Symantec Endpoint Encryption Drive Encryption Administrator Command Line Guide Version 11.3.1

Table of Contents

Overview

About Administrator Command Line

Symantec™ Endpoint Encryption Drive Encryption Administrator Command Line provides access to Drive Encryption functionality using a command-line interface. Administrator Command Line provides administrative capabilities to those who support registered users on client computers. These capabilities can be done from the command line or scripted.

Administrator Command Line provides capabilities to:

- Manage encrypted disks, disk partitions, and registered users.
- Enable or disable Autologon bypass capabilities.
- Access an encrypted disk for recovery, if necessary.
- Extend the next due date before which the client computer should connect with the server.

Endpoint Encryption lets administrators perform some of these functions using Endpoint Encryption Client Administrator Console.

To run commands using the Administrator Command Line, you must have Windows Administrator privileges. To access the Administrator Command Line, Symantec recommends that you launch the Command Prompt as a Windows Administrator user.

Running commands also requires certain privileges.

About privileges

About scripting

See also the Symantec Endpoint Encryption Client Administrator Console online Help. This console is installed when Drive Encryption is installed.

Best practice

As a best practice, for critical disks before running any commands, such as `--recover` you must create a clone of these disks. The `--recover` command is irreversible. Therefore, it is best to make a clone of these disks and execute this command on the image. So that if required you can create a copy of this disk for data recovery.

About privileges

Client administrator privileges

The Management Console lets Symantec Endpoint Encryption Management Server policy administrators configure specific privileges while defining client administrators. This definition and configuration can happen in install-time, GPO, and native policies for Drive Encryption client computers. Client administrator privileges grant access to specific client administrator functions, such as decrypting drives and unlocking computers that missed their scheduled check-in date.

The following table describes the client administrator privileges that are available.

Table 1: Client administrator privileges

Privilege	Description
User management	Enables the client administrator to register new users and unregister existing users.
Decrypt drives	Enables the client administrator to manually decrypt disks and disk partitions on client computers.

Privilege	Description
Extend lockout	Enables the client administrator to extend the amount of time left for the next required check-in with the Symantec Endpoint Encryption Management Server to prevent a lockout.
Unlock	Enables the client administrator to unlock encrypted disks when Management Agent misses its scheduled check-in with the Symantec Endpoint Encryption Management Server.
Recover corrupted encrypted disk	Enables the client administrator to recover and copy data from a corrupted encrypted computer by connecting the corrupted hard drive as a USB (slave drive) to another computer with Drive Encryption installed.
Default administrator	Enables all of the available privileges for the client administrator.

About Administrator Command Line

Privileged user privileges

Privileged users are created by a policy administrator using Advanced Settings in the Symantec Endpoint Encryption Management Agent. The administrator designates an AD User Group to have client administrator privileges. The member users are privileged users, who have the privileges of a default administrator and are not required to enter client administrator credentials in commands.

Privileged users can run all commands except for WinPE recovery commands.

Commands that privileged users can run

SYSTEM user privileges

SYSTEM users are created by a policy administrator in Advanced Settings in the Symantec Endpoint Encryption Management Agent. SYSTEM users have privileges only to run Autologon commands, found in Chapter 7: Autologon boot bypass commands.

A primary advantage of having SYSTEM users run Autologon commands, especially in scripts, is that the client administrator credentials are not required and therefore not sent in the clear.

About Autologon

Commands that SYSTEM users can run

About scripting

Registered user privileges

Most of the Administrator Command Line commands require client administrator credentials. However, registered users can run a small subset of the commands, such as, to check the encryption status of a disk, or to view a list of authorized users on an encrypted disk.

Commands that registered users can run

Audience

The audience for this guide includes client administrators, privileged users, SYSTEM users, and registered users.

Important terms

Understanding the following terms makes it easier to use Administrator Command Line:

Symantec Endpoint Encryption Drive Encryption	A feature of Symantec Endpoint Encryption that encrypts the entire contents of a disk, including boot disks and partitions. View encryption status of a disk using the Management Agent and use Administrator Command Line to run disk management and user management commands.
Symantec Endpoint Encryption Drive Encryption Administrator Command Line	The command-line interface to the Symantec Endpoint Encryption Drive Encryption functionality.
password user	A user who authenticates to an encrypted disk using a Windows password.
passphrase user	A user who authenticates to an encrypted disk using a Drive Encryption user name and password.
encrypt	The process of scrambling data so that it is not usable unless you authenticate with valid credentials.
decrypt	The process of unscrambling encrypted data.
master boot record (MBR)	Software on a disk that is "in front" of the partition table; that is, it is implemented during the startup process before the operating system. The instructions in the MBR tell the system how to boot. In Drive Encryption, Symantec installs and enables its own MBR, which implements preboot authentication. Once a disk is instrumented, even if it is not fully encrypted, subsequent startups bring up the preboot authentication screen.

System requirements

Administrator Command Line has the same requirements as Drive Encryption.

Find the Symantec Endpoint Encryption Client system requirements here: System Requirements for Symantec Endpoint Encryption 11.3.x Client

Installing and uninstalling

Administrator Command Line gets installed automatically when Drive Encryption is installed on a computer.

To uninstall Administrator Command Line, uninstall Drive Encryption.

See the *Symantec Endpoint Encryption Installation Guide*.

The command-line interface

About syntax and usage

To run an Administrator Command Line command, at the command prompt enter `eedAdminCli`, followed by a space and the command name with the appropriate options. Then, press **Enter**.

All the Administrator Command Line commands have a long form: two hyphens "--" followed by the command name.

For example:

```
C:\>eedAdminCli --help <Enter>
```

This command displays the built-in help information for the Administrator Command Line commands.

> **NOTE**
>
> Further examples in this document do not include the command prompt `C:\>` or the **Enter** key.

A few commands also have a short form: either one hyphen and then a single letter or two hyphens and two letters.

For example:

`-h` for help instead of `--help`

You can mix long forms and short forms in a single command.

Invoking Administrator Command Line

About scripting

The Administrator Command Line commands can be inserted into scripts for automating common tasks, such as encrypting a disk or getting information about the status of an encrypted disk. The scripts must be written in a scripting language, such as Perl or Python.

> **NOTE**
>
> An advantage of having SYSTEM users or privileged users run commands is that these users do not require client administrator credentials and, therefore, scripts do not contain credentials in the clear.

Changing the path

Changing the path

By default, the Administrator Command Line application, `eedAdminCli.exe`, is installed in:

```
C:\Program Files\Symantec\Endpoint Encryption Clients\{{SEEDEFeature}}
```

To execute the Administrator Command Line commands from any location when you use a Windows command prompt, change the path on the system. The path must include the location of the Administrator Command Line application.

About scripting

Invoking Administrator Command Line

To invoke the Administrator Command Line

1. At the command line, set the current directory in which `eeAdminCli.exe` is installed and type the following:

   `eedAdminCli <--command> <--option> <parameter>`

2. Press `Enter`.

About syntax and usage

About passwords

Put passwords between single quotation marks to ensure that reserved characters and spaces are interpreted correctly. If you do not use reserved characters or spaces in your passwords, then you do not have to enclose them in single quotation marks.

On a Windows system, when you enter a password that contains a space, you must enclose the password in single or double quotation marks. If double quotation marks ("") are part of the password, you must escape them with a preceding double quotation mark. For example, if you want to use `Thomas "Stonewall" Jackson` as your password, you need to enter it as `'Thomas ""Stonewall"" Jackson'` on the command line. You need the quotation marks at the beginning and end for the spaces. You need to escape each double quotation mark in the password with another double quotation mark. Escaping means you put another special character in front of the character.

NOTE

If you have problems entering certain characters in your password, check how to handle reserved characters for your operating system or shell interpreter.

About syntax and usage

Help and version commands

About the --help command

The `--help` command lists and describes the commands and options available in Administrator Command Line.

--help (-h) command

--help (-h) command

Purpose: To view the list of commands and options and their descriptions available in Administrator Command Line.

Usage format (long form):

```
eedAdminCli --help
```

Usage format (short form):

```
eedAdminCli -h
```

Example:

```
eedAdminCli -h

Symantec Endpoint Encryption Drive Encryption

Administrator Command Line Tool.

Usage: eedAdminCli --action [--option, ...]

ACTIONS
  -h, --help
      Print this help

  --info
      Print disk system info
      --disk

  --enum
      Enumerate System Disks and Volumes

  --list-users
      List users and Offload info
```

This example shows a partial list of the commands and their descriptions in Administrator Command Line. For a complete list of commands and options, see the *Quick reference for commands and options* chapter.

List of commands

List of options

About the --help command

--version command

--version command

Purpose: The `--version` command displays information about your version of Administrator Command Line.

Usage format:

```
eedAdminCli --version
```

Example:

```
eedAdminCli --version

Symantec Endpoint Encryption Version 11.3.0 (Build 1234)
Copyright (C) 2019 Symantec Corporation. All rights reserved.
Request sent to Version was successful
```

This example shows the response to the `--version` command.

--help (-h) command

Disk information commands

About the --info command

Purpose: The `--info` command provides general status information for a specified disk.

> **NOTE**
>
> To see specific information, use the `--status` command.

The information you see about a disk using the `--info` command includes:

- Model information
- Total number of sectors on the disk
- The Universally Unique Identifier of the disk
- Whether the disk is an Opal disk and whether it is eDrive provisioned
- Whether the One-Time Password and Drive Encryption Self-Recovery recovery options are enabled or disabled on the disk.

--info command

--status command

--info command

Purpose: The `--info` command provides general status information for a specified disk.

Usage format:

```
eedAdminCli --info --disk <number>
```

Example 1:

```
eedAdminCli --info

Disk information for disk 0.
   Model Number: ST910021AS
   Total number of sectors on disk: 192426569
   Disk UUID: 3e6b9573-4014-4f9c-9981-9c63b6b47691
   OTP Used: False, DESR Used: False
Request sent to Display disk information was successful
```

This example shows the response for the `--info` command on disk 0. The `--disk` option is optional. If you do not specify a disk number along with the `--info` command, information of the boot disk, Disk 0, is displayed. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks.

Example 2:

```
eedAdminCli --info

Disk information for disk 0.
   Model Number: INTEL SSDSC2BF120A5
   Total number of sectors on disk: 234436545
   Disk UUID: 043f66ae-824f-4181-8542-b021237e1dd2
   Disk: Opal Disk
```

```
   OTP Used: False, DESR Used: False
Request sent to Display disk information was successful
```

This example shows the response to the `--info` command for an Opal v2 compliant drive. If the drive had been a Microsoft eDrive support - Opal v2 compliant drive, the Disk field would show "eDrive provisioned."

Table 2: Options for the --info command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks. **Note:** Secondary disks are not supported with Opal drives.

About the --info command

--status command

--show-config command

--enum command

Purpose: The `--enum` command displays disk designations (for example, Disk 0 as the boot disk), which are used in other Administrator Command Line commands. It also displays the number of fixed and removable storage disks, the number of volumes on a disk, the Universally Unique Identifier of the disk, and the Cipher algorithm being used for performing encryption or decryption on the disk.

Usage format:

```
eedAdminCli --enum
```

Example 1:

```
eedAdminCli --enum

Total number of installed fixed/removable storage device
(excluding floppy and CDROM): 1
Managed disks:

Disk 0 has 1 online volume(GPT):
   volume C:\ is on partition 2 with offset 80325
   Disk UUID: 3e6b9573-4014-4f9c-9981-9c63b6b47691
   Cipher Algorithm used: AES256
Request sent to Enumerate disks was successful
```

This example shows that the system has one disk, Disk 0, which is drive letter C and is the boot disk. Drive 0 is the boot disk on most systems.

Example 2:

```
eedAdminCli --enum

Total number of installed fixed/removable storage device
(excluding floppy and CDROM): 1
Managed disks:
```

```
Disk 0 has 1 online volumes , (Opal):
   Volume C:\ is on partition 4 with offset 1081344
   Partition managed: Yes
   BandId= 4
   BandStart Sector= 1081344
   Sectors per band= 233359360
   Write Lock Enable= NONPERSISTENT_UNLOCK - (T)
   Read Lock Enable= NONPERSISTENT_UNLOCK - (T)
   Crypto Algorithm Type= 0

   Disk UUID: 043f66ae-824f-4181-8542-bo21237e1dd2
Request sent to Enumerate disks was successful
```

This example shows the information for an Opal disk.

--info command

--status command

About the --status command

The `--status` command provides Drive Encryption functionality-specific status information for a specified disk and its partitions.

NOTE

To see general information about a disk, use the `--info` command.

The information you see about a disk using the `--status` command includes:

- Whether or not the disk is instrumented
- Whether or not the disk is encrypted
- The encryption or decryption status of the disk partitions, if any
- Whether the disk is software encrypted or hardware encrypted
- Whether the disk is an Opal disk and whether it is eDrive provisioned
- The number of sectors on a disk
- The high-water mark (the number of encrypted sectors on the disk)
- The number of volumes on a disk
- The Universally Unique Identifier of the disk
- The Cipher algorithm that is used for performing encryption or decryption on the disk
- The block mode of the BIOS-based disk

If you begin disk decryption and you want to check progress, you can run the `--status` command periodically to check the high-water mark. This number decreases as the decryption progresses.

--status command

--info command

--enum command

--status command

Purpose: The `--status` command provides the Drive Encryption functionality-specific status information for a specified disk.

Usage format:

```
eedAdminCli --status --disk <number>
```

Example 1:

```
eedAdminCli --status --disk 0

Disk 0 is instrumented by Drive Encryption.
 Disk UUID: 3e6b9573-4014-4f9c-9981-9c63b6b47691
  Encryption process complete.
  Current key is valid.
  Current disk block mode is 3
Volume Status - 7
Volume C:\ on partition 4 : Encryption.
  Total sectors: 192426569 highwatermark: 192426569
  Cipher Algorithm used: AES256
Request sent to Disk status was successful.
```

In this example, Disk 0 is instrumented so the preboot authentication screen is present. Also, the disk is encrypted, the total number of sectors on the disk is 192426569, and the high-water mark (number of sectors encrypted) is 192426569.

Example 2:

```
eedAdminCli --status --disk 1

Disk  1 is not instrumented by Drive Encryption
Request sent to Disk status was successful
```

In this example, disk 1 is not instrumented.

Example 3:

```
eedAdminCli --status

Disk 0 is instrumented by Drive Encryption.
 Disk: Opal Disk
 Disk: eDrive Provisioned
 Disk UUID: 043f66ae-824f-4181-8542-b021237e1dd2
   Encryption process complete.
   Current key is valid.
   Current disk block mode is 3
Volume Status - 8
Volume C:\ on partition 4 : Hardware Encrypted.
  Total sectors: 233359360 highwatermark: 233359360
Request sent to Disk status was successful
```

This example shows the information for a Microsoft eDrive support - Opal v2 compliant drive. The command output differs, depending on how the drive was provisioned. A hardware encrypted Opal v2 compliant drive shows that the whole disk is encrypted. A hardware encrypted Microsoft eDrive support - Opal v2 compliant drive shows that only the C drive is encrypted.

Example 4:

```
eedAdminCli --status --verbose

Disk 0 is instrumented by Drive Encryption.
   Disk UUID: 043f66ae-824f-4181-8542-b021237e1dd2
```

```
   Encryption process complete.
   Current key is valid.
   Current disk block mode is 3
Volume Status - 1
Volume C:\ on partition 4 : Encryption.
  Total sectors: 233359360 highwatermark: 233359360
 Double write mode is ON.
 Skip Unused Disk space mode is ON.
Request sent to Disk status was successful
```

This example shows the use of the `--verbose` option. This example shows whether the Skip unused disk space mode and the Double-write sectors mode are enabled or disabled.

Table 3: Options for the --status command

Option	Description
`--disk`	Specifies the disk to which the information applies.
`<number>`	The disk number on the system. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks.
`--verbose`	Specifies whether disk encryption was run with the Skip unused disk space mode ON or OFF and the Double-write sectors mode ON or OFF.

About the --status command

--show-config command

Disk operation commands

About the disk operation commands

The disk operation commands let you encrypt and decrypt a disk or partition, and stop and resume these processes. You can also re-encrypt a disk using a new session key.

NOTE

If you are a privileged user, do not include client administrator credentials in a command.

About the --decrypt command

The `--decrypt` command starts the process of decrypting an encrypted disk or an individual disk partition.

Decryption cannot begin until encryption is completed or stopped. To stop the encryption that is in process, use the `--stop` command.

If you begin to decrypt an encrypted disk or partition, you can pause the decryption and then restart the decryption process. However, you cannot stop the decryption and then encrypt only the portion that was decrypted. If you begin to decrypt an encrypted disk or partition, you must fully decrypt it before you can re-encrypt it.

To check the decryption progress, use the `--status` command.

NOTE

If you are a privileged user, do not include client administrator credentials in the command.

--decrypt command

--status command

--stop command

--encrypt command

--decrypt command

Purpose: The `--decrypt` command starts the process of decrypting an encrypted disk or an individual partition.

Usage format:

```
eedAdminCli --decrypt --disk <number> --partition-list <drive letters>
--au <AdminUserName> --ap <AdminPassword>
```

Example: 1

```
eedAdminCli --decrypt --disk 0 --au jsmith --ap safepass

Request sent to Start decrypt disk was successful.
```

This example shows a boot disk being decrypted.

Example: 2

```
eedAdminCli --decrypt --disk 0 --partition-list c;d --au jsmith --ap safepass

Request sent to Start decrypt disk was successful.
```

This example shows partitions C: and D: on disk 0 being decrypted.

Table 4: Options for the --decrypt command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.
`--partition-list`	Specifies the disk partitions to which the operation applies.
`<drive letters>`	The drive letters of the disk partitions to which the operation applies. Drive letters are separated by the semicolon (;) symbol.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

About the --decrypt command

--status command

--stop command

--resume command

--encrypt command

--encrypt command

Purpose: The `--encrypt` command starts the process of encrypting a disk or partition.

> **NOTE**
>
> If a Remote Decryption policy is in effect on a client computer, this encrypt command fails with a message. The computer remains in a decrypted state until a policy administrator reverses that policy.

Usage format:

```
eedAdminCli --encrypt --disk <number> --partition-list <drive letters>
--au <AdminUserName> --ap <AdminPassword>
```

Example 1:

```
eedAdminCli --encrypt --disk 0 --au jsmith --ap safepass

Request sent to Start encrypt disk was successful.
```

This example shows a boot disk being encrypted.

Example 2:

```
eedAdminCli --encrypt --disk 0 --partition-list c --au jsmith --ap safepass

Request sent to Start encrypt disk was successful.
```

This example shows a single partition on a disk being encrypted. On a partitioned disk, this could be the boot drive.

Usage format:

```
eedAdminCli --encrypt --disk <number> --partition-list <drive letters>
            --skip-unused-space --au <AdminUserName> --ap <AdminPassword>
```

Example 3:

```
eedAdminCli --encrypt --disk 0 --partition-list c,d  --skip-unused-space
            --au jsmith --ap safepass
```

Command output:

```
Request sent to Start encrypt disk was successful.
```

This example shows that the administrator with the username *jsmith* and password *safepass* has started encryption skipping the unused sectors on the boot disk 0. The `--encrypt` command with the `--skip-unused-space` option skips the encryption of unused disk space and encrypts only those sectors on the disk that contain data. You can use this command even if the **Include unused disk space when encrypting disks and partitions** policy option is not selected on the Drive Encryption - Encryption policy installed on a client computer.

NOTE

To know whether the feature to skip the encryption of the unused disk space is enabled, use the `--status` command with the `--verbose` option.

Table 5: Options for the --encrypt command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks.
`--partition-list`	Specifies the disk partitions to which the operation applies.
`<drive letters>`	The drive letters of the disk partitions to which the operation applies. Drive letters are separated by the semicolon (;) symbol.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.
`--skip-unused-space`	Skips the encryption of unused disk space and encrypts only those sectors on the disk that contain data.

--status command

--stop command

--resume command

--decrypt command

About the --re-encrypt command

The re-encrypt command lets you re-encrypt a disk using a new session key. The command changes the block cipher mode from PlumbCFB to CBC.

> **NOTE**
>
> Use this command after upgrading v10.3.2 clients. Re-encryption is blocked for new v11 clients and all other clients that are upgraded from v8.2.1 or v11.0.x.

The re-encrypt command only changes the block cipher mode from PlumbCFB to CBC (zero to three). It does not change the AES strength of the disk, which is already encrypted.

Re-encryption works only at the time that the fully encrypted clients are upgraded. After the block cipher mode is changed, the command will not run.

As a client administrator or privileged user, you cannot trigger decryption until after the re-encryption process finishes. However, you can pause and resume the re-encryption process.

The status message *re-encryption is in progress* is displayed in the command-line interface and in the Client Administrator Console interface. The Symantec Endpoint Encryption Management Console does not display any information for the re-encryption process. However, an audit event is sent to the server to indicate the start and completion of the re-encryption process.

--re-encrypt command

--stop command

--resume command

--re-encrypt command

Purpose: The `--re-encrypt` command lets you re-encrypt a disk using a new session key. The command changes the block cipher mode from PlumbCFB to CBC.

> **NOTE**
>
> Use this command after upgrading v10.3.2 clients. Re-encryption is blocked for new v11 clients and all other clients that are upgraded from v8.2.1 or v11.0.x.

Usage format:

```
eedAdminCli --re-encrypt --disk <number> --au <AdminUserName>
--ap <AdminPassword>
```

Table 6: Options for the --re-encrypt command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.

Option	Description
<AdminPassword>	The password of this client administrator.

About the --re-encrypt command

--stop command

--resume command

--stop command

Purpose: The --stop command halts the current encryption or decryption process.

Usage format:

```
eedAdminCli --stop --disk <number> --partition-list <drive letters>
--au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --stop --disk 0 --au jsmith --ap safepass

Request sent to Stop encrypt or decrypt was successful.
```

This example shows all of the encryption or decryption processes on disk 0 being stopped.

Table 7: Options for the --stop command

Option	Description
--disk	Specifies the disk to which the operation applies.
<number>	The disk number on the system. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks.
--au	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
<AdminUserName>	The user name of the existing client administrator.
--ap	Specifies the password of this client administrator.
<AdminPassword>	The password of this client administrator.

To continue the process, use the --resume command.

--resume command

--resume command

Purpose: The --resume command continues the current process, either the encryption or the decryption of a disk or any of its partitions.

Usage format:

```
eedAdminCli --resume --disk <number> --au <AdminUserName>
--ap <AdminPassword>
```

Example:

```
eedAdminCli --resume --disk 0 --au jsmith --ap safepass

Request sent to Resume encrypt or decrypt was successful.
```

This example shows all of the encryption or decryption processes on disk 0 being resumed.

Table 8: Options for the --resume command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

To halt the process, use the `--stop` command.

--stop command

Preboot configuration setup and display commands

About the preboot configuration setup and display commands

The preboot configuration setup and display commands let you configure the visual and auditory characteristics of the preboot authentication screen. Commands include the ability to define the input and display language, the presence or absence of audio cues, and how a password is displayed as a user authenticates. You can also view the overall configuration of the preboot authentication environment, including the login message, any startup screen appearance, and the computer name.

NOTE

If you are a privileged user, do not include client administrator credentials in a command.

--set-language command

Purpose: The `--set-language` command sets the display language and the input language for the preboot authentication screen. The preboot authentication screen supports the following languages: English, French, German, Japanese, and Spanish. However, Japanese is supported on BIOS-based systems only; it is not supported for the preboot authentication screen on UEFI-based systems.

This command is supported on systems booting in BIOS and UEFI modes.

Usage format:

```
eedAdminCli --set-language --disk <number> --display <language>
--keyboard <language> --au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --set-language --disk 0 --display de --keyboard de
--au jsmith --ap safepass

Boot Language is set to Keyboard=en    Display=en
Boot Language now set to Keyboard=de  Display=de
Request sent to Set boot languages was successful
```

This example shows the change in the display language and the input language from English to German at the preboot authentication screen on the disk 0.

NOTE

You can run the `eedAdminCli.exe --help` command to view all the supported languages that you can set.

Table 9: Options for the --set-language command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system. Disk 0 indicates the boot disk. Any other disk number indicates secondary disks.

Option	Description
`--display`	Specifies the display screen that is used at the preboot authentication screen. The preboot authentication screen supports the following languages: English, French, German, Japanese, and Spanish. By default, the preboot authentication screen is displayed in the language that your administrator configures. **Note:** Japanese is not a supported language for the preboot authentication screen on UEFI-based systems.
`<language>`	Specifies the language of the display screen, which is limited to the following languages: English, German, Spanish, French, and Japanese.
`--keyboard`	Specifies the keyboard that is used at the preboot authentication screen.
`<language>`	Specifies the language of the keyboard.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

--set-sound command

Purpose: The `--set-sound` command enables or disables audio beeps during preboot authentication.

This command is supported on systems booting in BIOS and UEFI modes.

Usage format:

```
eedAdminCli --set-sound --disk <number> --beep | --nobeep
--au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --set-sound --disk 0 --no-beep
--au jsmith --ap safepass

Accessibility Sounds set to [NO]
Request sent to Set accessibility sounds was successful.
```

This example disables audio beeps during preboot authentication on disk 0.

Table 10: Options for the --set-sound command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system. The preboot authentication screen supports the following languages: English, French, German, Japanese, and Spanish. However, Japanese is not a supported language for the preboot authentication screen on UEFI-based systems.
`--beep`	Specifies that audio beeps are enabled during preboot authentication.

Option	Description
`--nobeep`	Specifies that audio beeps are disabled during preboot authentication.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

--show-config command

--bootprop-set --name “PWDFORMAT” command

Purpose: The `--bootprop-set --name “PWDFORMAT”` command sets the display characters that appear when a user or an administrator types a password on the preboot authentication screen. The characters that are displayed are either asterisk characters or the random stepping of the cursor through blank spaces. By default, the preboot authentication screen displays asterisk characters.

Usage format:

```
eedAdminCLi --bootprop-set --name "PWDFORMAT" --val <num>
--au <AdminUserName> --ap <AdminPassword>
```

Example 1:

```
eedAdminCLi --bootprop-set --name "PWDFORMAT" --val 0
--au jsmith --ap safepass
```

This example configures preboot authentication to use asterisk characters.

Example 2:

```
eedAdminCLi --bootprop-set --name "PWDFORMAT" --val 1
--au jsmith --ap safepass
```

This example configures preboot authentication to use random stepping of the cursor.

Table 11: Options for the --bootprop-set --name “PWDFORMAT” command

Option	Description
`--name`	Specifies the name of the boot property being set.
`"PWDFORMAT"`	Identifies the format in which characters are displayed when a user or an administrator types their password on the preboot authentication screen.
`--val`	Specifies which password format is set in preboot authentication.
`<num>`	`0` sets asterisks `1` sets random stepping of the cursor
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.

Option	Description
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

--show-config command

Purpose: The `--show-config` command displays information about how the preboot authentication screen is configured on an encrypted disk.

Usage format:

```
eedAdminCli --show-config --disk <number>
```

Example:

```
eedAdminCli --show-config --disk 0

Login Message: Welcome to Symantec Endpoint Encryption. install time
Display Startup Screen: No
  Display Machine Name: No
          Machine Name: INSPIRION. WORKGROUP.SYSTEM.
     Use Audio Prompts: No

Request sent to Show configurations was successful.
```

This example shows the preboot information for a boot disk that is encrypted.

Table 12: Options for the --show-config command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.

--set-sound command

Autologon boot bypass commands

About Autologon

Autologon lets a system restart one or more times without a user having to authenticate at the Symantec Endpoint Encryption preboot authentication screen.

> **NOTE**
>
> Using this boot bypass feature weakens the protection that Drive Encryption provides. Pay extra attention to the physical security of systems when Autologon is enabled and the bypass count starts. Use the `--disable-{{SEEAutolgn}}` command to remove any unnecessary remaining bypass restarts.

Autologon is generally used for remote deployment or upgrade scenarios when one or more restarts are required. Patch management is an example of a process that can require multiple restarts.

> **NOTE**
> Beginning with the Symantec Endpoint Encryption 11.3.1 release, the Autologon policy options are bundled with the Drive Encryption MSI, and no separate Autologon utility is required to install on the client system.

After the Drive Encryption MSI is deployed to the client computers with the Autologon policy options, you may be able to use the Administrator Command Line to manage Autologon. The `--enable-{{SEEAutolgn}}` or `--disable-{{SEEAutolgn}}` commands enable or disable the Autologon functionality on the client computer. You can set the count of authentication screen bypasses using the `--enable-{{SEEAutolgn}}` command with the --count option.

> **NOTE**
> If the policy administrator has disabled the autologon completely, through the install-time **Do not use Autologon** policy option, then you cannot enable autologon on the client computers even through Drive Encryption Administrator Command Line. To enable autologon in such a case, you need to uninstall the client and install again with the **Do not use Autologon** policy option deselected.

The following conditions affect the management of the Autologon locally from Administrator Command Line:

- A policy administrator can deploy a Drive Encryption - Autologon policy to enable or disable autologon on a client computer. When the administrator uses policies to manage autologon, and at the same time if you attempt to manage autologon using Administrator Command Line, you receive an error message. The command line is disabled.
- If the policy administrator wants client administrators, privileged users, or SYSTEM users to manage autologon, the administrator deploys a policy to support that local management. When this transfer of management takes place, the default state of Autologon is disabled. You must issue the `--enable-{{SEEAutolgn}}` command to activate autologon.
- Beginning with the Symantec Endpoint Encryption 11.3.1 release, the client administrator can enable or disable autologon locally, if the **Autologon only when activated by admin locally** policy option is selected in either install-time setting, GPO, or native policy.
  In a scenario, where the Symantec Endpoint Encryption client is deployed in an never-connected environment, then ensure to select the**Autologon only when activated by admin locally** option for autologon and only then the client administrator can manage autologon locally.

  > **NOTE**
  >
  > If you are a privileged user or a SYSTEM user, do not include client administrator credentials in a command.

--check-Autologon command

--enable-Autologon command

--disable-Autologon command

--check-Autologon command

Purpose: The `--check-{{SEEAutolgn}}` command indicates whether Autologon boot bypass is configured for the boot drive. In addition, it indicates whether TPM-based authentication is enabled for Autologon users on client computers that support the feature.

Usage format:

```
    eedAdminCli --check-Autologon

--au <AdminUserName> --ap <AdminPassword>
```

Example:

```
    eedAdminCli --check-Autologon --au jsmith --ap safepass

    Autologon Enabled
    No.of reboots remaining:1
    TPM Usage: Yes
    Request sent to Check Autologon was successful.
```

This example shows that Autologon is enabled and has one remaining reboot, and that TPM-based authentication is enabled for Autologon on that client computer.

Autologon precedence policy

The policy administrator can enforce a check-in policy to schedule and monitor client computers through periodic contact with the server. When a client computer fails to contact the server within the prescribed schedule, the computer is locked out at preboot. However, if Autologon has been enabled when a computer is locked out, a user can log on to that computer without authenticating at preboot. To protect the data while Autologon is enabled, the policy administrator can configure the Autologon precedence policy and enable the **Client monitor lockout takes precedence over Autologon** policy. When this policy is enabled and when the lockout occurs, the computer remains in a preboot state after restart. Also, users cannot log on to the computer without the assistance from the help desk or until a client administrator unlocks the system.

To verify whether the Autologon precedence policy is enabled on a client computer, you can use the `-- show config` command in the following format:

Usage format:

```
eedAdminCli --show-config [--disk <number>]
```

Example:

```
eedAdminCli --show-config

     Login Message: Welcome to Symantec Endpoint Encryption.
     Display Startup Screen: No
       Display Machine Name: No
              Machine Name: INSPIRION. WORKGROUP.SYSTEM.
          Use Audio Prompts: No
Autologon precedence policy: Client Monitor Lockout takes
                             precedence over Autologon

Request sent to Show configurations was successful
```

If the policy administrator enabled users to log on to a locked out computer when Autologon is enabled, then the output of the `-- show config` command displays the following:

```
Autologon precedence policy: Autologon takes
precedence over Client Monitor Lockout
```

Table 13: Options for the --check-Autologon command

Option	Description
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user or SYSTEM user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.
`--disk`	Specifies the disk to which the command applies.
`<number>`	The disk number on the system.

--enable-Autologon command

--disable-Autologon command

--enable-Autologon command

Purpose: The `--enable-{{SEEAutolgn}}` command enables Autologon boot bypass on a system.

Usage format:

```
eedAdminCli --enable-Autologon --count <count> --au <AdminUserName>
--ap <AdminPassword>
```

Example:

```
eedAdminCli --enable-Autologon --count 3 --au jsmith --ap safepass

            Request sent to Enable Autologon was successful
```

This example shows that three bypass restarts were added to the boot disk on the system.

Table 14: Options for the --enable-Autologon command

Option	Description
`--count`	Specifies the number of times Autologon can restart a system. The maximum count can be set to 10. The default count is 1, if you have enabled autologon and did not mention the `--count` option in command.
`<count>`	The number of restarts allowed.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user or SYSTEM user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

About Autologon

--check-Autologon command

--disable-Autologon command

--disable-Autologon command

Purpose: The `--disable-{{SEEAutolgn}}` command removes Autologon boot bypass from the system, including the original and the remaining bypass counts.

Usage format:

```
eedAdminCli --disable-Autologon --au <AdminUserName>
--ap <AdminPassword>
```

Example:

```
eedAdminCli --disable-Autologon --au jsmith --ap safepass

Request sent to Disable Autologon was successful
```

This example shows the removal of Autologon boot bypass from a disk.

Table 15: Options for the --disable-Autologon command

Option	Description
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user or SYSTEM user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

About Autologon

--check-Autologon command

--enable-Autologon command

Client-server commands

About the client-server commands

The client-server commands display the next due date for client check-in with the server or extend the date by which a client must check in.

NOTE

If you are a privileged user, do not include client administrator credentials in a command.

--show-client-monitor command

Purpose: The `--show-client-monitor` command displays the next due date before which the client computer should connect with the server at least once.

Usage format:

```
eedAdminCli --show-client-monitor --au <AdminUserName>
--ap <AdminPassword>
```

Example:

```
eedAdminCli --show-client-monitor --au jsmith --ap safepass

Next due date: Tue Aug 12 15:45:24 2014
Request sent to Show client monitor was successful
```

This example shows the next time that this client computer must check in.

Table 16: Options for the --show-client-monitor command

Option	Description
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of an existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

--extend-client-monitor command

Purpose: The `--extend-client-monitor` command extends the next due date before which the client computer should connect with the server. The maximum number of days by which the client computer can be extended to connect with the server is 180 days.

Usage format:

```
eedAdminCli --extend-client-monitor --days <number>
--au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --extend-client-monitor --days 2
--au jsmith --ap safepass

Next due date: Tue Aug 14 15:45:24 2014

Request sent to Extend client monitor was successful
```

This example shows that administrator has extended the client computer due date for synchronization with the server by 2 days.

Table 17: Options for the --extend-client-monitor command

Option	Description
`--days`	Specifies the days by which the client computer check-in time is extended.
`<number>`	The number of days by which the client computer is extended to connect with the server. The maximum number of days by which the client computer can be extended to connect with the server is 180 days.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

User management commands

About the user management commands

Using the user management commands you can:

- Register users to a Drive Encryption-encrypted disk on a computer
- List and verify the registered users on a computer
- Unregister users from a Drive Encryption-encrypted disk
- Change a registered user's password or domain

A registered user is one who is registered with Drive Encryption. Only a registered user of Drive Encryption can access an encrypted disk. Symantec Endpoint Encryption Drive Encryption supports three types of users. Using Administrator Command Line, you can register the following types of users:

- Users authenticating using Windows credentials at preboot and at the Windows logon screen.
- Users authenticating at preboot with a Windows user name and Drive Encryption password, then authenticating to Windows using Windows credentials.
- Users authenticating at preboot using a Drive Encryption user name and a Drive Encryption password, then authenticating to Windows using Windows credentials.

NOTE

The `--disk` option is optional when you issue a command. If you do not specify a disk number along with a command, information of the boot disk is displayed. Disk 0 indicates the boot disk. Any other disk number indicates a secondary disk.

NOTE

If you are a privileged user, do not include client administrator credentials in a command.

--list-users command

Purpose: The `--list-users` command lists user information for all registered users, client administrators, and the Autologon user, if applicable.

Usage format:

```
    eedAdminCli --list-users [--disk <number>]
 --au <AdminUserName> --ap <AdminPassword>
```

Example:

```
    eedAdminCli --list-users --disk 0 --au jsmith --ap safepass

    Registered Windows Users: 3
    User 1: Name: Alice Cameron1 Type: Symmetric A: W
    User 2: Name: Alice Cameron2 Type: Symmetric A: WP
    User 3: Name: Alice Cameron3 Type: Symmetric A: P

    Console Admin User:2
    User 1: Name: jsmith1 Type:Symmetric A: M Privileges: DD,UM,UL,EL
    User 2: Name: jsmith2 Type:Symmetric A: M Privileges: DD,UL,EL

    Attribute Information:
```

```
L = Locked out, M = Console Admin, W = Windows User
WP = Windows user with Non-Windows Password,
P = Passphrase User
AE = Auto Encrypt , AL = Autologon,
DESR = DE Self Recovery Available
DD = Decrypt Drives, UM = User Management,
UL = Unlock, EL = Extend Lockout
T = Token User, TW = Token User with SSO

Request sent to List users on disk was successful
```

This example list users who can authenticate to the encrypted boot disk.

Table 18: Options for the --list-users command

Option	Description
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.

--verify-user command

--register-user command

--unregister-user command

--verify-user command

Purpose: The `--verify-user` command verifies whether the password of an authorized user is registered to an encrypted disk. The authorized user can be a registered user, a client administrator, or a Drive Encryption Self-Recovery user. You may specify a domain name of the user account that you want to verify.

Usage format:

```
eedAdminCli --verify-user [--disk <number>] -u <username>
-p <phrase> [--domain <domain>]
--admin <admin> --au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --verify-user --disk 0 -u "Alice Cameron" -p userpass
--au jsmith --ap safepass

Successfully verified user
Name: Alice Cameron: Type Symmetric A: S

Attribute Information:
S = SSO,  L = Locked out, M = Console Admin, W = Windows User
```

```
AE = Auto Encrypt , AL = Auto Logon,
DESR = DE Self Recovery Available

Request sent to Verify user authentication was successful.
```

This example shows a password that is verified by specifying the user name and disk number.

Table 19: Options for the --verify-user command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.
`-u`	Specifies a user name for an operation.
`<username>`	The user name of an authorized user account on the disk.
`-p`	Specifies the password for the operation.
`<phrase>`	The password of an authorized user on the disk.
`--domain`	Specifies the domain for the user account. The default is the current domain, if one has been established. The domain is required for any user who has a domain.
`<domain>`	The domain for the user account.
`--admin`	Specifies that this user is a client administrator.
`<admin>`	The name of the user client administrator.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

--list-users command

--unregister-user command

--register-user command

Purpose: The `--register-user` command adds an authorized user to an encrypted disk.

To issue the `--register-user` command you need to have the User Management client administrator privilege.

Usage format:

```
eedAdminCli --register-user [--disk <number>] [--token] [--sso] -u <username>
-p <phrase> --user-type <w/wp/p>
[--certificatepath <user_certificate_filepath>]
[--domain <domain>]
[--otp <otpVal>] [--admin]
--au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --register-user --disk 0 -u "Alice Cameron"
```

```
-p alicepass --user-type wp --au jsmith --ap safepass

 Warning: Domain name missing or invalid domain name specified.

 Request sent to Register user was successful
```

This example shows that password-based user Alice Cameron has been added as a registered user to the boot disk with `alicepass` as the password. The user type, **wp**, indicates that the Windows user is registered with a Drive Encryption password. The password `safepass`, which belongs to an existing client administrator, is used for authentication.

Table 20: Options for the --register-user command

Option	Description
`--token`	Specifies a token user. **Note:** You must include this command option if you use the `--certificatepath` option to register a user certificate.
`--sso`	Creates a user as a single sign-on user.
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.
`-u`	Specifies a user name for an operation.
`<username>`	The user name of the user being added.
`-p`	Specifies the user's password.
`<password>`	The password for this authorized user.
`--domain`	Specifies the user's domain. The default is the current domain, if one has been established. The domain is required for any user who has a domain.
`<domain>`	The user's domain.
`--user-type`	Specifies the following types of users: • W – Windows user; users authenticate using Windows credentials at preboot and at the Windows logon screen. • WP – Windows user with Drive Encryption password; users authenticate at preboot with a Windows user name and Drive Encryption password, then authenticate to Windows using Windows credentials. • P – Passphrase user; users authenticate at preboot using a Drive Encryption user name and a Drive Encryption password, then authenticate to Windows using Windows credentials.
`--otp`	The One-Time Password (OTP) for this disk to be used for authentication.
`--certificatepath`	Specifies the file path of the user certificate to be registered. **Note:** If you include the `--certificatepath` command option, you must include the `--token` option as well.
`<user_certificate_filepath>`	The file path of the user certificate.
`<otpVal>`	The value of the OTP.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.

Option	Description
<AdminUserName>	The user name of the existing client administrator.
--ap	Specifies the password of this client administrator.
<AdminPassword>	The password of this client administrator.

--unregister-user command

--unregister-user command

Purpose: The `--unregister-user` command removes an authorized user from the encrypted disk. To issue the `--unregister-user` command you need to have the User Management client administrator privilege.

Usage format:

```
eedAdminCli --unregister-user [--disk <number>] -u <username>
-p <phrase> [--domain <domain>]
--admin <admin> --au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --unregister-user --disk 0 -u "Alice Cameron"
-p alicepass --au jsmith --ap safepass

Request sent to Unregister user was successful
```

This example shows user Alice Cameron being removed from the boot disk by an existing client administrator.

Table 21: Options for the --unregister-user command

Option	Description
--disk	Specifies the disk to which the operation applies.
<number>	The disk number on the system.
-u	Specifies a user name for an operation.
<username>	The user name of the user being removed.
-p	Specifies the password for the operation.
<phrase>	The password of the authorized user being removed.
--domain	Specifies the domain to which the user authenticates.
<domain>	The domain for the user account.
--admin	Specifies that this user is a client administrator.
<admin>	The user client administrator's name.
--au	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
<AdminUserName>	The user name of the existing client administrator.
--ap	Specifies the password of this client administrator.
<AdminPassword>	The password of this client administrator.

--register-user command

--change-passphrase command

Purpose: The `--change-passphrase` command changes a user's password.

> **NOTE**
>
> You cannot use this command to change a Windows or Active Directory password of a Windows user. Using this command, you can change a Drive Encryption password of a Windows user or a Passphrase user.

Usage format:

```
eedAdminCli --change-passphrase [--disk <number>] -u <username>
-p <phrase>  --new-passphrase <newpass>
[--domain <domain>] [--otp <otpVal>]
--au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --change-passphrase --disk 0 -u "Alice Cameron"
--new-passphrase isAlice -p wasAlice --au jsmith --ap safepass

Request sent to Change user's passphrase was successful.
```

This example shows a client administrator changing an existing user's password on an encrypted disk.

Table 22: Options for the --change-passphrase command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.
`-u`	Specifies a user name for an operation.
`<username>`	The user name of the authorized user account on the disk.
`-p`	Specifies the user's password.
`<phrase>`	The user's password.
`--domain`	Specifies the user authentication domain.
`<domain>`	The domain to which the user authenticates.
`--new-passphrase`	Indicates changing an existing password to a new password.
`<newpass>`	The text of the new password.
`--otp`	The One-Time Password (OTP) for this disk is used for authentication.
`<otpVal>`	The value of the OTP.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

--change-userdomain command

--change-userdomain command

Purpose: The `--change-userdomain` command changes a user's authentication domain.

Usage format:

```
eedAdminCli --change-userdomain [--disk <number>] -u <username>
--new-domain <newdomain> [--domain <domain>] --au <AdminUserName>
--ap <AdminPassword>
```

Example:

```
eedAdminCli --change-userdomain --disk 0 --user "Alice Cameron"
--new-domain EXAMPLECORP --au jsmith --ap safepass

Request sent to Change user's domain was successful
```

This example shows the client administrator "jsmith" changing a user's existing authentication domain to a new domain.

Table 23: Options for the --change-userdomain command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.
`-u`	Specifies a user name for an operation.
`<username>`	The user name of the authorized user account on the disk.
`--new-domain`	Indicates changing an existing domain to a new domain.
`<newdomain>`	The name of the new domain.
`--domain`	Specifies the current user domain.
`<domain>`	The domain to which the user authenticates.
`--au`	Specifies the user name of an existing client administrator. **Note:** If you are running the command as a privileged user, do not include client administrator credentials.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

--change-passphrase command

Recovery command

--recover command

Purpose: The `--recover` command restores the Drive Encryption Master Boot Record (MBR) if the encrypted disk's MBR is corrupt and the preboot authentication screens does not appear.

Usage format:

```
eedAdminCli --recover
```

NOTE

As a best practice, for critical disks before running the `--recover` command, you must create a clone of these disks. The `--recover` command is irreversible. Therefore, it is best to make a clone of these disks and execute this command on the image. So that if required you can create a copy of this disk for data recovery.

Disk authentication for WinPE recovery command

--auth or --auth-disk command

Purpose: The `--auth` or `--auth-disk` command authenticates to the disk for a WinPE recovery.

Usage format:

```
eedAdminCli --auth-disk --disk <number> --au <AdminUserName> --ap <AdminPassword>
```

Example:

```
eedAdminCli --auth-disk --disk 0 -u "Alice Cameron"
-p alicepass --au jsmith --ap safepass

Request sent to Authenticate disk was successful
```

This example authenticates disk 0 with the user Alice Cameron using a password to authenticate to the boot disk.

Table 24: Options for the --auth-disk command

Option	Description
`--disk`	Specifies the disk to which the operation applies.
`<number>`	The disk number on the system.
`-u`	Specifies the user name for the operation.
`<username>`	The user name of the authorized user account on the disk.
`-p`	Specifies the password of the user.
`<phrase>`	The user's password.
`--au`	Specifies the user name of an existing client administrator.
`<AdminUserName>`	The user name of the existing client administrator.
`--ap`	Specifies the password of this client administrator.
`<AdminPassword>`	The password of this client administrator.

Slave disk recovery

About slave disk recovery

You can recover and copy data from a locked encrypted computer by connecting the locked hard drive as a USB device (slave drive) to another computer with Drive Encryption installed. The locked hard drive can also be connected to an extra hard disk slot if any.

You can recover locked encrypted computer with Drive Encryption version 11.2.1 and later installed by connecting the locked hard drive to another computer with Drive Encryption 11.3.0 installed.

If the slave drive is encrypted on a system running Windows 10, ensure that it is connected to another computer running Windows 10 with Drive Encryption installed. If the other computer has a Windows operating system earlier than Windows 10, the slave drive may not be detected and the disk cannot be unlocked.

NOTE

The slave drive recovery feature is not supported on a hardware-encrypted Opal v2 compliant drive.

However, if the Opal v2 compliant drive is software encrypted, the slave drive recovery feature can be used to recovery such software-encrypted Opal disks.

Supported commands on slave disk

The following commands are supported for the slave disk recovery:

- `--enum`
  --enum command
- `--info`
  --info command
- `--status`
  --status command
- `--list-users`
  --list-users command
- `--auth` or `--auth-disk` command using client administrator credentials
  You can run the authentication command as a client administrator or as a help desk administrator.
  You can use this command to authenticate the slave disk using client administrator credentials as follows and recover boot as well as secondary disk of the slave drive:
  `eedAdminCli --auth-disk --disk <number> --au <AdminUserName> --ap <AdminPassword>`
  Where specifies the disk number of the slave disk to which the operation applies.
  --auth or --auth-disk command
- `--auth` command using help desk administrator
  You can use the `auth` command using the help desk recovery token to recover data only from the boot disk of the slave drive. You cannot recover data from the secondary disk of the slave drive using the auth command with the help desk recovery token. However, you can recover the data on the secondary disk of the slave disk with client administrator credentials.
  You can use the help desk recovery token (response key) to authenticate and decrypt the corrupted disk; stop and resume decryption.
  You can use the `--verbose (or -v)` parameter to print the challenge key also.
  Run the following commands for recovery:
  – To authenticate the disk

```
eedAdminCli.exe --auth --disk <disk number of slave drive> --response-key <response key
received from {{SEEMgmtServer}} help desk administrator>
```

– To decrypt the corrupted disk

```
eedAdminCli.exe --decrypt --disk <disk number of slave drive> --response-key <response key
received from {{SEEMgmtServer}} help desk administrator>
```

– To stop decryption

```
eedAdminCli.exe --stop <disk number of slave drive> --response-key <response key recovered
from Symantec Endpoint Encryption Management Server help desk administrator>
```

– To resume decryption

```
eedAdminCli.exe --resume <disk number of slave drive> --response-key <response key recovered
from Symantec Endpoint Encryption Management Server help desk administrator>
```

- `--decrypt`
  You can run the decrypt command to start, stop, or resume decryption.
  --decrypt command
- `--recover` or `--recover disk`
  Use this command to recover the corrupted Master Boot Record (MBR).
  --recover command

Quick reference for commands and options

List of commands

The tables list the Administrator Command Line commands by function.

Table 25: Generic commands

Command	Description
`--help` (`-h`)	Displays help information for Administrator Command Line. Includes the syntax and the commands with options.
`--version` (`-v`)	Displays Administrator Command Line version information.

Table 26: Disk information commands

Command	Description
`--enum`	Lists the system disks and volumes.
`--info`	Lists general system disk information.
`--show-config`	Displays the preboot configuration information.
`--status`	Displays the Drive Encryption status of the disk.

Table 27: Disk operation commands

Command	Description
`--decrypt`	Decrypts a specified disk or partition.
`--encrypt`	Encrypts a specified disk or partition.
`--re-encrypt`	Re-encrypts the disk using a new session key, changing the block cipher mode from PlumbCFB to CBC.
`--resume`	Resumes a halted encryption or decryption process.
`--stop`	Halts the encryption or decryption process.

Table 28: Preboot configuration set and display commands

Command	Description
`--bootprop-set --name "PWDFORMAT"`	Sets the preboot authentication screen with asterisk characters or random-stepping of the cursor through blank spaces when a password is being typed.
`--set-language`	Sets the display language and the input language for the preboot authentication screen.
`--set-sound`	Enables or disables audio beeps at preboot authentication.
`--show-config`	Displays the preboot configuration information.

Table 29: Autologon commands

Command	Description
`--check-{{SEEAutolgn}}`	Checks if the Autologon function is enabled.
`--disable-{{SEEAutolgn}}`	Disables the Autologon function.
`--enable-{{SEEAutolgn}}`	Enables the Autologon function.

Table 30: Disk authentication for WinPE recovery command

Command	Description
`--auth-disk`	Authenticates to the disk for a WinPE recovery.

Table 31: Client-Server commands

Command	Description
`--extend-client-monitor`	Extends the next due date before which the client computer should connect with the server.
`--show-client-monitor`	Connects to the server and displays the next due date before which the client computer should connect with the server.

Table 32: User management commands

Command	Description
`--change-passphrase`	Changes the password of a specified user.
`--change-userdomain`	Changes the authentication domain of a specified user.
`--list-users`	Lists the authorized users on an encrypted disk.
`--register-user`	Adds a user to the disk.
`--unregister-user`	Removes a user from a specified disk.
`--verify-user`	Verifies a user's password.

List of options

List of options

The alphabetical list of Administrator Command Line options follows.

Table 33: Administrator Command Line Options (alphabetical)

Option	Description
`--admin`	Used to verify or remove a client administrator.
`--ap`	Specifies the password of an existing client administrator.
`--au`	Specifies the user name of an existing client administrator.
`--beep`	Enables beep sound when preboot authentication screen appears.

Option	Description
`--count`	Indicates the number of times a restart can be performed using autologon.
`--days`	Specifies the days by which the client computer should connect with the server.
`--disk` (`-d`)	Specifies the number of the target disk. Zero (0) is the boot disk.
`--display`	Specifies the display screen that is used at the preboot authentication.
`--domain`	Specifies the user authentication domain.
`--keyboard`	Specifies the keyboard that is used at the preboot authentication screen.
`--language`	Specifies the language of the display screen, which is limited to the following languages: English, German, Spanish, French, and Japanese. Also specifies the language of the keyboard.
`--new-domain`	Specifies a new domain for a user.
`--new-passphrase`	Specifies a new password for an existing user.
`--no-beep`	Specifies that audio beeps are disabled during preboot authentication.
`--otp`	Specifies the One-Time Password, which is the Response key. The Response key is provided by the help desk administrator during the help desk recovery.
`--passphrase` (`-p`)	Specifies a password for an operation.
`--skip-unused-space`	Skips the encryption of unused disk space and encrypts only those sectors on the disk that contain data. Used with the `--encrypt` command.
`--sso`	Creates a user as a single sign-on user.
`--token`	Specifies a token user.
`--user` (`-u`)	Specifies a user name for an operation.
`--verbose`	Specifies in the disk status information whether the Skip unused disk space mode is ON or OFF and the Double-write sectors mode is ON or OFF during encryption.

List of commands

Commands that privileged users can run

Privileged users can run all Administrator Command Line commands, except for WinPE recovery commands. When privileged users run commands, they must not use client administrator credentials.

Commands that SYSTEM users can run

The table lists the commands that SYSTEM users can run. Client administrator credentials must not be used.

Table 34: Commands that SYSTEM users can run

Type of command	Command
Autologon boot bypass commands	`--check-Autologon`
	`--disable-Autologon`

Type of command	Command
	`--enable-Autologon`

Commands that registered users can run

The table lists the commands that registered users can run. No client administrator credentials are required.

Table 35: Commands that registered users can run

Type of command	Command
General commands	`--help`
	`--version`
Disk information commands	`--info`
	`--enum`
	`--status`
Preboot configuration display commands	`--show-config`

Copyright statement


Symantec
A Division of Broadcom