# McAfee Endpoint Encryption for PC v6.0 Patch 2

Best Practice Guide

# Contents

# Introduction

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

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

EEPC has the advantage over other industry encryption products because it engages encryption prior to loading of the Windows Operating System, providing full protection from the moment the system is powered on.

**Contents**



# 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 EEPC 6.0 Patch 2, it is important to understand:

- The features of ePO Server
- The process of scaling the back end component
- AD/LDAP
- The associated Endpoint Encryption Communication

This document encapsulates the professional opinions of Endpoint Encryption certified engineers, and is not an exact science. You must understand both the product and the environment in which 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.

NOTE: Please review the best practices and use the guidelines that best fit your environment.

## Abbreviations

The following table lists the abbreviations used in this document.

## Abbreviations

| Titles | Designations |
|---|---|
| EEPC | Endpoint Encryption for PC |
| ePO | ePolicy Orchestrator |
| EEM | Endpoint Encryption Manager |
| PC | Personal Computer |
| AD | Active Directory |
| LDAP | Lightweight Directory Access Protocol |
| OS | Operating System |
| ASCI | Agent Server Communication Interval |
| BIOS | Basic Input/Output System |
| UBP | User Based Policy |
| SSO | Single Sign On |
| MBR | Master Boot Record |
| OU | Organizational Unit |
| NIST | National Institute of Standards and Technology |

# Design Philosophy

### Centralized management using ePO 4.5.0

McAfee ePO Server 4.5.0 is a central store of configuration information for all systems, servers, policies, and users.

Each time the administrator initiates a policy update, or an ASCI (Agent Server Communication Interval), the EEPC protected system connects with ePO.

The Endpoint Encryption protected system queries ePO 4.5.0 for any configuration updates and downloads them. Example updates might be: a new user assigned (by the administrator) to the client system, a change in policies, or, a change in server settings specified by the administrator.

### Contents



# EEPC Policies

EEPC is managed through the ePolicy Orchestrator 4.5.0 using a combination of Product Setting and User Based Policies. The ePO console allows the administrator to enforce policies across groups of computers, or, a single computer. Any new policy enforcement through ePO overrides the existing policy that is already set on the individual systems. There are two types of policies: Product Settings and User Based Policies. Product Setting Policies are specific to a system or a group of systems. User Based Policies are specific to a user, or a group of users, on a system or a group of systems.

The Product Setting Policy controls the behavior of the EEAgent. For example, it contains the options for enabling encryption, enabling automatic booting, and controlling the theme for the Pre-Boot environment.

The User Based Policy controls the parameters for EEPC user accounts. For example, it contains the options for selecting a token type (for example: password, smartcard, and so on), password content rules.

# Pre-Boot Authentication in EEPC V6.0 Patch 2

EEPC's Pre-Boot Authentication (PBA) is part of a mini operating system (EEPC) that acts as a trusted authentication layer by serving as an extension of the BIOS, or boot firmware, and

guarantees a secure, tamper-proof environment external to the Microsoft Windows Operating System. The PBA prevents Windows from loading until the user has authenticated with the correct password; it eliminates the possibility that one of the millions of lines of OS code can compromise the privacy of personal or company data.

The Pre-Boot Authentication provided by EEPC has been proven time and time again as the best Data Protection solution on the market. The Pre-Boot Authentication solution is an unmatched best practice to be followed by any organization for system security and data protection.

# How Endpoint Encryption works

A boot sequence executes during the startup process of Windows Operating System. 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 boot loader first looks at a boot record or partition table, which is the logical area **zero** (or starting point) point of the disk drive.

McAfee Endpoint Encryption for PC replaces the zero point area of the drive. EEPC alters the MBR and presents the modified Pre-Boot environment. This changed Pre-Boot screen then prompts the user for authentication credentials. The policies for a user can be configured in such a way, that at this point, the computer will ask for additional credentials such as a smart card or token.

After the user enters valid authentication credentials, the Operating System continues to load and the user can use the computer in a normal way.

Encrypting a PC with EEPC 6.0 Patch 2 is the best and the most important practice that any organization can have for protecting their data.

# ePO Server requirements

McAfee ePO Server 4.5.0, the management console, is a central store of configuration information for all systems, servers, policies and users. McAfee ePO Server 4.5.0 can be installed only on Windows Server 2003 or 2008 Operating Systems. For detailed information about installing or using ePO, refer to the McAfee ePolicy Orchestrator 4.5.0 – Installation/Product Guide.

### Supported environments for ePO and EEPC

As new operating systems and Service Packs are released, the original McAfee Product Guides for ePO and EEPC might not reflect the current McAfee support policy for those platforms. To view supported environments for ePO and EEPC, read the Knowledge Base article https://kc.mcafee.com/corporate/index?page=content&id=KB51109, or, refer to the Endpoint Encryption 1.0.0 Product Guide.

### Hardware requirements for ePO

Refer to McAfee ePolicy Orchestrator 4.5.0 - Installation/Product Guide for the details on the hardware requirements for ePO 4.5.0.

## Software requirements

Refer to Endpoint Encryption 1.0.0 Product Guide for the details on McAfee ePO and McAfee Agent for Windows minimum requirement for EEPC.

# Software configuration and policies

When planning for a rollout and deployment of EEPC, it is recommended that you understand:

- the best practices for configuring an LDAP server in ePO.
- how to schedule and run the **EE LDAP Server User/Group Synchronization** task.
- how to configure policies and different strategies for a phased deployment.

**Contents**



# Active Directory configuration

EEPC users are not created from the ePO server. They are assigned to the client systems from an Active Directory or an Open LDAP server registered in ePO 4.5.0. McAfee ePO Server 4.5.0 is responsible for the connection between the client and AD, or, Open LDAP, and the client.

NOTE: Open LDAP is supported only with ePO 4.5.0 Patch 3 and higher.

Another important reason to have an LDAP server for installing and managing EEPC is that the User Based Policies are applied to the users using policy assignment rules which are assigned from LDAP server to control their logon and authentication options.

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

NOTE: It is better to key in the IP address of the domain server in the **Server name** field than entering the domain name of the domain server.

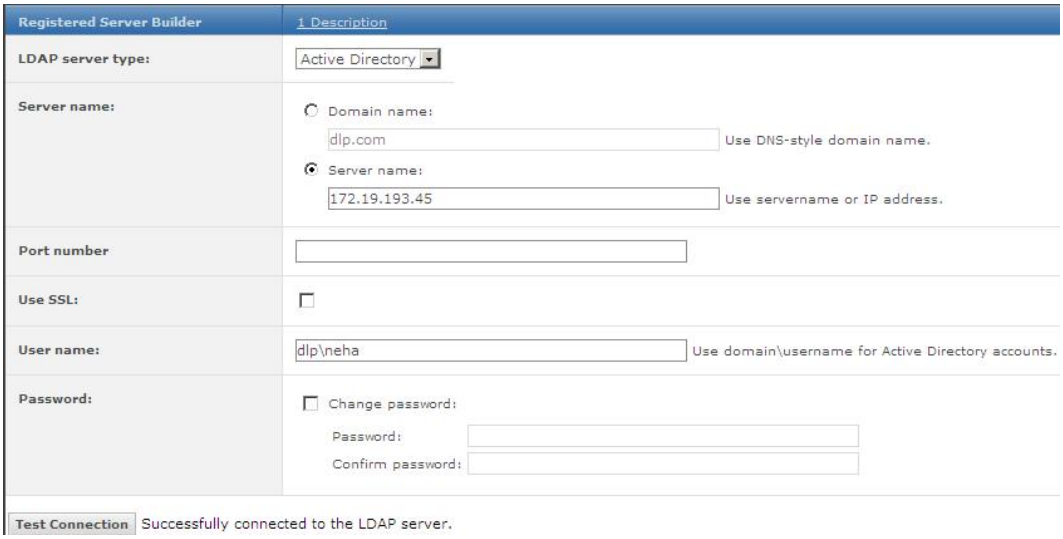



Figure 1: Register Active Directory

There could be instances when the **Test Connection** would get through even if you haven't keyed in the domain name and the user name in correct format, however, the same error could hinder the EEPC activation.

The ePO Server allows the administrator to filter user accounts that can be imported into EEPC, based on a portion of LDAP. For example, if the configured LDAP has two major Organizational Units (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 ePO Server.

Select specific OUs or Group(s) while assigning users using **Menu** | **Data Protection** | **Encryption Users** | **Actions** | **Endpoint Encryption** | **Add User(s)** option. Add User(s) page provides three options such as **Users**, **From the groups** and **From the organizational**

**units** with recursive option for Groups and OUs. You can click on the corresponding **Browse** button and list the Users/Groups/OUs present in the configured LDAP server.

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


Figure 2: Add EE users

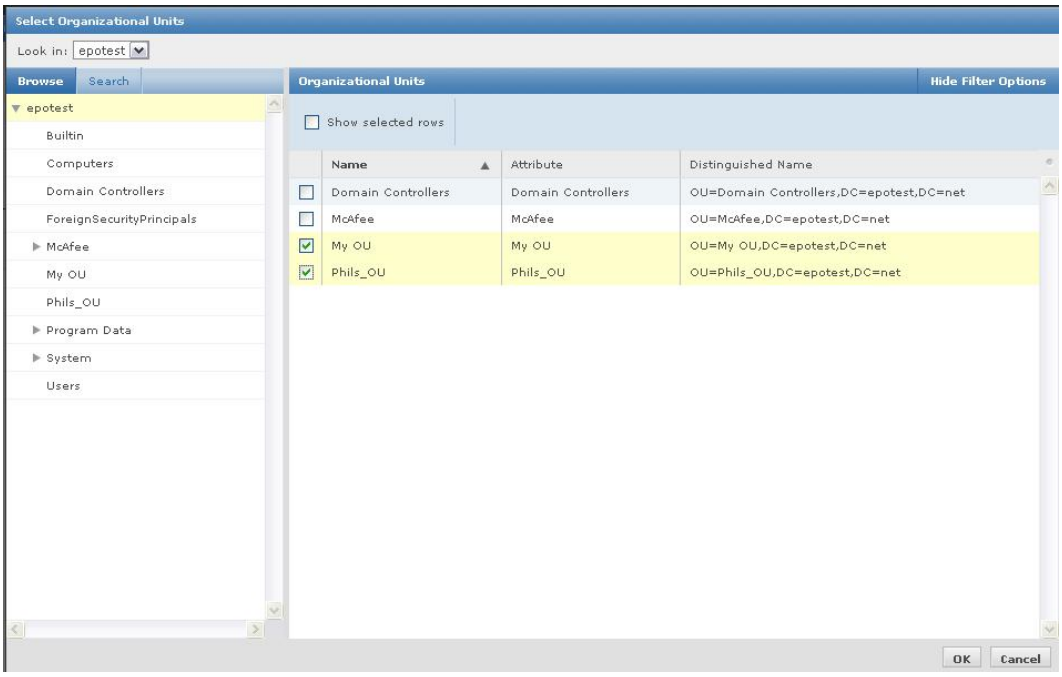



Figure 3: Assigning users from OUs

# EE LDAP Server User/Group Synchronization

Ensure you use the correct user attribute format in the **EE LDAP Server User/Group Synchronization** task. Match the correct user attributes in the fields.

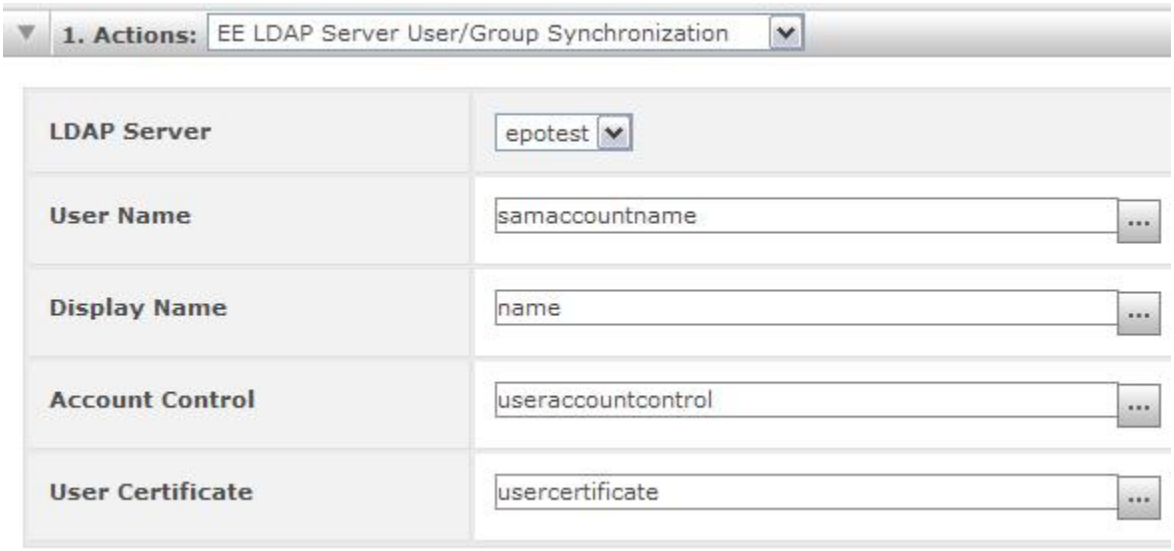



Figure 4: EE LDAP Server User/Group Synchronization

### User Name

The value of this field determines the format of the Pre-Boot Authentication **User Name**. For example, if the **User Name** value is set to **samaccountname**, then the user will need to provide the **samaccountname** at the PBA and EE Windows Logon pages.

### Display Name

The value of this field decides the format of the **User Name** displayed in ePO (**Menu** | **Reporting** | **Queries** | **Endpoint Encryption** | **EE: Users** and **Menu** | **Data Protection** | **Encryption Users** | **Actions** | **Endpoint Encryption** | **View Users**) pages. For example, if the **User Name** attribute is set to **samaccoutname** and **Display Name** attribute is set to **userprincipalname**, then the **User Name** will appear as **name** (paul)**@domain.com**.

If the **Display name** attribute is set to **userprincipalname**, then the user name will appear as **name** (paul)**@mcafee.com** whereas the user will be allowed to login 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).

### Account Control

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

NOTE: Ensure to select the **useraccountcontrol** attribute in the **Account Control** filed. Attributes other than this will not activate EEPC on the client.

### User Certificate

The User Certificate attribute is used by the ePO Server to determine which certificate should be sent from ePO to the client, for example, smartcard tokens. It is better not to set this attribute when you use the Password only token. Setting this attribute can accumulate large amount of

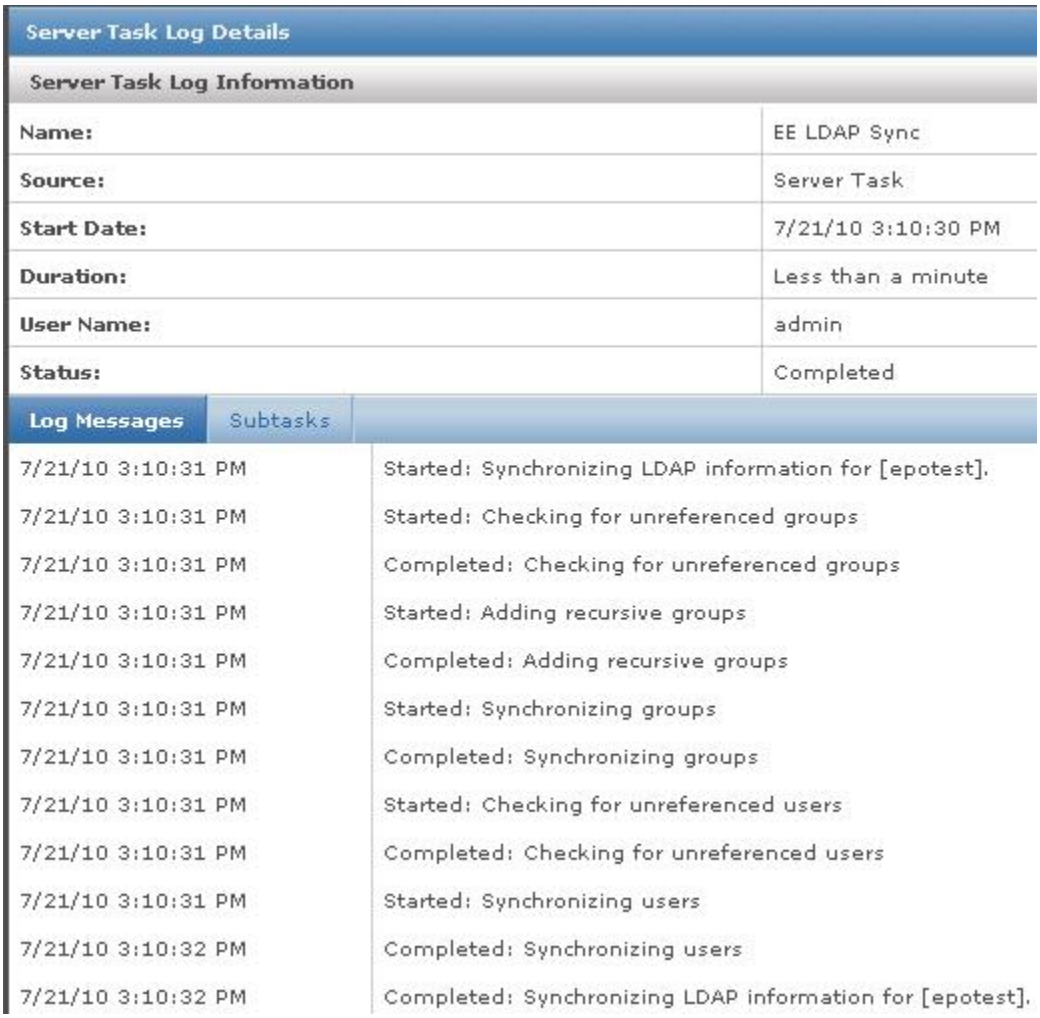
data in the database; therefore, you can remove the certificate query from **EE LDAP Server User/Group Synchronization** while using the Password only token.

NOTE: If the attribute value used for **User Name** or **Display Name** is not set in the LDAP server for any user, then EEPC uses the attribute distinguished name for that particular object.

NOTE: After changing the attribute value for any of the fields, the **EE LDAP Server User/Group Synchronization** task needs to be run, to ensure the ePO database is updated with the new values.

### EE LDAP Server User/Group Synchronization task log

The administrator can also view a log of this particular server task by double clicking the particular server task on the **Server Task Log** page in ePO. This log displays only a high level information about the users, groups or OUs, and not the detailed log; however, when an LDAP user assigned to **EE: Users** is deleted/disabled from the LDAP server, then the **EE LDAP Server User/Group Synchronization** task log will show the user information of the removed user account.



**Server Task Log Details**

**Server Task Log Information**

| | |
|---|---|
| **Name:** | EE LDAP Sync |
| **Source:** | Server Task |
| **Start Date:** | 7/21/10 3:10:30 PM |
| **Duration:** | Less than a minute |
| **User Name:** | admin |
| **Status:** | Completed |

**Log Messages** | Subtasks

| | |
|---|---|
| 7/21/10 3:10:31 PM | Started: Synchronizing LDAP information for [epotest]. |
| 7/21/10 3:10:31 PM | Started: Checking for unreferenced groups |
| 7/21/10 3:10:31 PM | Completed: Checking for unreferenced groups |
| 7/21/10 3:10:31 PM | Started: Adding recursive groups |
| 7/21/10 3:10:31 PM | Completed: Adding recursive groups |
| 7/21/10 3:10:31 PM | Started: Synchronizing groups |
| 7/21/10 3:10:31 PM | Completed: Synchronizing groups |
| 7/21/10 3:10:31 PM | Started: Checking for unreferenced users |
| 7/21/10 3:10:31 PM | Completed: Checking for unreferenced users |
| 7/21/10 3:10:31 PM | Started: Synchronizing users |
| 7/21/10 3:10:32 PM | Completed: Synchronizing users |
| 7/21/10 3:10:32 PM | Completed: Synchronizing LDAP information for [epotest]. |

Figure 5: Server Task Log

# Recommended Product Setting Policy

The Product Setting Policy controls the behavior of the EEPC 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 Setting Policies by navigating through **Menu** | **Policy** | **Policy Catalog**, then selecting **Endpoint Encryption 1.0.2** from the **Product** drop-down list. Select **Product Settings** from the **Category** drop-down list. Locate the **My Default** policy and click **Edit Settings**. Refer to Endpoint Encryption 1.0.0 Product Guide for explanation on individual policy setting.

## Recommended Product Setting Policies

| Policy Options | Recommendations |
|---|---|
| **General Tab** | • **Enable Policy** - Leave this option checked (enabled). This policy should be enabled to activate EEPC on the client. This option needs to be disabled to uninstall EEPC from the client. |
| **Encryption Tab** | • **Encrypt** - **All Disks** is a recommended option. (**None** option does not initiate the encryption)<br>• **Encryption Provider Priority** - PC Software |
| **Log On Tab** | • **Enable Automatic Booting** - Leave this option unchecked (disabled). If you enable this feature, the client system will not have the Pre-Boot Authentication. This is normally referred as Autoboot mode. It could be useful to enable this option when the administrator needs to manage the autobooting scenarios. There are multiple scenarios where you can have this option enabled or disabled, however, it is the responsibility of the administrator to decide on when to enable or disable this option.<br>• **Log on Message** - This could be an appropriate place to display your organization's legal disclaimer or any other appropriate messages.<br>TIP: For a pilot phase, you can have your administrator or helpdesk phone number here.<br>• **Do not display previous user name at log on** - Leave this option checked (enabled).<br>• **Always display on screen keyboard** - Leave this option unchecked (disabled).<br>• **Add local domain users** - Leave this option checked (enabled) ( This works only with Active Directory). This option adds the previously/currently logged in domain users to the client system. If this is enabled, the EEAgent queries the system for the domain users that have logged on to the client. EEAgent will then send the collected data to the ePO server using data channels of McAfee Agent 4.5.0. The users will then be added to EEPC users in ePO.<br>• **Enable SSO** - Leave this option checked (enabled).<br>  • **Must match user name** - Leave this option checked (enabled).<br>  • **Using smart card PIN** - Not Applicable.<br>  • **Synchronize Endpoint Encryption Password with Windows** - Leave this option checked (enabled). |

| Policy Options | Recommendations |
|---|---|
| | • **Allow user to cancel SSO** - Not Applicable.<br>• **Require Endpoint Encryption logon** - Leave this option checked (enabled).<br>• **Lock workstation when inactive** - Leave this option unchecked (disabled). |
| **Recovery Tab** | • **Enabled** - Leave this option checked (enabled). This is enabled by default to ensure that the recovery is possible at any stage of the EEPC management.<br>• **Key size** - Low. This refers to a recovery key size that creates a short Response Code for the recovery.<br>• **Message** - You could use this option to display your helpdesk phone number or instruct the user to use the self recovery option. |
| **Boot Options Tab** | • **Enable Boot Manager** - Leave this option unchecked (disabled).<br>• **Always enable Pre-Boot USB support** - Leave this option checked only when needed. (enabled).<br>• **Always enable Pre-Boot PCMCIA support** - Leave this option unchecked (disabled).<br>• **Graphics mode** - Automatic. |
| **Theme Tab** | It is better to have the default option enabled as it is simple to deploy and maange. |
| **Encryption Providers Tab** | • **User compatible MBR** - Leave this option unchecked (disabled).<br>• **Fix OS boot record sides** - Leave this option unchecked (disabled).<br>• **Use Windows system drive as boot drive** - Leave this option unchecked (disabled). |

# Recommended User Based Policy Settings

The User Based Policy controls the parameters for EEPC user accounts. For example, it contains the options for selecting a token type (for example: password, smartcard and so on) and password content rules. You can configure the User Based Policies by navigating through **Menu** | **Policy** | **Policy Catalog**, then selecting **Endpoint Encryption 1.0.2** from the **Product** drop-down list. Select **User Based Policies** from the **Category** drop-down list. Locate the **My Default** policy and click **Edit Settings**. Refer to Endpoint Encryption 1.0.0 Product Guide for explanation on individual policy setting.

NOTE: It is always better to configure the User Based Policies in the system level or branch level if possible, rather than assigning it using the Policy Assignment Rule. However, you can use the Policy Assignment Rule option, if required, for assigning different policies to different users.

## Recommended User Based Policy Settings

| Policy Options | Recommendations |
|---|---|
| **Authentication Tab** | • **Token type**: Select **Password only**. There are a number of other tokens that can be effectively used |

| Policy Options | Recommendations |
|---|---|
| | for your authentication as required. However, the Password only token is as strong as any other token that you could configure.<br>• **Certificate rule**<br>  • **Provide LDAP user certificate** - Leave this option checked (enabled).<br>  • **Use latest certificate** – Leave this option checked (enabled).<br>NOTE: The **Certificate rule** options will not be active if **Password only** token is selected.<br>• **Logon hours** - You could enable and set the logon day and time-line as required. It is better to have this disabled if you do not have a specific requirement. |
| **Password Tab** | • **Change Default Password** - Leave this option unchecked (disabled) - This leaves the default password as 12345 for all new users. All new users will be prompted to change the default password during user initialization.<br>• **Password Change** - Disable all of these settings as you would be using SSO and don't want to cause conflict with Windows password requirements.<br>  • **Enable Password history** - Leave this option unchecked (disabled).<br>  • **Prevent change** - Leave this option unchecked (disabled).<br>  • **Require change after _____ days (1-366)** - Leave this option unchecked (disabled).<br>  • **Warn user _____ days before password expiry (0-30)** -This is disabled by default when you disable the **Require change after _____ days (1-366)** option.<br>• **Incorrect Passwords**<br>  • **Timeout password entry after ----invalid attempts (3-20)** - Set required number of password invalid attempts.<br>  • **Maximum disable time ------ minutes (1-64)** - This is disabled by default when you disable the **Timeout password** option.<br>  • **Invalidate password after ------ invalid attempts** - Leave this option checked (enabled). |
| **Password Content Rules Tab** | • **Password length** - Use default.<br>• **Enforce password content** - Use default.<br>• **Password content restrictions** - Use default or enable restrictions for better password strength. |
| **Self-Recovery Tab** | • **Enable self-recovery** - Leave this option checked (enabled).<br>• **Invalidate self recovery after No. of invalid attempts**: Enable and set the number of attempts to a number that will not abruptly lock out the Self Recovery. |

| Policy Options | Recommendations |
|---|---|
| | • **Questions to be answered** - Can be set to 3. This can give you the required security without giving the user a lot of pain of keying in the characters. However, it is up to the administrator to decide this number depending on the requirement.<br>• **Logons before forcing user to set answers** - Set this to 0. This will ensure users to set the answers during the user initialization.<br>• **Questions** - Use the default ones or configure the questions as required. |

# Phased deployment strategies

EEPC 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 Pre-Boot Authentication will create challenges during the EEPC deployment. For a safe and smooth deployment and activation process, you can easily create different sets of EEPC 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 which will enable the encryption and the Pre-Boot Authentication.

**High level process**

- After deploying the EEPC packages, create an EEPC 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** | **Endpoint Encryption**.
  - Enable **Add local domain users** option under **Log On tab** | **Endpoint Encryption**.
- Enforce this policy to the client systems. This will now get the Pre-Boot Authentication out of the way on subsequent reboot.
- You can now configure the second set of policy with the required encryption option other than **None** and autobooting enabled.
- Use the automatic booting policy as the default. In this mode, the client will capture all Windows domain accounts that access the system. These accounts will be added as valid Pre-Boot enabled accounts to be used in the Pre-Boot environment.
- Create a query in ePO to find all systems that need to stop autobooting and start using Pre-Boot Authentication.
- Create a server task in ePO to apply the policy with Pre-Boot Authentication to all required systems.
- The systems will start with Pre-Boot Authentication as and when the new policy is received.

This phased deployment will temporarily enable automatic booting and then automatically enable the Pre-Boot Authentication policy after the set number of days. This gets Pre-Boot Authentication out of the way temporarily, however, it ensures that EEPC gets activated when

the system is in the field. It also ensures that the end user's account gets added as a valid Pre-Boot account.

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

## Auto booting

Auto Booting (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 will automatically authenticate without user or administrator intervention. The administrator can define a window of time-line during which autobooting remains active.

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

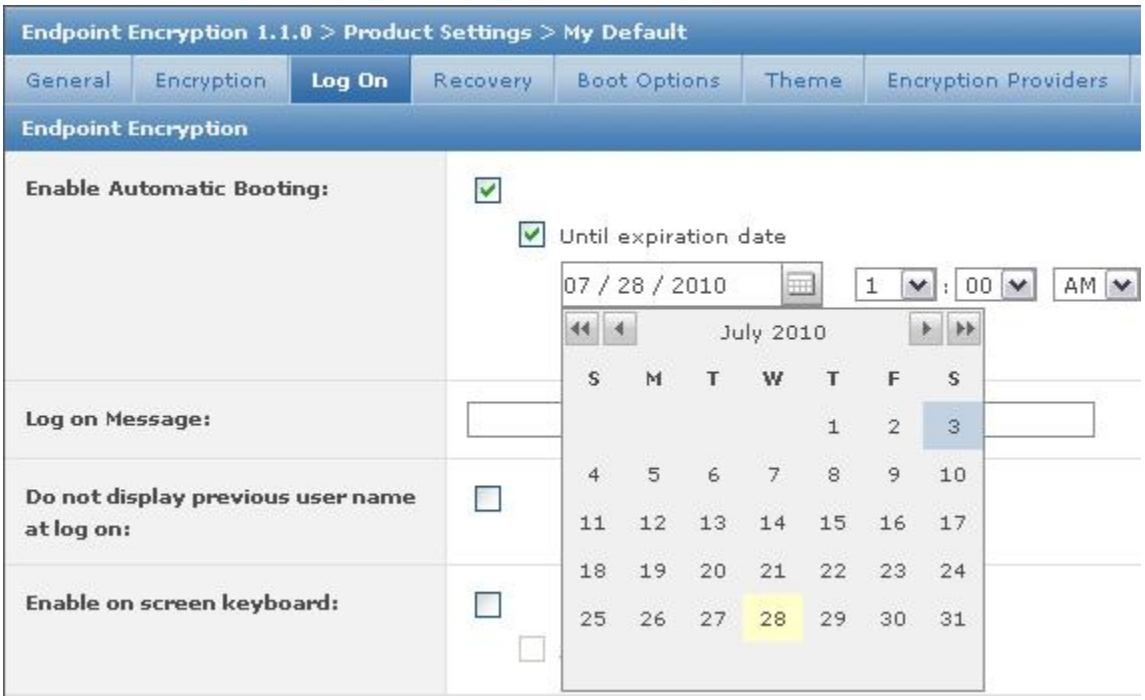



Figure 6: Configure autobooting

NOTE: Since this policy setting temporarily bypasses the normal logon process for EEPC installed systems, computers receiving this policy will be vulnerable while Autobooting remains active. To minimize the risk, make certain that you carefully review the inclusive dates and times that Autobooting will remain active before deploying this policy.

# Deployment and activation

**Troubleshooting why the Windows operating system will not start; encrypted systems do not allow access to the OS until Pre-Boot authentication is completed:**

Administrators should be mindful that fixing certain Windows problems on an encrypted system may require extra caution in the event that the registry must be edited or a driver should be modified.

Traditional recovery procedures will also change on a system encrypted with EEPC 6.0 Patch 2. For example, the entire disk is encrypted which means the file systems and disks are accessible only when the Pre-Boot authentication is complete.

The EETech User Guide provides instructions on how to create a customized pre-installation disk (EETech Windows PE V1) with the EEPC drivers loaded. This disk allows the administrator to access an encrypted hard drive to update the drivers or the registry.

**Booting the EEPC installed client will require the physical presence of the client user to supply credentials at EEPC Pre-Boot Authentication page.**

To gain access to an encrypted PC, the user must always enter credentials at the Pre-boot authentication 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/service packs to client systems as the system will inevitably require reboot after install.

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

**Contents**



# Basic preparations and recommendations

The following recommendations will ensure your data is protected during and after the encryption process.

### As with any roll out and deployment, it is advisable to back up the system before you encrypt it, and perform regular backups

It is good practice to back up the system before installing EEPC to ensure data is not lost in the unlikely event a problem occurs. The EETech recovery tools can also be used to decrypt and recover unbootable disks should something occur. Please refer to the EETech User Guide for more information.

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

Hard disks that are damaged, or have a high number of undiscovered bad sectors, may fail during the full disk encryption process. Run a CHKDSK/r prior to installing EEPC to ensure the disk is healthy.

### Understand the supported tokens/readers for EEPC

Ensure that the supported reader drivers are installed in your client system before trying to install Endpoint Encryption for PC. The supported tokens and readers are listed in the EEPC 6.0 Patch 2 Release Notes.

### 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 EEPC. Administrators are advised to:

- create and test the customized EETech Windows PE V1 Disk with EEPC drivers installed
- create and test an EETech Standalone Boot disk.

### Run a pilot to test software compatibility

It is recommended you run a pilot to test EEPC on a client PC. This will ensure that EEPC is not in conflict with any encryption software on the client computers before rolling out to a large number of clients.

This is particularly useful in environments that use a standardized client image.

Administrators should also run performance testing during the pilot.

McAfee professionals did not come across any performance related issues with EEPC during our own testing, however, this may vary depending upon the processor, memory, and drivers. In one specific case, a 50GB system with two disks, took 2-3 hours to encrypt.

### Do a phased deployment

An occasion may arise when the Pre-Boot Authentication creates challenges during deployment. For a successful deployment and activation, you can create a different set of EEPC system policies and deploy in phases enabling the **None** option under **Encrypt** and **Enable Automatic Booting** option under **Log on** tab. Create deployment tasks and deploy EEPC to systems arranged in groups or batches in the **System Tree**. You can also base it on a specific tag in ePO.

### Add user to the client system

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

### Perform disk recovery on decrypted disks

Where possible, as a best practice, if you need to perform any disk recovery activities on a disk protected with McAfee EEPC, it is recommended that you first decrypt the disk. Please refer to the McAfee Endpoint Encryption Product Guide and the McAfee EETech User Guide for the procedures to decrypt the EEPC installed disk.

### Educate the client user the Password/Token/PIN secrecy

Educate your client users to understand 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 may have been compromised.

# High level process of the installation

This section lists the steps and considerations involved in EEPC deployment and activation. This procedure is explained in more detail in the Endpoint Encryption 1.0.0 Product Guide and the EEPC Quick Start Guide.

### Before you begin

1. Download the EEPC v6.0 Patch 2 product.
2. Ensure that your ePO Server version is at least 4.5.0 Patch 1, upgrade to ePO 4.5.0 Patch 3 if possible.
3. Ensure that your McAfee Agent version is at least 4.5.0.
4. Note the hostname or IP address of an Active Directory Domain Controller/LDAP Server.
5. Read the EEPC v6.0 Patch 2 Release Notes for known issues, token/reader details, and other important information.
6. Consider engaging McAfee Support to assist in your production installation.

### Task

1. Install the EEPC extensions in to ePO 4.5.0. Check for the correct and latest version of the extension. Install EEAdmin extension first then EEPC.
2. Check in the EEPC packages in to ePO 4.5.0. Check for the correct and latest version of the EEAdmin and EEPC packages.
3. Register your LDAP Server. Check for the correct domain and Server IP address of your LDAP server configured.
4. Create **EE LDAP Server User/Group Synchronization** task and schedule it to run. Check for the correct format of the user attributes while scheduling the task.
5. Modify the Product Setting and User Based Policies. Plan and verify the policy settings for your organization's requirements.
6. Add a user to the client. Decide whether to add the users manually in ePO or to add users using the **Add local domain user** option present under the **Product Setting Policy**. At least one user must have been assigned to the client in order to activate EEPC on it.

7 Create a client task to deploy the EEPC components to the client systems. Ensure to deploy the packages in the right order.

8 Test for successful deployment, activation and encryption on targeted endpoints. Ensure to make use of the reporting facilities available in the ePO management software.

# Client task to deploy the EEAgent and EEPC packages

It is a good idea to create new system group in ePO for EEPC deployment. Name it EEPC Test Systems or EEPC 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 ePO

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

NOTE: This option works only with Active Directory.

NOTE: Refer to ePolicy Orchestrator 4.5 Installation/Product Guide for detailed procedures on how to import systems from Active Directory to ePO.

## Order of the EEAgent and EEPC deployment

There is no hard and fast rule to have two different tasks for the product deployment. You can create one single task to deploy both packages, but don't forget that they need to be deployed in the right order. The EEAgent package should be followed by the EEPC package. If you configure to deploy the EEPC package followed by the EEAgent package then the client system will restart in the middle as required and the EEAgent would never get deployed.

So, it is always better to execute the deployment using a single task wherein you need to deploy the EEAgent package first then the EEPC package.

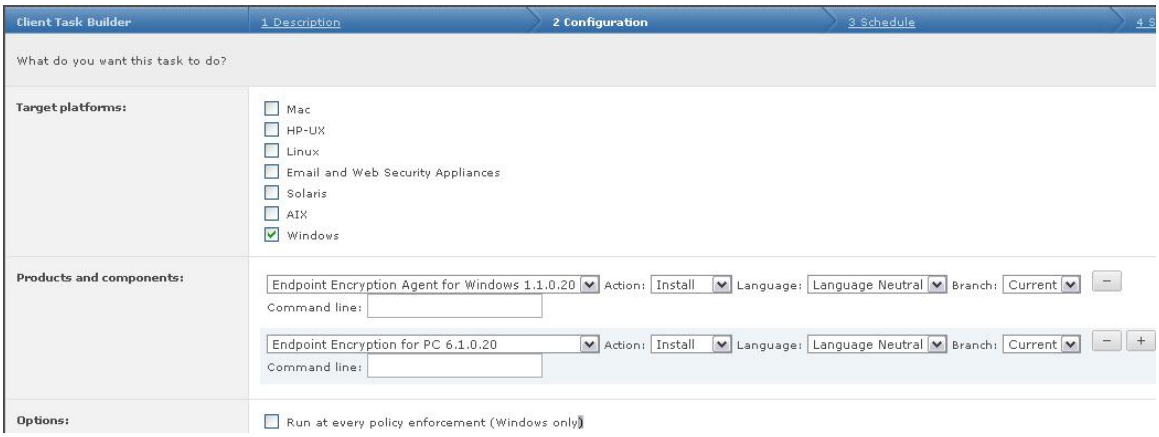



Figure 7: EEAgent and EEPC packages deployment

You can also create two separate tasks to deploy the packages, providing you wait for the first deployment (EEAgent) to complete before deploying the second package. You can also verify

the completion of the EEAgent deployment, before deploying the EEPC package, by creating and executing a customized query from the ePO server. If the EEPC package is deployed first, you can run the EEAgent task and deploy it later.

### End user experience

The deployment task will push both the Endpoint Encryption Agent and the EEPC components to the selected systems. The install is silent, however, the user will be prompted to restart the client when the EEPC component install is complete. It is vital that the user restart the client PC when prompted. If this does not happen, EEPC will not activate.

# Add group users

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

NOTE: If you choose to add a Group or an OU, you will not see the individual user names. Instead, you will see the entire DN of the Group or OU.

NOTE: All EEPC user accounts, even Group User, accounts get 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 for the first time you login with these user accounts.

## Users

To access the data on an encrypted computer, the user must go through the Pre-Boot Authentication. If the **Enable Auto Booting** option is not enabled then the client user is presented with the Pre-Boot Authentication screen when the system is restarted after activating EEPC. During the first Pre-Boot after activation, the user needs to initialize the user account with the default password and enroll for the self recovery if the same has been enabled in the policy.

During the initialization process, users set their Pre-Boot credentials to access Windows. Only the assigned users from a registered LDAP server will be accepted by EEPC Pre-Boot Authentication.

NOTE: At least one EEPC user is required to be assigned to EEPC on each client.

## 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 ePO console. This option can be enabled as when needed through the Endpoint Encryption Product Settings Policies (**Menu** | **Policy** | **Policy Catalog** | **Endpoint Encryption 1.0.2 (Product Settings)** | **Log on tab** | **Add local domain users**).

When enabled, the EEAgent queries the client system for the currently/previously logged in domain users to the client. The EEAgent will then send the collected data to the ePO Server using McAfee Agent 4.5.0 data channels. These user will then be assigned to the client system.

NOTE: It is a good practice to have this option enabled, so that you will always be able to authenticate to the Pre-Boot of the client without having to manually assign the users to the

client system in the ePO console. However, this is a responsibility of the administrator to decide whether this is required or not depending on corporate requirements.

### Prerequisites

The following prerequisites are required to add the local domain users to the Endpoint Encryption client systems.

- McAfee Agent 4.5.0 or above has been deployed.
- McAfee **EEAgent for Windows** package has been deployed to the required client systems.
- McAfee **Endpoint Encryption for PC** package has been deployed to the required client systems.
- Registered Active Directory should have been added and configured correctly.

  NOTE: Be advised that the **Add local domain users** option is not supported with OpenLDAP Server.

- An automated **EE LDAP Server User/Group Synchronization** task should have been scheduled and run.
  - This task is used to map Active Directory attributes to the Endpoint Encryption settings. This is required for every Registered LDAP server that is to be used with Endpoint Encryption.
- Client systems should be using 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-Server communication. If this option is enabled in the policy settings, the EEAgent queries the client system for the domain users who have logged on to the client. The EEAgent will then send the collected data to the ePO server using McAfee Agent 4.5.0 data channels.

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

### At the server side

When the EE Admin receives a data channel message for adding local domain users, it executes the following steps.

- It attempts to find the domain name that the user belongs to. This is done by querying the Registered Active Directory that has been configured with the automated **EE LDAP Server User/Group Synchronization** 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 then it will be 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** | **Endpoint Encryption** | **View Users**.

The **Add local domain users** can also be very useful in activating EEPC on the client without adding the users manually.

# EEPC activation sequence

When EEAgent and EEPC have been successfully deployed, the users will be prompted to restart their system.

NOTE: The restart can be cancelled, however, EEPC will not become active on the client until the restart has occurred. Therefore, the restart is essential for the activation of EEPC on the client.

### Endpoint Encryption Status

System restarts as initiated. You will not yet see the Pre-Boot Authentication page as the EEPC software is not yet active on the client. However, you should now be able to see the new option **Quick Settings** and sub-option **Show Endpoint Encryption Status** in the McAfee System tray icon.

### EEAgent synchronization with ePO Server

The status in the **Show Endpoint Encryption Status** sub-menu will show as **Inactive** until the EEAgent synchronizes with the ePO server. This is referred to as an ASCI event.

It can be manually triggered on the client by opening the **McAfee Agent Status Monitor** and clicking **Collect and Send Props**. It can also be triggered from the ePO server by doing an Agent wake-up call, otherwise, you will need to wait for the scheduled ASCI to occur (the default is 60 minutes). After an ASCI, the status will switch to **Active** and encryption will start based on the policy set. This ensures that the keys are backed up in ePO, so that they can be used for recovery.

### 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 will be completely transparent to the end user.

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

### Pre-Boot Authentication

When the client system is restarted and EEPC is first activated, the user should log in with the username that matches the user attribute set in the **LDAP User/Group Synchronization** task and the default password of 12345 (this is the McAfee default password which can be changed in the User Based Policy) in the Pre-Boot Authentication page. The user is then prompted to change this password and enroll for the self-recovery based on the policy set.

NOTE:

It is advisable to change the default password and enforce policies with stronger passwords.

### Single Sign On (SSO)

The system then boots to Windows. This first boot establishes SSO (if it has been enabled). On future restarts, the user will login to the Pre-Boot Authentication only. Once authenticated, SSO will auto-login to Windows.

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

NOTE: When the **Must match username** option is enabled, both the EEPC 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.

NOTE: When the **Synchronize Endpoint Encryption password with Windows** option is enabled, the EEPC password is reset to the Windows password, however, be aware if the **Password history** option is enabled, and the EEPC password is same as the Windows password, then synchronization will not occur.

NOTE: On changing the EEPC password, the synchronization will not be reset. Synchronization of the password will occur only when there is a change in the Windows password.

# Activating EEPC on client using Add local domain users without adding users in ePO

Using the **Add local domain users** option, you can activate EEPC on client systems without manually adding users in ePO.

1. Configure the **Product Setting Policy** with **Add local domain users** option enabled.
2. Log in to the client system. After the Agent Server Communication Interval, the **Add local domain users** option adds the previously/currently logged in domain users to the client system.
3. EEPC is activated in the client system during the next ASCI. You can now restart the client to log in using the Pre-Boot Authentication page.

   NOTE: This option provides automatic user assignment, which helps the administrators in not having to manually assign users to client systems in the ePO console. The recommended best practice is to manually assign at least one user to all systems to ensure that EEPC activation happens successfully 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 would be to manually add a group of support users to all systems, then activate EEPC using the **Add local domain users** option. You can remove these users at a later stage after completing the deployment.

# Operations and maintenance

### Managing servers and client systems

Managing your systems in different batches, branches or groups will make a great impact for EEPC deployment. It is a good practice to arrange the systems in ePO in department level or batch level, then deploy the product to these batches one by one.

Client deployment in batches with an appreciable number of systems is a good practice by itself.

NOTE: Do not try to create the EEPC deployment task at the root level of your system tree and activate it. It is a good practice to deploy EEPC to the systems at the sub-level branches.

NOTE: It is better not to deploy EEPC to the server systems that host your ePO servers.

NOTE: Secure your ePO server and database system in the most secured location and keep it accessible for authorized personnel only.

### Contents



# How does disabling/deleting a user in Active Directory affect the EEPC user

Every user account will have an objectGUID in LDAP and an entryUUID in Open LDAP. If a user account is deleted from LDAP and another is created with the same user name, this new user account will be a different entity. This is because the objectGUID will have changed for the new user.

### To disable a user in LDAP

You must first disable or delete the user in LDAP, then run the **EE LDAP Server User/Group Synchronization** task and send an Agent wake-up call. The user will disappear from EE Users list when the next **EE LDAP Server User/Group Synchronization** task is complete.

The ePO Server Setting option **If user disable in directory** within **Server Settings** | **Edit** | **General** can be configured to disable, delete or ignore the user if the user has been disabled in the LDAP Server.

### What if a user is disabled from LDAP?

The ePO Server Setting option **If user disable in directory** within **Server Settings** | **Edit** | **General** can be configured to disable, delete or ignore the user if the user has been disabled in the LDAP Server.

If a user account which has been initialized on the client system, and is later removed from LDAP, then it will be automatically deleted/ignored from the client as per the setting configured in the **Server Settings**. To authenticate through the client PBA with a disabled or deleted LDAP user name, you should once again add the user to the LDAP and initialize the same user name on the client with the default password.

This does not remove the users from the EEUsers list in ePO, however, it removes/deletes/ignores the users from the client system based on the option set in the Server Settings.

### Is it possible to just disable the EEPC user when removed from LDAP?

It is not possible to disable an EEPC user when it has been removed from LDAP. The user is removed from the EE Users list if deleted in LDAP during the next **EE LDAP Server User/Group Synchronization** task.

### What if the EEPC user assignment is deleted/removed?

If the EEPC user assignment is deleted from a system, the user may still be assigned back to the client system if the **Add local domain users** option is enabled in the **Product Setting Policy**. For this to work, the user must have logged into Windows at least once and the domain to which client system is connected should have been registered in ePO. You can also manually add users using **Add EE: Users** option in ePO.

# 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 ePO database to be used for client recovery when required.

### What happens to Machine Keys when an EEPC-active system is re-imaged?

All existing data of the system is lost and hence the machine Key is lost when an EEPC-active system is re-imaged.

### What happens to the Machine Key when you delete an EEPC-active system from ePO?

The Machine Key remains in the ePO database; however, the key association with the client system is lost when the client system is deleted from ePO. When the client system reports back to ePO during the next ASCI, it will appear 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 login, or, enable the **Add local domain user** option in the **Product Setting Policy**. Also, the administrator must configure the required policies in ePO.

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

- 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, ePO sends a Machine Key request. If the user is logged on to the client system, a data channel communication between the client and the ePO server ensures the Machine Key is updated in ePO and the users are updated on the client. Thereafter, the Machine Key will be available and admin recovery and policy enforcement will work.

- The users are assigned to the client system. Therefore, these users can straight away log in to the client system.

You cannot log in to the client system before a proper data channel communication occurs. In this situation, the re-association of the Machine Key can be performed using EETools . The recovery key will also be available; this can be used with the EETech tool to recover the client system.

For EETool details and procedures, refer to HotFix Release Notes (Readme_HF 582699).

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

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

When a transferred client system reports back to ePO during the next ASCI, it will appear as a new node and will therefore not have any users assigned to it. The administrator must assign users to allow login, or, enable the **Add local domain user** option in the **Product Setting Policy**. The administrator must also configure the required policies in ePO.

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

- 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, ePO sends a Machine Key request. If the user is logged on to the client system, a data channel communication between the client and the ePO server ensures the Machine Key is updated in ePO and the users are updated on the client. Thereafter, the Machine Key will be available and admin recovery and policy enforcement will work.

- The users are assigned to the client system. Therefore, these users can straight away log in to the client system.

You cannot log in to the client system before a proper data channel communication occurs. In this situation, the re-association of the Machine Key can be performed using EETools . The recovery key will also be available; this can be used with the EETech tool to recover the client system.

For EETool details and procedures, refer to HotFix Release Notes (Readme_HF 582699).

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

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

# Configuring role based access control for managing EEPC

ePO administrator rights management determines what administrators can perform while managing the Endpoint Encryption software. The administrator can set up Endpoint Encryption specific permission sets to different users in ePO. The Endpoint Encryption Administrator extension (EEADMIN.ZIP) enables ePO administrators to control Endpoint Encryption Systems that are managed through ePO.

The ePO administrator for EEPC will be able to:

- Manage Endpoint Encryption Policies
- Manage Endpoint Encryption Users
- Manage Endpoint Encryption Server Settings
- Run queries to view Endpoint Encryption systems current status
- View client system audits
- View ePO user audits
- Manage Endpoint Encryption Providers

Administrative roles can be configured and implemented using the **Endpoint Encryption Permission Sets** option present in ePO. It is possible to configure a number of admin roles using this option. For example, you can create admin roles such as:

- **Endpoint Encryption Administrator**: User accounts in this level have full control of EEPC, but cannot manage any other software in ePO.
- **Endpoint Encryption Helpdesk**: User accounts in this level can do EEPC password resets only.
- **Endpoint Encryption Engineer**: User accounts in this level can do password resets as well as export recovery files to be used with EE Tech tool.
- **Endpoint Encryption Auditor**: User accounts in this level can view EEPC reports only.

### Before you begin

- Ensure that your LDAP server is configured and registered in ePO.
- Ensure you schedule and run the **EE LDAP Server User/Group Synchronization** task.
- Ensure you enable the **Active Directory User Login** option in ePO. 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 **Endpoint Encryption Permission Sets** to different users.


Figure 8: Endpoint Encryption permission sets

To verify the configured permission sets, log off from ePO, then log in with a user account that belongs to any one of the new roles.

NOTE: Use correct format of the user name (domain\username) when logging in to ePO.

# EEPC 6.0 Patch 2 Scalability

EEPC v6.0 Patch 2 uses ePO Data Channel architecture for EEPC client-server communication, including the delivery of themes, policy, and user token data.

Use the following components for scalability:

- ePO 4.5 Patch 3 Hotfix 1.

  EEPC 6.0 Patch 2

The following will help improve scalability:

- Longer ASCI interval
- Password only deployments should remove certificate query from **EE LDAP User/Group Synchronization** task.

  NOTE: The User Certificate attribute is used by the ePO Server to determine which certificate should be sent from 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 **EE LDAP Server User/Group Synchronization** while using the Password only token.

The following will degrade scalability:

- Policy Assignment Rules

  The policy assignment rules should be setup 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 satisfied defines which UBP is assigned to the user.

  Given that ePO needs to send all users down to a client during activation, each user will need 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 allow this to be done.

- Large number of user per machine (>20)
- Deployment of unnecessary languages (recovery questions)

Evidence suggests that scalability with ePO 4.5 Patch 3 is around

- 10,000 with 4 hours ASCI
- 15,000 with 6 hours ASCI
- 25,000 with 10 hours ASCI

# Use ePO to report client status

McAfee ePolicy Orchestrator provides comprehensive management and reporting tools for EEPC. 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 Endpoint Encryption 1.0.0 Product Guide.

When the EEAgent has been deployed to the client systems and they are successfully managed by ePO, then any of the following queries can be used to retrieve data from your estate:

- EE: Disk Status
- EE: Encryption Provider
- IEE: nstalled Version
- EE: Users
- Product Client Events
- EE: Volume Status

**Contents**



# Track the progress of the deployment and encryption status

The progress of the EEPC deployment and the number of encrypted systems can be easily determined by running the Endpoint Encryption query under **Menu** | **Reporting** | **Queries** | **Endpoint Encryption** | **EE: Disk Status**. This will report the crypt state for all disks on systems that have the EEAgent installed.

You can also find the systems that don't have the EEAgent installed by running the query **Menu** | **Reporting** | **Queries** | **Endpoint Encryption** | **EE: Encryption Provider**.

# Reporting encryption status from 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

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

- Log in to ePO as an administrator.
- Locate the system in the System Tree.
- View system properties.
- Drill-down to encryption properties.
- Show encryption status

### Finding the user's system in 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 ePO and view its properties. You can use the reports to know the encryption status of the system.

# Index

## S



## T



## U