is enabled, the pen driver finds a supported pen hardware and displays the OSK.</td>
</tr>
<tr>
<td></td>
<td>If you do not select this option, the BIOS uses mouse emulation. In such a situation, the BIOS treats the digitizer as a standard mouse, which might lead to the cursor being out of sync with the stylus on USB-connected Wacom pen digitizers.</td>
</tr>
</tbody>
</table>

If the required TPM is not available, automatic booting is not enabled and the PBA screen is displayed. The system is secure.

This option is applicable only for systems installed with Drive Encryption 7.2.0. If you apply a policy to earlier versions of Drive Encryption (i.e., EEPC) with automatic booting enabled and set TPM use to Required, the client system is left in an unprotected state because autoboot is enabled with no protection of the disk encryption key.

Allow temporary automatic booting Allows you to turn (on or off) the PBA screen, with a client-side utility. This eliminates the need to modify the policy in McAfee ePO, and fully automates patching and other client management scenarios.

Use of TPM for automatic booting Select one of these options:

• **Never** — The encryption key is written to a plain-text file, which is unencrypted. The system is not secure.

• **If available** — If the TPM is available, the encryption key is written to a plain-text file, which is encrypted. The system is secure.

If the TPM is not available, the encryption key is written to a plain-text file, which is unencrypted. The system is not secure.

• **Required (Note: if TPM is not available on the system, automatic booting will not be enabled)** — If the required TPM is available, the encryption key is written to a plain-text file, which is encrypted. The system is secure.

If the required TPM is not available, automatic booting is not enabled and the PBA screen is displayed. The system is secure.

Log on message Type a message that appears to the client user.

Do not display previous user name at log on Leave this option checked (enabled). This option prevents the client system from displaying the user name of the last logged on user automatically on all Drive Encryption logon dialog boxes.
### Table 5-13 Log On (Drive Encryption) tab (continued)

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always display on screen keyboard</td>
<td>Forces the Pre-Boot to always display a clickable on-screen keyboard regardless of whether the pen driver finds suitable hardware or not. This is valid for BIOS-based hardware only. On UEFI, the digitizer is managed by the UEFI software, so the UEFI implementation needs to contain drivers for the digitizer.</td>
</tr>
</tbody>
</table>
| Add local domain users (and tag with ‘EE:ALDU’)      | • Disabled — Selecting this option does not add any local domain users to the client system.  
• Add all previous and current local domain users of the system — Any domain users who have previously and are currently logged on to the system, are able to authenticate through the Pre-Boot, even if the administrator has not explicitly assigned the user to the client system.  
• Only add currently logged on local domain user(s); activation is dependent on a successful user assignment — Leave this option selected (enabled) so that only the domain users who are logged on to the current Windows session are added to the system. As a result, Drive Encryption is activated, even if the administrator has not explicitly assigned the user to the client system.  
| Enable Accessibility (Windows BIOS systems only)    | Leave this option checked (enabled). This option is helpful to visually challenged users. If selected, the system beeps as a signal when the user moves the focus from one field to the next using a mouse or keyboard in the Pre-Boot environment.  
The USB audio functionality allows visually impaired users to hear an audio signal (spoken word) as guidance when the user moves the cursor from one field to the next in the pre-boot environment. The USB speakers and headphones can be used to listen to the audio signal.  
| Disable pre-boot authentication when not synchronized | Leave this option checked (enabled). This option blocks the user from logging on to PBA in the client system, if the client system is not synchronized with the McAfee ePO server for the set number of days. When the user is blocked from logging on to PBA, the user should request the administrator to perform the Administrator Recovery to unlock the client system. This allows the client system to boot and communicate with the McAfee ePO server.  
The client system will continue to block the user from logging on to the system until the synchronization with ePolicy Orchestrator happens. This is especially useful to prevent unauthorized access to laptops that have been misplaced, lost or stolen. 

If you select this option, at least one user should be added to the client system for successful Drive Encryption activation on the client. The activation doesn’t happen until a user logs on to Windows as a domain user. This domain should have been registered in McAfee ePO.
Table 5-13 Log On (Drive Encryption) tab (continued)

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read username from smartcard</td>
<td>Leave this option checked (enabled). This option automatically retrieves the</td>
</tr>
<tr>
<td></td>
<td>available user information on the client system from the inserted smartcard;</td>
</tr>
<tr>
<td></td>
<td>hence the Authentication window does not prompt for a username. The user can</td>
</tr>
<tr>
<td></td>
<td>then authenticate just by typing the correct PIN.</td>
</tr>
<tr>
<td></td>
<td>You need to enable the matching rules that are required for matching smartcard</td>
</tr>
<tr>
<td></td>
<td>user principle name (UPN) with Drive Encryption usernames.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Match certificate user name field up to @ sign</strong> — Match the certificate</td>
</tr>
<tr>
<td></td>
<td>user name up to the @ sign of the user name. For example, if the UPN is Some</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:User@SomeDomain.com">User@SomeDomain.com</a> and the Drive Encryption user name is SomeUser, a match is</td>
</tr>
<tr>
<td></td>
<td>found.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hide user name during authentication</strong> — On selecting this option, the Drive</td>
</tr>
<tr>
<td></td>
<td>Encryption user name does not appear in the Authentication window.</td>
</tr>
<tr>
<td>Lock workstation when inactive</td>
<td>Leave this option uncheck (disabled). The client system is locked when it is</td>
</tr>
<tr>
<td></td>
<td>inactive for the set time.</td>
</tr>
</tbody>
</table>

Table 5-14 Log On tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSO</td>
<td>Leave this option checked (enabled).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Must match user name</strong> — Leave this option checked (enabled). This option ensures the SSO details are only captured when the user's Drive Encryption and Windows user names match. This ensures that the SSO data captured is replayed for the user for which it was captured. When you select the Enable SSO option, the Must match user name option is also enabled by default.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Using smart card PIN</strong> — Leave this option checked or unchecked based on whether the eToken or smart card is used or not. This option allows Drive Encryption to capture the smart card PIN for SSO.</td>
</tr>
<tr>
<td>Synchronize Drive Encryption Password with Windows</td>
<td>Leave this option checked (enabled). If selected, the Drive Encryption password synchronizes to match the Windows password when the Windows password is changed on the client system. For example, if users change their password on the client, the Drive Encryption password is also changed to the same value.</td>
</tr>
<tr>
<td>Allow user to cancel SSO</td>
<td>Leave this option checked (enabled). This option allows the user to cancel the SSO to Windows in Pre-Boot. When this option is enabled, the user has an additional checkbox at the bottom of the Pre-Boot logon dialog box.</td>
</tr>
<tr>
<td>Require Drive Encryption logon (only supported on V6 clients)</td>
<td>This makes it mandatory for you to log on to PBA for EEPC 6.x.x systems, thereby disabling the SSO functionality.</td>
</tr>
<tr>
<td>Lock workstation when inactive</td>
<td>Leave this option unchecked (disabled). The client system is locked when it is inactive for the set time.</td>
</tr>
</tbody>
</table>
Table 5-15 Recovery tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Leave this option checked (enabled). This is enabled by default to make sure that the recovery is possible at any stage of the Drive Encryption management.</td>
</tr>
</tbody>
</table>
| Administrator recovery | • **Key size** — After consulting with your IT security, set the to the size adequate for your organization requirements. This refers to a recovery key size that creates a short Response Code for the recovery.  
  • **Low** — A recovery key size that creates a short Response Code for the recovery.  
  • **Medium** — A recovery key size that creates a medium size Response Code for the recovery.  
  • **High** — A recovery key size that creates a lengthy Response Code for the recovery.  
  • **Full** — A recovery key size that creates a Response Code, with the maximum number of characters, for the recovery.  
  • **Message** — Displays a text message when you select **Recovery**. This can include information such as your help desk contact details. |
| Self-recovery | Allow users to re-enroll self-recovery information at PBA — Leave this option checked (enabled) only when required. On enabling this option, the client user's self-recovery details can be reset, then the user has to enroll the self-recovery details with new self-recovery answers.  
  
  **Before resetting the self-recovery questions on the client system, make sure that you have enabled the Enable Self Recovery option under User Based Policy | Self-recovery.**  
  
  When this option is enabled, the Pre-Boot Authentication (user name) screen includes the Reset self-recovery option. On selecting Reset self-recovery, the user is prompted for a password, then self-recovery enrollment.  
  
  **Only initialized users can reset their self-recovery details.** |

Table 5-16 Boot Options tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Boot Manager</strong></td>
<td>Leave this option unchecked (disabled). This option activates the built in pre-boot partition manager. This allows you to select the primary partition on the hard disk that you wish to boot. Naming of the partition is also possible with the boot manager. The time out for the booting to start can also be set.</td>
</tr>
</tbody>
</table>
| **Always enable pre-boot USB support** | Leave this option checked (enabled) only when needed.  
  This option forces the Drive Encryption Pre-Boot code to always initialize the USB stack. USB audio functionality allows the visually impaired users to listen to an audio signal (spoken word) as a guidance when the user moves the cursor from one field to the next, in the Pre-Boot environment. The USB speakers and headphones can be used to listen to the audio signal.  
  To enable the USB audio functionality, select Enable Accessibility on the Log On (Drive Encryption) tab.  
  
  **You might notice an improper synchronization of the mouse cursor and the stylus on USB-connected Wacom pen digitizers. To avoid this, enable this option.** |
### Table 5-16 Boot Options tab (continued)

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable pre-boot PCMCIA support</td>
<td>Leave this option unchecked (disabled) unless you require support for PCMCIA devices in pre-boot.</td>
</tr>
<tr>
<td>Graphics mode</td>
<td>Leave the default setting, Automatic. This option allows you to select the screen resolution for a system or a system group.</td>
</tr>
</tbody>
</table>

We recommend that you leave the default options on the Theme tab for easier deployment and management.

### Table 5-17 Out-of-Band tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable at PBA</td>
<td>Select this option to enable the Drive Encryption out-of-band management features through policies, and then perform actions on Intel® AMT provisioned client systems. You can select this option only if you have installed the Drive Encryption: Out Of Band Management extension in McAfee ePO.</td>
</tr>
</tbody>
</table>

### Table 5-18 Encryption Providers tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use compatible MBR</td>
<td>Leave this option unchecked (disabled). This option causes Drive Encryption to boot a built-in fixed MBR instead of the original MBR that was on the system after pre-boot logon. It is used to avoid problems with some systems that had other software that runs from the MBR and no longer work if Drive Encryption is installed.</td>
</tr>
<tr>
<td>Fix OS boot record sides</td>
<td>Leave this option unchecked (disabled). Some boot records report an incorrect number of sides. Selecting this option fixes this on the client system. This is available only when you install the Drive Encryption extension.</td>
</tr>
<tr>
<td>Use Windows system drive as boot drive</td>
<td>Leave this option unchecked (disabled). This is for maintaining the compatibility with some systems where the disk 0 is not the boot disk. Selecting this option forces the client system to assume that the boot disk is the one that contains the Windows directory but not disk 0.</td>
</tr>
<tr>
<td>Enable Pre-Boot Smart Check (BIOS-based systems only)</td>
<td>Leave this option checked (enabled) only when needed. When you enable this feature, it modifies the Drive Encryption activation sequence and creates a pre-activation stage, where a series of hardware compatibility checks are performed prior to actual activation and subsequent encryption to successfully activate Drive Encryption on platforms where BIOS issues might exist. This feature is available only for BIOS systems using PC software encryption, and is not available for UEFI or Opal systems. The client system reboots several times before the Smart Check is completed.</td>
</tr>
<tr>
<td>Force system restart once activation completes</td>
<td>Leave this option checked only when needed (enabled). This option is selected by default when you select the Enable Pre-Boot Smart Check (BIOS based systems only) option to restart your system after activation.</td>
</tr>
<tr>
<td>Opal</td>
<td>This option requires all the drives in your client system to be Opal for the PC Opal encryption provider to be activated.</td>
</tr>
</tbody>
</table>

Table 5-19   Companion Devices tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Companion Device Support</td>
<td>Select this option to allow the user to perform system recovery using a smartphone or mobile device.</td>
</tr>
<tr>
<td></td>
<td>The Companion Device application is now known as McAfee Endpoint Assistant.</td>
</tr>
</tbody>
</table>

User-based policy settings

The user-based policy settings are organized into these tabs: Authentication, Password, Password Content Rules, Self-Recovery, and Companion Devices.

Table 5-20   Authentication tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token type</td>
<td>The authentication token type, for example, password or smartcard.</td>
</tr>
<tr>
<td>Certificate rule</td>
<td>Drive Encryption enhances the use of PKI and tokens to allow users to authenticate using their certificates. You can use certificate rules to quickly make your Drive Encryption enterprise aware of all certificate-holding users, and allow them to be allocated to PCs using Drive Encryption without having to create new smart cards or other forms of token for their use.</td>
</tr>
<tr>
<td></td>
<td>• Provide LDAP user certificate — This provides the latest LDAP user certificate.</td>
</tr>
<tr>
<td></td>
<td>• Enforce certificate validity period on client — By default, this is enabled to enforce certificate validity period for the added certificate rule.</td>
</tr>
<tr>
<td></td>
<td>• Use latest certificate — This uses the latest certificate available.</td>
</tr>
<tr>
<td>Logon Hours</td>
<td>The days and the hours when the user can log on to the client system. The restrictions are applied using the Apply Restrictions option.</td>
</tr>
</tbody>
</table>

Table 5-21   Password tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default password</td>
<td>Change default password — The default password is 12345. If the administrator changes the default password, the new password becomes the default password for this policy under the User Based Policy category.</td>
</tr>
<tr>
<td></td>
<td>• Do not prompt for default password — Skips the default password entry and immediately asks the user to enter an encryption password.</td>
</tr>
<tr>
<td>Password change</td>
<td>• Enable password history__changes (1-100) — This keeps track of the specified number of previous passwords set by the user and does not allow the user to set previous passwords again.</td>
</tr>
<tr>
<td></td>
<td>• Prevent change — This option prevents the user from changing the password.</td>
</tr>
<tr>
<td></td>
<td>• Require change after__days (1-366) — The number of days after which the system prompts the user to change the password.</td>
</tr>
<tr>
<td></td>
<td>• Warn user__days before password expires (0-30) — The number of days in advance that the system prompts the user with a warning message about the number of days left for the password expiry.</td>
</tr>
</tbody>
</table>
### Table 5-21 Password tab (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect passwords</td>
<td>• Timeout password entry after _invalid attempts (3-20) — The number of invalid password entries after which the system times out the password attempts.</td>
</tr>
<tr>
<td></td>
<td>• Maximum disable time _minutes (1-64) — The maximum timeout duration for the timeout password entry.</td>
</tr>
<tr>
<td></td>
<td>• Invalidate password after _invalid attempts (3-100) — The number of wrong attempts a user can make before the password becomes invalid.</td>
</tr>
<tr>
<td>Allow showing of password</td>
<td>Enable this option to display the password of the user while entering it.</td>
</tr>
</tbody>
</table>

### Table 5-22 Password Content Rules tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display list of password rules</td>
<td>Enable this option to display the password requirements to users.</td>
</tr>
<tr>
<td>Password length</td>
<td>The number of characters in a user password.</td>
</tr>
<tr>
<td></td>
<td>• Minimum (3-40) — The minimum number of characters for a user password.</td>
</tr>
<tr>
<td></td>
<td>• Maximum (3-255) — The maximum number of characters for a user password.</td>
</tr>
<tr>
<td>Enforce password content</td>
<td>The number of different characters like alpha, numeric, alphanumeric, and symbols that are required to form a password.</td>
</tr>
<tr>
<td></td>
<td>• Alpha — The number of letters that must be present in a user password.</td>
</tr>
<tr>
<td></td>
<td>• Numeric — The number of numeric characters that must be present in a user password.</td>
</tr>
<tr>
<td></td>
<td>• Alphanumeric — The number of alphanumeric characters that must be present in a user password.</td>
</tr>
<tr>
<td></td>
<td>• Symbols — The number of symbols that must be present in a user password.</td>
</tr>
<tr>
<td>Password content restrictions</td>
<td>The password content restrictions for the user password.</td>
</tr>
<tr>
<td></td>
<td>• No anagrams — A word or phrase spelled by rearranging the letters of a previous password can’t be a password.</td>
</tr>
<tr>
<td></td>
<td>• No palindromes — A word or phrase that reads the same backward as forward can’t be a password.</td>
</tr>
<tr>
<td></td>
<td>• No sequences — The new password can’t be in sequence with the previous password.</td>
</tr>
<tr>
<td></td>
<td>• Can’t be user name — A user name can’t be set as a password.</td>
</tr>
<tr>
<td></td>
<td>• Simple content rules — Follow the standard Windows password content rules; a Windows password should contain at least three of the following:</td>
</tr>
<tr>
<td></td>
<td>• Lowercase letters</td>
</tr>
<tr>
<td></td>
<td>• Uppercase letters</td>
</tr>
<tr>
<td></td>
<td>• Numbers</td>
</tr>
<tr>
<td></td>
<td>• Symbols and special characters</td>
</tr>
<tr>
<td></td>
<td>• No simple words — The set of words defined as simple words that cannot be used as passwords.</td>
</tr>
</tbody>
</table>
Table 5-23  Self-recovery tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable self-recovery</td>
<td>Enables self-recovery for users assigned to the system.</td>
</tr>
<tr>
<td>Invalidate self-recovery after no. of invalid attempts</td>
<td>The number of attempts after which self-recovery is disabled.</td>
</tr>
<tr>
<td>Questions to be answered</td>
<td>The number of questions to be answered by the user to perform the self-recovery. This lists the default questions for the selected language, also provides an option to add more questions.</td>
</tr>
<tr>
<td>Logons before forcing user to set answers</td>
<td>The number of logons before forcing the user to set answers.</td>
</tr>
<tr>
<td>Questions</td>
<td>Allows you to select a language, set the question, and set the minimum answer length. This lists the default questions for the selected language, and provides an option to add more questions.</td>
</tr>
</tbody>
</table>

If a language does not have enough questions or includes an error, the language appears in red.

Table 5-24  Companion Devices tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery</td>
<td>Enable this option to allow the user to perform system recovery through smartphone. The Companion Device application is now known as McAfee Endpoint Assistant.</td>
</tr>
<tr>
<td>Password Definition</td>
<td>Enable this option to create a password according to the option selected. If the user has once set a higher password definition to the system, the user cannot change the password to a lower password definition (that is less secure) even if that policy is set in McAfee ePO.</td>
</tr>
</tbody>
</table>

Recommended user-based policy settings

The user-based policy controls the parameters for Drive Encryption user accounts. For example, it contains the options for selecting a token type (including password and smartcard) and password content rules.

You can configure the user-based policies by clicking Menu | Policy | Policy Catalog, then selecting Drive Encryption 7.2 from the Product drop-down list.

Select User Based Policies from the Category drop-down list. Locate the My Default policy and click Edit Settings. For more information about individual policy settings, see the McAfee Drive Encryption 7.2.0 Product Guide.

User-based policies in Drive Encryption

Drive Encryption 7.2.0 requires that you specify which groups of users are allowed to use the Policy Assignment Rules. The allowed users get their required user-based policies. Users that are not allowed to use the Policy Assignment Rules inherit the default user-based policies assigned to the system.
Enforce the desired user-based policy to a user assigned to a client system by enabling the Configure UBP enforcement option.

If possible, it is always better to assign user-based policies at the system level or branch level, rather than using the Policy Assignment Rules. However, you can use the Policy Assignment Rule option, if required, to assign different policies to different users.

The user-based policy options are organized into these tabs.

### Table 5-25 Authentication tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token type</td>
<td>Select <strong>Password only</strong>. There are a number of other tokens that can be effectively used for your authentication as required. However, the <strong>Password only</strong> token is as strong as any other token that you could configure.</td>
</tr>
<tr>
<td>Certificate rule</td>
<td>Drive Encryption enhances the use of PKI and tokens to allow users to authenticate using their certificates. You can use certificate rules to efficiently update Drive Encryption about all certificate-holding users, and allow them to be allocated to PCs using Drive Encryption without having to create new smart cards or other forms of token for their use.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Provide LDAP user certificate</strong> — Leave this option checked (enabled).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enforce certificate validity period on client</strong> — Leave this option checked (enabled) to enforce certificate validity period for the added certificate rule.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use latest certificate</strong> — Leave this option checked (enabled).</td>
</tr>
<tr>
<td></td>
<td>The <strong>Certificate rule</strong> options are not active if <strong>Password only</strong> is selected.</td>
</tr>
<tr>
<td>Logon Hours</td>
<td>You can set the days and the hours when the user can log on to the client system. The restrictions are applied using the <strong>Apply Restrictions</strong> option. We recommend enabling this option only if you have a specific requirement.</td>
</tr>
</tbody>
</table>

### Table 5-26 Password tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Default Password</td>
<td>• <strong>Do not prompt for default password</strong> — Leave this option checked (enabled). When enabled, users are prompted to type in their Drive Encryption password without having to remember a common default password. If you enable this option, you don't have to enable the <strong>Change Default Password</strong> option.</td>
</tr>
<tr>
<td>Password Change</td>
<td>Disable all of these settings as you would be using SSO and don't want to cause conflict with Windows password requirements.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable password history changes</strong> (1-100) — Leave this option checked (enabled) to prevent users from reusing passwords unless your security policy exempts users from using new passwords.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Prevent change</strong> — Leave this option unchecked (disabled).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Require change after ___ days</strong> (1-366) — Leave this option unchecked (disabled).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Warn user ___ days before password expiry</strong> (0-30) — This is disabled by default when you disable the <strong>Require change after ___ days</strong> (1-366) option.</td>
</tr>
</tbody>
</table>
### Table 5-26 Password tab (continued)

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| Incorrect Passwords     | • Timeout password entry after ___ invalid attempts (3-20) — Set the number of invalid attempts to trigger a timeout.  
                          | • Maximum disable time ___ minutes (1-64) — This is disabled by default when you disable the Timeout password option.  
                          | • Invalidate password after ___ invalid attempts — Leave this option checked (enabled). |
| Allow showing of password | Enable this option if you want the password of the user to be displayed while entering it. |

### Table 5-27 Password Content Rules tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display list of password rules</td>
<td>Enable this option to display the password requirements to users.</td>
</tr>
<tr>
<td>Password length</td>
<td>Leave the default value.</td>
</tr>
<tr>
<td>Enforce password content</td>
<td>Leave the default value.</td>
</tr>
<tr>
<td>Password content restrictions</td>
<td>Leave the default value or enable restrictions for increased password strength.</td>
</tr>
</tbody>
</table>

### Table 5-28 Self-Recovery tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable self-recovery</td>
<td>Leave this option checked (enabled).</td>
</tr>
<tr>
<td>Invalidate self-recovery after no. of invalid attempts</td>
<td>Enable and set the number of attempts to a number that does not abruptly lock out the Self Recovery.</td>
</tr>
</tbody>
</table>
| Questions to be answered        | Can be set to 3. This can provide the required security without overly inconveniencing the user.  
                          | It is up to the administrator to decide how many questions are required.         |
| Logons before forcing user to set answers | Set this to 0. This makes sure that the users set the answers during the user initialization. |
| Questions                       | Leave the default questions or configure new questions as required.             |

### Table 5-29 Companion Devices tab

<table>
<thead>
<tr>
<th>Policy Options</th>
<th>Recommendations</th>
</tr>
</thead>
</table>
| Enable Companion Device Support | Select this option to allow the user to perform system recovery using a smartphone or mobile device.  
                          | The Companion Device application is now known as McAfee Endpoint Assistant.     |
| Password Definition             | Enable this option to create a password according to the option selected.       |
|                                 | If the user has once set a higher password definition to the system, the user cannot change the password to a lower password definition (that is less secure) even if that policy is set in McAfee ePO. |
Server policy settings

The server settings are organized into these tabs: General, Incompatible Products, Theme, Simple Words, Tokens, LDAP Attributes, PC software, PC Opal.

Table 5-30   General tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>If user is disabled in LDAP Server</td>
<td>Allows you to disable, delete, or ignore a user if the user has been disabled on the LDAP Server.</td>
</tr>
<tr>
<td>Machine key re-use</td>
<td>Enables activation of the system with the existing key present in the McAfee ePO server. This option is useful when a boot disk gets corrupted and the user can't access the system. The corrupted system's disks, other than the boot disk, can be recovered by activating it with the same key from McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>Machine key re-use is not applicable to systems having self-encrypting (Opal) drives.</td>
</tr>
<tr>
<td>Batch size for retrieving users</td>
<td>Allows the system to send users to the client in batches rather than sending them all at the same time. Specify the number of users that are sent in each batch. Increasing the batch size increases the amount of memory required on the server and the client. But, this reduces the number of recommended messages required to be sent between the client and server.</td>
</tr>
</tbody>
</table>

Table 5-31   Incompatible Products tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage incompatible products</td>
<td>Allows you to manage the list of products that are not compatible with Drive Encryption. You can also import an incompatible product rule that can detect and add the incompatible product to the list. You cannot activate Drive Encryption on a client system where these incompatible products are present.</td>
</tr>
</tbody>
</table>

Table 5-32   Themes tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Themes</td>
<td>Allows you to add and customize a theme that is used as a background in the Pre-Boot Authentication page.</td>
</tr>
</tbody>
</table>

Table 5-33   Simple Words tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add group</td>
<td>Allows you to create a group that can have a number of simple words. This will not be available for shared policy from another McAfee ePO.</td>
</tr>
<tr>
<td>Remove group</td>
<td>Deletes a group of simple words.</td>
</tr>
<tr>
<td>Import words to group</td>
<td>Allows you to browse to a text file with a number of simple words that can't be used as passwords. You can also select an encoding type for the file.</td>
</tr>
<tr>
<td>Regenerate missing simple word package</td>
<td>Compiles all the simple word groups and creates the simple words package files (.xml file).</td>
</tr>
</tbody>
</table>

Table 5-34   Tokens tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Tokens</td>
<td>Allows you to add and manage extra token definitions. This allows the user to deploy and manage additional token modules any time after the initial installation.</td>
</tr>
</tbody>
</table>
### Table 5-35 LDAP Attributes tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage LDAP Attributes</td>
<td>Allows you to manage user attributes for Active Directory and User Directory.</td>
</tr>
</tbody>
</table>

*The User Directory attributes appear only if you have installed the User Directory extension.*

### Table 5-36 PC software tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm</td>
<td>Specifies the algorithm AES-256-CBC for the software encryption.</td>
</tr>
<tr>
<td>Pre-boot storage size</td>
<td>Allows you to set the size of the pre-boot file system. Increasing the size of the PBFS increases the number of users that can be successfully assigned to the client system. The size is specified in MB from 20 MB to 100 MB. If you are assigning a large set of users to the system, the PBFS size must be 100 MB.</td>
</tr>
<tr>
<td>50MB (20-100)</td>
<td>The default Pre-Boot storage size for PC software is 50 MB.</td>
</tr>
</tbody>
</table>

### Table 5-37 PC Opal tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-boot storage size</td>
<td>Allows you to set the size of the pre-boot file system for the client systems with self-encrypting (Opal) drives. Increasing the size of the PBFS increases the number of users that can be successfully assigned to the client system. The size is specified in MB from 20 MB to 100 MB. If you are assigning a large set of users to the system, the PBFS size must be 100 MB.</td>
</tr>
<tr>
<td>50MB (20-100)</td>
<td></td>
</tr>
</tbody>
</table>

---

**Create a policy from the Policy Catalog**

You can add a custom policy to the Policy Catalog before or after the Drive Encryption software is deployed.

**Task**

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

1. Click Menu | Policy | Policy Catalog.
2. Click Actions | New Policy.
3. Select the policy category from the drop-down list.
4. From the Create a policy based on this existing policy drop-down list, select the policy that you want to duplicate.
5. Type a name for the new policy.
6. Type a description in the Notes field, if required, then click OK to open the Policy Settings wizard.
7. Edit the policy settings on each tab as needed, then click Save.

By default, the new policy is not assigned to any groups or systems.
Edit Drive Encryption policy settings from the Policy Catalog

Modify and assign the Drive Encryption policies to systems or users, as appropriate, to meet your corporate requirements. Use McAfee ePO to modify the settings of a policy.

Before you begin
Your user account must have administrator rights to edit policy settings for the required product.

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

1. Click Menu | Policy | Policy Catalog, then from the Product drop-down list, select Drive Encryption 7.2.
2. Select the policy Category from the drop-down list. The policies for the selected category appear in the details pane.
3. Click the required policy, edit the required settings, then click Save.

Assign a policy to a system group

Assign a policy to multiple managed systems within a group. You can assign policies before or after deploying Drive Encryption to the client systems.

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

1. Click Menu | Systems | System Tree | Systems, then select a group in the System Tree. All the systems within this group (but not its subgroups) appear in the details pane.
2. Select a system, then click Actions | Agent | Modify policies on a single system. The Policy Assignment for My Organization page appears.
3. From the Product drop-down list, select Drive Encryption 7.2.
4. Select the Category and Policy from the drop-down lists, then click Save.

Enforce Drive Encryption policies on a system 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. Click Menu | Systems | System Tree | Assigned Policies tab, then select a group in the System Tree.
2. Select Drive Encryption from the Product drop-down list, then click Enforcing next to Enforcement Status. The Enforcement page appears.
3. To change the enforcement status, you must first select Break inheritance and assign the policy and settings below.
4 Next to Enforcement status, select Enforcing or Not enforcing accordingly.

5 Select whether to lock policy inheritance so that groups and systems that inherit this policy can't break enforcement, then click Save.
Managing Drive Encryption users

The McAfee ePO server allows administrators to assign users from Microsoft Active Directory or User Directory to Drive Encryption managed systems.

The user's authentication credentials, token type, and the user information fields are managed from the McAfee ePO server. Drive Encryption gives the administrator the freedom of adding and removing the users to and from systems or system groups at any time.

Contents

- Manage the users assigned to a system
- Add group users
- User management through User Directory
- Edit user inheritance
- How Drive Encryption controls the Windows logon mechanism
- Enable Single-Sign-On (SSO) on a system
- Synchronize the Drive Encryption password with the Windows password
- Configure password content rules
- Manage a disabled user in Microsoft Active Directory or User Directory
- Managing the blacklist rule with the ALDU function
- Configure global user information
- Manage logon hours
- Define Drive Encryption permission sets for McAfee ePO users
- How disabling/deleting a user in Active Directory affects the Drive Encryption user

Manage the users assigned to a system

You can use the McAfee ePO server to view the Drive Encryption users assigned to the client system. The Drive Encryption software can be activated on a client system only after adding one or more users and enforcing the required encryption policies correctly.

Before you begin
You must have administrator rights to perform this task.

You can also remove users from a client system. Make sure that you have assigned the user at the system level or branch level. If a user is assigned at the branch level, the user is assigned to other client systems even after removing one system.

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

1. Click **Menu** | **Data Protection** | **Encryption Users** to open the **My Organization** page.

2. From the **System Tree** pane, select a system.
Click **Actions | Drive Encryption | View Users**. The **Encryption Users** page lists the users for the selected system.

- This page does not display the user groups that are assigned at the branch level.

To remove a user:

- Select the user name from the list, then click **Actions | Drive Encryption | Delete Users**.
- When prompted for confirmation, click **Yes** to delete the selected user.

### Add group users

Group Users are the Drive Encryption user accounts that are allocated to every encrypted system. They are typically administration accounts used for troubleshooting and supporting the client in a given group.

- If you choose to add a Group or an Organizational Unit (OU), the individual user names do not appear. Instead, the entire Domain Name of the Group or Organizational unit appears.

If you do not follow the recommendations on **Change default password** and **Do not prompt for default password** options, then all Drive Encryption user accounts, including Group User accounts, are assigned the default password upon creation. If the default password is not changed in the User-Based Policies, then use **12345** as the default password the first time you log on with these user accounts.

If you want the system to automatically capture the user’s credentials without requiring them to use a default password on PBA, enable the **Do not Prompt for default password** option under **User Based Policies | Password**.

### Users

To access the data on an encrypted computer, the user must go through the PBA. If the **Enable automatic booting** option is not enabled, the client user is presented with the PBA screen when the system is restarted after activating Drive Encryption.

During the first pre-boot after activation, the user needs to initialize the user account with the default password and enroll for self recovery (if enabled in the policy).

- Make sure that at least one manually added user is assigned to the client system. For example, this could be an admin user assigned to all systems.

During the initialization process, users set up their pre-boot credentials to unlock the disk.

- At least one Drive Encryption user must be assigned to Drive Encryption on each client; this could be an administrative user.

### Add local domain users

This option automatically adds the previously logged in domain users to the client system, so that administrators don't have to manually assign users to the client systems in the ePolicy Orchestrator console.

This option can be enabled when needed through the Drive Encryption Product Settings Policies (**Menu | Policy | Policy Catalog | Drive Encryption 7.2 (Product Settings) | Log on tab | Add local domain users**).
When enabled, the DEAgent queries the client system for the currently/previoulsy logged on domain users. The DEAgent then sends the collected data to the McAfee ePO server. These users are then assigned to the client system.

We recommend that you enable this option so that you can authenticate to the client pre-boot without having to manually assign the users to the client system in the ePolicy Orchestrator console. However, it is the responsibility of the administrator to decide whether or not this is required depending on corporate requirements.

Prerequisites

These prerequisites must be met to add the local domain users to the Drive Encryption client systems:

- The McAfee Agent package is deployed.
- The McAfee DEAgent package is deployed to the required client systems.
- The Drive Encryption package is deployed to the required client systems.
- Registered Active Directory is added and configured correctly.

The Add local domain users option is supported with Active Directory only.

- An automated LDAP Server User/Group Synchronization task (LdapSync: Sync across users from LDAP) is scheduled and run.

This task is used to map Active Directory attributes to the Drive Encryption settings. This is required for every Registered LDAP server that is to be used with Drive Encryption.

- Client systems should use Active Directory for authentication.
- These domain users must be previously or currently logged in users.

At the client side

The Add local domain user option is processed during the next agent-to-server communication. If this option is enabled in the policy settings, the DEAgent queries the client system for the domain users who have logged on to the client. The DEAgent then sends the collected data to the McAfee ePO server.

The transmitted data is a list of user names and the domain names. Local Domain users are detected by examining the Windows registry that has the profile list, which lists the users who have logged in to the system.

At the server side

When the DE Admin receives a message for adding local domain users, it executes these steps.

- It attempts to find the domain name that the user belongs to. This is done by querying the Registered Active Directory that is configured with the automated LdapSync: Sync across users from LDAP task.

- If a registered LDAP server is found, then it matches the domain name of the user. An LDAP query is performed and attempts to find an LDAP node with a samaccountname that matches the user name.

If the user name is found, it is assigned to the corresponding client system. You can query the added users by using the View Users option under Menu | Data Protection | Encryption Users | Actions | Drive Encryption | View Users.
User management through User Directory

Drive Encryption 7.2.0 provides support for user management using the User Directory feature to remove the dependency on LDAP server.

The User Directory feature utilizes the LDAP Sync extension within McAfee ePO and provides user management for Drive Encryption users using the UserDirectory.zip extension. Once you install the UserDirectory.zip extension into the McAfee ePO server, you can create Organizational Units (OUs) and users and manage them on the User Directory page, without requiring to register on LDAP server.

You can also perform user management through User Directory using Web API commands. For more information, see *McAfee Drive Encryption 7.2 Scripting Guide*.

User Directory does not support user certificates for Drive Encryption 7.2.

User Directory does not support adding groups. Groups can only be added for users who are created from registered LDAP servers.

Manage Organizational Units from the User Directory page

You can manage Organizational Units (OUs) on the User Directory page using the Tree Tasks function.

**Task**

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


2. To add an OU:
   - Click Tree Tasks | Add sub-OU, enter the OU name, then click OK.

   An error message appears when you add a sub-OU using the Internet Explorer (IE) 8.0.7601.17514 browser version. We recommend you to use the 8.0.6001.18702 version, if you are using the IE 8 version.

3. To edit an OU, select the OU, then click Tree Tasks | Edit OU.

4. To delete an OU, select the OU, then click Tree Tasks | Delete OU. When prompted for confirmation, click Yes.

5. To move an OU, select the OU, click Tree Tasks | Move OU, then select the destination OU and click OK.

Manage Users from the User Directory page

You can manage Organizational Units (OUs) on the User Directory page using the options in Actions menu.

**Task**

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


2. To add a user:
   - Click Actions | Add user, enter the user name and enable the user account control, if required, then click OK.

3. To edit a user, select the user, then click Actions | Edit user.

   You can add or remove the user’s attributes by using the + and - buttons.
4 To delete a user, select the user, then click Actions | Delete user(s). When prompted for confirmation, click Yes.

5 To enable a user, select the user, then click Actions | Enable user(s). When prompted for confirmation, click Yes.

6 To disable a user, select the user, then click Actions | Disable user(s). When prompted for confirmation, click Yes.

7 To move a uses, select the user, click Actions | Move user(s), then select the destination OU and click OK.

---

Edit user inheritance

You can group users at different organizational levels and edit the inheritance as required. Inheritance is used to assign multiple users to systems from a centralized location without having to work on the individual systems.

**Before you begin**

You must have administrator rights to perform this task.

**Task**

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

1 Click Menu | Data Protection | Encryption Users to open the My Organization page.

2 Select the Organizational Unit from the System Tree, then click the Group Users tab.

3 Click Edit in Inheritance broken to open the Edit Group Inheritance page.

4 Select Break inheritance, then click OK.

The user inheritance broken status appears:

- **True** — Specifies that the inheritance is broken. Breaking inheritance on a branch prevents inheritance of users and groups from any parent branch. It has no effect on users and groups assigned to the branch or child.

- **False** — Specifies that the inheritance is not broken. When inheritance is not broken on a branch, users and groups are inherited from the parent until the inheritance is broken.

---

How Drive Encryption controls the Windows logon mechanism

Drive Encryption intercepts the Windows logon mechanism using a Passthrough Shim Gina on Windows 2003 and Windows XP, and a Credential Provider on Vista.

On Windows 2000 and XP operating systems, a custom .ini file (EPEPCGINA.INI) helps Drive Encryption analyze the logon page and port the credentials into the correct boxes on the logon page. In Windows Vista, Microsoft has replaced the original MSGINA (Graphical Identification and Authentication) with a new method called Microsoft Credential Provider.

Drive Encryption supports the Single Sign On architecture and implements a Credential Provider to communicate with Windows. Drive Encryption displays each token as a potential logon method. During log on, Drive Encryption prompts for your Windows credentials only for the first time and Drive Encryption stores the Windows credentials securely. On subsequent logon events, Drive Encryption retrieves the stored Windows credentials to log on.
Enable Single-Sign-On (SSO) on a system

Enabling SSO on a system allows the user to log on to the system with a single authentication process. It allows automatic logon to the operating system once the user authenticates through the Pre-Boot Authentication page.

**Task**

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

1. Click Menu | Systems | System Tree, then select a group from the System Tree.
2. Select the target system, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page.
3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system's assigned policy.
4. Select the Product Settings policy category, then click Edit Assignments to open the Product Settings page.
5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6. From the Assigned Policy drop-down list, select the policy, then click Edit Policy to open the Policy Settings page.

   From this page, you can edit the selected policy or create a new policy.
8. If required, select these options:
   - **Must match user name** — This option makes sure that the SSO details are captured only when the user’s Drive Encryption and Windows user name match. This should be used, where possible, to make sure that the Drive Encryption user who authenticated through pre-boot does not inadvertently capture SSO for a different user.
   - **Using smart card PIN** — This option allows the administrator to capture the smart card PIN for SSO.
   - **Synchronize Drive Encryption password with Windows** — When the user changes on the client, this option synchronizes the new password to the Drive Encryption user.
   - **Allow user to cancel SSO** — This option allows the user to cancel the SSO to Windows in the pre-boot stage only. When this option is enabled, an additional checkbox appears at the bottom of the Pre-Boot logon dialog box. This setting lasts for a single boot only.
9. Click Save on the Policy Settings page, then click Save on the Product Settings page.
10. Send an agent wake-up call.

Synchronize the Drive Encryption password with the Windows password

Use this task to synchronize the Drive Encryption password with the Windows password. This synchronizes the Windows password to the Drive Encryption password, so the user needs to authenticate on the Pre-Boot Authentication page with Windows password.
Task
For details about product features, usage, and best practices, click Help.

1. Click Menu | Systems | System Tree, then select a group from the System Tree.
2. Select a System, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page.
3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system's assigned policy.
4. Select the Product Settings policy category, then click Edit Assignments to open the Product Settings page.
5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6. From the Assigned Policy drop-down list, select the policy, then click Edit Policy to open the Policy Settings page.
   From this page, you can edit the selected policy, or create a new policy.
7. On the Log On tab, click Enable SSO, then select Synchronize Drive Encryption password with Windows under Windows pane.
8. Click Save on the Policy Settings page, then click Save on the Product Settings page.
   Make sure that the Windows password adheres to the Drive Encryption password restriction policy. Otherwise, the password synchronization does not run.
9. Send an agent wake-up call.

Configure password content rules
This policy setting determines whether the Drive Encryption passwords must meet complexity requirements. Complexity requirements are enforced when the updated policy is assigned to the required user on a system.

Before you begin
You must have administrator rights to perform this task.

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

1. Click Menu | Systems | System Tree, then select the group from the System Tree.
2. Select the system, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page.
3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system's assigned policy.
4. Select the User Based Policy category, then click Edit Assignments to open the policy page.
5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6. From the Assigned Policy drop-down list, select the policy, then click Edit Policy to open the Policy Settings page.
   From this page, you can edit the selected policy, or create a new policy.
7 On the Password Content Rules tab, enable the Display list of password rules option to display the password requirements to users.

8 Enter the Password Length in the Minimum and Maximum fields.

9 Under Enforce password content, type the number of Alpha, Numeric, Alphanumeric, and Symbols characters required to form a password.

10 Under Password content restrictions, select or deselected the options to define the password content restriction rules.

11 Click Save in the Policy Settings page, then click Save in the User Based Policies settings page.

12 Send an agent wake-up call.

When changing the Windows password and synchronizing to Drive Encryption password, Windows does not provide the old password.

Manage a disabled user in Microsoft Active Directory or User Directory

Use this task to disable, delete, or ignore a user who has been disabled in Active Directory or User Directory.

**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 Drive Encryption, then click Edit to open the Drive Encryption page.

3 On the General tab, select Disable, Ignore or Delete from the If user disable in directory drop-down list.

Options in the drop-down list are applicable only to users disabled in the Active Directory or User Directory.

4 Click Save.

Managing the blacklist rule with the ALDU function

With the Add Local Domain User (ALDU) function, domain users who have previously and are currently logged on to the client system can authenticate through the Pre-Boot, even if the administrator has not explicitly assigned the user to the client system.

While this captures the regular users of the system, in some cases, an administrator who has previously configured the system is also granted access. This might be applicable to some, but not all, users.

To address this situation, you can add a blacklist of users to the Add Local Domain User Settings policy. Users added to the blacklist are excluded from the list of users assigned by the ALDU function.

Prioritization of policy assignment rules is not applicable to the ALDU blacklist policy.
Add an ALDU blacklist policy

You can add regular expressions to blacklist user accounts. Any users who match the configured regular expression are excluded from the ALDU list. Regular Expression ECMA 262 standard is supported with the ALDU blacklist policy.

**Before you begin**
- You must have administrator rights to perform this task.
- Make sure that you have installed the DEAdmin extension on the McAfee ePO server.

**Task**

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

1. Click Menu | Systems | System Tree, then select a group from the System Tree.
2. Select a System, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page.
3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system's assigned policy.
4. Select the Add Local Domain User Settings policy category, then click Edit Assignments.
5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6. From the Assigned Policy drop-down list, select the policy, then click Edit Policy to open the Policy Settings page.
   From this page, you can edit the selected policy, or create a new policy.
7. Click Add from Regular expression and type the regular expressions that help to exclude the local domain users from being assigned to the client system.
   - `\\domainname\username` — This blacklists the specified user from the given domain.
   - `\\.*\username` — This blacklists the specified user name from all the domains available.
   - `\\.*\a.*` — This blacklists all user names that starts with the letter "a" from all available domains.
   - `\\.*\[a-n]*` — This blacklists all user names that starts with the letter "a" to "n", from all available domains.

   You can add multiple regular expressions under a single policy. All comparisons are case-insensitive.
8. Click Test to verify the regular expression.
9. Enter the user name in the Value field and validate the specified regular expression.
10. On the Policy Settings page, click Save, then click Save on the Product Settings page.
11. Send an agent wake-up call.

During the next ASCI, this rule is applied to the new local domain users assigned to the client system where the policy is enforced.

Users assigned before the blacklist is assigned are not removed from the system.

You can also add or remove a blacklist rule to or from an existing ALDU blacklist policy.
Configure global user information

Global users have read and write permissions to all operations. You can create additional global administrator accounts for people who require global administrator rights. Configure the user information fields in the Server Settings within Drive Encryption.

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

1. Click Menu | Configuration | Server Settings.
2. Click Drive Encryption in the Setting Categories pane, then click Edit. The Edit Drive Encryption page opens to the General tab.
3. Click Add next to the user information fields.
4. Type the question related to the user, then select the required user attribute name from the LDAP Attribute Name list.
   
   LDAP refers to Microsoft Active Directory.
5. Click + or - in the interface to add or remove user information fields.
6. Click Save.

User information fields can be set by selecting the individual user in the DE User Query. To display the users, click Menu | Reporting | Queries | Shared Groups | Drive Encryption, then click Run in DE:Users.

Manage logon hours

You can control and limit the timeline when a user can log on to the Drive Encryption client system. This option does not force the users to log out from the current session, although the current time is scheduled to be part of the logon restriction. However, once the user logs out from the system, the user will not be able to log on to the client system until the next allowed logon hour.

Logon hours policy is applied only when the user is not logged on.

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

1. Click Menu | Systems | System Tree then select a group from the System Tree.
2. Select a System, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page.
3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption displays the system's assigned policy.
4. Select the User Based Policy category, then click Edit Assignments to open the User Based Policies page.
5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6. From the Assigned Policy drop-down list, select the policy, then click Edit Policy to open the Policy Settings page.
   From this page, you can edit the selected policy, or create a new policy.
7 On the Authentication tab, select Apply restrictions in Logon Hours, then schedule the logon timing by blocking or allowing specific logon hours.

8 Click Save in the Policy Settings page, then click Save in the User Based Policies page.

9 Send an agent wake-up call.

Define Drive Encryption permission sets for McAfee ePO users

User accounts provide a means for users to access and use the Drive Encryption software. They are associated with permission sets that define what users are allowed to do with the software. You must create user accounts and permission sets to accommodate the needs of each user who logs on to the McAfee ePO server.

The administrator can set up Drive Encryption product-specific permission sets for different users and systems on McAfee ePO.

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

1 Click Menu | User Management | Permission Sets.

2 Click New Permission Set.

3 Enter a permission set name in the Name field.

4 Select the Active Directory groups mapped to this permission set. To add a new Active Directory group, click Add, then browse to the group and click OK.

5 Select the Server name, then click Save to open the Permission Set page.

6 Click Edit next to Drive Encryption under the new permission set to open the Edit Permission Set page.

7 Select the required permission settings, then click Save.

You can assign this permission set to a new or existing McAfee ePO user by selecting Menu | User Management | Users.

How disabling/deleting a user in Active Directory affects the Drive Encryption user

Every user account has an objectGUID in LDAP. If a user account is deleted from LDAP and another is created with the same user name, this new user account is a different entity. This is because the new user has a different objectGUID.

How to delete a user in LDAP
You must first delete the user in LDAP, then run the LdapSync: Sync across users from LDAP task and send an Agent wake-up call. The user disappears from DE Users list after the LdapSync: Sync across users from LDAP task is complete.

The McAfee ePO Server Settings option If user is disabled in LDAP server within Configuration | Server Settings | Drive Encryption | General | Edit can be configured to disable, delete, or ignore the user if the user has been disabled in the LDAP Server. The default setting is Disable.
What if a user is disabled from LDAP?

If a user account is initialized on the client system and is later disabled from LDAP, it is automatically disabled or deleted from the client or ignored when the next LdapSync: Sync across users from LDAP task runs. To authenticate through the client PBA with a disabled or deleted LDAP user name, you should set the policy to ignore or again enable this user in the LDAP, then initialize the same user name on the client with the default password.

This does not remove the user from the DE Users list in ePolicy Orchestrator, however, it removes the users from the client system based on the option set in the Server Settings.

Is it possible to just disable the Drive Encryption user when removed from LDAP?

It is not possible to disable a Drive Encryption user when it has been removed from LDAP. The deleted user is removed from the DE Users list in LDAP during the next LdapSync: Sync across users from LDAP task.

What if the Drive Encryption user assignment is deleted/removed?

If the Drive Encryption user assignment is deleted from a system, the user might still be assigned back to the client system if the Add local domain users option is enabled in the Product Settings Policy. For this to work, the user must have logged on to Windows at least once and the domain to which client system is connected should have been registered in ePolicy Orchestrator. You can also manually add users using the Menu | Data Protection | Encryption users | Add Users option in ePolicy Orchestrator.
Managing client computers

System management helps administrators import system information from the Active Directory server into McAfee ePO. This is useful in the process of installing Drive Encryption and assigning the users to the systems.

Contents
- Add a system to an existing system group
- Move systems between groups
- Select the disks for encryption
- Enable or disable automatic booting
- Enable or disable temporary automatic booting
- Set the priority of encryption providers
- Maintain a list of incompatible products
- Enable accessibility (USB audio devices) in the Pre-Boot environment
- Allow user to reset self-recovery answers
- Manage the default and customized themes
- Assign a customized theme to a system
- Manage simple words
- Drive Encryption system recovery
- Managing servers and client systems — general recommendations
- Configure role-based access control for managing Drive Encryption

Add a system to an existing system group

Use McAfee ePO to import systems from your Network Neighborhood to groups for working with Drive Encryption. You can also import a network domain or Active Directory container.

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

1 Click Menu | Systems | System Tree, then click Actions | New Systems.
2 Select the required option under How to add systems.
3 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.
4 If you select Push agents and add systems to the current group, you can enable automatic System Tree sorting. Do this to apply the sorting criteria to these systems. Select the following options:
### 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.

Even if you have a well organized System Tree that mirrors your network hierarchy, and uses automated tasks and tools for synchronization, you can manually move systems between groups. For example, you can move systems from the Lost&Found group.

You can also drag-and-drop systems from the Systems table to any group in the System Tree.

**Task**

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

1. Click Menu | Systems | System Tree | Systems, then browse and select the systems.
2. Click Actions | Directory Management | Move Systems to open the Select New Group page.
3. Select whether to enable or disable or maintain the System Tree sorting on the selected systems when they are moved.
4. Select the group where you want to place the systems, then click OK.

### Select the disks for encryption

To encrypt the target disk on your client system, you need to select the required encryption type and set the encryption priority from the Product Setting policy available with the Drive Encryption product.

**Before you begin**

You must have administrator rights to perform this task.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Systems | System Tree, then select a group from the System Tree.

2. Select a system, then click Actions | Agent | Modify Policies on a Single System. The Policy Assignment page for that system appears.

3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system’s assigned policy.

4. Select the Product Settings policy category, then click Edit Assignments to open the Product Settings page.

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

6. Select the policy from the Assigned policy drop-down list, then click Edit Policy to open the Policy Settings page.
   From this location, you can edit the selected policy or create a new policy.

7. On the Encryption tab, select the disks to be encrypted. For the Self-Encrypting (Opal) drives, select PC Opal with All disks or Boot only.
   The Encryption type options such as None, All disks except boot disk, and Selected partitions are not applicable to Self-Encrypting (Opal) drives.
   
   ![info] To initiate the encryption on the client, the user must select any one of the options other than None. The default option, None, does not initiate the encryption.

8. On the Policy Settings page, click Save, then click Save on the Product Settings page.

9. Send an agent wake-up call.

---

**Enable or disable automatic booting**

The Drive Encryption Pre-Boot logon environment allows you to select a logon method and to require authentication credentials such as user name and password.

If the user provides the correct authentication details, the Drive Encryption boot code starts the crypt driver in memory and boots the original operating system of the protected system.

Enabling automatic booting removes the Pre-Boot Authentication from the client system.

![info] If you enable this option without requiring the use of TPM, Drive Encryption doesn’t protect the data on the drive when it is not in use, because unauthorized users can boot the system.

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

1. Click Menu | Systems | System Tree, then select a group from the System Tree.

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

3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system’s assigned policy.

4. Select the Product Settings policy category, then click Edit Assignments to open the Product Settings page.
5 If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherit from**.

6 From the **Assigned Policy** drop-down list, select the policy, then click **Edit Policy** to open the **Policy Settings** page.

   From this page, you can edit the selected policy, or create a new policy.

7 From the **Log On** tab, select **Enable automatic booting** under the Drive Encryption pane to enable the Pre-Boot environment.

   A security warning *This will remove the pre-boot authentication. Are you sure?* appears.

8 Click **Yes** to enable the automatic booting.

9 Set the expiration date and time for the automatic booting, if required.

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

11 Send an agent wake-up call.

---

**Enable or disable temporary automatic booting**

Drive Encryption allows you to turn on the Pre-Boot authentication screen with a client-side utility. This feature eliminates the need to modify the policy in McAfee ePO, and fully automates patching and other client management scenarios.

**Task**

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

1 In the Drive Encryption Admin Tools directory, extract **EEAdminTools.zip**, and locate the **EpeTemporaryAutoboot.exe** file. Distribute this file to your client systems.

2 Log on to McAfee ePO and navigate to **Menu | Policy | Policy Catalog**, select **Drive Encryption 7.2** from the **Product** drop-down menu, then select **Product Settings** from the **Category** drop-down list.

3 Click the policy that you want to change.

4 On the **Log on** tab, select **Allow temporary automatic booting**.

   *If this option is not selected, you can’t use EpeTemporaryAutoboot.exe on the client system.*

5 Send an agent wake-up call, so that the client systems receive this new policy. You can now use this feature on the client systems.

6 Write a script or use a client management application to run **EpeTemporaryAutoboot.exe**.

   There are four basic options available that must be run with administrator privileges on the client system.

   - Temporarily reboot for X number of reboots. **Example syntax:** `EpeTemporaryAutoboot.exe --number-of-reboots 3`.
   - Temporarily reboot for X number of minutes. **Example syntax:** `EpeTemporaryAutoboot.exe --timeout-in-minutes 15`.
   - To clear the temporary autoboot. **Example syntax:** `EpeTemporaryAutoboot.exe --clear`.
   - For help. **Example syntax:** `EpeTemporaryAutoboot.exe --help`. 
Set the priority of encryption providers

The priority of the encryption providers (PC software and Opal) can be set using the Drive Encryption Product Setting policy.

**Before you begin**
You must have administrator rights to perform this task.

You can set the encryption priority by moving the encryption provider rows up and down, as appropriate. The encryption priority determines the encryption technology applied.

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

1. Click Menu | Systems | System Tree, then select a group from the System Tree.
2. Select a system, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page for that system appears.
3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system's assigned policy.
4. Select the Product Settings policy category, then click Edit Assignments to open the Product Settings page.
5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6. From the Assigned Policy drop-down list, select the policy, then click Edit Policy to open the Policy Settings page.
   From this page, you can edit the selected policy, or create a new policy.
7. On the Encryption tab, set the Encryption Provider priority by moving the encryption provider rows up and down, as appropriate. The encryption priority determines the order of encryption on the client systems.
   By default, software encryption is used on both Opal and non-Opal systems in this version of Drive Encryption. To ensure that Opal technology is the preferred software encryption option, we recommend that you always set Opal as the default encryption provider by moving it to the top of the list on the Encryption Providers page. This makes sure that Opal management is used on Opal drives; non-Opal drives default to software encryption.
8. Click Save in the Policy Settings page, then click Save in the Product Settings page.
9. Send an agent wake-up call.

Maintain a list of incompatible products

Using McAfee ePO, you can create and import a rule with a set of product names that are marked as incompatible with Drive Encryption.

**Before you begin**
You must have administrator rights to perform this task.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Click Menu | Configuration | Server Settings.

2. Click Drive Encryption in the Setting Categories pane, then Manage incompatible products. The Drive Encryption incompatible products page lists the products that are not compatible with Drive Encryption.

3. To import an incompatible product definition, click Actions | Import incompatible product rule.

4. Browse and select the .xml file that defines the rule to detect the incompatible products, then click OK. The products are added to the incompatible product list.

Enable accessibility (USB audio devices) in the Pre-Boot environment

The USB audio functionality enables visually challenged users to listen to a voice (spoken words) as guidance when the user moves the focus from one field to the next using mouse or keyboard in the Pre-Boot environment.

Before you begin
- Make sure that the DEAdmin extension is installed on the McAfee ePO server.
- Make sure that the Enable Accessibility option is enabled under Log On | Drive Encryption.

Accessibility allows any external USB audio device to be used and to play back pre-recorded audio files. These vocal prompts can indicate which control or option has the focus (that is, Username, Password, OK) and specific error conditions.

This functionality provides the audio guidance in the English language only.

When you install or update the product, the vocal prompts are installed on the client system only. Only when the policy setting is enabled, the audio files are transferred to the PBFS. This saves space in the PBFS system, which does not need this functionality.

508 compliance audio is not available under UEFI due to the lack of audio drivers in the UEFI environment.

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

1. Click Menu | Systems | System TreeMenu | Systems | System Tree, then select a group from the System Tree.

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

3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system’s assigned policy.

4. Select the Product Settings policy category, then click Edit Assignments to open the Product Settings page.

5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6. From the **Assigned Policy** drop-down list, select the policy, then click **Edit Policy** to open the **Policy Settings** page. From this page, you can edit the selected policy, or create a new policy.

7. On the **Boot Options** tab, select **Always enable pre-boot USB support** to enable USB on the client system. Make sure that you also enable the **Enable Accessibility** option under **Log On | Drive Encryption**.

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

9. Send an agent wake-up call.

When the user tries to authenticate on the client system after enforcing this policy, the user can listen to the audio guidance in the Pre-Boot environment.

---

**Allow user to reset self-recovery answers**

The client user's self-recovery details can be reset using the **Allow users to re-enroll self-recovery information at PBA** option available with the Product Settings policy.

**Before you begin**

Make sure that the **Enable Self-recovery** option is enabled under **User Based Policy | Self-recovery**.

**Task**

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

1. Click **Menu | Systems | System Tree**, then select a group under **System Tree**.

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

3. From the **Product** drop-down list, select **Drive Encryption 7.2**. The policy **Categories** under Drive Encryption appears with the system's assigned policy.

4. Select the **Product Settings** policy category, then click **Edit Assignments** to open the **Product Settings** page.

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

6. From the **Assigned Policy** drop-down list, select the policy, then click **Edit Policy** to open the **Policy Settings** page. From this page, you can edit the selected policy, or create a new policy.

7. On the **Recovery** tab, select **Allow users to re-enroll self-recovery information at PBA** to enable the option.

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

9. Send an agent wake-up call.

When this policy is saved and enforced to the client system, the Pre-Boot Authentication (Username) screen includes the **Reset Self Recovery** option. The user selects this option and is prompted for a password, and then the self-recovery enrollment. The user should then enroll the self-recovery details with new self-recovery answers.

**i** Only initialized users can reset their self-recovery details.
Manage the default and customized themes

The default theme is downloaded to the client system when the DEAgent and Drive Encryption software package deployment task is sent to the client computers. You can add and manage a theme to be used as a background in the Pre-Boot Authentication page.

Before you begin
You must have administrator rights to perform this task.

The Drive Encryption Themes package is added automatically to the Master Repository after installing the EEAadmin.zip extension in McAfee ePO.

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

1. Click Menu | Configuration | Server Settings.
2. On the Setting Categories pane, click Drive Encryption, then click Manage Themes to open the Drive Encryption Theme page.
3. Click Actions | Add.
4. Type a theme name in the Name field, then select Create a new theme based on an existing theme option.
5. Select a theme from the Based on drop-down list.
6. Browse to the Background Image, then click OK. This creates the new theme package in the C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\EETHEME\DAT\0000 folder.
   You can also browse and install a theme package using the Select Theme package to install option.
7. Download the custom themes on the client using one of these methods:
   - Update Now option under Menu | Systems | System Tree | Actions | Agent in ePolicy Orchestrator
   - Product Update task
   - Update Security from the client
   All themes have a unique ID. When you run the update task, the theme IDs are verified against the existing theme IDs on the client, then the new theme is downloaded to the client if it has changed.

   The downloaded theme packages are stored in this folder on the client:
   C:\Program files\McAfee\Endpoint Encryption Agent\Repository\Themes
8. Change the theme in the Product Setting Policy, then send an agent wake-up call to apply the customized theme.

Assign a customized theme to a system

You can customize an existing theme and assign it to a client system and the customized theme can be used as a background in the Pre-Boot Authentication page.

Before you begin
You must have administrator rights to perform this task.
To create a custom theme, you need to make sure the following:

- The image must have the dimensions 1024x768
- Required file format is .PNG
- The .PNG file size limit that can be uploaded is 2.5 MB

**Task**

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

1. Click **Menu | Systems | System Tree**, then select the group from the **System Tree**.
2. Select a **System**, then click **Actions | Agent | Modify Policies on a Single System** to open the **Policy Assignment** page.
3. From the **Product** drop-down list, select **Drive Encryption 7.2**. The policy categories under **Drive Encryption** display the system's assigned policy.
4. Select the **Product Settings** policy category, then click **Edit Assignments** to open the **Product Settings** page.
5. If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherit from**.
6. From the **Assigned Policy** drop-down list, select the policy, then click **Edit Policy** to open the **Policy Settings** page.

   From this page, you can edit the selected policy, or create a new policy.
7. On the **Theme** tab, select the customized theme from the **Select theme** drop-down list.
8. Click **Save** on the **Policy Settings** page, then click **Save** on the **Product Settings** page.
9. Send an agent wake-up call.

---

**Manage simple words**

Use McAfee ePO to add and manage simple words that can’t be used as passwords. The Drive Encryption simple words are added to the **Master Repository** when you select **Regenerate Missing Simple Word package** in Manage Simple Words that is available after the EEAdmin.zip extension is installed on McAfee ePO.

**Before you begin**

You must have administrator rights to perform this task.

**Task**

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

1. Click **Menu | Configuration | Server Settings**.
2. Click **Drive Encryption** in the **Setting Categories** pane, then click **Manage simple words**.
3. Click **Group Actions | Add group**.
4. Type the name of the group, then click **OK** to create the simple word group.
5. Click **Actions | Add**, then type the simple words that can't be used as passwords.
6 Click Group Actions | Regenerate missing simple word package, then click Yes when prompted for confirmation. This creates the simple words package (.xml file) for the simple words group in the C:\Program Files\McAfee\ePolicyOrchestrator\DB\Software\Current\EESWORD\DAT\0000 folder.

7 Download the simple word package on the client using one of these methods:
   - Update Now option under Menu | Systems | System Tree | Actions | Agent in McAfee ePO
   - Product Update task
   - Update Security from the client

   All simple word packages (.xml file) have a unique ID. When you run the update task, the package IDs are verified against the existing package IDs on the client, then the new package file is downloaded to the client if it has changed.

The downloaded simple word packages are stored in these folders on the client system:
   - DE: Windows — C:\Program files\McAfee\Drive Encryption Agent\Repository\SimpleWords

8 Enable the No simple words option under User Based policies | Password Content Rules, select the required word group from the drop-down list, then send an agent wake-up call to apply the policy to the client.

### Drive Encryption system recovery

The purpose of encrypting the client’s data is to control access to the data by controlling access to the encryption keys. It is important that keys are not accessible to users.

The key that encrypts the hard disk sectors needs to be protected. These keys are referred to as Machine Keys. Each system has its own unique Machine Key. The Machine Key is stored in the McAfee ePO database to be used for client recovery, when required. There are four different system recovery options available in Drive Encryption that can be reached through: Menu | Systems | System Tree | System | Actions | Drive Encryption.

| Table 7-1 Drive Encryption system recovery |
| Option | Definition |
| Decrypt offline recovery file | The encrypted machine key is stored in a recovery information file (xml) on the client system. To enable the recovery procedures on the client systems, the user can use McAfee ePO to decrypt the offline recovery file that is retrieved from the client system. |
| Destroy all recovery information | When you want to secure-erase the drives in your Drive Encryption installed system, remove all users from the system (including those inherited from parent branches in the System Tree). This makes the disks inaccessible through normal authentication as there are no longer any users assigned to the system. You need to then destroy the recovery information for the system using the option Menu | Systems | System Tree | Systems | Actions | Drive Encryption | Destroy All Recovery Information in the McAfee ePO console. This means that the system can never be recovered. |
| Key Re-use | This option is used to activate the system with the existing key present in the McAfee ePO server. This option is highly useful when a boot disk gets corrupted and the user cannot access the system. Other disks on the system can be recovered by activating it with the same key from McAfee ePO. |
Table 7-1  Drive Encryption system recovery (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Export recovery information | This option is used to export the recovery information file (.xml) for the desired client system from McAfee ePO. Every client system that is encrypted using Drive Encryption has a recovery information file in McAfee ePO. Any user trying to enable the recovery procedures on the client systems should get the file from the McAfee ePO administrator for Drive Encryption. For more information, see the DETech User Guide.  
  
  The recovery information file has a general format of client system name.xml.

| Export recovery information based on Disk Keycheck | This option is used to export the recovery information file (.xml) for a disk of a client system from McAfee ePO. Every disk of a client system has a disk keycheck value. For instance, if a client system has a disk called 'Disk1', you can recover that client system (when on unrecoverable state) using the keycheck value of 'Disk1'. However, if a new disk 'Disk2' is installed and activated in that same client system, you must use the keycheck value of 'Disk2' and the keycheck value of 'Disk1' loses priority.  
  
  To perform this task, you need to access the client system using DETech and obtain the disk keycheck value using the Disk Information option from the DETech user interface.  
  
  • In McAfee ePO, click Actions | Drive Encryption | Export recovery information based on Disk Keycheck and enter the obtained disk keycheck value in the Key Check field.  
  
  • The recovery information file (.xml) appears, export it to the inserted removable media.  
  
  • Use this file to authenticate to the client system using DETech. For more information, see DETech User Guide. |

What happens to the Machine Key when you delete a Drive Encryption active system from McAfee ePO?

The Machine Key remains in the McAfee ePO database; however, the key association with the client system is lost when the client system is deleted. When the client system reports back to McAfee ePO during the next ASCI, it appears as a new node. A new node does not have any users assigned to the client system. The administrator must assign users to allow logon, assign administrative users to the McAfee ePO branch where the systems are added (by default. Lost&Found), or enable the Add local domain user option in the Product Setting Policy. The administrator must also configure the required policies in McAfee ePO.

After adding the users and configuring the policies, the next agent-to-server communication makes sure that:

• The Machine Key is re-associated with the client system and the recovery key is available.
  
  When the associated Machine Key is not present with the new node, McAfee ePO sends a Machine Key request. If the user is logged on to the client system, an agent-server communication between the client and the McAfee ePO server makes sure that the Machine Key is updated in McAfee ePO and the users are updated on the client. After that, the Machine Key becomes available and admin recovery and policy enforcement work.

• The users are assigned to the client system and can log on to the client system.

You cannot log on to the client system before a proper agent-server communication occurs. In this situation, use the DETech tool to obtain the Key Check value from the client and obtain the recovery key for this machine from the McAfee ePO console to perform an Emergency Boot.
Managing servers and client systems — general recommendations

Client deployment in batches for a considerable number of systems is a good practice in itself. Keep these recommendations in mind when managing servers and client systems:

• Do not try to create the Drive Encryption deployment task at the root level of your System Tree and activate it. It is a good practice to deploy Drive Encryption to the systems at the sub-level branches.

• Do not deploy Drive Encryption to the server systems, especially the server hosting your McAfee ePO server.

• Secure your McAfee ePO server and database system in the most secured location and keep it accessible for authorized personnel only.

Configure role-based access control for managing Drive Encryption

ePolicy Orchestrator administrator rights management determines what administrators can do while managing the Drive Encryption software.

The administrator can set up Drive Encryption-specific permission sets for different users in ePolicy Orchestrator. The permission sets can be created for a variety of roles including but not restricted to Executive Reviewer, Global Reviewer, Group Admin, and Group Reviewer. The Drive Encryption extension enables ePolicy Orchestrator administrators to control Drive Encryption Systems that are managed through ePolicy Orchestrator.

The McAfee ePO administrator for Drive Encryption can:

• Manage Drive Encryption users, policies and server settings

• Run queries to view the encryption status of the client systems

• View client system audits

• View McAfee user audits

• Manage Drive Encryption providers

Administrative roles can be configured and implemented using the User Management | Permission Sets option in ePolicy Orchestrator. It is possible to configure a number of admin roles using this option. For example, you can create admin roles such as:

• Drive Encryption Administrator: User accounts in this level have full control of Drive Encryption, but cannot manage any other software in ePolicy Orchestrator.

• Drive Encryption Helpdesk: User accounts in this level can do Drive Encryption password resets only.

• Drive Encryption Engineer: User accounts in this level can do password resets as well as export recovery files to be used with DETech tool.

• Drive Encryption Auditor: User accounts in this level can view Drive Encryption reports only.

For more information on configuring roles, see the documentation for the relevant version of ePolicy Orchestrator.
Before you begin:

- Make sure that your LDAP server is configured and registered in ePolicy Orchestrator.
- Make sure that you schedule and run the LdapSync: Sync across users from LDAP task.
- Make sure that you enable the Active Directory User Login option in ePolicy Orchestrator. To enable, navigate through Menu | Configuration | Server Settings | Active Directory User Login | Edit, then enable Allow Active Directory users to login if they have at least one permission set option.

You can create different permission roles and assign them with different Drive Encryption Permission Sets to different users.

To verify the configured permission sets, log off from ePolicy Orchestrator, then log on with a user account that belongs to any one of the new roles.

*i* Use the correct format of the user name when logging on to ePolicy Orchestrator.
Managing client computers
Configure role-based access control for managing Drive Encryption
McAfee Drive Encryption out-of-band management

Out-of-band management allows the administrator to connect to a computer’s management controller when the computer is turned off, in sleep or hibernate mode, or unresponsive through the operating system.

Intel® Active Management Technology (Intel® AMT) is a hardware-based technology for remotely managing and securing Intel® AMT systems using out-of-band communication. Part of the Intel® Management Engine, which is built into systems with Intel® vPro technology, Intel® AMT allows network administrators to maintain, manage, and protect the Intel® AMT client systems through hardware-assisted security and manageability capabilities.

The DEDeep extension, available with Drive Encryption and the McAfee ePO Deep Command product, uses Intel® AMT to allow out-of-band encryption management of Intel® AMT systems, locked at the Drive Encryption Pre-Boot screen.

Contents

- The DEDeep extension
- Enable the out-of-band feature
- Configure the out-of-band remediation functionality
- Configure the out-of-band unlock PBA feature
- Configure the out-of-band management feature
- Checklist for using Intel® AMT and Drive Encryption

The DEDeep extension

The Intel® AMT out-of-band feature provides system actions that include Out Of Band - Remediation, Out Of Band - Unlock PBA, and Out Of Band - User Management.

For more information, see Configure the Out Of Band - Remediation feature, Configure the Out Of Band - Unlock PBA feature, and Configure the Out Of Band - User Management feature, respectively.

These actions are available on the McAfee ePO Deep Command console only after installing the DEDeep extension.

You must install the McAfee ePO Deep Command product extensions before installing the DEDeep extension.

For more information about requirements for configuring your Intel® AMT systems, see the McAfee ePO Deep Command Product Guide.
Enable the out-of-band feature

Using McAfee ePO, you can enable the Drive Encryption out-of-band management features through policies, then perform actions on Intel® AMT provisioned client systems. To enable the configured out-of-band settings, you must enable the Product Settings Policy Out-of-Band | Enable at PBA.

Before you begin
- You must have administrator rights to perform this task.
- Make sure that your client system meets the requirements for Intel® AMT out-of-band management. For more information about Intel® AMT configurations and settings, see the McAfee ePO Deep Command Product Guide.

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

1. Log on to the McAfee ePO server as a user with valid Drive Encryption permissions.
2. Click Menu | Systems | System Tree.
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 Drive Encryption 7.2. The policy categories under Drive Encryption display the system’s assigned policy.
5. Click Edit Assignment corresponding to the Product Settings Policy to open the Drive Encryption 7.2 : Product Settings page.
6. If the policy is inherited, in the Inherit from field, select the Break inheritance and assign the policy and settings below option.
7. From the Assigned policy drop-down list, select the Product Settings Policy, then click Edit Policy to open the Policy Settings page.
   From this location, you can edit the selected policy or create a new policy.
8. Click the Out-of-Band tab, then select Enable at PBA.
9. Click Save in the Policy Settings page, then click Save in the Drive Encryption 7.2 : Product Settings page.
10. Send an agent wake-up call.
    The Drive Encryption out-of-band functionality is enabled successfully.

Configure the out-of-band remediation functionality

Using McAfee ePO, you can select a managed system and perform an emergency restart or restore the MBR (assuming that the managed system is connected to a network) by remotely forcing a reboot of the system from a specialist disk image.

Before you begin
- You must have administrator rights to perform this task.
- Make sure that your client system meets the requirements for Intel® AMT out-of-band management. For more information about Intel® AMT configurations and settings, see the McAfee ePO Deep Command Product Guide.
Even though DEDeep is able to determine which specialist disk image to use for each task based on the type of system, you can also manually select a disk image using the McAfee ePO console.

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

1. Log on to the McAfee ePO server as a user with valid Drive Encryption permissions being assigned.
2. Click Menu | Systems | System Tree.
3. Select a system, then click Actions | Drive Encryption | Out Of Band - Remediation to open the Out Of Band - Remediation page.
4. Select one of these options:
   - **Emergency Boot** — Select this option to perform an Emergency Boot on the client system. The Automatic option automatically deploys the correct type of image to the system, however, you can select MBR recovery image or MBR OPAL recovery image from the Disk image to use drop-down list, if you are aware of your system's hardware.
   - **Restore Drive Encryption MBR** — Select this option to restore the MBR on the client system. The Automatic option automatically deploys the correct type of image to the system, however, you can select MBR recovery image from the Disk image to use drop-down list, if you are aware of your system's hardware.

   These options are not supported for UEFI systems.
5. Click OK.

---

**Configure the out-of-band unlock PBA feature**
You can remotely unlock the PBA of Intel® AMT configured/provisioned client systems, so that they can automatically boot and bypass PBA. This feature enables patching processes or security update deployment in your organization on unattended encrypted machines.

**Before you begin**
- You must have administrator rights to perform this task.
- Make sure that your client system meets the requirements for Intel® AMT out-of-band management. For more information about Intel® AMT configurations and settings, see the McAfee ePO Deep Command Product Guide.

This is a secure unlock that requires an automated authentication through the server, in contrast to the insecure autoboot feature, which doesn't require authentication.

There are different ways of performing this action:
- Unlock a system or group temporarily for a specific number of times (reboots).
- Unlock a system or group temporarily for a specific time period.
- Unlock a system or group permanently with a schedule during specific hours during the week.
- Unlock a system or group permanently.
Each type of unlock can be configured in two ways:

- Enterprise network only (Client Initiated Local Access (CILA) only) — Automated authentication through PBA occurs only if the system is located inside the trusted enterprise network.
- Any network — Automated authentication through PBA occurs if the system is located inside or outside the trusted enterprise network.

**Task**

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

1. Log on to the ePolicy Orchestrator server as a user with valid Drive Encryption permissions.
2. Click Menu | Systems | System Tree.
3. Select a system, then click Actions | Drive Encryption | Out Of Band - Unlock PBA to open the Drive Encryption: Out Of Band - Unlock PBA page.
4. Select Client Initiated Local Access (CILA) only to restrict unlocks within the enterprise network.

**Enabling the Disable listening for CILA/CIRA messages on Agent Handlers (This will prevent CILA/CIRA and DE Unlock from working) option (under Menu | Configuration | Server Settings | Edit Intel® AMT Credentials of the McAfee ePO Deep Command product) prevents the CILA/CIRA and Drive Encryption unlock features from working.**

The next time a user restarts that client system, PBA appears but it is bypassed automatically after a period of time.

5. In the Bypass pre-boot authentication field, select one of these options:

   - **Number of times** — Type a preferred number from 1 to 32 to pass through PBA that many times without requiring to authenticate manually.
   - **From - Until** — Specify the required date and time within which PBA will be remotely unlocked.
     
     The default time standard on the McAfee ePO server is UTC.
   - **Schedule** — Specify the day and time for a week within which PBA will be remotely unlocked. The unlock indicator signifies that unlocking of PBA is allowed and the lock indicator signifies that unlocking of PBA is prevented in that time period.
   - **Permanently** — To remotely unlock the PBA of the client system each time the system is booted.

The next time a user restarts that client system, PBA appears but it is bypassed automatically after a period of time. The PBA page lists the machine name and ID. The user can give exact system details to the Helpdesk, making it easy for the administrator to identify the system that requires the out-of-band action.

6. Click Save.

To enforce the configured out-of-band unlock PBA settings, you must enable the Product Settings policy Out-of-Band | Enable at PBA.
Configure the out-of-band management feature

Using McAfee ePO, you can remotely reset the password of a user of an encrypted system while it is in the Pre-Boot environment. The user can then log on through Pre-Boot using their new password, and is forced to change the password immediately.

Before you begin

- You must have administrator rights to perform this task.
- Make sure that your client system meets the requirements for Intel® AMT out-of-band management. For more information about Intel® AMT configurations and settings, see the McAfee ePO Deep Command Product Guide.

Task

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

1. Log on to the McAfee ePO server as a user with valid Drive Encryption permissions.
2. Click Menu | Systems | System Tree.
3. Select the required system, then click Actions | Drive Encryption | Out Of Band - User Management to open the OOB User Management page.
   The Select action pane appears with the Reset user's password token option selected.
4. Click Next to open the Select user pane.
   The Select user page lists only the users with password token data. You can select only one user at a time.
5. Select the required user, then click Next.
   You can select only one user at a time.
6. In the Configure pane, type a temporary password in the Password and Confirm fields.
   If a user performs an OOB password reset, the administrator provides a temporary password, which the users might have to type in PBA. If the policy requires that the default password be used, the user must type the new temporary password before entering a new password. If no default password is required, the user doesn't have to type the temporary password, and instead types the new password immediately.
7. Click Save.
   The next time a user restarts that client system, after entering the temporary password, the user is forced to set a new password and perform the user enrollment.

In Queries & Reports | Shared Groups | Drive Encryption OOB | DE : OOB Action Queue | Run, an action appears in the Action queue for the action selected. If the action is Transient, the Action queue disappears from the DE : OOB action Queue page after the action is performed. If the action is Permanent, the action does not disappear. Moreover, once the password is reset, the user hears a beep confirming the password change.
Checklist for using Intel® AMT and Drive Encryption

The Intel® AMT out-of-band feature within Drive Encryption 7.2.0 provides system actions that include Out Of Band - Remediation, Out Of Band - Unlock PBA, and Out Of Band - User Management.

For more information about these actions, see the Configure the Out Of Band - Remediation feature, Configure the Out Of Band - Unlock PBA feature, and Configure the Out Of Band - User Management feature sections in the Drive Encryption 7.2.0 Product Guide. These actions are available on the McAfee ePO console only after installing the EEDeep extension.

You must install the ePO Deep Command product extensions before installing the EEDeep extension.

For more information about requirements for configuring your Intel® AMT systems, see the ePO Deep Command Product Guide.

Preparation for using Intel® AMT with Drive Encryption

• Make sure that the client system has been provisioned for Intel® AMT.

• The ePO Deep Command software has been installed and its policies have been configured correctly.

• Make sure that CILA/CIRA policies have been applied and CILA/CIRA has not been disabled at ePO Deep Command Server Settings.

• Make sure that the client system is managed by McAfee ePO and the Intel® AMT policy has been successfully deployed.
  • Check the AMTService.log file to verify that the Intel® AMT policy is enforced correctly.
  • At this point, you should be able to power the system on into BIOS to verify this.

• Make sure that you have installed the DEAdmin, Drive Encryption, and EEDeep extensions.

• Make sure that you have configured the DE Product Settings policy for out-of-band features and sent to the client system.

• Deploy the Drive Encryption Agent and Drive Encryption packages to the client system.

• Activate Drive Encryption and restart client system.

Best practices and recommendations for using Intel® AMT and Drive Encryption

• Enable CIRA only when it is necessary for the security requirements of your organization.

• Limit the usage of EEDeep unlock feature during wake-and-patch cycles to the smallest time/number of reboots.

• While performing any out-of-band action, do not power off or disconnect the client system from network until the system successfully boots into Windows.

• Out-of-band: remediation — Always allow Automatic disk image to be used when possible.

• Out-of-band: user management — Even though password policy is not enforced on the temporary password, make sure to follow the enterprise password policy for setting the temporary password.

Time-based out-of-band actions, such as unlock on schedule, are based on the clock on the server. They are not based on the local time of the client system even if it is on another time zone.
Configuring and managing tokens and readers

McAfee Drive Encryption supports different logon tokens, for example, Passwords, Stored Value SmartCards, PKI SmartCards, CAC SmartCards, and Biometric tokens. This section describes how to configure the Drive Encryption software to support these SmartCards.

Contents

- Modify the token type associated with a system or group
- Using a Stored Value token in Drive Encryption
- Using a PKI token in Drive Encryption
- Using a Self-Initializing token in Drive Encryption
- Setup scenarios for the Read Username from Smartcard feature
- Using a Biometric token in Drive Encryption

Modify the token type associated with a system or group

You can create a new user-based policy with a required token type and deploy it to the required system or a system group. You can also edit and deploy an existing policy.

Before you begin

Make sure that:
- The user is already created in Active Directory.
- Drive Encryption is installed on at least the minimum supported McAfee ePO version.
- The server task DE LDAP Server User/Group Synchronization is scheduled and runs normally between McAfee ePO and Microsoft Active Directory.

Task

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

1. Click Menu | Systems | System Tree, then select a group from the System Tree pane.
2. Select a System, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page.
3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system's assigned policy.
4. Select the User Based Policy category, then click Edit Assignments to open the User Based Policies page.
5. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.
6 From the **Assigned Policy** drop-down list, select the policy, then click **Edit Policy** to open the **Policy Settings** page.
   From this page, you can edit the selected policy, or create a new policy.

7 From the **Token type** drop-down list on the **Authentication** tab, select the required token type.

   For SmartCards that conform to the PKI, PIV, or CAC standards, Drive Encryption uses the information present in a public certificate store of a PKI smartcard to look up users and encrypt their unique Drive Encryption key with the public key available in their certificate. This certificate must be configured while selecting the PKI SmartCard token.

8 Click **Save** in the **Policy Settings** page, then click **Save** in the **User Based Policies** settings page.

9 Send an agent wake-up call.

---

### Using a Stored Value token in Drive Encryption

A Stored Value token supported in Drive Encryption stores some token data on the token itself. You must initialize these tokens with Drive Encryption before you can use them for authentication. The token needs to contain the necessary token data to allow successful authentication of the user.

The Stored Value token is initialized the first time the user logs on to the Pre-Boot environment or the Windows authentication page. Drive Encryption, primarily the Pre-Boot environment, is responsible for initializing the token. The initialization process does not require access to the Active Directory.

### Associate a Stored Value token with a system or group

You can add a user or group to a system and associate a Stored Value token with that user or group. This task explains how to use a Stored Value token with a single user.

**Before you begin**

You must have administrator rights to perform this task.

**Task**

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

1 Create or edit a user-based policy with the Stored Value token type and deploy it to the required system or group. See **Modify the token type associated with a system or group**.

2 In the **Policy Settings** page, in the **Authentication** tab, from the **Token type** drop-down list, select the required token type, then click **Save**.

3 Click **Save** in the **Policy Settings** page, then click **Save** in the User Based Policies settings page.

4 Send an agent wake-up call.
Using Single-Sign-On (SSO)
If you selected SSO to be enforced in your policy, on the initial boot, Drive Encryption captures the SSO credentials when the user logs on to Windows. On subsequent boots, the user only has to authenticate in Pre-Boot because SSO credentials are now captured.

Using a PKI token in Drive Encryption
A PKI token is a smartcard supported in Drive Encryption that finds the necessary certificate information for the user in a PKI store (such as Active Directory) and used to initialize the Drive Encryption token data. You must initialize these tokens before they can be used to authenticate a user.

The McAfee ePO extensions initializes the token using the relevant certificate information present in Active Directory. This information is obtained through the Lightweight Directory Access Protocol (LDAP) synchronization task that is created when Drive Encryption is first installed on McAfee ePO, and before users are assigned to systems.

The token data for the user is contained in the PBFS on the client. It can be successfully unlocked when the user presents the appropriate smartcard, which matches the certificate information found in Active Directory, and the correct PIN.

Associate a PKI token with a system or group
You can add a user or group to a system and associate a PKI token with that user or group. This section explains how to use a PKI token with a single user.

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

1 Create or edit a user-based policy with the PKI token type and deploy it to the required system or group. See Modify the token type associated with a system or group.

2 From the Token type drop-down list on the Policy Settings page, select the required token type, then click Save.

3 Click Save in the Policy Settings page, then click Save in the User Based Policies settings page.

4 Send an agent wake-up call.

Using a Self-Initializing token in Drive Encryption
A Self-Initializing token is a form of PKI token, but rather than referencing certificate information and pre-initializing the token data in McAfee ePO, the client sees the card and performs the necessary initialization steps. Only the client performs the initialization of the token data. One of the assumptions for using a Self-Initializing token is that the necessary certificate information cannot be referenced in Active Directory or any other supported Directory Service.

The token is initialized the first time the card is presented to Drive Encryption, which happens in the Pre-Boot environment.
**Associate a Self-Initializing token with a system or group**

You can add a user or group to a system and associate a Self-Initializing token with that user or group. This section explains how to use a Self-Initializing token with a single user.

**Task**

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

1. Create or edit a user-based policy with the Self-Initializing token type and deploy it to the required system or group. See Modify the token type associated with a system or group.

2. On the **Policy Settings** page, from the **Token type** drop-down list on the **Authentication** tab, select the required token type, then click **Save**.

3. Click **Save** in the **Policy Settings** page, then click **Save** in the User Based Policies settings page.

4. Send an agent wake-up call.

**Using Single-Sign-On (SSO)**

If you selected SSO to be enforced in your policy, on the initial boot, Drive Encryption captures the SSO credentials when the user logs on to Windows. On subsequent boots, the user only has to authenticate in Pre-Boot because SSO credentials are now captured.

---

**Setup scenarios for the Read Username from Smartcard feature**

You can set up your environment using the new Drive Encryption feature Read Username from Smartcard.

**Before you begin**

- Make sure that you have enabled the Read Username from Smartcard option under Product Settings | My Default | Log On.
- Make sure you have scheduled and run the DE LDAP Sync.

These scenario examples are provided to help you with the installation:

- Set up using the **Subject** field.
- Set up using the **Subject Alternative Name - Other Name** field.

**Finding the Read Username from Smartcard feature in McAfee ePO**

The Read Username from Smartcard feature is configured on the **Log On** tab of Product Settings page.

**Finding the LDAP Sync Task User Name attribute field in McAfee ePO**

The LDAP Sync Task User Name attribute is configured on the Server Task Builder page. Click **Menu** | Automation | **Server Tasks**, select the server task name you created for your LDAP Sync Task, then click **Actions** | **Edit** to edit the task properties.
Setting up your environment using the Subject field

This example shows setting up your environment using the Subject field.

• The user has a token that supports the Read Username from Smartcard feature.

• The user wants to log on as User1, which is the Drive Encryption user name.

• The user name that the user wants to log on as (User1) resides in the Subject field on the certificate (for example: CN=User1,DC=DomainComponent,DC=com).

• Therefore, under McAfee ePO Logon Product Settings, the user should select Subject as the certificate field that contains the user name.

• Because the user wants to match the whole certificate field, deselect Match certificate username field up to the @ sign.

• The user should check their DE LDAP Sync Task User Name attribute field in McAfee ePO. In this situation, distinguishedname is the correct field to use because it contains the exact same information as the cert field Subject, so a valid comparison can be made.

• Finally, the user should run their DE LDAP Sync Task, and synch their product policy on the system where they want to use the Read Username from Smartcard feature.

Setting up your environment using the Subject Alternative Name - Other Name field

This example shows setting up your environment using the Subject Alternative Name - Other Name field.

• The user has a token that supports the Read Username from Smartcard feature.

• The user wants to log on as User2, which is the Drive Encryption user name.

• The user wants to poll the Subject Alternative Name - Other Name field on the certificate. The user name that the user wants to log on as (User2) resides in the Subject Alternative Name - Other Name field on the certificate (for example, Other Name: Principal Name=User2@domain.com).

• Under McAfee ePO Logon Product Settings, the user should select Subject Alternative Name - Other Name as the certificate field that contains the user name.

• Because the user wants to match only the user name from the certificate field, and not the whole certificate field, select Match certificate username field up to @ sign.

• The user should check their EE LDAP Sync Task User Name attribute field in McAfee ePO. In this situation, the default samaccountname is the correct field to use because this contains the Drive Encryption user name User2, which the user normally logs on with, and this field can be found on the certificate field Subject Alternative Name - Other Name.

• Finally, the user should run their DE LDAP Sync Task, and synchronize their product policy on the system they wish to use the Poll Card feature on.
Using a Biometric token in Drive Encryption

A Biometric token allows fingerprints to authenticate to Drive Encryption instead of using passwords. Currently, Drive Encryption 7.2 supports two Biometric fingerprint readers in specific laptop models. These Biometric readers are manufactured by UPEK and Validity. For more information about supported laptops, see the Drive Encryption 7.2 supported readers KnowledgeBase article.

Biometric tokens are supported in single user mode only (that is, the user has to register on each system where they want to use fingerprints). The fingerprint template is not distributed across multiple systems.

Use a UPEK Biometric token in Drive Encryption

To use the UPEK Biometric token, you need to first enable it in McAfee ePO by creating a user-based policy and synchronizing it with the client systems.

In the client system, you need to install the Protector Suite 2011 software and configure it accordingly to use your fingerprints to authenticate to Drive Encryption.

Enable the UPEK Biometric token in McAfee ePO

You need to first enable the UPEK Biometric token by creating a user-based policy in McAfee ePO, then synchronize it with the client systems.

Before you begin

You must have administrator rights to perform this task.

If you are modifying an active password for a user (where the user has already logged on and changed the default password), when you set the token type to **UPEK Fingerprint Reader**, the password for logging on to Drive Encryption is reset to the system default value. The default password is "12345" unless it has been modified.

Task

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

1. Perform the steps in *Modify the token type associated with a system or group* to create or edit a user-based policy with the Biometric token type, and deploy it to the required system or group.

2. On the Policy Settings page, from the Token type drop-down list on the Authentication tab, select **Upek Fingerprint Reader**, then click Save.

3. Click Save in the Policy Settings page, then click Save in the User-Based Policies settings page.

4. Send an agent wake-up call.

Set up the client system and enroll your fingerprints

You must set up your client system by first installing the Protector Suite 2011 software, then enrolling your fingerprints to authenticate to Drive Encryption without using passwords.

The Protector Suite 2011 software is available from its respective vendor and/or its respective vendor's download page. Currently, only Protector Suite (common) is supported.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Run the Protector Suite 2011 setup on the client system.
2 In the Protector Suite 2011 Setup wizard, select the default settings.
3 When prompted, click Yes to restart your system.
   After you authenticate to Drive Encryption (through password) and Windows, click the Protector Suite 2011 icon in the system tray.
4 In the End User Agreement screen, click Accept.
5 In the Enrollment Mode Selection screen, verify that you selected the Enrollment to the biometric device option, then click Apply.
6 Close Protector Suite and restart your system.
7 When the Drive Encryption logon screen appears, type the user name assigned to the UPEK token type, then click Next.
8 Enter the default password 12345, then click Logon. After Windows restarts, the Fingerprint Reader Registration window appears.
9 Click Register to open the User Fingerprint Enrollment page, deselect Run interactive tutorial, then click Next.
10 For each finger you want to enroll:
   a Click Skip Tutorial to open the Enrollment screen.
   b Select a square object that corresponds to the finger that you want to enroll, then click Next.
   c Scan your finger to register your fingerprint, making sure to wait until the progress bar reaches 100%.
11 When prompted to enable power-on fingerprint security, click No, then click OK.
   The Enrollment screen for the user's fingers appears.
     After a few moments (10-15 seconds), a pop-up saying "You've successfully enrolled" appears.
12 Click Next to open the Finish screen, then click Finish.
You can now use fingerprints to authenticate to Drive Encryption instead of passwords.

Use a Validity Biometric token in Drive Encryption
To use the Validity Biometric token, you must first enable it in McAfee ePO by creating a user-based policy and synchronizing it with the client systems.

Before you begin
Perform the steps in Enable the UPEK Biometric token in McAfee ePO
You can use the Protector Suite 2011 software to customize the default settings. If you delete all the users' fingerprints from the reader using the Protector Suite 2011 software, all authentication data is lost and you can't log on at PBA.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the client system's PBA by entering the system's default password, then log on to Windows to open the Fingerprint Reader Registration.

2. Click Register to open the User Fingerprint Enrollment page.

3. Select the button for the required finger.

4. Scan your finger to register your fingerprint, making sure to wait until the progress bar reaches 100%.

5. When the Congratulations, your fingerprints have been registered with Drive Encryption message appears, click OK.

You can now use fingerprints to authenticate to Drive Encryption instead of passwords.
Managing Drive Encryption reports

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

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 a dashboard monitor.

Contents

- Queries as dashboard monitors
- Create Drive Encryption custom queries
- View the standard Drive Encryption reports
- Drive Encryption client events
- Create the Drive Encryption dashboard
- View the Drive Encryption dashboard
- Report the encrypted and decrypted systems

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

Drive Encryption 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 these 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 webpage.
- PDF — Print the results.
Create Drive Encryption custom queries

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

Before you begin
You must have administrator rights to perform this task.

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

1. Click Menu | Reporting | Queries & Reports, then click Actions | New to open the Query Builder wizard.

2. On the Result Type page, select Drive Encryption, then select Result Type for the query, then click Next to open the Chart page.
   This choice determines the options available on subsequent pages of the wizard.

3. Select the type of chart or table to display the primary results of the query, then click Next to open the Columns page.
   If you select Boolean Pie Chart, you must configure the criteria to include in the query.

4. Select the columns to be included in the query, then click Next to open the Filter page.
   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.

5. Select 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 does not 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.

6. In the Save Query page, type a name for the query, add any notes, and select one of these options:
   • New Group — Type the new group name and select either:
     • Private group (My Groups)
     • Public group (Shared Groups)
   • Existing Group — Select the group from the list of Shared Groups.

7. Click Save.

View the standard Drive Encryption reports

You can run and view the standard Drive Encryption reports from the Queries page.

Before you begin
You must have administrator rights to perform this task.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1  Click Menu | Reporting | Queries & Reports.

2  In the Groups pane, select Drive Encryption from the Shared Groups drop-down list to open the Standard DE query list.


<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE: Activation Report</td>
<td>Displays the list of systems that have failed activation and allows you to identify the reason for failure for each system.</td>
</tr>
<tr>
<td>DE: Disk Status</td>
<td>Displays the status of the disk.</td>
</tr>
<tr>
<td></td>
<td>If a disk has a volume that is not assigned, then the disk status in queries would be displayed as partially encrypted, despite all assigned volumes being shown as encrypted.</td>
</tr>
<tr>
<td>DE: Disk Status (Rollup)</td>
<td>Displays the DE: Disk Status compiled from various McAfee ePO servers.</td>
</tr>
<tr>
<td></td>
<td>Drive Encryption 7.2 supports both Full and Incremental rollup reports. For details, see the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>DE: Encryption Provider</td>
<td>Displays which encryption provider is active on each system.</td>
</tr>
<tr>
<td>DE: Installed version</td>
<td>Displays the version of the Drive Encryption installed in systems.</td>
</tr>
<tr>
<td>DE: Installed Version (Rollup)</td>
<td>Displays the DE: Installed version details compiled from various McAfee ePO servers.</td>
</tr>
<tr>
<td></td>
<td>Drive Encryption 7.2 supports both Full and Incremental rollup reports. For details, see the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>DE: Migration log (Windows only)</td>
<td>Displays the log details and the results of the v5.x.x user import.</td>
</tr>
<tr>
<td>DE: Migration Lookup (Windows only)</td>
<td>Displays the details about the assignments of the user group, machines, and users.</td>
</tr>
<tr>
<td>DE: Product Client Events</td>
<td>Displays Drive Encryption client events.</td>
</tr>
<tr>
<td>DE: Systems With Uninitialized Users</td>
<td>Displays the list of active systems containing uninitialized users that are potentially insecure.</td>
</tr>
</tbody>
</table>
### Query Definition

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DE: Users</strong></td>
<td>Lists all Drive Encryption users. From here, the user can use these options to manage the users in the selected system:</td>
</tr>
<tr>
<td></td>
<td>• Clear SSO details — Clears the SSO details of the selected user (only for Windows).</td>
</tr>
<tr>
<td></td>
<td>• Configure UBP enforcement — Allows a user to use a non-default User Based Policy.</td>
</tr>
<tr>
<td></td>
<td>• Force user to change password — Prompts the user to change the password in the Drive Encryption authentication.</td>
</tr>
<tr>
<td></td>
<td>• Reset Token — Resets the token associated with the selected user.</td>
</tr>
<tr>
<td></td>
<td>• Reset self-recovery — The client user's self-recovery details is reset, then the user has to enroll the self-recovery details with new self-recovery answers.</td>
</tr>
<tr>
<td></td>
<td>• User Information — Maintains the user information with a list of questions and answers.</td>
</tr>
<tr>
<td><strong>DE: V5 Audit</strong></td>
<td>Displays the imported audit logs from v5.x.x.</td>
</tr>
<tr>
<td>(Windows only)</td>
<td>If you had only selected the audit option during the export process, the audit log is not displayed.</td>
</tr>
<tr>
<td><strong>DE: Volume Status</strong></td>
<td>Displays the encryption status of the disk volumes. For self-encrypted (Opal) drives, the DE: Volume Status appears blank without any details because it does not allow volume level encryption.</td>
</tr>
<tr>
<td><strong>DE: Volume Status</strong></td>
<td>Displays the DE: Volume Status compiled from various ePolicy Orchestrators.</td>
</tr>
<tr>
<td>(Rollup)</td>
<td>Drive Encryption 7.2 supports both Full and Incremental rollup reports. For more information, see the product documentation for your version of McAfee ePO.</td>
</tr>
</tbody>
</table>

3. Select a query from the Queries list.

4. Click Actions | Run to display the query results.

5. Drill down into the report and take actions on items as necessary. Available actions depend on the permissions of the user.

   The user can edit the query and view the query details.

6. Click Close when finished.

### Drive Encryption client events

While implementing and enforcing the Drive Encryption policies that control how sensitive data is encrypted, the administrators can monitor real-time client events and generate reports using the **DE: Product client events** query.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event</th>
<th>Event description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30000</td>
<td>Logon Event</td>
<td>This event is reported in McAfee ePO whenever a Pre-Boot happens.</td>
</tr>
<tr>
<td>30001</td>
<td>Password Changed Event</td>
<td>This event is reported in McAfee ePO whenever the user changes the Drive Encryption password.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Event</td>
<td>Event description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>30002</td>
<td>Password Invalidated Event</td>
<td>This event is reported in McAfee ePO whenever the Drive Encryption password is invalidated after a fixed number of unsuccessful login attempts.</td>
</tr>
<tr>
<td>30003</td>
<td>Token Initialization Event</td>
<td>This event is reported in McAfee ePO when the user changes the default password during the first pre-boot logon.</td>
</tr>
<tr>
<td>30004</td>
<td>System Boot Event</td>
<td>This event is reported in McAfee ePO whenever the system restarts after making Drive Encryption active.</td>
</tr>
<tr>
<td>30005</td>
<td>Administrator Recovery Event</td>
<td>This event is reported in McAfee ePO for every successful Administrator Recovery.</td>
</tr>
<tr>
<td>30006</td>
<td>Self-recovery Event</td>
<td>This event is reported in McAfee ePO for every successful Self-recovery.</td>
</tr>
<tr>
<td>30007</td>
<td>Self-recovery Invalidated Event</td>
<td>This event is reported in McAfee ePO whenever the Self-recovery is invalidated after a fixed number of unsuccessful login attempts.</td>
</tr>
<tr>
<td>30008</td>
<td>Crypt Start Event</td>
<td>This event is reported in McAfee ePO when the encryption starts on the client system.</td>
</tr>
<tr>
<td>30009</td>
<td>Crypt Paused Event</td>
<td>This event is reported in McAfee ePO when the encryption pauses on the client system.</td>
</tr>
<tr>
<td>30010</td>
<td>Crypt Complete Event</td>
<td>This event is reported in McAfee ePO when the encryption finishes on the client system.</td>
</tr>
<tr>
<td>30011</td>
<td>Crypt Volume Start Event</td>
<td>This event is reported in McAfee ePO when the specified volume encryption/decryption starts.</td>
</tr>
<tr>
<td>30012</td>
<td>Crypt Volume Complete Event</td>
<td>This event is reported in McAfee ePO when the specified volume encryption/decryption is completed.</td>
</tr>
<tr>
<td>30013</td>
<td>Policy Change Start Event</td>
<td>This event is reported in McAfee ePO when a policy change is initiated.</td>
</tr>
<tr>
<td>30014</td>
<td>Policy Change Complete Event</td>
<td>This event is reported in McAfee ePO when the policy change is completed.</td>
</tr>
<tr>
<td>30015</td>
<td>Activation Start Event</td>
<td>This event is reported in McAfee ePO when the Drive Encryption activation starts on the client system.</td>
</tr>
<tr>
<td>30016</td>
<td>Activation Complete Event</td>
<td>This event is reported in McAfee ePO when the Drive Encryption activation is completed on the client system.</td>
</tr>
<tr>
<td>30017</td>
<td>General Exception Event</td>
<td>This event is reported in McAfee ePO whenever an exception occurs on the client system.</td>
</tr>
<tr>
<td>30018</td>
<td>Emergency Recovery Start</td>
<td>This event is reported in McAfee ePO whenever the Emergency Recovery is initiated.</td>
</tr>
<tr>
<td>30019</td>
<td>Emergency Recovery Complete</td>
<td>This event is reported in McAfee ePO whenever the Emergency Recovery is completed.</td>
</tr>
<tr>
<td>30020</td>
<td>Upgrade Start</td>
<td>This event is reported in McAfee ePO whenever the Upgrade process is initiated.</td>
</tr>
<tr>
<td>30021</td>
<td>Upgrade Complete</td>
<td>This event is reported in McAfee ePO whenever the Upgrade process is complete.</td>
</tr>
<tr>
<td>30022</td>
<td>User Update Error</td>
<td>This event is reported in McAfee ePO whenever a user update error occurs.</td>
</tr>
<tr>
<td>30026</td>
<td>Encryption Key Not Available</td>
<td>This event is reported in McAfee ePO whenever the encryption key is not available.</td>
</tr>
<tr>
<td>30031</td>
<td>Automatic Booting Activated</td>
<td>This event is reported in McAfee ePO when the automatic booting is activated.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Event Description</td>
<td>Event Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>30032</td>
<td>System Automatically Booted</td>
<td>This event is reported in McAfee ePO when the system is booted automatically.</td>
</tr>
<tr>
<td>30033</td>
<td>Automatic Booting Deactivated</td>
<td>This event is reported in McAfee ePO when the automatic booting is deactivated.</td>
</tr>
<tr>
<td>30034</td>
<td>User Expired</td>
<td>This event is reported in McAfee ePO when the user account is expired.</td>
</tr>
<tr>
<td>30035</td>
<td>Provider Not Installed</td>
<td>This event is reported in McAfee ePO when the encryption provider is not installed.</td>
</tr>
<tr>
<td>30036</td>
<td>Drive Encryption - Activation Failure: Boot Disk Not Supported</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the boot disk is unsupported.</td>
</tr>
<tr>
<td>30037</td>
<td>Drive Encryption - Activation Failure: Unsupported Algorithm</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the algorithm is unsupported.</td>
</tr>
<tr>
<td>30038</td>
<td>Drive Encryption - Activation Failure: Boot Disk is not GPT</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the boot disk is not GPT.</td>
</tr>
<tr>
<td>30039</td>
<td>Drive Encryption Activation Failure: Can't Find ESP Partition</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the ESP partition is not found.</td>
</tr>
<tr>
<td>30040</td>
<td>Drive Encryption - Activation Failure: Mounting ESP Failed</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the mounting of the ESP partition fails.</td>
</tr>
<tr>
<td>30041</td>
<td>Drive Encryption - Activation Failure: Failed to Shrink OS Partition</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the shrinking of the OS partition fails.</td>
</tr>
<tr>
<td>30042</td>
<td>Drive Encryption - Activation Failure: Failed to create EPE partition on boot disk</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the creation of an EPE partition on boot disk fails.</td>
</tr>
<tr>
<td>30043</td>
<td>Drive Encryption - Activation Failure: Could not find Boot Disk</td>
<td>This event is reported in McAfee ePO when the activation of Drive Encryption fails because the boot disk is not found.</td>
</tr>
<tr>
<td>30044</td>
<td>Recovered From Audit Log Corruption</td>
<td>This event is reported in McAfee ePO when the audit log corruption is recovered.</td>
</tr>
<tr>
<td>30045</td>
<td>Activation Failure</td>
<td>This event is reported in McAfee ePO when the Drive Encryption activation fails.</td>
</tr>
<tr>
<td>30046</td>
<td>Deactivation Event</td>
<td>This event is reported in McAfee ePO when the event is deactivated.</td>
</tr>
<tr>
<td>30047</td>
<td>Drive Encryption - TPM Not Working</td>
<td>This event is reported in McAfee ePO when TPM is not working.</td>
</tr>
<tr>
<td>30050</td>
<td>Drive Encryption - Out of band : Unlock PBA</td>
<td>This event is reported in McAfee ePO when the Out Of Band - Unlock PBA feature is enabled.</td>
</tr>
<tr>
<td>30051</td>
<td>Drive Encryption - Out of band : Reset User Password</td>
<td>This event is reported in McAfee ePO when the Out Of Band - Reset User Password feature is enabled.</td>
</tr>
<tr>
<td>30060</td>
<td>Pre-Boot Smart Check : System has started to deactivate after failing tests</td>
<td>This event is reported in McAfee ePO when Pre-Boot Smart Check starts to deactivate the machine after failing its tests.</td>
</tr>
<tr>
<td>30061</td>
<td>Pre-Boot Smart Check : System has completed deactivating after failing tests</td>
<td>This event is reported in McAfee ePO when Pre-Boot Smart Check completes deactivation after failing its tests.</td>
</tr>
</tbody>
</table>
### Event ID | Event | Event description
--- | --- | ---
30070 | Automatic Booting Deactivated - Exceeded maximum failed logon(s) | This event is reported in McAfee ePO when automatic booting is deactivated if the maximum number of Windows logons that are allowed is exceeded.
30080 | Drive Encryption - McAfee Endpoint Assistant User Recovery | This event is reported in McAfee ePO when the system was recovered using the McAfee Endpoint Assistant application.
30081 | Drive Encryption - McAfee Endpoint Assistant Registration | This event is reported in McAfee ePO when a user registered the smartphone or tablet with the system using the McAfee Endpoint Assistant application.
2411 | Deployment Successful | This event is reported in McAfee ePO for every successful deployment of Drive Encryption.
2412 | Deployment Failure | This event is reported in McAfee ePO for every deployment failure of Drive Encryption.

### Create the Drive Encryption 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 default McAfee ePO dashboards.

**Before you begin**
You must have administrator rights to perform this task.

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

1. Click Menu | Reporting | Dashboards, then click Options | Manage Dashboards.
2. Click New Dashboard, then enter a new name.
3. For each monitor, click New Monitor, select the monitor from the shared groups Drive Encryption to display in the dashboard, then click OK.
4. Click Save.

You can make this dashboard public by editing the dashboard and selecting PUBLIC.

All new dashboards are saved to the private My Dashboards category.

### View the Drive Encryption dashboard
You can select and configure monitors that provide current data about your data protection status and other environments and make them part of your active set of dashboards.

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

1. Click Menu | Reporting | Dashboards, then select a private dashboard.
2. Open the Drive Encryption queries to view the selected dashboard.
Report the encrypted and decrypted systems

The disk and volume status reflects the encryption and decryption status of the managed client system, for example, **Encrypted** or **Decrypted**.

**Task**

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

1. Click **Menu | Reporting | Queries & Reports** to open the Query page.
2. In the **Groups** pane, click **Shared Groups | Drive Encryption**.

   Edit the **DE: Disk Status** and **DE: Volume Status** queries to display the system details in table format. This gives you a simplified view of the system and the encryption status. Make sure to include the **State (Disk)** and **State (Volume)** columns in the table.

3. Click **Run** in the **DE: Disk Status** and **DE: Volume Status** from the Queries list.

The **DE: Disk Status** and **DE: Volume Status** pages appear accordingly with the list of client systems and their details configured in the query. The **State (Disk)** and **State (Volume)** columns indicate the system's status as **Encrypted** or **Decrypted**.
11 Recovering users and systems

Resetting a remote user's password or replacing the user's lost logon token requires a challenge and response procedure.

Contents

- Enable or disable the self-recovery functionality
- Perform self-recovery on the client computer
- Enable or disable the administrator recovery functionality
- Perform administrator recovery on the client system
- Generate the response code for the administrator recovery
- Smartphone recovery
- Perform system recovery using the Data Protection Self Service Portal

Enable or disable the self-recovery functionality

The Self-recovery option allows the user to reset a forgotten password by answering a set of security questions. A list of security questions is set by the administrator using McAfee ePO. If the answers from the user match what has been stored with their self-recovery information, they can proceed through the recovery process.

A list of security questions is set by the administrator using McAfee ePO. If the answers from the user match what is stored with their self-recovery information, they can proceed through the recovery process.

Use McAfee ePO to enable or disable the self-recovery functionality in the client computer.

Task

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

1. Click Menu | Systems | System Tree, then select a group from the System Tree.

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

3. From the Product drop-down list, select Drive Encryption 7.2. The policy categories under Drive Encryption display the system's assigned policy.

4. Locate a User Based Policies policy category, then click Edit Assignments to open the User Based Policies page.

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

6. Select a policy from the Assigned policy drop-down list, then click Edit Policy to open the Policy Settings page.

   From this page, you can edit the selected policy, or create a new policy.
7 On the **Self-recovery** tab, enable or disable the self-recovery functionality for the specified user or user group.

8 Select **Invalidate self-recovery after no. of attempts** and type the number of attempts.

   The self-recovery token is invalidated if the user types invalid answers for more than the number of attempts specified in the policy.

9 Type the number of **Questions to be answered** to perform the self-recovery. The client user is prompted with these questions when trying to recover the user account at the client system.

10 Type the number of **Logons before forcing user to set answers** to determine how many times a user can log on without setting their self-recovery questions and answers.

11 Click + to create a new question, then select the question **Language** and type the **Min answer length** for the answer to this question.

   Answers to these questions are typed by the user on the client system during the recovery process. The user is prompted for recovery enrollment during every logon. The user can cancel the enrollment until the user exceeds the specified number of logon attempts. After exceeding the defined number of logon attempts, the **Cancel** button is disabled and the user is forced to enroll for self-recovery.

12 Click **Save**.

13 Send an agent wake-up call.

### Perform self-recovery on the client computer

Use this option to recover the user on the client computer, if the user’s password or the logon token has been lost.

**Before you begin**

Make sure that you have successfully enrolled for self-recovery on the client system. This task should be performed by the client user on the client computer.

**Task**

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

1 Click **Options | Recovery**.

2 Select **Self-recovery** for the recovery type.

3 Enter the user name, then click **OK**. The **Recovery** dialog box lists the questions that the user answered while enrolling for the self-recovery.

4 Enter the answers for the prompted questions, then click **Finish** to open the **Change Password** dialog box.

5 Enter and confirm the new password, then click **OK**.
Enable or disable the administrator recovery functionality

The client system prompts for authentication on the pre-boot logon page to access the system. When a user forgets the password, is disabled in the Active Directory, or loses the token, the user can't log on to the system.

Resetting the user's password, unlocking the disabled user, replacing a lost logon token, and performing machine recovery require a challenge and response procedure. The users must start their system and click Recovery on the Drive Encryption pre-boot logon page. This option needs to be enabled on the McAfee ePO server before performing this task on the client systems.

Use McAfee ePO to enable or disable the administrator (system and user) recovery functionality on the client computer.

**Task**

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

1. Click **Menu | Systems | System Tree**, then select a group from the **System Tree**.
2. Select a system, then click **Actions | Agent | Modify Policies on a Single System** to open the Policy Assignment page for that system.
3. From the **Product** drop-down list, select **Drive Encryption 7.2**. The policy categories under **Drive Encryption** display the system's assigned policy.
4. Select the **Product Settings** policy category, then click **Edit Assignments** to open the **Product Settings** page.
5. If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherit from**.
6. From the **Assigned policy** drop-down list, select a product setting policy, then click **Edit Policy** to open the **Policy Product Settings** page.

   From this page, you can edit the selected policy, or create a new policy.
7. On the **Recovery** tab, enable or disable the system recovery functionality.
8. From the **Key size** drop-down list, select the required recovery key size, then enter the message to appear on the recovery page.
9. Click **Save** on the **Product Settings** page.
10. Send an agent wake-up call.

Perform administrator recovery on the client system

If the user's password or the logon token has been lost, perform this task on the client computer to recover the user or the system.

![Warning](image)

Make sure that the client user performs this task on the client system.

**Task**

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

1. Restart the client system.
2. Click **Options | Recovery**.
3. Select the **Administrator / Smartphone Recovery** for the recovery type, then click **OK** to open the **Recovery** dialog box with the challenge code.
4 Read the **Challenge Code** and get the **Response Code** from the administrator who manages McAfee ePO.

It is the administrator's responsibility to authenticate that the client user's identify.

5 Enter the response code in the Line field, then click Enter.

Each line of the code is checked when it is entered.

6 Click Finish.

The generated response code depends on the recovery key size set in the policy and the selected recovery type, that is, machine recovery or user recovery.

---

**Generate the response code for the administrator recovery**

The administrator types the challenge code, which is provided by the user, on the McAfee ePO console and generates the response code required for the administrator (system and user) recovery.

**Before you begin**

Make sure that McAfee ePO administrator performs this task in McAfee ePO.

**Task**

1 Click **Menu** | **Data Protection** | **Encryption Recovery**. The Drive Encryption **Recovery** wizard displays the **Challenge Code** field.

2 Ask the client user to read the **Challenge Code** and get the **Response Code** from the administrator who manages McAfee ePO.

It is the administrator's responsibility to authenticate that the client user's identify.

3 Type the **Challenge Code**, then click **Next** to open the **Recovery Type** page.

4 Select the required recovery type from the **Recovery Type** list, then click **Next** to open the **Response Code** page with the response codes.

The generated response code depends on the recovery key size set in the policy and the selected recovery type, system recovery or user recovery.

5 Read out the response code to the user.

---

**Smartphone recovery**

When a Drive Encryption user forgets the PBA password or loses the logon token, the user must perform the smartphone recovery on the client system to reset the password or replace the logon token.

To perform the smartphone recovery, the user must first download and install the McAfee Endpoint Assistant application onto the smartphone or tablet. The user can download the McAfee Endpoint Assistant free application from Google Play for Android supported smartphones or Apple Appstore for iOS supported smartphones.

McAfee recommends the Drive Encryption users to perform smartphone recovery over administrator recovery and self recovery for a quicker and better experience.
Enable or disable the smartphone recovery functionality

You must enable the smartphone recovery functionality in McAfee ePO if a user forgets the PBA password and requires to reset it.

The client system prompts for authentication on the pre-boot logon page to access the system. When a user forgets the password, is disabled in the Active Directory, or loses the token, the user can't log on to the system.

Resetting the user's password, unlocking the disabled user, replacing a lost logon token, and performing system recovery require a challenge and response procedure. The users must start their system and click Recovery on the Drive Encryption pre-boot logon page. This option needs to be enabled on the McAfee ePO server before performing this task on the client systems.

Use McAfee ePO to enable or disable the administrator (system and user) recovery functionality on the client computer.

**Task**

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

1. Click **Menu | Systems | System Tree**, then select a group from the **System Tree**.

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

3. From the **Product** drop-down list, select **Drive Encryption 7.2**. The policy categories under Drive Encryption display the system's assigned policy.

4. Select the **Product Settings** policy category, then click **Edit Assignments** to open the **Product Settings** page.

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

6. From the **Assigned policy** drop-down list, select a product setting policy, then click **Edit Policy** to open the **Product Settings** page.

   From this page, you can edit the selected policy, or create a new policy.

7. On the **Companion Devices** tab, enable or disable the **Enable Companion Device Support** option to perform system recovery through smartphone.

8. Click **Save**.

9. Select the **User Based Policies** policy category, then click **Edit Assignments** to open the **User Based Policies** page.

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

11. From the **Assigned policy** drop-down list, select a user based policy, then click **Edit Policy** to open the **User Based Policies** page.

   From this page, you can edit the selected policy, or create a new policy.

12. On the **Companion Devices** tab, enable or disable the **Recovery** option to perform system recovery through smartphone.

13. Select the required **Password Definition** option to create a password according to the option selected. If the user has once set a higher password definition to the system, the user cannot change the password to a lower password definition (that is less secure) even if that policy is set in McAfee ePO.
14. Click Save on the User Based Policies page.

15. Send an agent wake-up call.

**Perform smartphone recovery on the client system**

To perform smartphone recovery on the client system, the user must first register the client system with the smartphone or tablet, and then perform the recovery process on the client system.

**Smartphone registration**

**Task**

1. During Pre-Boot Authentication (PBA), in the User Selection screen, select the Register Smartphone option. The Smartphone Registration page may also appear automatically the first time a user logs on to a system, or the first time that the user logs on after the policy was enabled in McAfee ePO (policy option to support smartphone recovery has been set for the user in McAfee ePO).

2. Enter your credentials and authenticate.

   When the password is accepted, the QR Code Recovery Registration window is shown on PBA.

3. Open the Endpoint Assistant application on your smartphone or tablet and click Scan to scan the image that appears on the QR Code Recovery Registration dialog box.

   After the image is scanned properly, you will receive a successful notification on your smartphone or tablet specifying that you have registered the system with your smartphone or tablet.

4. On the QR Code Recovery Registration window, click Finish to proceed to Windows.

   The first time a user logs on to initialize or the first time the policy option to support smartphone recovery is switched on, the system displays the registration screen automatically. However, if the user clicks Finish, the screen does not appear again. If the user clicks Skip, it appears again at the next logon attempt.

**Recovery process**

**Task**

1. Click Options | Recovery.

2. Select the Administrator / Smartphone Recovery recovery type, then click OK to open the Recovery dialog box that appears with the challenge code.

3. On your smartphone or tablet, select Tap to Scan to scan the image that appears on the Recovery dialog box.

   Once the image is scanned properly, you will receive the response code on your smartphone or tablet.

4. Click Next.

5. Enter the Response Code in the Line field, then click Enter.

   Each line of the code is checked when it is entered.

6. Click Finish.

   You can also manage your keys by selecting the Manage option on your smartphone or tablet.
Perform system recovery using the Data Protection Self Service Portal

This section describes the installation, configuration, and operation of the Data Protection Self Service Portal (DPSSP), which can be used with DE to allow users to obtain the recovery key or response code for a Drive Encryption system.

Important: Privacy Notice

DPSSP collects users' login names, system names, IP addresses, and audit data. Access to this information is available in DPSSP reports within McAfee ePO. Ensure that access to these reports is authorized and appropriately managed.

The administrator must first install the dpssp.zip extension in McAfee ePO, and make the required DPSSP server settings. An authorized client user can open the DPSSP portal on a system to obtain a response code for Drive Encryption upon entering the corresponding challenge code for the system to be recovered.

The full DPSSP URL is 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 default port number used in the DPSSP URL is 8443. To review an issue where using Port 8444 causes a problem with the website's security certificate when accessing DPSSP, see KB86781.

Configure DPSSP server settings on McAfee ePO

The administrator must configure DPSSP server settings within McAfee ePO to allow a user to obtain the recovery key or response code 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 Drive Encryption. We recommend that you create a specific McAfee ePO user for DPSSP recoveries, and limit the permission set privileges to Drive Encryption recovery only.

6 Next to Authentication, select the Active Directory sever that the users need to authenticate to.

Make sure to note that the administrator has selected the registered AD in McAfee ePO.

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

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

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.

Next to **Session**, type the numeric value in minutes to log off the user’s session after the specified number of minutes.

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 ![Help](#) 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 ![Help](#) or ![Help](#).

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

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

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

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

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 Drive Encryption, 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.

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 for the DPSSP provided by your administrator or Help Desk, which will be of the general form, https://<ePO_IP_address>:<Port_Number>/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 recovery key ID for the Drive Encryption system to be recovered, then click Get key.

4 Obtain the Recovery code that will be displayed to recover the Drive Encryption system.

Make sure to note that you must be listed as a user against the client system you are trying to recover.

If the entered 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.

Important: Privacy and DPSSP reports

Ensure that access to these reports is authorized and appropriately managed. DPSSP reports within McAfee ePO contain users' login names, system names, IP addresses, and audit data.
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.
Additional information

This additional information includes guidelines for installing and using Drive Encryption in FIPS mode. It also includes guidelines for implementing Drive Encryption in its Common Criteria mode of operation.

Contents

- FIPS 140-2 certification
- Common Criteria EAL2+ mode operation

FIPS 140-2 certification

The 140 series of Federal Information Processing Standards (FIPS) is a set of U.S. government computer security standards that specify requirements for cryptography modules. McAfee Core Cryptographic Module (MCCM) is undergoing certification for FIPS 140-2 and these cryptographic modules are included in Drive Encryption.

The Drive Encryption Admin and Drive Encryption PC (installed on McAfee ePO) consume the certified cryptography provided by McAfee ePO running in FIPS mode, and thus do not need to be certified independently.

The current status of this certification is available on the National Institute of Standards and Technology (NIST) website.

Contents

- Prerequisites to use Drive Encryption in FIPS mode
- Installing or upgrading the Drive Encryption client packages in FIPS mode
- Impact of FIPS mode
- Uninstalling the Drive Encryption client packages in FIPS mode

Prerequisites to use Drive Encryption in FIPS mode

For Drive Encryption 7.2 to be in compliance with FIPS 140-2, the software must meet these conditions.

- The Drive Encryption client package must be installed on the client in FIPS mode.
- Depending on compliance requirements mandated by your auditor (with particular regard to key generation), you might also need to install McAfee ePO in FIPS mode. For more information, refer to the Knowledge Base article KB83483.
If you don't install both McAfee ePO and Drive Encryption in FIPS mode, the configuration does not operate in a FIPS-certified manner.

Drive Encryption must be operating in FIPS mode at the time of activation of a client to ensure that keys are generated in a FIPS-approved manner. Upgrading an active Drive Encryption client to a FIPS mode version of Drive Encryption 7.2 does not imply that the client is now running with FIPS quality keys. A Drive Encryption active client should be decrypted, deactivated, and then reactivated using a FIPS mode client installation in order to be FIPS-compliant.

### Installing or upgrading the Drive Encryption client packages in FIPS mode

For the Drive Encryption client to operate in FIPS mode, install the Drive Encryption client package in FIPS mode before activating Drive Encryption on the client.

This is to make sure that encryption keys are generated in a FIPS-certified manner during the activation process.

If Drive Encryption is already installed on systems without enabling the FIPS mode, perform these tasks to make it operate in the FIPS mode.

1. Decrypt the client systems.
2. Deactivate Drive Encryption on the client systems.
3. Remove the Drive Encryption product from the client systems.
4. Reinstall Drive Encryption in the FIPS mode.

### Deploying Drive Encryption through a McAfee ePO deployment task

When installing or upgrading Drive Encryption client packages in FIPS mode using a McAfee ePO deployment task, make sure to add the keyword `FIPS` on the command line of the Drive Encryption deployment task in McAfee ePO.

### Deploying Drive Encryption through a third-party deployment software

When installing or upgrading Drive Encryption client packages in FIPS mode using third-party deployment software, make sure to add the parameter `FIPS_MODE=1` when you install the Drive Encryption client package, as in the following command:

- 32-bit system — `msiexec.exe/q/i MfeEEPc32.msi FIPS_MODE=1`
- 64-bit system — `msiexec.exe/q/i MfeEEPc64.msi FIPS_MODE=1`

### Impact of FIPS mode

In FIPS mode, certain self-tests are performed in Windows and pre-boot environments. These self-tests might impact the performance of the pre-boot.

If self-tests of FIPS fail, the failed components of the system stop completely, in one of these ways.

- If the Windows Drive Encryption FIPS component fails self-test, the system doesn't activate or enforce policies.
- If the Windows Drive Encryption driver fails self-test, the driver performs a bug-check (BSOD).
- If the Pre-Boot Drive Encryption FIPS component fails self-test, pre-boot stops functioning.
Move your mouse in Pre-Boot

Additionally, FIPS 140-2 defines minimum requirements for entropy during key generation. This might lead to key generation errors in pre-boot where insufficient entropy (randomness) is available at the point of key generation. To avoid this, you can supply entropy (randomness) into pre-boot by moving the mouse randomly before you perform the action that produced the error.

Uninstalling the Drive Encryption client packages in FIPS mode

The removal of Drive Encryption client packages in FIPS mode doesn't vary from the normal removal of the Drive Encryption client.

For details about uninstalling the Drive Encryption client, see Uninstalling the Drive Encryption client.

Common Criteria EAL2+ mode operation

To use your implementation of Drive Encryption in its Common Criteria mode of operation, make sure that these conditions are met.

1. You need to install Drive Encryption in FIPS mode.
2. You need to invalidate user's password after 10 or less invalid logon attempts.
3. You need to encrypt all hard disks.
4. You need to force users to log on with PBA.

Administrator guidance

To comply with Common Criteria regulations, you must apply these policy settings in the Policy Catalog page before installing Drive Encryption.

• For each user-based policy that is assigned to one or more Drive Encryption clients, make sure that you enable the *Invalidate password after invalid attempts* option under User-Based Policy | Password | Incorrect passwords. Also make sure that the \( nn \) variable is greater than or equal to 10.

• For product settings that are assigned to one or more Drive Encryption clients, make sure that:
  • On the General tab, the Enable policy checkbox is selected.
  • On the Encryption tab, the Encrypt field is set to All disks.
  • On the Logon and General tabs, the Enable automatic booting option is disabled.

User guidance

Administrators should make sure that the users are aware of how to construct strong passwords.

• Use passwords with eight characters or more.
• Do not use words that are available in the dictionary.
• Do not use a name, or any variation of the account name or administrator identity.
• Do not use accessible information such as phone numbers, birthdays, license plates, or social security numbers.
• Use a mixture of uppercase and lowercase letters, as well as digits or punctuation. When choosing a new password, make sure it is unrelated to any previous password.
Additional information
Common Criteria EAL2+ mode operation
Index

A
about this guide 7
activation sequence 26
Active Directory 25
    adding users 21
    deleting/disabling users 93
    permission sets 93
    registering 21
Add Local Domain User 90, 91
    adding blacklist policy 91
add local domain users 28, 54, 67
administrative roles 106
administrator guidance, Common Criteria mode 143
administrator recovery
    enabling and disabling 133, 135
    performing 133
    response code 134
Agent wake-up call 26
agent wake-up call, sending 28
agent-server communication interval 28
ALDU 93
See also Add Local Domain User

ALDU feature 28
AMT, out-of-band actions 114
answers, self-recovery 131
AOAC 14
ASCI 28, 31
audio accessibility 100
authentication
    recommended user-based policy settings 76
auto boot 28, 84
    enabling 67
automatic booting
    enabling and disabling 97
    policies 58
    trusted platform module 13
automatic booting, temporary
    Drive Encryption 98
automatic repair 23

B
backup 23

biometric tokens 120
    fingerprint enrollment 120
    UPEK, enabling 120
    validity 121
blacklist policies
    adding and removing 91
    configuring 90
boot options 67

C
challenge code, generating 133
client computers
    adding users 29
    assigning theme 102
    encrypting 96
    managing 95
client events, viewing 124
client software, Drive Encryption
    deactivating 41
    FIPS mode 142
    installing 19
    uninstalling 43
    upgrading 37
client systems
    logging on 52
    managing 106
    removing users 83
    requirements testing 16
client tasks, editing 33
companion devices
    product policy 58
    user-based policy 74
customizations
    assigning to a system 102
    creating 102

dashboards, Drive Encryption
    creating 129
    viewing 129
DEAgent
- add local domain users 84
deployment 25
- synchronization with McAfee ePO 26

DEDeep extension 109
default password 84
deployment 25
- phased 23

DETech 23
disable user 93
disk check 23
disk encryption
  - encrypting and decrypting 10
  - Pre-Boot Authentication 9
disk status
  - encryption and decryption 130
  - reporting 124
disks
  - encrypting 96
  - partitions 58
documentation
  - audience for this guide 7
  - product-specific, finding 8
  - typographical conventions and icons 7

Drive Encryption
- about 19
- deleting/disabling users 93
deployment task 25
- installing offline activation package 52
machine keys 54
- managing servers and client systems 106
mode 142, 143
- password content rules 89
- password synchronization 88
removing 41, 143
- role-based access control 106
temporary automatic booting 98
- upgrading 37
- users 84
- using AMT 114

Drive Encryption GO 33
- installing 34
tests 33

E
- elevated security crypt mode 14
enable accessibility
  - audio signal 58, 100
  - enabling USB support 58
enCRYPTION
  - recommended product policy settings 67
encryption provider 67
enCRYPTION providers
  - PC Opal and PC software 58

encryption providers (continued)
  - setting priority 99
encryption status 26
encryption type
  - all disks and boot disks 96
  - selecting 58

Endpoint Encryption for PC
- upgrading 40
extensions, Drive Encryption
  - FIPS mode 141
  - installing 20
  - removing 42
  - uninstalling 41

F
- features, centralized management and Pre-Boot 11
  - FIPS mode, installing 142

G
- group users 84
  - adding systems 29
  - assigning policy 30
  - breaking inheritance 87
  - removing 83
  - user information 92
  - viewing 83

I
- import 25
incompatible products
  - adding rule 99
  - product settings 58
inheritance, breaking 87
installation
  - DE extensions 20
  - using third-party tool 29

Intel® Active Management Technology 11, 109–111, 113
Intel® vPro technology 109

K
- key server public key 47
KnowledgeBase
  - entropy 142
  - operating system refresh 19

L
- LDAP server 84
  - access control 106
  - deleting users 93
  - users 84
local domain users
  - adding 90
  - blacklisting 91
local domain users, adding 84, 93
log on, recommended product policy settings 67
logon hours
  applying restrictions 74
  managing 92

M
machine keys
  impact of deleting DE from ePO 54
  impact of transferring client systems 54
  reuse 54
MBR
  settings 67
McAfee Agent, creating install package 46
McAfee Endpoint Assistant 23
McAfee ePO
  DE activation sequence 26
  machine keys 54
  managing servers and client systems 106
McAfee ServicePortal, accessing 8
Microsoft Active Directory
  managing disabled users 90
  registering 21
MSI package extraction 47

O
offline activation
  Drive Encryption 52
  EpeOaGenXML.exe file 47
  generate package 49
  how it works 45
  installing McAfee Agent package 51
  installing software packages on client 51
  key server public key 47
  optional features 49
  performing 50
  user configuration 48
Opal drives 12
organizational units 84
organizational units, managing 86
out-of-band
  enabling 110
  remediation 109, 110
  unlock PBA 109, 111
  user management 109, 113
out-of-band options 67

P
packages, installing
  Drive Encryption 21
password content rules 74
passwords
  default 84
  recommended user-based policy settings 76
  strength 23
  synchronizing 26
passwords, Drive Encryption
  changing 132, 133, 135
  configuring content rules 89
  synchronizing 88
PBA 26
  product policy settings 67
  user account initialization 84
permission sets 106
permission sets, Drive Encryption
  defining 93
phased development 23
pilot test 23
PKI tokens
  associating with systems or groups 117
  initializing 117
policies 58
  assigning to systems 31, 81
  assigning to users 30
  categories 57
  configuring 81
  creating 80
  disabling 41
  editing 81
  enforcing 32, 81
  managing 57
  password content rules 89
  server settings 79
  user-based 74, 79
power fail recovery 49
Pre-Boot
  enabling accessibility 100
  enabling smart check 35
  FIPS mode performance 142
  removing 97, 98
pre-boot smart check 34
pre-boot smart check, enabling 67
preparations, basic 23
product components
  client system 10
  extensions 10
  LDAP Server 10
  McAfee ePO 10
  policies 10
  software packages 10
product setting policy
  automatic booting 97
  boot options 58
  disabling 41
  enabling accessibility 100
  encryption 58
  encryption provider 58
  encryption providers 99
product setting policy (continued)
- encryption type 96
- incompatible products 99
- logon 58
- managing themes 102
- recovery 58
- temporary automatic booting 98
- theme 58
- updating self-recovery information 101
Product Settings Policy 28, 54
recommendations 67
product version, reporting 124

Q
queries, Drive Encryption
- creating 124
- dashboard monitor 123
- running 124
Quick Response code 23

R
Read Username from Smartcard 118
- using other name 119
- using subject 119
readers, supported 23
recommendations, basic 23
recovery
- destroying information 54
- key size, changing 133, 135
- McAfee Endpoint Assistant 23
- power fail 49
- Quick Response code 23
- recommended product policy settings 67
- recommended user-based policy settings 76
- tasks 53
- tools 23
regular expression, adding and testing 91
remediation, out-of-band 114
reports, Drive Encryption
- encryption and decryption 130
- exporting results 123
- managing 123
- viewing 124
requirements testing 16, 33
- Drive Encryption GO 33, 34
- enabling pre-boot smart check 35
- pre-boot smart check 34
requirements, Drive Encryption 15
response code
- generating 134
- getting 133
restriction, logon hours 92
Role Based Access Control (RBAC) 106

S
secure-erase 54
self recovery 84
- recommended user-based policy settings 76
self-encrypting drives 12
self-initiating tokens
- associating with a system or group 118
- initializing 117
- supported types 48
self-recovery
- enabling and disabling 131
- enabling and resetting 101
- McAfee Endpoint Assistant 23
- performing 132
- user-based policy settings 74
self-tests, FIPS mode 142
server settings, Drive Encryption
- general 79
- incompatible products 79
- policy 79
- simple words 79
- themes 79
- tokens 79
servers
- settings 93
ServicePortal, finding product documentation 8
simple words
- adding and managing 103
- creating 103
- managing 79
Single Sign On 117, 118
Single Sign On, enabling and canceling 88
skip unused sectors 49
smart check, enabling 35
smartphone, self-recovery tool 23
software package, Drive Encryption
- removing 41-43
software packages, Drive Encryption
- checking in 21
- deploying 22
software requirements 15
SSO 26
- recommended settings 67
stored value tokens 116
system groups
- adding a system to 95
- moving 96
system requirements 15
System Tree 25
systems
- adding and importing 95
- recovery 131
T

technical support, finding product information 8
terminology 9
theme package
  creating and customizing 102
  installing 102
token certificates, configuring 115
token type 76
tokens
  biometric 120
  modifying type 115
  offline activation 48
  PKI 117
  PKI, associating with systems or groups 117
  self-initiating 117
  self-initiating, associating with a system or group 118
  stored value 116
  supported 23
  UPEK biometric 120
  UPEK biometric, enabling 120
  validity biometric 121
trusted platform module 13

U
unlock PBA, out-of-band 114
UPEK biometric tokens 120
user 23
user attribute, selecting 92
user configuration file
user guidance, Common Criteria mode 143
user information, configuring 92
user management, out-of-band 114
user-based policies
  authentication 74
  companion devices 74
  configuring 31
user-based policies (continued)
  enabling self-recovery 131
  password 74
  password content rules 74
  self-recovery 74
user-based policy 84
  recommended settings 76
users 58, 84
  adding 29
  adding before offline activation 48
  assigning 83
  changing passwords 133, 135
  global 92
  LDAP, deleting 93
  local domain 84
  managing 83, 90
  managing, User Directory page 86
  policies 74
  recovery 131
  removing 83
  reporting 124
  resetting self-recovery information 101
  role-based access control 106
  viewing 83

V
volume status, reporting 124

W
Windows logon
  controlling 87
  MSGINA 87
  Single Sign On 87
word package, regenerating 103