Symantec Encryption Desktop for Windows Release Notes

10.4.2
Symantec Encryption Desktop 10.4.2 for Windows Release Notes

Documentation version: 10.4.2

Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTECCORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration
If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:
support.symantec.com

Customer service
Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:
- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan        customercare@symantec.com
Europe, Middle-East, and Africa    semea@symantec.com
North America and Latin America  supportsolutions@symantec.com
Symantec Encryption Desktop for Windows
Release Notes 10.4.2

This document includes the following topics:

- What's new in this release
- Resolved issues
- Known issues
- Installation or upgrade
- Documentation resources

What's new in this release

The Symantec Encryption Desktop 10.4.2 for Windows release includes the following improvements and fixes:

- **Compatibility added for Microsoft 10 Fall Creators Update (version 1709) (32-bit and 64-bit)**
  This release supports the in-place upgrade to Windows 10 Fall Creators Update, without having to decrypt and re-encrypt your disk. For more information, see symantec.com/docs/HOWTO128174.

- **Added multiple security updates**
  This release contains multiple security updates and enhancements to ensure strong protection against various security alerts.
Resolved issues

The following issues have been resolved in this release of Symantec Encryption Desktop for Windows.

**Symantec Encryption Desktop**

- On HP Z400 computers running in the UEFI mode, the **Domain** field on the preboot authentication screen now displays the domain name properly. [4008236]
- Installing Symantec Encryption Desktop on a Windows client computer no longer causes network issues. The **NetworkProvider** registry settings are retained and **PGPpwflt** is appended properly to the registry settings on the client computer. [4070675]
- Upgrading to the version 10.4.2 from an earlier version of Symantec Encryption Desktop that contains keys with bad signatures no longer causes key synchronization issues. The user enrollment process and the email encryption process are now successful. Also, any new policy settings are applied successfully on the client computer. [4156635]

**Symantec File Share Encryption**

- Users can successfully open the Microsoft Office files that are protected using Symantec File Share Encryption and stored in the shared folders. Computers no longer crash with a blue screen error message. Environment: Windows 7/10 computers. [4151822] [4151818] [4151820]

**PGP Messaging**

- The encrypted and signed emails that are sent on behalf of a user using the PGP-EML encoding format are no longer sent as attachments to recipients. Environment: Internal users using Outlook with the send-on-behalf-of permission enabled. [4106123]
- The current enforced mail security policy is now properly displayed in the **PGP Messaging > Security Policies** section. Environment: Symantec Encryption Management Server with Symantec Encryption Desktop enabled for PGP Messaging. [4113007]

**Known issues**

This section lists the known issues, any available workarounds, and references to Symantec support center articles for using Symantec Encryption Desktop for Windows.
Symantec Encryption Desktop

- **Incompatibility with Symantec Encryption Desktop when the Controlled Folder Access feature of Windows 10 version 1709 is enabled**: On Windows 10 computers using Symantec Encryption Desktop 10.4.2 with the Controlled Folder Access feature enabled, Symantec Encryption Desktop does not work as expected. To work around this issue, disable the Controlled Folder Access feature and use Symantec Encryption Desktop. [4150124]

- **Preboot authentication fails**: Users of Windows 10 (version 1709) workgroup may not be able to authenticate at the BootGuard screen of Symantec Encryption Desktop 10.4.2. To work around this issue, see the following Workarounds section.

- **Incompatibility of the Windows 10 (1709) Windows Automatic Restart Sign-On (ARSO) with Symantec Encryption Desktop**: On Windows 10 (version 1709) workgroup computers using Symantec Encryption Desktop 10.4.2, Single Sign-On (SSO) may not work even when the policy is enabled. To work around this issue, see the following Workarounds section. [4129711]

**Workarounds**

Perform either of the following workarounds before installing Symantec Encryption Desktop 10.4.2 or before auto-encryption begins on your client computer:

- **Workaround 1**: Disable the *Use my sign in info to automatically finish setting up my device after an update or restart* option. Restart the computer twice. To see this option, navigate to *Windows Settings > Accounts > Sign-in options > Privacy*. For more information, refer to the Microsoft article, [Winlogon Automatic Restart Sign-On (ARSO)](http://www.symantec.com/docs/HOWTO119349).

- **Workaround 2**: Create the following registry:
  
  [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System] DisableAutomaticRestartSignOn=dword:1.

- **Microsoft Windows 10 computers fail to resume from hibernation**: After upgrading your system to Windows 10, Windows restarts instead of resuming from hibernation. For more information, see the following Symantec Knowledgebase article: [http://www.symantec.com/docs/HOWTO119349](http://www.symantec.com/docs/HOWTO119349).

- **Software incompatibility with Acronis True Image**: Removable storage devices are not detected after users disconnect and reconnect them on client systems that have Acronis True Image 2014 installed.

  To work around this issue, make sure that you install Acronis True Image before you install Symantec Encryption Desktop, or disable the Acronis NonStop Backup service. [3670445]

- **Microsoft Surface Pro 3 systems become unresponsive at pre-boot authentication**: If users disconnect and then reconnect the physical keyboard to Microsoft Surface Pro 3 devices at the pre-boot authentication screen, the system becomes unresponsive.
To work around this issue, do not connect or disconnect the Microsoft Surface Pro 3's physical keyboard during pre-boot authentication. Alternatively, if the system has already become unresponsive, reboot the device. [3970715]

Symantec File Share Encryption

- **Office files become corrupt when created using the right-click context menu:** When a PowerPoint 2010 or Excel 2010 file is created using the right-click context menu in a shared folder, the file may become corrupt. Environment: Windows computers using Symantec File Share Encryption 10.4.2. To work around this issue, do one of the following:
  - **Workaround 1:** Open the Excel 2010 or PowerPoint 2010 application first, create the file, and then save the file in the shared folder. Do not use the right-click context menu to create an Excel or PowerPoint 2010 file.
  - **Workaround 2:** Create Excel 2010 or PowerPoint 2010 files on your local drive, and then copy the files to the shared folder.
  - **Workaround 3:** Repair the corrupted file, and then overwrite the file using the *Save As* option. For information on how to repair an Excel or PowerPoint 2010 file, see the Microsoft documentation. [4165819]

- **Key icons are not displayed in file share properties on Windows 10 (64-bit) systems:** On Windows 10 (64-bit) systems, when you view the properties of files that are protected by Symantec File Share Encryption, no icons are displayed next to the keys that are listed in the *Symantec File Share* tab. [3817868]

- **Software incompatibility with Symantec File Share Encryption and Microsoft OneNote:** When you edit the Microsoft OneNote file located on the DFS-shared folder protected by Symantec File Share Encryption, the Microsoft OneNote file may become corrupted. [3794108]

- **Deleting the encryption key from the keyring:** When you create a network shared folder and encrypt it with an encryption key using Symantec File Share Encryption, then later delete the encryption key from the keyring, you can still access the folder using the encryption key stored in the cache. [3565621]

- **Saving files from protected folders to unprotected folders:** When users open files from folders that are protected by Symantec File Share Encryption, and then save them to unprotected folders, the files might remain encrypted instead of being saved in an unencrypted state.

To work around this issue, after you open a file from a protected folder, wait for 30 seconds before you save it to an unprotected folder. Alternatively, save the file using a different file name. [3574072]

**Messaging**

- **Microsoft Outlook in offline mode:** When you send an email from a system running Symantec Encryption Desktop with Microsoft Outlook in offline mode, then the email is incorrectly copied to the 'Sent Items' folder even though the email is not sent. [3376092]
Known issues

Symantec Drive Encryption

- Modifying disk partition with Symantec Encryption Desktop installed causes data loss after disk decryption: If users add, modify, or delete disk partitions after Symantec Encryption Desktop is installed on the system, those partitions become RAW if the disk is later decrypted. Any data that used to exist in those partitions is lost. [3902583]

- Drives encrypted by Microsoft Windows BitLocker: Symantec Drive Encryption does not detect when drives are already encrypted by BitLocker, and gives users the option to encrypt those drives manually. [3690857]

- Software incompatibility with the Symantec Drive Encryption feature: The HP ProtectTools Suite Drive Encryption feature will block encryption of the disk with Symantec Drive Encryption or cause a system crash with a blue screen error message, depending on the order in which the applications are installed. For details on known software compatibility issues with Symantec Encryption Desktop, refer to the Symantec Knowledgebase article TECH223625 (https://support.symantec.com/en_US/article.TECH223625.html). [3406884]

- Refreshing or resetting Microsoft Windows 8, 8.1, and 10 systems. When the boot drive of your Windows 8/8.1 system is encrypted with Symantec Drive Encryption, the refresh and reset features of Windows 8/8.1 do not work properly. To refresh or reset your system, copy your PGP Keys to a USB drive (if applicable), decrypt the boot drive first, refresh or reset your system, install Symantec Drive Encryption, and encrypt the boot drive again. If you have performed refresh or reset operation on your encrypted system and your system does not boot Windows, then decrypt the drive using the Symantec Drive Encryption recovery CD, and then reset or refresh your system using the Windows boot disk. [2984615]

- Hibernating on Microsoft Windows 7 systems. For systems running Microsoft Windows 7 and later, hibernation is not supported during encryption or decryption operations. To avoid data corruption, disable hibernation until the disk is fully encrypted or decrypted. [2827186]

- Hibernating on Microsoft Windows 7 systems. You might run into problems with hibernation after you encrypt your disk. When that happens, delete the hibernation file on resume and continue to boot into Windows. This problem will only occur once after encryption. To avoid the problem, do a reboot after disk encryption is done. [22706/2467652, 27274/2472229]

- Software incompatibility with the Symantec Drive Encryption feature: Certain programs are incompatible with the Symantec Drive Encryption feature; do not install these products on a system with Symantec Encryption Desktop, and do not install Symantec Encryption Desktop on a system with these products installed:
  - Symantec Endpoint Encryption Full Disk [2584593]
  - Faronics Deep Freeze (any edition) [15443/2460632]
  - Utimaco Safeguard Easy 3.x. [8010/2453188]
Hard disk encryption products from GuardianEdge Technologies: Encryption Anywhere
Hard Disk and Encryption Plus Hard Disk products, formerly known as PC Guardian
products. [12065/2457250]

Safeboot Solo co-exists on the system but blocks Symantec Drive Encryption.

SecureStar SCPP co-exists on the system but blocks Symantec Drive Encryption.

Wave Systems’ Dell Embassy Trust Suite co-exists on the system but causes the system
to slow down. [19297/2464461]

Operating system updates during encryption: While your disk is encrypting, do not
accept any operating system updates if they are offered. If the update occurs automatically,
do not restart your computer until the encryption process has completed. [25451/2470403,
25612/2470565]

Do not hibernate during encryption or decryption. If you receive a "Windows Resume
Warning" that "your system's firmware did not preserve the system memory map across
the hibernation transition," you can choose to resume the system. [28625/2473581]

PGP NetShare Command Line

Driver mode cannot be changed on Windows 7 systems: Using the PGP NetShare
Command Line, the--set-driver command does not change the state of the Symantec
File Share Encryption driver.
Workaround: This is an expected behavior which prevents individual users from enabling
or disabling Symantec File Share Encryption on systems that have more than one user.
[2680456]

Installation or upgrade

For information about installing or upgrading to this release of Symantec Encryption Desktop,
see the Symantec Encryption Desktop for Windows User's Guide version 10.4.2. Download

Documentation resources

Documentation is available in PDF format at the Symantec Support Center. Download the
documentation for Symantec Encryption Desktop 10.4.2, 10.4.2, and Symantec Encryption