Best Practices Guide

McAfee Drive Encryption 7.1.0 Software

For use with ePolicy Orchestrator 4.6.7 and 5.1.0 Software

Contents

Preface

This guide provides the information on best practices on using McAfee Drive Encryption.

Contents

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.

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

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction

McAfee® Drive Encryption (DE) provides superior encryption across a variety of endpoints such as desktops and laptops. The McAfee Drive Encryption solution uses strong access control with Pre-Boot Authentication (PBA) and a NIST-approved algorithm to encrypt data on endpoints. Encryption and decryption are completely transparent to the end user and are performed without hindering system performance.

Administrators can easily implement and enforce security policies that control how sensitive data is encrypted. These policies allow the administrators to monitor real-time events and generate reports to demonstrate compliance with internal and regulatory requirements.

Drive Encryption offers an advantage over other competitive encryption products, because it engages encryption prior to loading the operating system, while data is at rest.

Contents

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), Extensible Firmware Interface (EFI), and Unified Extensible Firmware Interface (UEFI).

This release supports UEFI-based tablets, using a McAfee 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.

Purpose of this guide

This guide suggests best practices for deployment and activation. It also discusses optimization and maintenance before and after deployment.

When planning a large-scale deployment of Drive Encryption 7.1, it is important to understand:

- The features of McAfee® ePolicy Orchestrator (McAfee ePO)
- The process of scaling the back-end component
- Active Directory and LDAP
- The associated Drive Encryption communication

This document encapsulates the professional opinions of Drive Encryption certified engineers, and is not an exact science. You must understand both the product and the environment where it will be used before deciding on an implementation strategy. Calculations and figures in this guide are based on field evidence and not theoretical system testing; they are our **best advice** at the time of writing.

Review the best practices and use the guidelines that best fit your environment.

Abbreviations

The following table lists the abbreviations used in this document.

Table 1-1 Abbreviations

Abbreviation	Definition
AD	Active Directory
ALDU	Add Local Domain User
ASCI	Agent Server Communication Interval
BIOS	Basic Input/Output System
DN	Domain Name
DE	Drive Encryption
DEAgent	Drive Encryption Agent
EFI	Extensible Firmware Interface
ePO	ePolicy Orchestrator
GPT	GUID Partition Table
GUID	Globally Unique Identifier
LDAP	Lightweight Directory Access Protocol
MBR	Master Boot Record
NIST	National Institute of Standards and Technology
OS	Operating System
OU	Organizational Unit
PBA	Pre-Boot Authentication
PC	Personal Computer
SSO	Single Sign On
UBP	User-Based Policy
UEFI	Unified Extensible Firmware Interface

2 Design overview

The McAfee ePO server is a central store of configuration information for all systems, servers, policies, and users.

Each time the administrator initiates a policy update or an Agent Server Communication Interval (ASCI), the Drive Encryption protected system connects with McAfee ePO. The Drive Encryption protected system queries McAfee ePO for any configuration updates and downloads them. Examples of updates include a new user assigned to the client system, a change in policies, or a change in server settings specified by the administrator.

The Drive Encryption protected system also updates any changes on the client system back to the McAfee ePO server, for example, change of user's password token data.

Contents

Support for self-encrypting (Opal from Trusted Computing Group) drives

Opal drives are self-contained, standalone Hard Disk Drives (HDDs) that conform to the TCG Opal standard. Drive Encryption 7.1 provides a management facility for Opal drives.

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, they need to be managed by management software like McAfee ePO. If an Opal drive is not managed, it behaves and responds like a normal HDD.

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

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

The overall experience and tasks of administrators and users in installing and using Drive Encryption is the same, whether the target system has an Opal drive or a normal HDD. The installation of the product extension, deployment of the software packages, policy enforcement, and the method of management are the same for systems with Opal and Non-Opal HDDs.

Drive Encryption Policies

Drive Encryption is managed through the McAfee ePO server, using a combination of Product Settings, User-Based, and Add Local Domain User Settings policies.

The McAfee ePO console enables the administrator 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.

There are three types of policies:

- **Product Settings Policy** — The policy settings control the behavior of the Drive Encryption installed systems. For example, it contains the options for enabling encryption, enabling automatic booting, and controlling the theme for the pre-boot environment. These settings are specific to a system or a group of systems.
- **User-Based Policy** — These policy settings control 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. These settings are specific to a user, or a group of users, on a system or a group of systems.
- **Add Local Domain User Settings Policy** — These policy settings are used to add a blacklist of users to the ALDU functionality. Blacklisted users are excluded from the list of users assigned by the ALDU function.

Configure UBP enforcement

By default, all users inherit the default user-based policy (UBP) assigned to a system and are prevented from using Policy Assignment Rules. This allows maximum system scalability. User-based policies should be kept to a minimum because UBPs impact on performance and activation time.

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

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

Failing to assign UBP using Policy Assignment Rule to users, with UBP enforcement enabled, might cause Drive Encryption activation to fail.

User-based policies in Drive Encryption 7.1

Drive Encryption 7.1 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.

For option definitions, click **?** in the interface.

Task

1 Click **Menu** | **Reporting** | **Queries**.

2 Under **Shared Groups** in the **Groups** pane, select **Drive Encryption**. The standard DE query list appears.

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

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

5 Click **Actions** | **Drive Encryption** | **Configure UBP enforcement**.

6 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.

PBA in Drive Encryption 7.1

On BIOS-based systems, the Drive Encryption operating system provides security by booting prior to Windows and requiring Pre-Boot Authentication before the user is allowed to access the main operating system. On UEFI-based systems, the Drive Encryption software runs as a trusted application providing the same level of functionality.

PBA in Drive Encryption prevents the Windows operating system from loading until the user has authenticated with the correct password. It eliminates the possibility that one of the millions of lines of the OS code can compromise the privacy of personal or company data.

The PBA provided by Drive Encryption has proven time and time again to be the best Data Protection solution in the market. The PBA solution is an unmatched best practice to be followed by any organization for system security and data protection.

How Drive Encryption works

A boot sequence is executed by the BIOS leading to the starting of the bootable operating systems.

The boot sequence is the initial set of operations that the computer performs when it is switched on. A boot loader (or a bootstrap loader) is a short computer program that loads the main operating system for the computer. The BIOS first looks at a boot record, which is the logical area **zero** (or starting point) point of the disk drive, known as the Master Boot Record (MBR), which contains the boot loader.

On BIOS systems

Drive Encryption alters the MBR; the BIOS loads the modified MBR, which then loads the sector chain containing the Pre-Boot environment. This pre-boot screen prompts the user for authentication credentials, which might be a password, smart card, or token.

On UEFI systems

The UEFI specification defines a boot manager, a firmware policy engine that is in charge of loading the OS loader and all necessary drivers. The boot configuration is controlled by a set of global NVRAM variables, including boot variables that indicate the paths to the loaders.

PBA is a UEFI application started by the UEFI Boot Manager before the Windows bootloader uses standard UEFI protocols for GUI implementation (Graphics Output Protocol, Simple Pointer Protocol, and so on.)

GPT Headers and Partition Tables cannot be encrypted:

- The data in these regions is required before the disk is unlocked
- The disk would not be recognized as a valid GPT disk and the system would be unable to boot

After the user enters valid authentication credentials, the operating system starts to load and the user can use the computer in a normal way.

Encrypting a PC with Drive Encryption is the best and the most important practice that any organization can implement for protecting their data.

McAfee ePO requirements

The McAfee ePO server is a central store of configuration information for all systems, servers, policies, and users. It can be installed only on Windows Server 2003, 2008, or 2012 operating systems. For detailed information about installing or using McAfee ePO, see the ePolicy Orchestrator product documentation.

Supported environments for McAfee ePO and Drive Encryption

As new operating systems and service packs are released, the original product guides for McAfee ePO and Drive Encryption might not reflect the current McAfee support policy for those platforms.

To view supported environments for McAfee ePO and Drive Encryption, read this Knowledge Base article: https://kc.mcafee.com/corporate/index?page=content&id=KB79422

For more details, you can also refer to the *McAfee Drive Encryption 7.1 Product Guide*.

Hardware requirements for McAfee ePO

For details on the hardware requirements for McAfee ePO, see the product documentation for your version of McAfee ePO.

Software requirements

For details on the software requirements for McAfee ePO and McAfee Agent, see the Release Notes for Drive Encryption.

Clients communicating with McAfee ePO 4.6 through VPN disappear from the McAfee tree. For details, , read this Knowledge Base article: https://kc.mcafee.com/corporate/index?page=content&id=KB52949

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) 7.1 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* in the *McAfee Drive Encryption Product Guide*.

3 Software configuration and policies

When planning for a rollout and deployment of Drive Encryption, we recommend that you understand these important tasks.

- How to configure an LDAP server in McAfee ePO
- How to schedule and run the **Ldapsync: Sync across users from LDAP** task
- How to configure policies and different strategies for phased deployments

Contents

Active Directory configuration

Drive Encryption users are assigned to the client systems from an Active Directory (AD) registered in ePolicy Orchestrator. The McAfee ePO Server is responsible for the connection between the client and AD.

Drive Encryption users can also be created from the McAfee ePO server when the user directory is installed.

Check for the correct format of the Domain name, Username, and Server Address while registering the LDAP server in McAfee ePO.

AD users are different from Drive Encryption users.

- A user exists in AD.
- User string is added as a pre-boot user.
- User string is then matched to AD to verify if it exists.
- User string is used to login into pre-boot.

- If the correct SSO options are selected, the user string is compared.
- The end user perceives that he is logging on only once using a single user, however, the underlying mechanism still uses two different users, one to log on at pre-boot and another to log on against Active Directory.

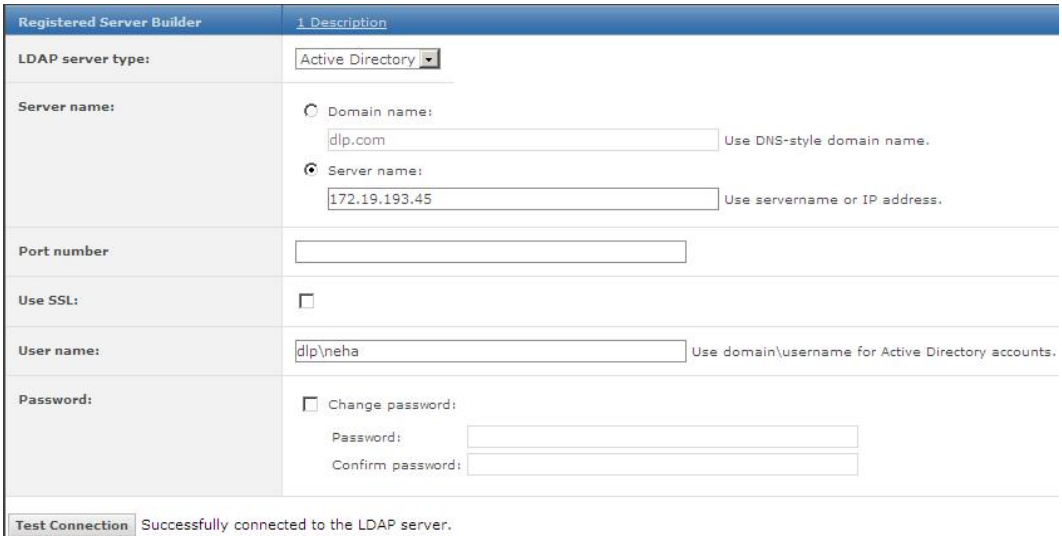

Figure 3-1 Register Active Directory

It is better to enter the IP address of the domain server in the **Server** name field than to enter the domain name of the domain server. This is due to the potential problems caused by DNS failures and/or canonical DNS servers failing to resolve the LDAP servers for the domain.

The Test Connection might sometimes be successful even if you haven't keyed in the domain name and the username in the correct format, however, the error could hinder the Drive Encryption activation. These issues are primarily seen with misconfiguration of the LDAP or DNS server. To investigate such issues further, perform troubleshooting in those areas. Common issues are non-accessible LDAP or referral server; or incorrect name resolution.

Managing LDAP attributes

Make sure you use the correct user attribute format to manage LDAP attributes for Drive Encryption.

Username

The value of this field determines the username attributes at PBA. For example, if the username value is set to samaccountname, the user must provide the samaccountname on the Pre-Boot Authentication page.

Display Name

The value of this field determines the form of the username displayed in ePolicy Orchestrator (**Menu** | **Reporting** | **Queries** | **Drive Encryption** | **DE: Users** and **Menu** | **Data Protection** | **Encryption Users** | **Actions** | **Drive Encryption** | **View Users**) pages. For example, if the username attribute is set to samaccountname and Display Name attribute is set to userprincipalname, the username appears as name *(paul)@domain.com*.

If the Display name attribute is set to userprincipalname, the username appears as *name* (paul)*@mcafee.com* whereas the user will be allowed to log on with the name value *name* (paul). (This can be different depending on the attribute selected in the username field and value of the attribute set in the LDAP).

If the attribute value used for username or display name is not set in the LDAP server for any user, Drive Encryption uses the attribute distinguished name for that particular object.

Account Control

This attribute checks for the status of the user, for example, if the user is enabled or disabled on the LDAP server.

User Certificate

The User Certificate attribute is used by the McAfee ePO Server to determine which certificate should be sent from ePolicy Orchestrator to the client, for example, smartcard tokens. It is better to clear this attribute when you use the Password only token. Setting this attribute can accumulate large amount of certificate data in the McAfee ePO database and impact LDAP performance; therefore, you can remove the certificate query from DE **LdapSync: Sync across users from LDAP** task while using the Password only token.

After changing the attribute value for any of the fields, the DE **LdapSync: Sync across users from LDAP** task needs to be run, to make sure the ePolicy Orchestrator database is updated with the new values.

Adding users

Select specific OUs, Users, or Groups while assigning users using **Menu** | **Data Protection** | **Encryption Users** | **Actions** | **Drive Encryption** | **Add User(s)** option. The **Add Drive Encryption Users** page provides three options, **Users**, **From the groups**, and **From the organizational units** with recursive option for Groups and OUs. You can click on the corresponding **Browse** button to list the Users, Groups, or OUs present in the configured LDAP server.

Although Drive Encryption 7.1 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.

The McAfee ePO server allows the administrator to filter user accounts that can be imported into Drive Encryption, based on a portion of LDAP. For example, if the configured LDAP has two major OUs: OU=My OU and OU=Phils_OU and if only the user accounts from OU=My OU need to be imported, then it can be achieved easily using McAfee ePO Server.

The **Recursive** option, if selected, adds the users of the sub-groups and sub-OUs in the selected groups and OUs.

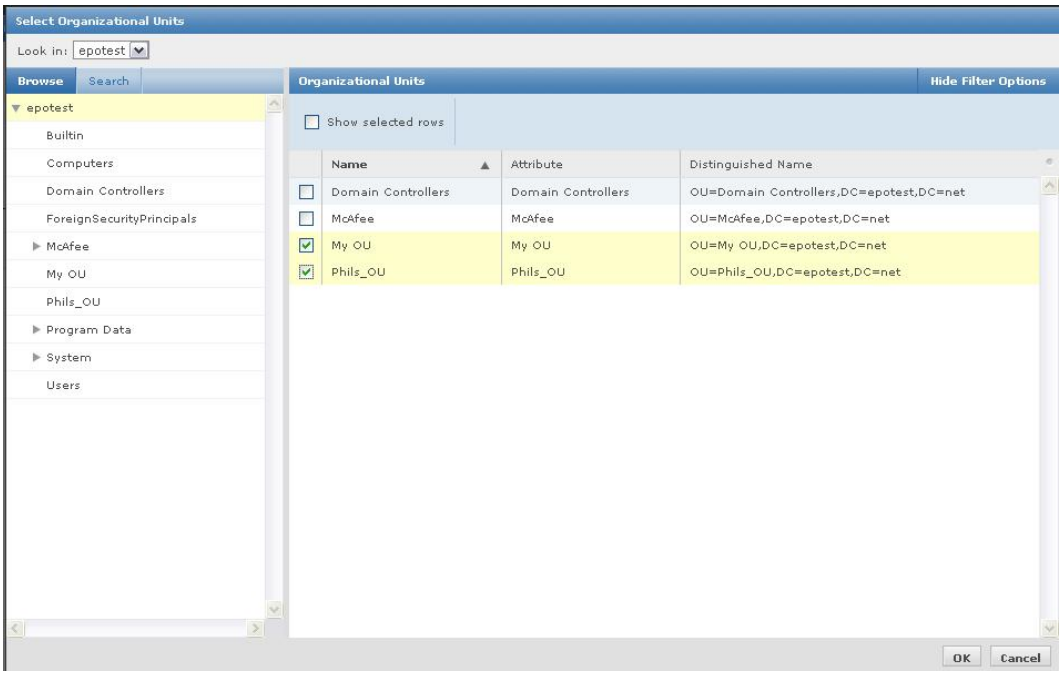

Figure 3-2 Assigning users from OUs

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 7.1** 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 7.1 Product Guide*.

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

Table 3-1 General tab

Policy Options	Recommendations
Enable Policy	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. The **Only activate if Health Check (Drive Encryption GO) check passes** option is applicable only if the DEGO extension is installed in McAfee ePO.
Logging Level	Set the required logging level. To overwrite the logging level defined in ePolicy Orchestrator, the **LoggingLevelOverride** registry key needs to be set on the client system. • **None** — Does not create any log for the client system managed by McAfee ePO. • **Error** — Logs only error messages. • **Error and Warnings** — Logs the error and warning messages. • **Error, Warnings, and Informational** — Logs the error and warning messages with more descriptions. • **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.
Harden against cold boot attacks when	Allows you to use the Elevated Security Crypt mode to help protect against cold-boot and other RAM-based attacks, when: • **The system is locked** —The encryption driver switches to the Elevated Security Crypt mode when the user locks the screen. • **The user is logged off** — The encryption driver switches to the Elevated Security Crypt mode when the user logs off. • **The system is in standby** — The encryption driver switches to the Elevated Security Crypt mode when the system in standby For more information, see *Protection of systems in Windows lock, log off, and standby states* in the *McAfee Drive Encryption 7.1 Product Guide*.
Expire users who do not login	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.
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 3-2 Encryption tab

Policy Options	Recommendations
Encrypt	Allows you to select the required encryption type and to set the encryption priority.
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 3-3 Log On (Drive Encryption) tab

Policy Options	Recommendations
Enable automatic booting	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. If you enable this option, the Drive Encryption software does not protect the data on the drive when it is not in use. • **Disable and restart system after 3 (1-10) failed logons or unlocks (Windows only, Vista onwards)** — We recommend that you enable this option if you enabled the **Enable automatic booting** option. This option disables the system autoboot after a specific number of failed Windows logons.
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.

Table 3-3 Log On (Drive Encryption) tab *(continued)*

Policy Options	Recommendations
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. This option is applicable only for systems installed with Drive Encryption 7.1. 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.
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.
Enable on screen keyboard	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. 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.
Always display on screen keyboard	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.

Table 3-3 Log On (Drive Encryption) tab *(continued)*

Policy Options	Recommendations
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.  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.
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.  USB audio functionality requires that the **Always enable pre-boot USB support** option be selected on the **Boot Options** tab.
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.

Table 3-3 Log On (Drive Encryption) tab *(continued)*

Policy Options	Recommendations
Read username from smartcard	Leave this option checked (enabled). This option automatically retrieves the available user information on the client system from the inserted smartcard; hence the Authentication window does not prompt for a username. The user can then authenticate just by typing the correct PIN. You need to enable the matching rules that are required for matching smartcard user principle name (UPN) with Drive Encryption usernames. This feature is supported on the Gemalto .Net V2+ tokens, and PIV and CAC tokens. • **Match certificate user name field up to @ sign** — Match the certificate user name up to the @ sign of the user name. For example, if the UPN is SomeUser@SomeDomain.com and the Drive Encryption user name is SomeUser, a match is found. • **Hide user name during authentication** — On selecting this option, the Drive Encryption user name does not appear in the Authentication window.
Lock workstation when inactive	Leave this option unchecked (disabled). The client system is locked when it is inactive for the set time.

Table 3-4 Log On tab

Option	Definition
Enable SSO	Leave this option checked (enabled). • **Must match user name** — 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. • **Using smart card PIN** — 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.
Synchronize Drive Encryption Password with Windows	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.
Allow user to cancel SSO	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.
Require Drive Encryption logon (only supported on V6 clients)	This makes it mandatory for you to log on to PBA for EEPC 6.x.x systems, thereby disabling the SSO functionality.
Lock workstation when inactive	Leave this option unchecked (disabled). The client system is locked when it is inactive for the set time.

Table 3-5 Recovery tab

Policy Options	Recommendations
Enabled	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.

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 3-6 Boot Options tab

Policy Options	Recommendations
Enable Boot Manager	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.
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 3-6 Boot Options tab *(continued)*

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

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

Table 3-7 Out-of-Band tab

Policy Options	Recommendations
Enable at PBA	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.

Table 3-8 Encryption Providers tab

Policy Options	Recommendations
Use compatible MBR	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.
Fix OS boot record sides	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.
Use Windows system drive as boot drive	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.
Enable Pre-Boot Smart Check (BIOS-based systems only)	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.
Force system restart once activation completes	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.
Opal	This option requires all the drives in your client system to be Opal for the PC Opal encryption provider to be activated.

Table 3-9 Companion Devices tab

Policy Options	Recommendations
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.

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 7.1** 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 7.1 Product Guide*.

User-based policies in Drive Encryption

Drive Encryption 7.1 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 3-10 Authentication tab

Policy Options	Recommendations
Token type	Select **Password only**. There are a number of other tokens that can be effectively used for your authentication as required. However, the **Password only** token is as strong as any other token that you could configure.
Certificate rule	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. • **Provide LDAP user certificate** — Leave this option checked (enabled). • **Enforce certificate validity period on client** — Leave this option checked (enabled) to enforce certificate validity period for the added certificate rule. • **Use latest certificate** — Leave this option checked (enabled). The **Certificate rule** options are not active if **Password only** is selected.
Logon Hours	You can set the days and the hours when the user can log on to the client system. The restrictions are applied using the **Apply Restrictions** option. We recommend enabling this option only if you have a specific requirement.

Table 3-11 Password tab

Policy Options	Recommendations
Change Default Password	• **Do not prompt for default password** — 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 **Change Default Password** option.

Password Change	Disable all of these settings as you would be using SSO and don't want to cause conflict with Windows password requirements.
	• **Enable password history____changes (1-100)** — Leave this option checked (enabled) to prevent users from reusing passwords unless your security policy exempts users from using new passwords.
	• **Prevent change** — Leave this option unchecked (disabled).
	  • **Require change after ____ days (1-366)** — Leave this option unchecked (disabled).
	  • **Warn user _____ days before password expiry (0-30)** — This is disabled by default when you disable the **Require change after ____ days (1-366)** option.

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 3-12 Password Content Rules tab

Policy Options	Recommendations
Display list of password rules	Enable this option to display the password requirements to users.
Password length	Leave the default value.

Table 3-12 Password Content Rules tab *(continued)*

Policy Options	Recommendations
Enforce password content	Leave the default value.
Password content restrictions	Leave the default value or enable restrictions for increased password strength.

Table 3-13 Self-Recovery tab

Policy Options	Recommendations
Enable self-recovery	Leave this option checked (enabled).
Invalidate self-recovery after no. of invalid attempts	Enable and set the number of attempts to a number that does not abruptly lock out the Self Recovery.
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 3-14 Companion Devices tab

Policy Options	Recommendations
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.

Checklist for using Intel® AMT and Drive Encryption

The Intel® AMT out-of-band feature within Drive Encryption 7.1 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 7.1 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.

Phased deployment strategies

Drive Encryption deployment (first time installation) can be done in various phases with different policy settings for different corporate environments. A model policy setting is explained in the recommended policy settings sections.

Phased deployment (first-time installation)

There can be a number of scenarios where the PBA creates challenges during the Drive Encryption deployment. For a safe and smooth deployment and activation process, you can easily create different sets of Drive Encryption system policies and do the deployment in various phases.

During the first time installation, it is a best practice to create the first set of policy settings with **Encryption** set to **None** and **Automatic Booting** enabled. You can create a second set of policy settings that enables the encryption and the PBA.

When the first set of policies is in use, the client systems are unprotected.

High level process

- After deploying the Drive Encryption packages, create an Drive Encryption system policy with the following settings:
  - Select the encryption option as **None** under **Encryption tab** | **Encrypt**.
  - Enable the **Enable Automatic Booting** option under **Log On** tab | **Drive Encryption**.
  - Enable **Add local domain users** option under **Log On** tab | **Drive Encryption**.
- Enforce this policy to the client systems. This activates Drive Encryption, but encrypts no disks and requires no authentication.
- You can now configure the second set of policy with the required encryption option other than **None** and autobooting disabled.
- Use the automatic booting policy as the default. In this mode, the Add Local Domain Users feature captures all Windows domain accounts that access the system. These accounts are added as valid pre-boot enabled accounts to be used in the pre-boot environment.
- Create a query in ePolicy Orchestrator to find all systems that need to stop autobooting and assign the second policy to these systems.
- Send an agent wake-up call from ePolicy Orchestrator to apply the policy with Pre-Boot Authentication to all required systems.
- The systems start with PBA when the new policy is received.

This phased deployment temporarily enables automatic booting and when the query is run, it enables the Pre-Boot Authentication policy. This ensures that Drive Encryption is activated when the system is in the field and ensures that the end user's account is added as a valid pre-boot account before encrypting and activating PBA.

This kind of phased deployment can be very useful when the administrator meets with challenges such as patching cycles, re-imaging process, deploying products, and managing other autoboot scenarios.

Perform phased deployment in batches of systems from the **System Tree**.

Automatic booting

Autobooting (**Enable Automatic Booting**) is used by administrators for re-imaging process, patching cycles, and product deployments. Many software installation packages require one or more restarts of the target computer, and autobooting automatically authenticates without user or administrator intervention. The administrator can define a window of time-line during which auto booting remains active.

The autoboot feature terminates when the defined time-line window has elapsed.

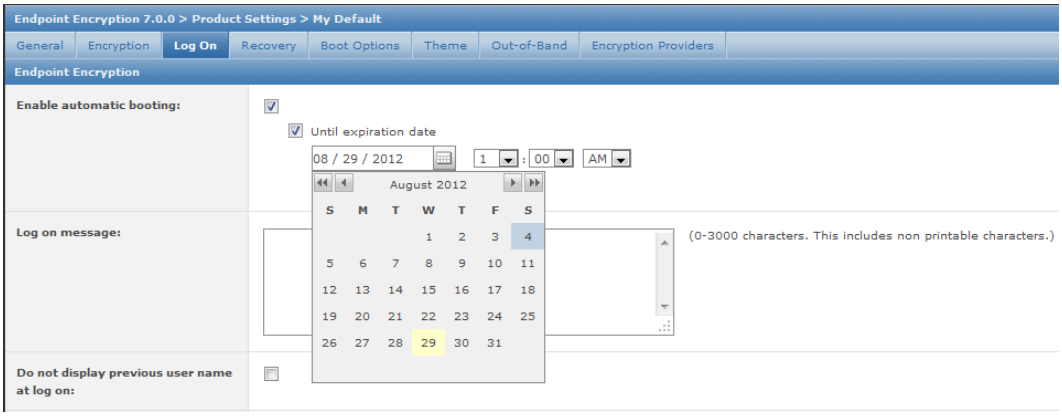

Figure 3-3 Configure auto booting

Because this policy setting temporarily bypasses the normal logon process for Drive Encryption installed systems, computers receiving this policy are vulnerable while autobooting remains active. To minimize the risk, make sure that you carefully review the inclusive dates and times that autobooting remains active before deploying this policy.

4 Deployment and activation

This section provides guidance and troubleshooting on why the Windows operating system will not start; encrypted systems do not allow access to the operating system until PBA is completed.

Administrators should be mindful that fixing certain Windows problems on an encrypted system might require extra caution if the registry needs to be edited or a driver needs to be modified.

Traditional recovery procedures also change on a system encrypted with Drive Encryption 7.1. For example, the entire disk is encrypted, meaning that the file systems and disks are accessible only when the Pre-Boot Authentication is complete.

The *DETech User Guide* provides instructions on how to create a customized pre-installation disk with the Drive Encryption drivers loaded, which allows the administrator to access an encrypted hard drive or Opal drive to update the drivers or the registry.

Booting the Drive Encryption installed client requires the physical presence of the client user to supply credentials on the Drive Encryption PBA page

To gain access to an encrypted computer, the user must always enter credentials at the PBA screen. It is important that this change in client operation be understood and adopted into your operating procedures. Administrators should be mindful of dispatching drivers and service packs to client systems as the system will inevitably require reboot after install.

The **Enable Automatic Booting** option in the **Product Settings Policy** allows access to the Drive Encryption installed systems without actually having to authenticate through PBA. It is the administrators' responsibility to ensure that system security is not compromised if this option is selected, as Autoboot effectively removes system security. Alternatively, you can also use the OS refresh process to keep the systems secure with minimal user intervention.

Contents

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

Occasionally, the PBA creates challenges during deployment. For a successful deployment and activation, you can create a different set of Drive Encryption system policies and deploy them in phases enabling the **None** option under **Encrypt** and **Enable Automatic Booting** option under **Log on** tab. 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 7.1 Product Guide* and the *McAfee DETech User Guide*.

Automatic Repair should be disabled in Windows 8 systems

Automatic Repair of an encrypted disk in Windows 8 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:
`bcdedit /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.

High-level process of installation

This section lists the steps and considerations involved in Drive Encryption deployment and activation. The individual tasks are explained in detail in the *McAfee Drive Encryption 7.1 Product Guide*.

For option definitions, click **?** in the interface.

Task

1. Install the Drive Encryption extensions in ePolicy Orchestrator. Check for the correct and latest version of the extension. Install the DEAdmin extension before the Drive Encryption extension.
2. Check in the Drive Encryption packages to ePolicy Orchestrator. Check for the correct and latest version of the DEAdmin and Drive Encryption packages.
3. Register your LDAP Server. Check for the correct domain and Server IP address of your LDAP server configured.
4. Modify the Product Settings and User-Based Policies, as appropriate. Plan and verify the policy settings for your organization's requirements.
5. Add a user to the client system. Decide whether to add the users manually in ePolicy Orchestrator or to add users using the **Add local domain user** option under the **Product Settings Policy**. At least one user must be assigned to each client to activate Drive Encryption on it.
6. Create a client task to deploy the Drive Encryption components to the client systems. Make sure that you deploy the packages in the correct order (DEAgent then Drive Encryption).
7. Test for successful deployment, activation, and encryption on targeted endpoints. Make sure to use the reporting facilities available in the ePolicy Orchestrator management software.

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.

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 7.1 (Product Settings)** | **Log on tab** | **Add local domain users**).

When enabled, the DEAgent queries the client system for the currently/previously 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 Synchoronization 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**.

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 Window 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.

It is safe and risk-free to restart the client system during encryption.

PBA

When the client 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.

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 option definitions, click **?** in the interface.

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.

Skip Unused Sectors

Skip Unused Sectors is one of the new features of offline activation introduced in Drive Encryption 7.1.

For more information about offline activation, see the *McAfee Drive Encryption 7.1 Product Guide*.

If you have enabled the SkipUnused option, you need to 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".

5 Operations and maintenance

Managing your systems in different batches, branches, or groups greatly impacts on Drive Encryption deployment. It is a good practice to arrange the systems in ePolicy Orchestrator in department level or batch level, then deploy the product to these batches one by one.

Contents

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.

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.

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 ePolicy Orchestrator database to be used for client recovery when required.

For more information about reusing Machine Keys, refer to the KnowledgeBase article https://kc.mcafee.com/corporate/index?page=content&id=KB71839.

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 an Drive Encryption active system is re-imaged.

What happens to the Machine Key when you delete a Drive Encryption active system from ePolicy Orchestrator?

The Machine Key remains in the ePolicy Orchestrator database; however, the key association with the client system is lost when the client system is deleted from ePolicy Orchestrator. When the client system reports back to ePolicy Orchestrator 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 ePolicy Orchestrator.

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, ePolicy Orchestrator 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 ePolicy Orchestrator 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 7.1 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 ePolicy Orchestrator 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 ePolicy Orchestrator 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 ePolicy Orchestrator.

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, ePolicy Orchestrator 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 ePolicy Orchestrator 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 ePolicy Orchestrator?

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

How to destroy the recovery information for an 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** | **System Tree** | **Systems tab** | **Actions** | **Drive Encryption** | **Destroy All Recovery Information** in the ePolicy Orchestrator console. You must also disable the **Add local domain user** option in the **Product Setting Policy**. This means that the system can never be recovered.

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.

Use the correct format of the user name when logging on to ePolicy Orchestrator.

Drive Encryption 7.1 scalability

Use these configurations, recommendations on components, and considerations for scalability.

- ePolicy Orchestrator 4.6.7 or 5.1.0
- Drive Encryption 7.1

These considerations and settings help improve scalability:

- Longer ASCI interval
- Password-only deployments should remove the certificate query from **LDAPSync: Sync across users from LDAP** task.

The User Certificate attribute is used by the McAfee ePO server to determine which certificate should be sent from McAfee ePO to the client, for example, for smartcard tokens. It is better not to query this attribute when you use the password-only token as tests have shown that LDAP query performance decreases when certificates are included in the query. Setting this attribute can also accumulate a large size of data in the database; therefore, you can remove the certificate query from **LDAPSync: Sync across users from LDAP** while using the password-only token.

- Phased rollout during migration, upgrade, or first time installation of Drive Encryption.

These configurations and factors degrade scalability:

- **Policy Assignment Rules** — The policy assignment rules should be set up in a logical order to ensure minimal processing. Create an ordered list of rules associated with a user-based policy. For each user, the rules engine evaluates the rules in order, and the first rule that is matched defines which UBP is assigned to the user.

  

  Make sure that you enable the Policy Assignment Rules for a small number of users to minimize overloading ePolicy Orchestrator.

  Given that ePolicy Orchestrator needs to send all users down to a client during activation, each user needs to have rules run to associate a UBP with them (if UBPs are enabled and rules are defined). With **r** rules, **m** machines and **u** users, the worst case scenario would be an O[n^3] calculation (**r*m*u**), which is not recommended.

  Best practice is therefore to configure the rules in the correct order, such that they are defined in descending order of the number of users that each rule would "catch". For example, if rule A catches 10% of users, rule B catches 80% of users, C 5%, D 2%, E 3%, the most efficient way of ordering the rules would be B->A->C->E->D, if the logic of your rules allows this to be done.

- Large number of users per machine (>20)

  

  Although Drive Encryption 7.1 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.

- Deployment of unnecessary languages (recovery questions)

The rate of activation can be calculated with the formula, $N_{max}=ASCI_{secs}/M_{upstream}.DC_{rate}$

Where,

- DC_{rate}depends on hardware configuration of ePolicy Orchestrator and Database
- $M_{upstream}$ is the number of data channels (two) being sent from each client

6 Migration and upgrade

Due to the improved architecture and interface of Drive Encryption 7.1, some functionality from earlier versions of the product is now handled differently.

Contents

Best practices for migration and upgrade

This section provides information to help you to understand the best practices and prerequisites for Drive Encryption migration and upgrade.

The detailed procedures for these migration tasks are given in the *Drive Encryption 7.1 Migration Guide*.

- Migrating from EEPC 5.2.6 or later to Drive Encryption 7.1 without the migration tool
- Migrating from EEPC 5.2.6 or later to Drive Encryption 7.1 with the migration tool
  - Exporting users and user assignments from the 5.x.x database
  - Importing users and user assignments into Drive Encryption 7.1
- Viewing Drive Encryption migration reports

Migration tool

Make sure that you have the latest **EEMigration.ZIP** file of Drive Encryption 7.1 to implement and perform the export. We recommend that you copy and extract the **EEMigration.ZIP** file to the folder where Endpoint Encryption Manager (EEM) is installed.

Exporting 5.x.x database

- Make sure that you have access rights to view system and user properties on EEM and the McAfee ePO server.

Importing the systems or users from 5.x.x database into the McAfee ePO server

- Make sure that EEPC 5.x.x and Drive Encryption 7.1 are connected to the same LDAP server during the export and import process.
- Make sure that you have registered an LDAP server on the McAfee ePO server before initiating the import process.

- Make sure that you have scheduled and run the **LdapSync: Sync across users from LDAP** task before initiating the import process.
- Analyze the color-coordinated results in different phases of the import. It guides you to make appropriate decisions before proceeding to the next step.
- Do not navigate away or shut the browser when the import is running on ePolicy Orchestrator. Doing so interrupts the import thread and stops the import process. When the import is running, the message **Please wait, assigning users to systems** appears at the McAfee ePO console.
- After you import the systems or users from 5.x.x database into the McAfee ePO server, check that the systems, users, and the audit details are imported as you expected. Check that the password token, self recovery, SSO details, if available, are imported as you expected.
- Conduct a policy review after the import process. If you need your 5.x.x policy settings for 7.1, you must set them before upgrading the client. Make sure that you enable the **Encrypt product setting policy** under **Drive Encryption 7.1** | **Product Settings** | **Encrypt**. If this is not set, encrypted client system starts decrypting by default.

To initiate the encryption on the client, you must select any one of the options other than **None**. The default option **None** does not initiate the encryption.

Some firewall software enforces HTTP session timeouts. During the import you should review your firewall settings in the manufacturer documentation and take the necessary actions to prevent the firewall from timing out the session.

- Before upgrading the client, make sure that the user's UBP enforcement settings are correct and the appropriate Policy Assignment Rule is created on McAfee ePO if those users are intended to use the non-default UBP.

Upgrading to Drive Encryption 7.1

- Make sure that the system to be migrated is managed by the McAfee ePO server.
- Migration of users directly from 5.x.x client to the new Drive Encryption 7.1 client is not supported. Any migration of user assignments must be done on ePolicy Orchestrator before or after deploying Drive Encryption 7.1 to the client system.
- To upgrade the client, first install the DEAgent, then the Drive Encryption software packages.
- If 5.x.x users are found in the assigned LDAP OU/Group, the 5.x.x password token, SSO and Self Recovery data are transferred to Drive Encryption 7.1. If new users are present in the assigned LDAP OU/Group, they are added to Drive Encryption as users not being initialized.

FIPS mode

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 7.1.

For Drive Encryption 7.1 to be in compliance with FIPS 140-2, the software must meet these conditions.

- McAfee ePO (4.6.7 or 5.1) installed in FIPS mode
- Drive Encryption client package installed on the client 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.

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. For details on the impact of FIPS mode and how to install or upgrade the Drive Encryption client in FIPS mode, see FIPS 140-2 certification in the *McAfee Drive Encryption Product Guide*.

General recommendations

- Retain the 5.x.x database for some time, so that you can access it in case of the loss or theft of a device after migration.
- Migrate only a small number of systems as an initial test before doing a large-scale migration.
- If you are using the $autoboot$ user id in 5.x.x to boot your systems without actually having to authenticate through the PBA, note that the same option is now a feature in 7.1. Make sure that you enable this option (**Menu | Policy | Policy Catalog | Drive Encryption 7.1 | Product Settings | Logon | Enable Automatic Booting**) to activate **Autoboot** while migrating the users and systems from 5.x.x to 7.x. To enable automatic booting without adding a user, you need to configure the **Add local domain users** feature.

  The **Enable Automatic Booting** option in the Product Setting Policy allows access to the Drive Encryption installed systems without actually having to authenticate through PBA. It is the administrators' responsibility to ensure that system security is not compromised if this option is selected.

  If you enable this option, the Drive Encryption software doesn't protect the data on the drive when it is not in use.

Export user assignments from 5.x.x database

The export tool provided with Drive Encryption allows the administrator to export the user assignments from a 5.x.x database. The purpose of exporting the user assignments is to reduce the amount of configuration required by the administrator to upgrade from 5.x.x to 7.x.x.

The export output is a .ZIP file, which can be imported into the the McAfee ePO server. The import process uses an import wizard on the McAfee ePO server after installing the applicable Drive Encryption extensions.

The purpose of exporting systems from a 5.x.x database is to export the user assignments. Migration export is not required if you do not want to migrate the user assignments.

Best practices

- Make sure that you have the latest **EEMigration.ZIP** file from the Drive Encryption 7.1 release package to implement and perform the export from EEM 5.x.x.
- We recommend that you copy and extract the **EEMigration.ZIP** file to the folder where EEM is installed.
- Make sure that you have the access rights to view system and user properties on EEM and the McAfee ePO server.

- It is important to understand the export options; **Machines** and **Users** in the export wizard. You can select any one of the options to export the required user assignments from EEM 5.x.x.
  - On selecting the **Machines** option in the export wizard, all users assigned to the selected machines from 5.x.x database are exported. This also provides the option to select a specific machine, so that all the user assigned to that particular system can be exported.
  - On selecting the **Users** option in the export wizard, all systems to which the selected users are assigned are exported. This also provides the option to select specific users so that all the systems that have the selected users are exported.
- By default, system or user audit event data is not exported. It is the responsibility of the administrator to select the **Export Machine and User audit events** option during the export process.

Importing the audit logs increases the size of the McAfee ePO database. We recommend that you keep the number of days to a minimum.

Import user assignments to McAfee ePO

The Drive Encryption Admin extension provides a user interface to import the export file (.ZIP) created during the export from the 5.x.x administrator system.

Important prerequisites for importing user assignments

- Make sure that you have the permission to **Allow Import of v5 users** to perform this task. You can enable this permission by navigating through **Menu | Users | Permission sets | Drive Encryption | Allow Import of v5 users**.
- Make sure that you have copied the export file (.ZIP) to a location where you can access it from the McAfee ePO server.
- Make sure that the systems to be upgraded are managed by ePolicy Orchestrator.
- Make sure to register the LDAP server on the McAfee ePO server and make sure it is the same server registered on the 5.x.x database.
- If you intend to migrate standalone users, User Directory should be installed before initiating the import process.

Key notes on importing user assignments

- If users are manually added to the 5.x.x database and the same users are not present in the Active Directory, then those 5.x.x users appear as unmatched users in ePolicy Orchestrator during the import process. In this situation, you need to make sure that you assign these unmatched users to configured LDAP users. Unmatched users can also be matched with the User Directory users.
- EEPC 5.x.x users disabled in the Active Directory are imported to ePolicy Orchestrator during the import process, however, the properties of these disabled users are determined by the Drive Encryption Server Setting configured in ePolicy Orchestrator.
- The application performs the system matching using the 5.x.x machine name and the McAfee ePO system name. The results are color-coordinated, so that it is easy for the administrator to analyze the results.
  - Green indicates a successful matching
  - Red indicates an unsuccessful matching
- The application performs the user matching using the binding attributes if they are present. If no match is found, the rules are used to search every LDAP server that has been set up with DE LDAP

attributes. The results are color-coordinated, so that it is easy for the administrator to analyze the results.

- Green indicates a single match
- Orange indicates more than one match
- Red indicates no match

Are 5.x.x policies imported to 7.1.x during the migration?

No, 5.x.x policies are not imported to 7.x as part of the migration process. The user should set the required 5.x.x policies, more importantly the **Encrypt** policy, in 7.x before upgrading the client.

If you do not change the default **Encrypt** policy from **None** to **Encrypt** in 7.x before the upgrade, the client system starts decrypting after the upgrade. It is always a best practice to configure the required policies before initiating the import process.

What happens if the LDAP server used by 5.x.x is not registered in ePolicy Orchestrator?

All imported users of 5.x.x appear as unmatched users in ePolicy Orchestrator. Unmatched users can be created in the User Directory as standalone users. Make sure you register the same LDAP server used by 5.x.x.

What happens if the 5.x.x machines are not managed by ePolicy Orchestrator?

All imported machines of 5.x.x appear as unmatched machines in ePolicy Orchestrator. Make sure that the systems to be migrated are managed by ePolicy Orchestrator before initiating the import process.

Upgrade to Drive Encryption 7.1

The primary goal of upgrading from the EEPC 5.x.x series to Drive Encryption 7.1.x is to retain the disk encryption. This is to make sure that a decrypt and a re-encrypt of the disk is not required during the upgrade.

Only one encryption algorithm can be active for all disks, so no matter which algorithm is set in 7.1.x, if the 5.x.x system has a different algorithm, then that algorithm is used for all disks even after migrating to 7.1.x.

The only way to change the client algorithm is to deactivate McAfee on the client and decrypt all disks, then reactivate Drive Encryption on it.

All the recovery settings have four times as many lines as the AES algorithm. Setting recovery key size as **Low** gives 4 lines of response code with RC5 algorithm.

On migrating from EEPC 5.x.x to McAfee 7.1.x, the available user password token, SSO, and self-recovery details are transferred to McAfee 7.1.x. To use 5.x.x SSO and Self Recovery data in 7.1.x, you need to enable Self-Recovery and SSO in the 7.1.x policies after importing the users.

What happens to a partially encrypted 5.x.x system after the migration?

A partially encrypted 5.x.x system gets fully encrypted or decrypted as per the policies set in 7.1.x.

What happens if the user initiates the upgrade process while the 5.x.x client is still in encrypting or decrypting state?

It completes the encryption or decryption process as per the policies set in 7.1.x.

What happens to a removable media that is encrypted with 5.x.x?

We recommend that you decrypt your removable media before initiating the upgrade.

There is no way to decrypt your removable media after the upgrade, other than using the DETech recovery tool.

Are the 5.x.x token details migrated to 7.1.x?

Yes, 5.x.x Password token details are migrated if it is available.

Are the SSO and Self Recovery details migrated from 5.x.x to 7.1.x?

Yes, the SSO and Self Recovery details are migrated from 5.x.x to 7.1.x only when the 5.x.x Password token is available. Otherwise, the user needs to enable SSO in the 7.1.x Product Settings Policy and Self-recovery in the corresponding user-based policy. The user does not have to enroll again for Self Recovery when the product is upgraded from 5.x.x to 7.1.x.

What happens to a 5.x.x system after migration if it has been encrypted using an algorithm that is different from 7.1.x?

The system remains encrypted with same algorithm as set in 5.x.x, and you can apply all the policies of 7.1.x to the migrated system as usual. To change the algorithm, you need to first deactivate Drive Encryption, change the algorithm, then activate.

7 Client status reporting in ePolicy Orchestrator

McAfee ePolicy Orchestrator provides comprehensive management and reporting tools for Drive Encryption.

Administrators can create standard and customized dashboards, queries, and reports. The procedures on how to create standard dashboards, queries, and reports are documented in the *McAfee Drive Encryption 7.1 Product Guide*.

When the Drive Encryption Agent and Drive Encryption software packages are deployed to the client systems and they are successfully managed by ePolicy Orchestrator, any of these queries can be used to retrieve data:

- **DE: Disk Status**
- **DE: Encryption Provider**
- **DE: Installed Version**
- **DE: Users**
- **DE: Product Client Events**
- **DE: Disk status (Rollup)**
- **DE: Installed version (Rollup)**
- **DE: Migration log**
- **DE: Migration lookup**
- **DE: Volume status**
- **DE: Volume status (Rollup)**
- **DE: V5 audit**
- **DE: Systems with uninitialized users**
- **Intel AMT out-of-band queries**

Contents

Track the progress of the deployment and encryption status

The progress of the Drive Encryption deployment and the number of encrypted drives can be easily determined by running the Drive Encryption query under **Menu** | **Reporting** | **Queries** | **Drive Encryption** | **DE: Disk Status**. This reports the crypt state for all disks on systems where the DEAgent is installed.

You can also find the systems that don't have the DEAgent installed by running the query under **Menu** | **Reporting** | **Queries** | **Drive Encryption** | **DE: Encryption Provider**.

Report encryption status from McAfee ePO

To comply with data protection regulations, IT staff must be able to produce evidence that a suitable technical measure was in place to protect sensitive information on, for example, a missing computer.

The organization must encrypt the device and be able to prove that the device is encrypted after it is reported lost or stolen.

High level process

Drive Encryption makes this task easy. An administrator can log on to McAfee ePO and, in just a few clicks, be able to produce a report showing that the missing computer was encrypted.

- Log on to ePolicy Orchestrator as an administrator.
- Locate the system in the **System Tree**.
- In the McAfee ePO server, drill-down to encryption properties.
- Check the encryption status under the **Disks** tab.

Finding the user's system in McAfee ePO

The encryption status is stored as a property of the system, not the user. To confirm that a missing computer is encrypted, you must find the system in McAfee ePO and view its properties. You can use the queries and reports to know the encryption status of the system.

Index

F

G

H

I

L

M

O

P

Q

R

S

T

U