Migration Guide

McAfee Drive Encryption 7.1.0
For use with ePolicy Orchestrator 4.6.7 and 5.1.0 Software
COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>5</td>
</tr>
<tr>
<td>- About this guide</td>
<td>5</td>
</tr>
<tr>
<td>- Audience</td>
<td>5</td>
</tr>
<tr>
<td>- Conventions</td>
<td>5</td>
</tr>
<tr>
<td>- What's in this guide</td>
<td>6</td>
</tr>
<tr>
<td>- Find product documentation</td>
<td>6</td>
</tr>
<tr>
<td>1  Introduction</td>
<td>7</td>
</tr>
<tr>
<td>- Using this guide</td>
<td>8</td>
</tr>
<tr>
<td>- User management through User Directory</td>
<td>8</td>
</tr>
<tr>
<td>- Best practices</td>
<td>8</td>
</tr>
<tr>
<td>- Requirements</td>
<td>10</td>
</tr>
<tr>
<td>2  Migrating from EEPC 5.x.x to Drive Encryption 7.1 without the migration tool</td>
<td>11</td>
</tr>
<tr>
<td>- Migrate to Drive Encryption 7.1 without the migration tool</td>
<td>11</td>
</tr>
<tr>
<td>3  Migrating from EEPC 5.x.x to Drive Encryption 7.1 with the migration tool</td>
<td>13</td>
</tr>
<tr>
<td>- Overview of the migration process</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>- Exporting user and user assignments from the EEPC 5.x.x database</td>
</tr>
<tr>
<td></td>
<td>- Importing users and user assignments into Drive Encryption 7.1</td>
</tr>
<tr>
<td></td>
<td>- Migrating to Drive Encryption 7.1</td>
</tr>
<tr>
<td>4  Managing Drive Encryption migration reports</td>
<td>27</td>
</tr>
<tr>
<td>- Queries as dashboard monitors</td>
<td>27</td>
</tr>
<tr>
<td>- View the Drive Encryption migration reports</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Migration checklist</td>
</tr>
<tr>
<td></td>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>Index</td>
<td>33</td>
</tr>
</tbody>
</table>
Preface

This guide provides the information on migrating to McAfee® Drive Encryption 7.1 from the previous versions.

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.
What's in this guide
This guide is organized to help you find the information you need.

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

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

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1. Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Select a product, then select a version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
McAfee® Drive Encryption 7.1 has an improved architecture and interface. Due to these improvements, some features and settings from earlier versions of the product are now handled differently.

- In this guide, EEPC 5.x.x refers to EEPC 5.2.6 or later versions.
- EEPC 7.0.x refers to EEPC 7.0, 7.0 Patch 1, 7.0 patch 2, and 7.0 Patch 3.

The McAfee Drive Encryption migration process consists of the following tasks:

- Export the user assignments from the 5.x.x database
- Import the user assignments into the McAfee® ePolicy Orchestrator® (McAfee ePO™) server that has Drive Encryption 7.1
- Export and import the 5.x.x password token when it is available and assign it to Drive Encryption 7.1 users

Drive Encryption 7.1 user names are obtained from Active Directory or User Directory. You can also create and manage users using User Directory, which removes the dependency on LDAP server. For more information, see the User management through User Directory section.

- Migrate supported tokens from EEPC 5.x.x to Drive Encryption 7.1, this may include the Single-Sign-On (SSO) and Self-recovery information
- Export the audit information
- Import the audit information
- Migrate the client system from EEPC 5.x.x
- Upgrade the client system from EEPC 7.0.x

Make sure that the Active Directory server used to add the Drive Encryption 7.1 users contains the same user information that you want to import from 5.x.x.

Contents
- Using this guide
- User management through User Directory
- Best practices
- Requirements
Using this guide

The information in this guide helps you to migrate EEPC 5.x.x systems into Drive Encryption 7.1. This guide helps you to:

- Understand the differences between the EEPC versions
- Export the combination of user groups and users from the 5.x.x database
- Import the exported users, password token, SSO, Self-recovery and audit details into McAfee ePO
- Re-create any settings that are not migrated
- Upgrade the client systems to Drive Encryption 7.1

User management through User Directory

Drive Encryption 7.1 provides support for user management using the User Directory feature, which removes the dependency on LDAP server.

The User Directory feature utilizes the LDAPSync extension in McAfee ePO and provides user management for Drive Encryption users using the UserDirectory.zip extension. Once you install the User Directory extension into the McAfee ePO server, you can create Organizational Units (OUs) and users and manage them on the User Directory page, without requiring to register an LDAP server. This allows the EEPC 5.x.x non-LDAP users, who are not registered on LDAP server to migrate to Drive Encryption 7.1. For more information about creating Organizational Units (OU) and users, see McAfee Drive Encryption 7.1 Product Guide.

Best practices

Follow these recommendations to make the migration process easier and more effective.

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 Endpoint Encryption Manager and the McAfee ePO server.

Importing the user assignments from 5.x.x database into the McAfee ePO server

- Make sure that the Active Directory server used to add the Drive Encryption 7.1 users contains the same user information that you want to import from 5.x.x.
- Make sure that you have registered an LDAP server on the McAfee ePO server before initiating the import process.

Before you begin the import process, the McAfee ePO task LDAPSync will automatically synchronize all users from all registered servers.

You can also manage users through User Directory, which removes the dependency on LDAP server. For more information, see the Import user assignments using McAfee ePO section.
• Make sure that you have added the required client systems to ePolicy Orchestrator to which you want to match and assign the users.

• Analyze the import preview results and perform manual assignments where automatic assignments have not been possible.

• Do not navigate away or close 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, you can see the message "Please wait, assigning users to systems" in the top left of the McAfee ePO page.

• After you import the users from 5.x.x database into the McAfee ePO server, check that the users, password token, SSO, Self-recovery, and the audit details are imported as you expected.

• Conduct a policy review after the import process. If you need your EEPC 5.x.x policy settings for Drive Encryption 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.

Migrating 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 7.1 client is not supported. Any migration of user assignments must be done on McAfee ePO before deploying Drive Encryption 7.1 to the client system.

• To migrate the client, first install the Drive Encryption Agent software package, then the Drive Encryption Windows software package.

• If the user is not initialized, initialize the user account and enroll for self-recovery after migrating the 5.x.x client.

General recommendations

• Retain the 5.x.x database for some time, so that you can access it in case of loss or theft of a device after the migration.

• Migrate only a small number of systems, for example 100 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 Pre-Boot Authentication, please be advised that the same option is now a feature in 7.1. So, make sure that you enable this policy feature (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 7.1. For detailed procedures, see McAfee Drive Encryption 7.1 Best Practices Guide.

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

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

The Enable Automatic Booting feature in Drive Encryption 7.1 doesn't require the $autoboot$ user id to be created in the Active Directory.
Requirements

This section provides the requirements for the McAfee ePO server and Drive Encryption 7.1 client. Make sure that your server and client systems meet these pre-requisites before installing Drive Encryption 7.1.

Table 1-1 System requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO server systems</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Client systems</td>
<td>• CPU: Pentium III 1 GHz or higher</td>
</tr>
<tr>
<td></td>
<td>• RAM: 512 MB minimum (1 GB recommended)</td>
</tr>
<tr>
<td></td>
<td>• Hard Disk: 200 MB minimum free disk space</td>
</tr>
</tbody>
</table>

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

Table 1-2 Software requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO</td>
<td>4.6.7 (minimum) or 5.1</td>
</tr>
<tr>
<td>McAfee Endpoint Encryption for PC and Drive Encryption</td>
<td>5.x.x (5.2.6 or later) and 7.0.x (7.0, 7.0 Patch 1, 7.0 Patch 2, or 7.0 Patch 3) and 7.1</td>
</tr>
<tr>
<td>Export/Migration tool with SbAdmDll.dll file</td>
<td>7.1</td>
</tr>
</tbody>
</table>

Table 1-3 Operating system requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO server systems</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Client systems</td>
<td>• Windows Server 2003 SP1 or later (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 (32- and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional SP3 (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista SP1 or later (32- and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 and SP1 (32- and 64-bit; not XP Mode)</td>
</tr>
<tr>
<td></td>
<td>For Opal activation, Windows 7 SP1 is required.</td>
</tr>
<tr>
<td></td>
<td>• Windows 8 and 8.1 (32- and 64-bit)</td>
</tr>
<tr>
<td></td>
<td>Drive Encryption 7.1 supports Windows 8 in BIOS (MBR) mode, and UEFI boot mode that runs only on Windows 8 logo-certified hardware.</td>
</tr>
<tr>
<td></td>
<td>Make sure to note that migrating from EEPC 5.x.x to Drive Encryption 7.1 is not supported on Windows 8 and 8.1 systems.</td>
</tr>
</tbody>
</table>
Migrating from EEPC 5.x.x to Drive Encryption 7.1 without the migration tool

This section describes how to migrate from EEPC 5.x.x to Drive Encryption 7.1 by directly assigning users to the client system or by using the product setting policy option Add Local domain users. You can directly assign users to the client system using:

• **Menu** | **Data Protection** | **Encryption Users**

• Add local domain users (add all previous and current local domain users of the system) under **Drive Encryption 7.1** | **Product Setting Policy** | **Log on (Drive Encryption)**

> Add local domain user is supported with Active Directory only.

On selecting the Add local domain users option, any domain users who have previously and are currently logged on to the client system, are able to authenticate through Pre-Boot, even if the administrator has not explicitly assigned the user to the client system.

The Add local domain users option adds the previously and currently logged on domain users to the client system. If this is enabled, the DEAgent queries the system for the domain users that have logged on to the client. The DEAgent sends the collected data to the McAfee ePO server. The collected data is a list of user names and the domain names.

See the product documentation for ePolicy Orchestrator 4.6 for steps to directly assign users to system using **Menu** | **Data Protection** | **Encryption Users**.

Migrate to Drive Encryption 7.1 without the migration tool

Use ePolicy Orchestrator to migrate from EEPC 5.x.x to Drive Encryption 7.1.

**Before you begin**

- Make sure that the client system’s domain is a registered server on the McAfee ePO server.
- Make sure that the McAfee Agent for Windows 4.6 or later is deployed to all the EEPC 5.x.x clients that need to migrate to Drive Encryption 7.1. Additionally, the client system needs to be in successful communication with and managed by the Drive Encryption server.
- The Password token is not migrated as part of this migration process.

**Task**

1. Install the necessary Drive Encryption 7.1 extensions into the McAfee ePO server.
2. Check in the Drive Encryption 7.1 software packages to the McAfee ePO server.
Define and assign the appropriate product and user-based policies to system and users. Make sure that you enable the option Add local domain users under Drive Encryption 7.1 | Product Setting Policy | Log On (Drive Encryption).

Deploy Drive Encryption Agent and Drive Encryption Windows software packages to the client system where 5.x.x is currently installed.

Restart the client system when prompted. The Drive Encryption 7.1 encryption status dialog box shows the status as 'Upgradable'. The user will still see the 5.x.x PBA.

Force a policy enforcement (during ASCI) from the McAfee Agent. The DEAgent now queries the system for the domain users that are logged on to the client. The DEAgent then sends the collected data to the McAfee ePO server. On successful policy enforcement, the Drive Encryption 7.1 encryption status dialog box shows the status as Active.

Restart the client system and initialize the user in the 7.1 PBA screen.
Migrating from EEPC 5.x.x to Drive Encryption 7.1 with the migration tool

This section describes how to export the user data and configuration from the EEPC 5.x.x database using the migration tool and import them to the McAfee ePO server, then upgrade the EEPC clients to Drive Encryption 7.1.

The encrypted disks on the client systems remain encrypted during the migration process.

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

Overview of the migration process

Use this high-level process to migrate from EEPC 5.x.x.

1. Copy the contents of the EEMigration tool from the Drive Encryption 7.1 product package and place it in the Endpoint Encryption manager folder.

2. Select the information to extract from the 5.x.x database. The export tool extracts the necessary data.

3. Make sure that the McAfee Agent for Windows 4.6 or later is deployed to all the systems that need to migrate to Drive Encryption 7.1. Additionally, the client system needs to be in successful communication with and managed by the McAfee ePO server.

4. Make sure that the Active Directory Server used to populate the Drive Encryption 7.1 users contains the same user information that you want to import from 5.x.x.

   You can also manage users through User Directory, which removes the dependency on LDAP server. For more information, see the Import user assignments using McAfee ePO section.

5. Install the Drive Encryption extensions and check in the Drive Encryption software packages to McAfee ePO.

6. Define the required policy settings in Drive Encryption 7.1.

7. Import the users exported from EEPC 5.x.x database into the McAfee ePO server.

8. In the import data, review the users and user groups that are not automatically matched with an LDAP user or group and manually match them to LDAP users and groups. You can also create the EEPC 5.x.x users and user groups using the User Directory feature.

9. In the imported user to system assignments, review the systems that cannot be automatically identified in ePolicy Orchestrator and manually match them to systems in McAfee ePO.
Deploy the Drive Encryption software packages to the selected systems.

Send an agent wake-up call from the McAfee ePO server to the client system that needs to be upgraded.

Exporting user and user assignments from the EEPC 5.x.x database

The command-line and GUI applications allow the administrator to export the users or the users assigned to 5.x.x systems from the 5.x.x database. The purpose of exporting the users that are assigned to systems is to reduce the amount of configuration required in ePolicy Orchestrator when upgrading to Drive Encryption 7.1.

Due to the complexity of exporting the user data from the EEPC 5.x.x database, the export can be a relatively slow operation — this is particularly true when exporting users with password tokens. On a typical server, it is common for the EEMigration tool to export password token users at a rate of 3,000 users per hour. This rate should be used to calculate the likely duration of the export and guide your decision to export users in small batches.

Contents

- Overview of the export process
- Run the export from the command prompt
- Run the export wizard
- Components that are exported
- Components and settings that must be reconfigured

Overview of the export process

With the migration tool you can export the user assignments based on the scenario that best suits your configuration.

You can export the information based on:

- Individual machine
- Group of machines
- Individual user
- Group of users

Use the following high-level process to export the data from the 5.x.x database.

1. Run the migration tool EEMigration.exe on the 5.x.x database server.
2. Specify the user assignments based on:
   - Machines/machine groups
   - Users/user groups
3. Provide the location of the CMSettings.xml to reduce the amount of work required in ePolicy Orchestrator during the import.
4. Select the system or users and audit events to be included in the export.
5. Specify the additional details such as file name and location for the migration data file.
The export output is a .ZIP file, which can be imported into the McAfee ePO server. It contains these components and settings:

- User to user group assignments from the EEPC 5.x.x database.
- User and user group assignment to machines and machine groups from the EEPC 5.x.x database.
- User binding information, if it is available. This is used to locate the user on the Active Directory server.
- User password token, SSO, and Self-recovery details, if they are available. To use 5.x.x SSO and Self-recovery data in 7.1, you need to enable them in the 7.1 policies after importing the users.
- Audit information such as user audit and system audit.

**Run the export from the command prompt**

The export process can also be performed using the command line interface, which can be used to support third party tools.

**Before you begin**

Make sure that you have appropriate permission to perform this task.

Run the export commands to retrieve the export file, which is a .ZIP file. After a successful export, this output file has the users or the users assigned to 5.x.x systems in the 5.x.x database. This file needs to be imported into the McAfee ePO server.

**Task**

1. Copy and extract the EEMigration.ZIP file to the folder where Endpoint Encryption Manager is installed.

2. From the command prompt, change directory to where Endpoint Encryption Manager is installed.
3 Run the export command `SBADMCL` and include export parameters as needed.

### Table 3-1 Parameters to export users and user assignments by selecting machine groups and machines

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>-AdminUser:&lt;username&gt;</td>
<td>Input the administrator user name of the 5.x.x database.</td>
</tr>
<tr>
<td>-AdminPwd:&lt;password&gt;</td>
<td>Input the administrator password of the 5.x.x database.</td>
</tr>
<tr>
<td>[-Database:&lt;database connection&gt;]</td>
<td>Select the Database Connection name that is used to define parameters for the MigrationExport command. If you do not select the database connect name, then it exports the details from the default database.</td>
</tr>
<tr>
<td>-Command:MigrationExport</td>
<td>This is the command to export the selected data.</td>
</tr>
<tr>
<td>-MachineGroup:&lt;machine group name&gt;</td>
<td>Input the required machine group name of the 5.x.x database.</td>
</tr>
<tr>
<td></td>
<td>This can be repeated as many times as required.</td>
</tr>
<tr>
<td>-Machine:&lt;machine name&gt;</td>
<td>Input the required machine name of the 5.x.x database.</td>
</tr>
<tr>
<td></td>
<td>This can be repeated as many times as required.</td>
</tr>
<tr>
<td>-File:&lt;exportoutput.zip&gt;</td>
<td>Specify the output file name with the file format (.ZIP).</td>
</tr>
<tr>
<td>[-Cm:&lt;&quot;CMSettings.xml fully qualified file name&quot;&gt;]</td>
<td>Specify the path to the CMSettings.xml file. (Optional)</td>
</tr>
<tr>
<td>[-Audit:&lt;All</td>
<td>numberofdays&gt;]</td>
</tr>
<tr>
<td></td>
<td>Importing the audit logs increases the size of the McAfee ePO database. We recommend that you keep the number of days as small as possible.</td>
</tr>
</tbody>
</table>

### Table 3-2 Parameters to export users and user assignments by selecting users groups and users

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>-AdminUser:&lt;username&gt;</td>
<td>Input the administrator user name of the 5.x.x database.</td>
</tr>
<tr>
<td>-AdminPwd:&lt;password&gt;</td>
<td>Input the administrator password of the 5.x.x database.</td>
</tr>
<tr>
<td>[-Database:&lt;database connection&gt;]</td>
<td>Select the Database Connection name that is used to define parameters for the MigrationExport command. If you do not select the database connect name, then it exports the details from the default database.</td>
</tr>
<tr>
<td>-Command:MigrationExport</td>
<td>This is the command to export the selected data.</td>
</tr>
<tr>
<td>-UserGroup:&lt;user group name&gt;</td>
<td>Input the required user group name of the 5.x.x database.</td>
</tr>
<tr>
<td></td>
<td>This can be repeated as many times as required.</td>
</tr>
</tbody>
</table>
Table 3-2  Parameters to export users and user assignments by selecting users groups and users (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-User: &lt;user name&gt;</td>
<td>Input the required user name of the 5.x.x database. This can be repeated as many times as required.</td>
</tr>
<tr>
<td>-File: &lt;exportoutput.zip&gt;</td>
<td>Specify the output file name with the file format (.ZIP).</td>
</tr>
<tr>
<td>[-Cm: &lt;&quot;CMSettings.xml fully qualified file name&quot;&gt;]</td>
<td>Specify the path to the CMSettings.xml file. (Optional)</td>
</tr>
<tr>
<td>[-Audit: &lt;All</td>
<td>numberofdays&gt;]</td>
</tr>
</tbody>
</table>

Importing the audit logs increases the size of the McAfee ePO database. We recommend that you keep the number of days as small as possible.

The machine or machine groups and user or user groups parameters cannot be specified at the same time.

4 Browse to the specified output location and retrieve the export file.

The export file is a .ZIP file containing XML files.

Run the export wizard

Run the export wizard (EEMigration.exe), which guides you through specifying the parameters of the export. This is another method to retrieve the export output file, which is a .ZIP file.

Before you begin

- Make sure that you have the latest EEMigration.ZIP file to implement and perform the export.
- Make sure that you have access rights to view system and user properties.

After a successful export, this output file has the users or the users assigned to 5.x.x systems in the 5.x.x database. This file needs to be imported into the McAfee ePO server.

Task

1 Copy and extract the EEMigration.ZIP file to the folder where Endpoint Encryption Manager is installed. A confirmation message to replace the SbAdmDll.dll file appears.

2 Click Yes to replace the SbAdmDll.dll file.

3 Run the EEMigration.exe tool to initiate the McAfee Endpoint Encryption Migration wizard. This checks if there is an SbAdmDll.dll file present at the same path that supports the MigrationExport command. If it is present, the application automatically uses the file and the wizard starts with the Endpoint Encryption Administrator Credentials page.

   a In the Locate SbAdmDll page, type the path to the SbAdmDll.dll file, or click Browse and select the SbAdmDll.dll file when the suitable SbAdmDll.dll file is not found.

   b Click Next. The Endpoint Encryption Administrator Credentials page appears.
Type the administrator **User** name, **Password**, and select the **Database Connection** name, then click **Next**. The Export Machines or Users page appears.

WARNING: The password is disabled message appears without a timeout while exceeding three wrong password attempts. However, when you log on to the EEM console, all cumulated timeouts that occurred on the EEMigration console are considered as timeouts on the EEM console.

5 Select **Machines** or **Users** to export the Machine Groups and Machines or User Groups and Users, then click **Next**. The Select Items page appears.

- Selecting machine — Exports all the users assigned to the selected machine. You can also select specific machine to be exported.
- Selecting users — Exports all the user assignments pertaining to the selected users.

6 Select the groups and group members to export. From here, you can:

- Select All groups
- Deselect All groups
- Select members; systems or users (dependent on selection on previous screen)

7 Click **Next**. The Optional Settings page appears.

8 Type the path or click **Browse** and select the **CmSettings.xml** file.

**Important:** If the CmSettings.xml file is not present, then you need to provide the binding details in ePolicy Orchestrator during the import process.

9 Select **Export Machine and User audit events** to export all audit events. By default no system or user audit event data is exported.

10 Select **Only export audit events created within the last __ days** to limit the audit events export to the specified days, then click **Next**. The Locate Output page appears.

**Information:** Importing the audit logs increases the size of the McAfee ePO database. We recommend that you keep the number of days as low as possible.

11 Specify the full path or click **Browse** to select the location for the output file, then click **Next**.

**Important:** This creates all the individual export files as one output .ZIP file. If you do not specify any file extension for the output file, the application appends the .ZIP extension to the file name.
12 Click **Finish** to run the export. The Export Status page appears. The application starts exporting each object and displays the message "Migration export completed successfully after completing the export", on the Export Status page.

13 Click **Close** to complete the export. You should now be able to get the export file from the specified location.

The export file is a .ZIP file containing XML files.

Use this table to determine which user assignments are exported when you run the Endpoint Encryption migration tool.

<table>
<thead>
<tr>
<th>Export Type</th>
<th>Items selected for export</th>
<th>Exported systems</th>
<th>Exported users</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine</strong></td>
<td>Selected Machine Groups</td>
<td>All systems in the selected Machine Group.</td>
<td>Every User Group (and individuals in those groups) assigned to the systems exported. Every User explicitly assigned to the exported systems.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Selected Machines</td>
<td>All specified systems.</td>
<td>Every User Group (and all individual group members) assigned to the specified systems. Every user explicitly assigned to the specified systems.</td>
<td></td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>Selected User Groups</td>
<td>Every system that a specified User Group (or individual user from a specified User Group) is assigned to.</td>
<td>All specified User Groups and the individual users in those groups.</td>
<td>You can use the Users export type to export users and User Groups that are not assigned to any systems. Non-password token data is not exported - but the user is exported. If you attempt to import an already imported user, then the user will not be imported. After you migrate a password token user to Drive Encryption 7.1, there is no synchronization of password or other user information between the EEPC 5 and the Drive Encryption 7.1 user.</td>
</tr>
<tr>
<td></td>
<td>Selected Users</td>
<td>Every system that the specified user is assigned to and any system that has a User Group that includes the specified user.</td>
<td>All specified users. All User Groups where the specified users are members (populated only with the specified users).</td>
<td></td>
</tr>
</tbody>
</table>

**Components that are exported**

This information lists the components and settings that are automatically exported as part of the migration process.

- User to user group assignments from the EEPC 5.x.x database.
- User and user group assignment to machines and machine groups from the EEPC 5.x.x database.
• User binding information, if it is available. This is used to locate the user on the Active Directory server.

• User password token, SSO, and Self-recovery details, if they are available. To use 5.x.x SSO and Self-recovery data in 7.1, you need to enable them in the 7.1 policies after importing the users.

• Audit information such as user audit and system audit.

**Components and settings that must be reconfigured**

This information lists the components and settings that are not exported and imported as part of the migration process, and must be reconfigured in McAfee ePO and the client system.

• Systems are not exported from the 5.x.x database, however, the user to machine assignments are exported.

• User tokens other than the password cannot be exported from the 5.x.x database. If you need any other token, assign it to the user manually.

• AD/LDAP/NT connectors credential information are not exported. It is the administrator’s responsibility to register the McAfee ePO Registered LDAP server.

• EEPC 5.x.x policies are not exported. If you need your 5.x.x policy settings for 7.1, you must configure them before upgrading the client.

**Importing users and user assignments into Drive Encryption 7.1**

The DE Admin extension for Drive Encryption 7.1 provides a user interface on the McAfee ePO console to import the export output file, obtained using the export process. This import wizard is available on the McAfee ePO server only after installing the DE Admin extension.

**Contents**

- **Overview of the import process**
- **Import users and user assignments using McAfee ePO**
- **Import scenarios**

**Overview of the import process**

Use this high-level process to import the user and system information, available within the export output file, into the McAfee ePO server.

1. Make sure that the Active Directory server used to add the Drive Encryption 7.1 users contains the same user information that you want to import from 5.x.x.

   You can also import users through User Directory, which removes the dependency on LDAP server. For more information, see the *Import user assignments using McAfee ePO* section.

2. Install the Drive Encryption 7.1 extensions into McAfee ePO.

3. Make sure that you have added the required client systems to ePolicy Orchestrator to which you want to match and assign the users.

4. Select the export file to import into the McAfee ePO server.

5. Specify the bindings details and rules associated with the import process.

6. Match the user groups to AD/LDAP Organizational Unit or Groups. You can also create the EEPC 5.x.x users and user groups using the User Directory feature.
7 Review any missing matches and select how to proceed with them.

8 Apply the changes to the McAfee ePO database.

**Import users and user assignments using McAfee ePO**

To import the users and user assignments from the EEPC 5.x.x database to the McAfee ePO server, you need to import the export output file to the McAfee ePO server. The export file (.ZIP) is the output file that you created during the export from 5.x.x database.

**Before you begin**

- Make sure that you have appropriate permission to perform the Allow Import of v5 users task in McAfee ePO. 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 matched are managed by McAfee ePO.

- 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.

> You can also import users through User Directory, which removes the dependency on LDAP server. Database Mirroring only needs to be enabled if you need to create Policy Assignment Rules for User Directory users or OUs. To enable the **Database Mirroring** option, click **Menu | Configuration | Server Settings | User Policies** to allow agent handler to communicate directly with the database without connecting to any LDAP servers.

**Task**

1 Make sure the McAfee Agent has been deployed to all target systems, and ensure all target systems are displayed in the System Tree. For more details on how to deploy the McAfee Agent to the client systems, refer to the McAfee Agent documentation.

2 On the McAfee ePO console, click **Menu | Data Protection | Encryption Users**. The My Organization page appears.

3 Click **Tasks | Import v5 users** to display the Upload page.

4 Click **Browse** and select the export (.zip) file that you created during the export process, then click **Next**. This uploads and validates the export file. On successful validation, the XML files are extracted to a temporary folder on ePolicy Orchestrator and the Bindings page opens.

> The validation checks for the existence of the bindings.xml file. If the file is not valid, then the McAfee ePO server displays a confirmation message "No bindings available, rules will be used for matching users."

5 Complete the binding mapping by selecting the LDAP Attribute and the corresponding LDAP Server. The binding names are automatically filled in if the binding attributes are available, otherwise, you must input them manually.

> For each binding attribute, you can select a corresponding LDAP server to use for locating the user. The LDAP server is also automatically selected based upon the information available with the **CmSettings.xml** file.
6 Enable the User Directory function and select the required Organizational Unit (OU) to add EEPC 5.x.x non-LDAP unassigned users.

Make sure to note that you can enable the User Directory function only if you have installed the User Directory extension.

7 After selecting the binding information, click Verify | Next to open the Rules page. This page allows you to define rules to locate the users when the binding match fails.

These rules can also be used to match manually added 5.x.x users, that are not imported from the LDAP.

8 From the Available Properties list, define the rules by selecting the available user property.

The user is not permitted to use the and option in the criteria builder.

9 Under Comparison, select the comparison criteria from the list.

10 Under Value, select the required user attribute name either for the corresponding LDAP server or User Directory.

For example, use CN attribute while defining a rule, so that a user name in 5.x.x database is compared to the user names available in the LDAP server, and the best match is found.

11 Click + or - to add or remove rules with different user attributes and comparison criteria. Click Next.

The Assignments page appears with User Groups.

By default, the machine group users are assigned to the individual system.

12 Under User Groups, select the V5 User Group Name and click Actions | Assign LDAP Group, Create User Directory OU(s), or De-assign LDAP Group.

- On selecting Assign LDAP Group, the Assign Group to V5 User Group page appears with V5 User Group name, LDAP server, and Group list. Select either the assigned LDAP server or User Directory. Then, select a LDAP OU or LDAP Group from Group list, then browse the ePO LDAP browser and select the LDAP OU or LDAP Group. Click OK. This assigns the 5.x.x user groups to system in the McAfee ePO server.

- On selecting Create User Directory OU(s), you will see a dialog box to confirm creating the User Directory. Click Yes to create the User Directory.

- On selecting De-assign LDAP Group, the group membership will not be used for user assignment. This will result in individual user assignments being used for matching. If there are no user assignments to individual machines then no users will be imported.
13 Click Next. The Preview page appears with the assigned users under the Users tab.

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 Active Directory and User Directory servers that has been set up with DE LDAP Synch attributes. We recommend that you initiate the user matching using the binding attributes, if not the import process will be slow. If there are multiple Active Directory servers, then the speed of the overall import process will be impacted. The import 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

If the users and user groups don't match with any of the registered LDAP servers, you can create them in the User Directory.

14 Click Next. The Results page appears with the results of the import. The overall import result is also color-coordinated, so that it is easy for the administrator to analyze the failure and success.

Navigating away or shutting the browser while the import is running stops the import thread and stops the import. While the import is running, the administrator can see the message "Please wait, assigning users to systems" in the top left of the page.

Import scenarios

The following import scenarios demonstrate some of the possible scenarios that can be encountered when users import the systems and users from version 5.x.x database into the McAfee ePO server.

Table 3-3 User groups

<table>
<thead>
<tr>
<th>Possible scenarios</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario</td>
<td>Not mapping user groups to organizational units or user groups.</td>
</tr>
<tr>
<td>Description</td>
<td>This scenario deals with importing a 5.x.x export file into the McAfee ePO server.</td>
</tr>
<tr>
<td>Pre-conditions</td>
<td>System exists in version 5.x.x administrator system, with one or more user groups assigned.</td>
</tr>
<tr>
<td></td>
<td>System has been added to McAfee ePO and has McAfee Agent installed.</td>
</tr>
<tr>
<td>Flow</td>
<td>Administrator imports the 5.x.x export file into ePolicy Orchestrator using the Drive Encryption extension wizard. This should use the default binding attributes.</td>
</tr>
<tr>
<td></td>
<td>Administrator elects not to assign user groups to an organizational unit or LDAP user groups.</td>
</tr>
</tbody>
</table>
Table 3-3 User groups *(continued)*

<table>
<thead>
<tr>
<th>Possible scenarios</th>
<th>Description</th>
</tr>
</thead>
</table>
| Post conditions    | • List of machine assignments appear for administrator to confirm.  
                       • List of user assignments appear for administrator to confirm. |
| Results            | • 5.x.x users assigned to 5.x.x machines, are added to the individual machine(s) in McAfee ePO.  
                       • 5.x.x users within the 5.x.x user groups, are added to the individual machine(s) in McAfee ePO. |

Table 3-4 Alternative 1

<table>
<thead>
<tr>
<th>Possible scenarios</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario Mapping user groups to organizational units or user groups.</td>
<td></td>
</tr>
<tr>
<td>Description This scenario deals with importing a 5.x.x export file into the McAfee ePO server.</td>
<td></td>
</tr>
</tbody>
</table>
| Pre-conditions | • Machine should exist in 5.x.x administrator system, with one or more users assigned.  
                       • Machine should have been added to ePolicy Orchestrator by installing McAfee Agent. |
| Flow | • Administrator imports the 5.x.x export file into McAfee ePO using the Drive Encryption extension wizard. This should use the default binding attributes.  
                       • Administrator selects to assign user groups to organizational unit or LDAP user groups. |
| Post conditions | • List of machine assignments appear for administrator to confirm.  
                       • List of user assignments appear for administrator to confirm. |
| Results | • 5.x.x users assigned to 5.x.x machines, are added to the individual machine(s) in McAfee ePO.  
                       • Organizational unit or LDAP group assigned to 5.x.x user groups that were assigned to systems, are added to the individual machine(s) in McAfee ePO.  
                       • If 5.x.x users are found in the assigned OU/Group, then the 5.x.x password token, SSO and Self Recovery data will be transferred to 7.1. If new users are present in the assigned OU/Group, then they are added to 7.1 as non initialized users.  
                       • If 5.x.x users are found in the assigned OU/Group, then the 5.x.x password token, SSO and Self Recovery data will be transferred to 7.1. If new users are present in the assigned OU/Group, then they are added to 7.1 as non initialized users.  
                       • 5.x.x users within the 5.x.x user groups not assigned to an organization unit or LDAP group, are added to the individual system(s) in McAfee ePO. |

Migrating to Drive Encryption 7.1

This section describes what happens during the migration of McAfee Endpoint Encryption for PC 5.x.x. The primary goal of migrating the EEPC 5.x.x series is to retain the disk encryption, to make sure that a decryption and a re-encryption of the disk is not required during the migration.

Make sure to note that EEPC 5.x.x refers to EEPC 5.2.6 or later versions.
Only one encryption algorithm can be active for all disks, so irrespective of the settings in Drive Encryption 7.1, if the original 5.x.x specifies a different algorithm, that algorithm will be used for all disks, even after migration. The only way to change the client algorithm is to allow the client to decrypt, deactivate, then reactivate all disks. The RC5 algorithms have keys that are four times as large as the keys of AES algorithm. Hence all the recovery settings have four times as many lines as the AES algorithm. So, setting recovery key size as Low gives four lines of response code with RC5 algorithm.

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

Contents

- Supported versions
- Migrate from EEPC 5.x.x to Drive Encryption 7.1
- User experience summary

Supported versions

Drive Encryption Migration tool supports the migration from EEPC 5.x.x to Drive Encryption 7.1. Any user willing to migrate the client system from a lower version needs to first upgrade it to EEPC 5.x.x, then migrate to Drive Encryption 7.1.

If EEPC 5.x.x is in FIPS mode, then you should migrate to Drive Encryption 7.1 in FIPS mode only. For more information about deploying the Drive Encryption client packages in FIPS mode, see Drive Encryption 7.1 Product Guide.

Migrate from EEPC 5.x.x to Drive Encryption 7.1

You need to migrate the client systems from EEPC 5.x.x to Drive Encryption 7.1 only after importing the users and systems from the 5.x.x database to the McAfee ePO server. Use the McAfee ePO server to migrate from EEPC 5.x.x to Drive Encryption 7.1.

Before you begin

- Make sure that the McAfee Agent for Windows 4.6 or later is deployed to all the EEPC 5.x.x clients that need to migrate to Drive Encryption 7.1. Additionally, the client system needs to be in successful communication with and managed by the McAfee ePO server.
- Make sure that you have already imported the 5.x.x users to the McAfee ePO server.

Task

1. Register the LDAP server on the McAfee ePO server and make sure it is the same server registered on the 5.x.x database.

   You can also import users through User Directory, which removes the dependency on LDAP server. For more information, see the Import user assignments using McAfee ePO section.

2. Install the Drive Encryption extensions into McAfee ePO.

3. Check in the Drive Encryption 7.1 software packages to McAfee ePO.

4. Define the appropriate policy settings for 7.1.

5. Deploy the Drive Encryption Agent 7.1 software package to the client system where 5.x.x is currently installed.
6 Deploy the Drive Encryption Windows 7.1 software package to the client system where 5.x.x is currently installed.

7 Restart the client system when prompted. The Drive Encryption 7.1 encryption status dialog box shows the status as Upgradable.

8 Configure and assign the product and user-based policies to system and users.

Make sure to enable UBP enforcement setting for the users not using the default UBP.

9 Force a policy enforcement from the McAfee Agent. On successful policy enforcement, the Drive Encryption 7.1 encryption status dialog shows the status as Active.

10 Restart the client system and initialize the user at the Drive Encryption 7.1 PBA screen.

**User experience summary**

This table highlights the summary of different phases and status before, during, and after the migration from EEPC 5.x.x to Drive Encryption 7.1.

<table>
<thead>
<tr>
<th>State</th>
<th>Pre-Boot</th>
<th>Windows EE Logon</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before deploying Drive Encryption 7.1</td>
<td>EEPC 5.x.x</td>
<td>EEPC 5.x.x</td>
<td>The client system has EEPC 5.x.x installed.</td>
</tr>
<tr>
<td>packages</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When deploying Drive Encryption 7.1 to the client</td>
<td>EEPC 5.x.x</td>
<td>EEPC 5.x.x</td>
<td>The Drive Encryption 7.1 deployment prompts for a restart of the client system.</td>
</tr>
<tr>
<td>After restarting the system due to the Drive Encryption 7.1 deployment</td>
<td>EEPC 5.x.x</td>
<td>EEPC 5.x.x</td>
<td>• The Drive Encryption 7.1 status appears as Upgradable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Single-Sign-On to Windows works with EEPC 5.x.x credentials.</td>
</tr>
<tr>
<td>After policy enforcement (during ASCI) and user assignment</td>
<td>Drive Encryption 7.1</td>
<td>Windows DE Logon screen will not appear for Drive Encryption 7.1</td>
<td>• The 5.x.x DE System Tray disappears.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• The Drive Encryption 7.1 status changes to Active.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Restart the client system and authenticate using the Drive Encryption 7.1 user name and the imported password. This is similar to a first time activation of Drive Encryption 7.1.</td>
</tr>
</tbody>
</table>
Managing Drive Encryption migration reports

Drive Encryption migration queries are configurable objects that retrieve and display data from the database.
These queries can be displayed in charts and tables. Any query result can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message.

Contents
- Queries as dashboard monitors
- View the Drive Encryption migration reports

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

Exported results
McAfee Drive Encryption query results can be exported to four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.
Reports are available in several formats:
- CSV — Use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Transform the data for other purposes.
- HTML — View the exported results as a web page.
- PDF — Print the results.
View the Drive Encryption migration reports

Use ePolicy Orchestrator to run and view the standard Drive Encryption migration report from the Queries page.

**Task**

1. Click **Menu | Reporting | Queries**. The Queries page opens.

2. From **Shared Groups** in **Groups** pane, select **Drive Encryption**. The migration related queries with the standard Drive Encryption query list appear.

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE: Migration log</td>
<td>Displays the log details and the results of the 5.x.x user import.</td>
</tr>
<tr>
<td>DE: Migration lookup</td>
<td>Displays the details about the assignments of the machine group, user group, machines, and users.</td>
</tr>
<tr>
<td>DE: V5 Audit</td>
<td>Displays the imported audit logs from 5.x.x.</td>
</tr>
</tbody>
</table>

   **Info** If only you selected the audit option during the export process, the audit log will be displayed.

3. Select a query from the **Queries** list.

4. Click **Actions | Run**. The query results appear. Drill down into the report and take actions on items as necessary. Available actions depend on the permissions of the user.

   **Info** The user has an option to edit the query and to view the details of the query.

5. Click **Close** when finished.
## Migration checklist

Print this page and use it as a checklist to verify that you have completed each important stage of the migration.

<table>
<thead>
<tr>
<th>Migration Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The migration is supported only from EEPC 5.x.x (5.2.6 or above) to Drive Encryption 7.1 and it is not supported for versions below 5.2.6.</td>
</tr>
</tbody>
</table>

### Creating the export file

2. Copy and extract the EEMigration.ZIP file to the EEM installed folder. Example: c:\Program Files\McAfee \Endpoint Encryption Manager.  
3. Create and save the export file (.ZIP).  

### Importing the export file into McAfee ePO

4. Make sure that the system(s) to be migrated is managed by the McAfee ePO server.  
5. Install all the extensions and packages of Drive Encryption 7.1 into McAfee ePO.  
6. Make sure that the permission is set to allow import of 5.x.x users in McAfee ePO.  
7. Register the same LDAP server used in 5.x.x database, on the McAfee ePO server.  

> You can also import users through User Directory, which removes the dependency on LDAP server. For more information, see the *Import user assignments using McAfee ePO* section.  

8. Place the export file (.ZIP) in a location where the file can be accessed from McAfee ePO.  
9. Import the export file (.ZIP) into McAfee ePO.  
10. Assign the 5.x.x user group to a group if required.  
11. Assign any unmatched system(s) to a system(s) in McAfee ePO if required.  
12. Assign any unmatched user(s) to a user(s) in LDAP, if required.  
13. Review the import results and it should display as **Success** in the **Results** column.  

### Client upgrade from 5.x.x to 7.1

14. Change the default policies of 7.1 to match the policies of 5.x.x.  
15. Deploy the Drive Encryption Agent 7.1 to the selected client.  
16. Deploy the Drive Encryption software package to the selected client and restart the client system when prompted.  
17. Enforce the policy update.  
18. Initialize the user at the Pre-Boot Authentication page when restarting the client after upgrading it.  

### Client upgrade from 7.0.x to 7.1

19. Change the default policies of 7.1 if required.
## Migration Checklist

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>20.</td>
<td>Deploy the Drive Encryption Agent 7.1 to the selected client system and restart it when prompted.</td>
</tr>
<tr>
<td>21.</td>
<td>Deploy the Drive Encryption software package to the selected client system and restart it when prompted.</td>
</tr>
</tbody>
</table>
Frequently Asked Questions

Q: What version of EEPC v5 is supported for migration?
A: Drive Encryption 7.1 migration supports the client upgrade from EEPC 5.x.x (5.2.6 or above) to Drive Encryption 7.1. Any user willing to upgrade from the lower version should first upgrade it to EEPC 5.x.x, then to Drive Encryption 7.1.

Q: Do 5.x.x policies get imported to Drive Encryption 7.1?
A: No, 5.x.x policies are not imported as part of the migration process. You should set the required 5.x.x policies, more importantly the Encrypt policy, in Drive Encryption 7.1 before upgrading the client. However, on migrating from EEPC 5.x.x to Drive Encryption 7.1, the available user password token, SSO, and Self Recovery details are transferred to Drive Encryption 7.1. To use 5.x.x SSO and Self Recovery data in Drive Encryption 7.1, you need to enable Self-Recovery and SSO in the Drive Encryption 7.1 policies after importing the users.

If you do not change the default Encrypt policy in Drive Encryption 7.1 before the upgrade, the client system will start decrypting after the upgrade.

Q: What happens if the 5.x.x systems are not managed by McAfee ePO?
A: All imported systems of 5.x.x will appear as unmatched systems in McAfee ePO. So, make sure that the system to be migrated is managed by McAfee ePO before initiating the import process.

Q: What happens if the 5.x.x user has been disabled in the AD?
A: The 5.x.x user disabled in AD will be imported, however the properties of the user will be determined by the Drive Encryption server settings policies in McAfee ePO.

Q: What happens to a partially encrypted 5.x.x system after the migration?
A: A partially encrypted 5.x.x system gets fully encrypted/decrypted as per the policies set in Drive Encryption 7.1.

Q: What happens if the user initiates the upgrade process while the 5.x.x client is in encrypting or decrypting state?
A: It completes the encryption or decryption process as per the policies set in Drive Encryption 7.1.

Q: What happens to a removable media that is encrypted with 5.x.x?
A: We recommend that you decrypt your removable media before initiating the upgrade.

Be aware that there is no way to decrypt your removable media after the upgrade, other than using the DETech recovery tool.
Q: Will the 5.x.x token details be migrated?
A: Yes, the 5.x.x token details (Password token, SSO, and Self-recovery) are migrated when they are available.

Q: Will the self recovery information be migrated?
A: On migrating from EEPC 5.x.x to Drive Encryption 7.1, the available Self Recovery details are transferred to Drive Encryption 7.1. To use 5.x.x Self Recovery data in Drive Encryption 7.1, you need to enable Self-Recovery in the Drive Encryption 7.1 policies after importing the users.

Q: Will the SSO and Self Recovery details be migrated?
A: Yes, the Single-Sign-On and Self-recovery details from the 5.x.x database, are migrated if only the user token is migrated.

Q: What happens to a 5.x.x system after migration if it has been encrypted using an algorithm that is different from Drive Encryption 7.1?
A: The system remains encrypted after migration as per the policies set in Drive Encryption 7.1, and you can apply all the policies of Drive Encryption 7.1 to the migrated system.

Only one encryption algorithm can be active for all disks, so irrespective of the settings in Drive Encryption 7.1, if the original 5.x.x specifies a different algorithm, that algorithm will be used for all disks, even after migration. The only way to change the client algorithm is to allow the client to completely deactivate and decrypt all disks, then reactivate it. The RCS algorithms have keys that are four times as large as the AES ones. Hence all the recovery settings have four times as many lines as the keys of AES algorithm. So, setting recovery key size as Low gives four lines of response code with RCS algorithm.

Q: What happens to a user account that has been manually added to v5 and not present in the AD?
A: All manually added users of 5.x.x can be created inside User Directory, which removes the dependency on LDAP server. For more information, see the Import user assignments using McAfee ePO section.

Q: Is McAfee ePO updated with the changes made on 5.x.x database after the migration?
A: No, any change made on the 5.x.x database after the completion of export will not have an effect upon McAfee ePO.

Q: What happens if you log on to an upgraded system with a user name that is already initialized in a different 7.0.x system? Should it be initialized again?
A: No, any user initialized in a 7.0.x system need not be initialized again on a different system that is upgraded.

Q: Is Windows operating system upgrade supported in the Drive Encryption installed systems?
A: No, Windows operating system upgrade in the Drive Encryption installed systems is not supported. We recommend that you completely remove Drive Encryption before doing any operating system upgrade.
Index

A
about this guide 5
Active Directory
    registering 8, 13, 20, 25
Active Directory group, assigning and de-assigning 21
Active Directory, registering 21
agent wake-up call, sending 13
algorithm, selecting 24

B
binding details, specifying 20

C
client system
    managing 25
    migrating 26
command prompt, using 15
components
    configuring 20
    exported 19
conventions and icons used in this guide 5

D
disk encryption, retaining 24
documentation
    audience for this guide 5
    product-specific, finding 6
    typographical conventions and icons 5
Drive Encryption, upgrading 24, 25

E
export command, running 15
export file
    retrieving 15, 17
    selecting 20
export wizard, running 17
exporting
    audit information 7, 19
    client systems 8
    encryption keys 20
    machine information 14
    systems 15, 17
    user assignments 14
exporting (continued)
    user information 14
    users 15, 17
extension
    installing 11, 13, 20, 25

I
importing
    audit information 7
    machine group 21
    output file 20
    password and self-recovery 8
    systems 20
    user 20
    user assignments 20
    user group 21
    users 13, 20

L
local domain users
    adding 11

M
McAfee ServicePortal, accessing 6
migration
    data file 14
    exporting systems 8
    exporting users 7, 8
    migration tool 13
    reports 28
    running the tool 13
    upgrading systems 8
    without the tool 11

P
policies
    assigning 11
    configuring 20
    defining 13, 25
    enabling 19, 24
    reviewing 8

McAfee Drive Encryption 7.1.0 Migration Guide 33
Q
queries, Drive Encryption
  creating 27
  dashboard monitors 27
  running 28
queries, McAfee Drive Encryption
  dashboard monitor 27
  running 27

R
recovery key, setting 24
reports, migration 28
requirements, Drive Encryption 10

S
scenarios
  importing 23
self-recovery, enabling 13
ServicePortal, finding product documentation 6
software package
  checking in 11, 25
  deploying 13, 25
summary
  user experience 26
system
  matching 20
  selecting 17
system branch, assigning and de-assigning 21
system status
  active 26
  (continued)
  inactive 26
  systems
    matching 21

T
Technical Support, finding product information 6
tokens
  assigning 20

U
upgrading
  client system 7
user
  password 15, 17
  selecting 17
user groups, matching 20
users
  adding 11
  assigning 13
  exporting 13
  initializing 11
  matching 20, 21
  selecting 14

W
what's in this guide 6