Scripting Guide

McAfee Drive Encryption 7.1
For use with ePolicy Orchestrator 4.6.7 and 5.1.0 Software
## Contents

**Preface**  
About this guide .................................. 5  
Audience .................................. 5  
Conventions .................................. 5  
What's in this guide .................................. 6  
Find product documentation .................................. 6

1 **Introduction**  
Purpose of this guide .................................. 7

2 **Web API commands for Drive Encryption**  
Using Web API commands for Drive Encryption .................................. 9  
Add a user or a user group to a system or branch .................................. 10  
Remove a user or a user group from a system or branch .................................. 10  
Change a user password .................................. 11  
Export disk encryption key(s) for a system .................................. 11  
Generate a Challenge Response Code .................................. 12  
Reset self recovery for a user .................................. 13

3 **User Directory Management (Non LDAP)**  
Web API commands for the User Directory .................................. 15  
Help command .................................. 17

**Index** .................................. 19
Preface

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

Contents

- About this guide
- Find product documentation

About this guide

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

Audience

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

The information in this guide is intended primarily for:

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

Conventions

This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**

  Title of a book, chapter, or topic; a new term; emphasis.

- **Bold**

  Text that is strongly emphasized.

- **User input, code, message**

  Commands and other text that the user types; a code sample; a displayed message.

- **Interface text**

  Words from the product interface like options, menus, buttons, and dialog boxes.

- **Hypertext blue**

  A link to a topic or to an external website.

- **Note:**

  Additional information, like an alternate method of accessing an option.

- **Tip:**

  Suggestions and recommendations.

- **Important/Caution:**

  Valuable advice to protect your computer system, software installation, network, business, or data.

- **Warning:**

  Critical advice to prevent bodily harm when using a hardware product.
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></td>
<td>3  Select a product document.</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>
Introduction

McAfee® Drive Encryption 7.1 introduces Web API commands that add scripting and automation capabilities to these management activities:

- Add or remove a user(s) from a system(s)
- Export disk encryption key(s) for a system
- Perform user directory management (Non LDAP)
- Generate a Challenge Response Code
- Change a user password
- Reset self recovery for a user

Purpose of this guide

This guide provides the Web API commands that you need to configure, use, and maintain Drive Encryption.

This guide is a companion document to the McAfee® ePolicy Orchestrator® Scripting Guide (4.6.x and 5.1.x).

The scripting functionalities of Drive Encryption 7.1 are supported only from the McAfee ePO 4.6 version onwards.

The McAfee ePO Scripting Guide describes the McAfee ePO Web API and how to use it. It also provides example scripts using the Python client.

For more information about Web API basics, see the McAfee ePO Scripting Guide.
Web API commands for Drive Encryption

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

The Web API is used primarily for two purposes:

- Scripting sequences of tasks
- Performing simple tasks without using the user interface

Contents

- Using Web API commands for Drive Encryption
- Add a user or a user group to a system or branch
- Remove a user or a user group from a system or branch
- Change a user password
- Export disk encryption key(s) for a system
- Generate a Challenge Response Code
- Reset self recovery for a user

Using Web API commands for Drive Encryption

A few Web API commands are more commonly used than others. Being familiar with their syntax will help you create scripts quickly. The following tables list the commonly used commands with their syntax and description.

The examples in this guide are taken from different categories of tasks that show how scripting can help keep your Drive Encryption maintained and up-to-date.

Before running any commands, you must authenticate with an McAfee ePO server.

If you use Python to change passwords or export machine keys, make sure that \texttt{CREATE\_LOG\_FILE} is not enabled in debug mode. When it is enabled, passwords and machine keys are logged to the file in plain text, making it a security risk. If you need to enable it, execute the command on a secure system, then make sure to shred the log file to prevent unauthorized users from accessing your passwords and machine keys.
Add a user or a user group to a system or branch

The Drive Encryption software can be activated on a client system only after adding a user and enforcing the required encryption policies correctly. Use the `eeadmin.assignUser` command to add a user or a user group to a system or branch in McAfee ePO.

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `eeadmin.assignUser` | `systemNode=<><>` `nodeId=<><>` `dn=<><>` `[recursive=<><>]` `[ldapServerName=<><>]` | Specify `systemNode='True'` to indicate that `nodeId=computer Id` refers to an McAfee ePO System, or `systemNode='False'` to indicate that `nodeId=branch Id` refers to an McAfee ePO Branch. Pass the Distinguished Name (DN) of the LDAP User or User Group to add accordingly. For LDAP Group addition, optionally specify:  
  - `recursive='True'` to recursively add all subgroups, or  
  - `recursive='False'` to avoid recursive addition (defaults to False)  
  You must specify the LDAP server name, if more than one server is in use in your organization; otherwise it is optional. |

Remove a user or a user group from a system or branch

Use the `eeadmin.deassignUser` to remove a user or a user group from a system or branch in McAfee ePO.

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `eeadmin.deassignUser` | `systemNode=<><>` `nodeId=<><>` `dn=<><>` `dnType=<><>` | Specify `systemNode='True'` to indicate that `nodeId=computer Id` refers to an McAfee ePO System, or `systemNode='False'` to indicate that `nodeId=branch Id` refers to an McAfee ePO Branch. Pass the DN of the user or user group to remove accordingly.  
  Specify whether the DN refers to a User, User Group, or Organizational Unit (OU) (1=User, 2=User Group, 3=OU). This is required to make sure that you do not have to run an overloaded LDAP query to process this command. |
Change a user password

Resetting or changing a remote user's password token requires an authorization from administrator. The `eeadmin.changeUserPassword` command allows the administrator to change the user password remotely.

Table 2-3  `eeadmin.changeUserPassword` command

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| `eeadmin.changeUserPassword` | `eeadmin.changeUserPassword userDn=<>`
  `newPassword=<>`
  `[oldPassword=<>]` | If you specify the correct old password, the user's password is changed successfully. |
  | If you specify an incorrect old password, the command fails and leaves the existing password unchanged.  |  |
  | If you don't specify the old password, users are reinitialized, leading to the loss of token, logon, Single-Sign-On (SSO), Self-Recovery, and password history data. This requires the users to reinitialize their data at next logon.  |  |

Export disk encryption key(s) for a system

The purpose of encrypting the client's data is to control access to the data by controlling access to the encryption keys. These keys are referred to as Machine Keys. Each system has its own unique Machine Key. The Machine Key is stored in McAfee ePO database to be used for client recovery when required.
Use the `eeadmin.exportMachineKey` command to remotely export disk encryption key(s) for a system.

**Table 2-4 eeadmin.exportMachineKey command**

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>eeadmin.exportMachineKey</code></td>
<td><code>eeadmin.exportMachineKey</code></td>
<td>A system may be activated and deactivated multiple times. Each activation produces a new disk encryption key. Specify the following:</td>
</tr>
<tr>
<td></td>
<td><code>[machineIdOrName=&lt;&gt;]</code></td>
<td>• the McAfee ePO System ID or McAfee ePO System Name to export disk encryption key(s) for a specific system, or</td>
</tr>
<tr>
<td></td>
<td><code>[keyCheck=&lt;&gt;]</code></td>
<td>• a disk Key-Check value to look up the encryption key related to the disk</td>
</tr>
<tr>
<td></td>
<td><code>[oldKeys=&lt;&gt;]</code></td>
<td>This lookup might take some time and the Key-Check value can be obtained for a disk from DETech.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The encryption key of a disk might not be the same as the encryption key of a system. This is applicable when the disk is removed from the (encrypted) system prior to a deactivation/reactivation. Specify <code>oldKeys='True'</code> to export all disk encryption keys related to the system.</td>
</tr>
</tbody>
</table>

**Generate a Challenge Response Code**

If the user's password or logon tokens have been lost, you need to perform administrator recovery on the client computer to recover the user or system.

User calls the administrator to perform the administrator recovery, and provides the Challenge Code. The administrator initiates the McAfee ePO Scripting API to generate the Challenge Response Code. A valid Response Code is supplied by the scripting API to the administrator. When typing the Response Code, access is granted to the Client system. Use the `eeadmin.administratorRecovery` command to generate the Challenge Response Code.

There are four different administrator recovery types:

- `machineRecovery='1'`
- `resetUserToken='2'`
• lockDisabledUser='3'
• reserUserToPasswordToken='4'

### Table 2-5  machineRecovery recovery type

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eeadmin.administratorRecovery</td>
<td>eeadmin.administratorRecovery challengeCode=&lt;&gt;&lt;br&gt; recoveryType=&lt;&gt;&lt;br&gt; userDn=&lt;&gt;&lt;br&gt;</td>
<td>Specify recoveryType='1', to perform Machine Recovery.</td>
</tr>
</tbody>
</table>

### Table 2-6  resetUserToken recovery type

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eeadmin.administratorRecovery</td>
<td>eeadmin.administratorRecovery challengeCode=&lt;&gt;&lt;br&gt; recoveryType=&lt;&gt;&lt;br&gt; userDn=&lt;&gt;&lt;br&gt;</td>
<td>Specify recoveryType='2' and pass the Distinguished Name (DN) of the user, to perform the Reset User Token Recovery.</td>
</tr>
</tbody>
</table>

### Table 2-7  unlockDisabledUser recovery type

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eeadmin.administratorRecovery</td>
<td>eeadmin.administratorRecovery challengeCode=&lt;&gt;&lt;br&gt; recoveryType=&lt;&gt;&lt;br&gt; userDn=&lt;&gt;&lt;br&gt;</td>
<td>Specify recoveryType='3' and pass the Distinguished Name (DN) of the user, to perform the Unlock Disabled User Recovery.</td>
</tr>
</tbody>
</table>

### Table 2-8  resetUserToPasswordToken recovery type

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eeadmin.administratorRecovery</td>
<td>eeadmin.administratorRecovery challengeCode=&lt;&gt;&lt;br&gt; recoveryType=&lt;&gt;&lt;br&gt; userDn=&lt;&gt;&lt;br&gt;</td>
<td>Specify recoveryType='4' and pass the Distinguished Name (DN) of the user, to perform the Reset User To Password Token Recovery.</td>
</tr>
</tbody>
</table>

### Reset self recovery for a user

The client user’s self-recovery details can be reset remotely, then the user can enroll the self-recovery details with new self-recovery answers. Use the `eeadmin.resetSelfRecovery` command to reset your self recovery details.

### Table 2-9  eeadmin.resetSelfRecovery command

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eeadmin.resetSelfRecovery</td>
<td>eeadmin.resetSelfRecovery</td>
<td>Pass the Distinguished Name (DN) of the user to reset your self recovery token.</td>
</tr>
</tbody>
</table>
User Directory Management (Non LDAP)

The User Directory feature utilizes the LDAP Sync extension and provides the ability for Drive Encryption to use users/groups from the User Directory (using the UserDirectory.zip extension).

Contents

- Web API commands for the User Directory
- Help command

Web API commands for the User Directory

Once you install the UserDirectory.zip extension into the McAfee ePO server, you can create users and groups, and manage them using these Web API commands, without requiring to register an LDAP server in McAfee ePO.

This allows the EEPC 5.x.x standalone users, who are not part of any LDAP server to be migrated to Drive Encryption 7.1.

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>userdirectory.addEditAttribute</td>
<td>userdirectory.addEditAttribute itemId=&lt;&gt; or itemDn=&lt;&gt;</td>
</tr>
<tr>
<td></td>
<td>stringAttributes=&lt;&gt;</td>
</tr>
<tr>
<td>userdirectory.addItem</td>
<td>userdirectory.addItem parentDn/parentId=&lt;&gt;</td>
</tr>
<tr>
<td></td>
<td>itemName=&lt;&gt;</td>
</tr>
<tr>
<td></td>
<td>itemType&lt;&gt;</td>
</tr>
<tr>
<td>userdirectory.deleteItem</td>
<td>userdirectory.deleteItem itemDn/itemId=&lt;&gt;</td>
</tr>
<tr>
<td>userdirectory.getAttribute</td>
<td>userdirectory.getAttribute itemDn/itemId=&lt;&gt;</td>
</tr>
<tr>
<td></td>
<td>attribName=&lt;&gt;</td>
</tr>
<tr>
<td>Command</td>
<td>Syntax</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>userdirectory.deleteAttribute</td>
<td><code>userdirectory.deleteAttribute</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>userdirectory.enableItem</td>
<td><code>userdirectory.enableItem</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>userdirectory.moveItem</td>
<td><code>userdirectory.moveItem</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>userdirectory.renameItem</td>
<td><code>userdirectory.renameItem</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>userdirectory.searchItems</td>
<td><code>userdirectory.searchItems</code></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There are seven different scripts for the search item function.
Help command

You can use the Help command to get the structure for any command.
For example, to export disk encryption key for a system, use the command `mc.help ("eeadmin.exportMachineKey")` to get the structure of the command.
Index

A
about this guide 5
add a user or a user group to a system or branch 10
API 7

C
change a user password 11
conventions and icons used in this guide 5

D
documentation
  audience for this guide 5
  product-specific, finding 6
  typographical conventions and icons 5

E
export disk encryption key(s) for a system 11

H
help command 17

M
McAfee ServicePortal, accessing 6

P
plain text 9
python client 7

R
remove a user or a user group from a system or branch 10

S
scripts 9
self-recovery 11
ServicePortal, finding product documentation 6
single-sign-on 11

T
Technical Support, finding product information 6
token 11

U
user interface 9

W
what's in this guide 6