Symantec™ Encryption Desktop Version 10.4.0 for Windows Release Notes

These Release Notes contain important information regarding this release of Symantec Encryption Desktop for Windows. Symantec strongly recommends you read this entire document.

Warning: Export of this software may be restricted by the U.S. government.

What's Included in This File

- Changes in This Release
- System Requirements
- Installation Instructions
- Licensing
- Known Issues
- Technical Support
- Copyright and Trademarks

Note: To view the most recent version of this document, see http://www.symantec.com/docs/DOC9311.

Changes in This Release

This section lists the changes in this release of Symantec Encryption Desktop.

What's New in Symantec Encryption Desktop Version 10.4 for Windows

Building on Symantec Corporation’s proven technology, Symantec Encryption Desktop 10.4 for Windows includes numerous improvements and the following new features.

- **Symantec Desktop Email no longer bounces a message if a recipient has a Key Not Found (KNF)**

  Previously, if an encrypted email could not be delivered due to one or more recipients having a Key Not Found (KNF), the email bounced. Now, if one or more recipients has a KNF, the email is delivered to the valid recipients. The user may receive a separate email listing the KNF recipients to whom the email was not delivered.

- **Symantec Encryption Desktop registration is simplified**

  You are no longer required to submit your Licensee Name, Licensee Organization, and Licensee Email Information to register a Symantec Encryption Desktop product license. Now, only the License Number is required.
• **TLS 1.2 support added for client-to-server communication**
  Symantec Encryption Desktop, Symantec Encryption Management Server, and PGP Command Line are capable of doing secure communication using TLS 1.2. Symantec Encryption Management Server does still support TLS 1.0, however, for backward compatibility.

• **Compatibility added for Microsoft Windows 10**
  This release supports the installation of Symantec Encryption Desktop on systems running Microsoft Windows 10 Enterprise, both 32- and 64-bit editions.

• **Support ended for Microsoft Windows Server 2003**
  This release ends support for the installation of Symantec Encryption Desktop and Symantec Drive Encryption on systems running Microsoft Windows Server 2003.

• **Compatibility added for Microsoft Office 2016**
  Symantec Encryption Desktop is now compatible with Microsoft Office 2016, both 32- and 64-bit versions.

• **Compatibility added for Microsoft Outlook 2016, both 32- and 64-bit versions.**
  In addition, **Symantec Encryption Desktop is compatible with these email clients:**
  - Mozilla Thunderbird 38.3
  - IBM Notes/IBM Domino Server 9.0.1 FP4
  - IBM Notes/IBM Domino Server 8.5.3

• **Support expanded for virtual servers**
  Symantec Encryption Desktop has been tested for compatibility with VMWare ESXi 6.0 (64-bit edition).

• **Compatibility expanded for Remote Desktop Services**
  Symantec File Share Encryption has been tested with Citrix XenApp 7.6 FP3 and 7.7.

• **Compatibility expanded for tablets**
  Symantec Encryption Desktop has been tested with Microsoft Surface Pro 4.

**Resolved Issues**

This section lists the issues that are resolved in this release.

• Resolved an issue so that the PGP icon overlays now appear correctly on the Dropbox files and folders when you enable Dropbox protection in the consumer policy. [3706942]

• Resolved an issue with Symantec Encryption Desktop so that the messaging library is loaded from the absolute path instead of just the file name. [3901915]

• Resolved an issue so that Symantec Encryption Desktop documentation shortcut links do not appear on the Start Menu or the Apps view on Windows 7 or later systems. [3901729]

For a list of issues that have been resolved since the previous release, please go to the Symantec Knowledgebase (http://www.symantec.com/business/support/index?page=home) and search for TECH166098, ”Symantec Encryption Desktop Resolved Issues.”

**System Requirements**

Symantec Encryption Desktop can be installed on systems running the following versions of Microsoft Windows operating systems:

- Windows 10 November 2015 Update (32-bit and 64-bit editions)
- Windows 10 Enterprise (32-bit and 64-bit editions)
- Windows 10 Pro (32-bit and 64-bit editions)
- Windows 8.1 November 2014 Update (32-bit and 64-bit editions)
- Windows 8.1 Update 2, August 2014 (32-bit and 64-bit editions)
- Windows 8.1 Update 1, May 2014 (32-bit and 64-bit editions)
- Windows 8.1 Enterprise (32-bit and 64-bit editions)
- Windows 8.1 Pro (32-bit and 64-bit editions)
- Windows 8 Enterprise (32-bit and 64-bit editions)
- Windows 8 Pro (32-bit and 64-bit editions)
- Windows 7 Enterprise (32-bit and 64-bit editions, including Service Pack 1)
- Windows 7 Pro (32-bit and 64-bit editions, including Service Pack 1)
- Windows Server 2012 R2 (64-bit edition)
- Windows Server 2012 (64-bit edition)
- Windows Server 2008 R2 (64-bit edition, including Service Pack 1)
- Windows Server 2008 (32-bit and 64-bit editions, including Service Pack 1 or 2)

The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

**Note:** Symantec Drive Encryption is not compatible with 32-bit systems running in UEFI mode.

**Note:** Symantec Drive Encryption is not compatible with other third-party software that could bypass the Symantec Drive Encryption protection on the Master Boot Record (MBR) and write to or modify the MBR. This includes such off-line defragmentation tools that bypass the Symantec Drive Encryption file system protection in the OS or system restore tools that replace the MBR.

Supported virtual servers include:

- VMware ESXi 5.1 (64-bit version)
- VMWare ESXi 6.0 (64-bit edition)

**Additional Requirements for Drive Encryption on UEFI Systems**

The following requirements apply only if you are encrypting your disk. If you are installing Symantec Encryption Desktop only for either email or other Symantec Encryption Desktop functions, you can install on supported 32-bit systems and boot using UEFI mode without having to meet these requirements.

To encrypt systems booting in UEFI mode, the following additional requirements must be met:

- System must be certified for the 64-bit editions of Microsoft Windows 7, Microsoft Windows 8/8.1, or Microsoft Windows 10
- UEFI firmware must allow other programs or UEFI applications to execute while booting
- Boot drive must be partitioned in GPT with only one EFI system partition on the same physical disk
• Boot drive must not be configured with RAID or Logical Volume Managers (LVM)
• Tablets and any systems without a wired or OEM-supplied attachable keyboard are not supported

For more information on the firmware and boot drive, contact your system administrator or hardware manufacturer.

**Symantec Drive Encryption on Windows Servers**

Symantec Drive Encryption is supported on all client versions above as well as the following Windows Server versions:

• Windows Server 2012 R2 64-bit Edition with internal RAID 1 and RAID 5
• Windows Server 2012 64-bit Edition with internal RAID 1 and RAID 5
• Windows Server 2008 R2 64-bit Edition with internal RAID 1 and RAID 5
• Windows Server 2008 64-bit Edition (Service Pack 1 and Service Pack 2) with internal RAID 1 and RAID 5

**Note:** Dynamic disks and software RAID are not supported.

For additional system requirements and best practices information, see the article [https://support.symantec.com/en_US/article.TECH149613.html](https://support.symantec.com/en_US/article.TECH149613.html) at the Symantec Support Center.

**Compatible Email Client Software**

Symantec Encryption Desktop for Windows will, in many cases, work with Internet-standards-based email clients other than those listed here. Symantec, however, does not support the use of other clients.

Symantec Encryption Desktop for Windows has been tested with the following email clients:

• Microsoft Outlook 2016 (32-bit and 64-bit)/Exchange Server 2016 (on-premise only)
• Microsoft Outlook 2016 (32-bit and 64-bit)/Office Cloud Server
• Microsoft Outlook 2013 (32-bit and 64-bit)/Exchange Server 2013 Cumulative Update 10 (on-premise only)
• Microsoft Outlook 2013 (32-bit and 64-bit)/Office 365 Cloud Server
• Microsoft Outlook 2010 (32-bit and 64-bit)/Exchange Server 2010 SP3 (on-premise only)
• Microsoft Outlook 2010 (32-bit and 64-bit)/Office 365 Cloud Server
• Microsoft Outlook 2007 SP2 (Outlook 12)/Exchange Server 2007 SP2
• Microsoft Outlook 2007 SP2 (Outlook 12)/Office 365 Cloud Server
• Microsoft Windows Live Mail version 2012
• Mozilla Thunderbird 38.3
• IBM Notes/IBM Domino Server 9.0.1 FP4
• IBM Notes/IBM Domino Server 8.5.3
Anti-Virus and Other Protection Software Compatibility for Windows

Symantec Encryption Desktop has been tested with the following anti-virus products:

- McAfee AntiVirus Plus (includes McAfee Anti-Virus and Anti-Spyware) 17.6
- Symantec Endpoint Protection 12.1 RU6 MP4
- McAfee AntiVirus LiveSafe 18.0
- McAfee Host Intrusion Prevention System 8.0
- AVG Antivirus Protection Free 16.71.7597
- Sophos Endpoint Security and Control 10.6
- Trend Micro Internet Security 10.0

In all anti-virus programs, enabling real-time scanning detects any viruses as the email or attachments are opened. Therefore, although it is recommended to disable email scanning for some of the anti-virus products listed, your email is still being scanned and you are still being protected by your anti-virus product from viruses spread via email.

Remote Desktop Services Compatibility

Symantec Encryption Desktop for Windows has been tested with the following remote desktop services software:

- Windows Server 2008 (32-bit, including Service Pack 1 or 2) Terminal Services
- Windows Server 2008 R2 (64-bit, including Service Pack 1 or 2) Remote Desktop Services
- Windows Server 2012 (64-bit) Remote Desktop Services
- Windows Server 2012 R2 (64-bit) Remote Desktop Services
- Citrix XenApp 7.6 FP3
- Citrix XenApp 7.7

Symantec Encryption Desktop supports the Symantec File Share Encryption feature in the Citrix XenApp environment. For more information, see the article https://support.symantec.com/en_US/article.INFO3668.html.

Compatible Smart Cards and Tokens for Symantec Drive Encryption BootGuard Authentication

This section describes the system requirements (compatible smart cards/tokens and readers).

Compatible Smart Card Readers for Symantec Drive Encryption Authentication

The following smart card readers are compatible when communicating to a smart card at pre-boot time. These readers can be used with any compatible removable smart card (it is not necessary to use the same brand of smart card and reader).

Generic smart card readers

Most CCID smart card readers are compatible. The following readers have been tested by Symantec Corporation:

- OMNIKEY CardMan 3121 USB for desktop systems (076b:3021)
- OMNIKEY CardMan 6121 USB for mobile systems (076b:6622)
- ActivIdentity USB 2.0 reader (09c3:0008)
- SCM Microsystem Smart Card Reader model SCR3311

**CyberJack smart card readers**
- Reiner SCT CyberJack pinpad (0c4b:0100)

**ASE smart card readers**
- AET SafeSign ASEDrive IIIe USB reader (0dc3:0802)

**Embedded smart card readers**
- Dell D430 embedded reader
- Dell E6410 embedded reader (Broadcom)
- Dell E6510 embedded reader (Broadcom)

**Compatible Smart Cards or Tokens for Symantec Drive Encryption**

This topic lists all of the smart cards or tokens that are supported in Symantec Encryption Desktop 10.4.

Supported smart cards for pre-boot authentication:
- ActivIdentity ActivClient CAC cards, 2005 model
- ActivIdentity ActivClient CAC cards, 2005 and older
- Charismathics CryptIdentity plug 'n' crypt Smart Card only stick
- EMC RSA Smart Card 5200
- Gemalto ASECard Crypto Smart Card
- Gemalto Cyberflex Access 32K V2
- Gemalto Cyberflex Access 64K v2c
- HID Global Crescendo JCOP 21 version 2.4.1 R2 64K
- Marx CrypToken MX2048 JCOP USB token
- Oberthur 64K CosmopolIC v5.2
- Rainbow iKey 3000
- S-Trust StarCOS smart card

**Note:** S-Trust SECCOS cards are not compatible.

- SafeNet 330 smart card
- SafeNet eToken PRO Java 72K
- SafeNet eToken NG-OTP 32K
- T-Systems Telesec NetKey 3.0 smart card

Supported Personal Identity Verification (PIV) cards:
- Gemalto TOP DL GX4 144K FIPS
- Gemalto TOP DM GX4 72k (FIPS)
- Giesecke & Devrient SmartCaf_ Expert 144K DI v3.2
- Giesecke & Devrient SmartCaf_ Expert 80K DI v3.2
• Giesecke & Devrient SmartCafe Expert 5.0
• Giesecke and Devrient Sm@rtCafe Expert 3.2 personal identity verification cards using ActivClient version 6.1 client software
• Oberthur ID-One Cosmo V5.2D personal identity verification cards using ActivClient version 6.1 client software
• Oberthur ID-One Cosmo v7.0 with Oberthur PIV Applet Suite 2.3.2
• Oberthur ID-One Cosmo 128 v5.5 for DoD CAC with V2.6.2b client software

Supported smart cards for storing user keys:
• EMC RSA SecurID 800 Rev A, B, and D
• Gemalto CryptoFlex 32K v1
• Gemalto Cyberflex Access 32K v2
• Gemalto IDBridgeK30 USB token
• Gemalto TOP DL GX4 144K with V2.6.2b Applets
• Oberthur IS-One Cosmo 128 5.5 for DoD CAC with V2.6.2b Applets
• SafeNet eToken PRO Java 72K
• SafeNet eToken PRO USB 64K
• SafeNet eToken PRO USB 32K
• SafeNet eToken NG-OTP 32K
• T-Systems Telesec NetKey 3.0 cards
• Giesecke and Devrient Sm@rtCafe Expert 3.2 personal identity verification cards using AET's SafeSign middleware

Supported smart cards for storing administrator keys:
• SafeNet eToken PRO 64k
• SafeNet eToken PRO 72k
• SafeNet iKey 2032
• AET ASEKey Crypto USB Token
• AET ASECard Crypto Smart Card

**Tablet Support**

Symantec Encryption Desktop for Windows supports the following tablet systems:

• Microsoft Surface Pro 4
• Microsoft Surface Pro 3
• Microsoft Surface Pro 2
• Microsoft Surface Pro 1

To enable compatibility with Secure Boot on Microsoft Surface Pro 1 and Surface Pro 2 laptops, download and run the Microsoft Surface Pro UEFI CA OEM PK Tool. Instructions and the download file are available at http://www.microsoft.com/en-us/download/details.aspx?id=41666. Note that this tool can only be run when your system is decrypted and Secure Boot is enabled.
Installation Instructions

**Note:** You must have administrative rights on your system in order to install Symantec Encryption Desktop.

- **To install Symantec Encryption Desktop on your Windows system**
  1. Locate the Symantec Encryption Desktop installer application and double-click it.
  2. Follow the on-screen instructions.
  3. If prompted to do so, restart your system.

For additional information, including upgrade instructions, see the *Symantec Encryption Desktop for Windows User's Guide*.

**Licensing**

Symantec Encryption Desktop uses a license key to determine what features will be active. Depending on the license key you have, some or all Symantec Encryption Desktop features will be active. Consult your Symantec Encryption Management Server administrator if you have questions about what features are available with your license key.

Use the Setup Assistant to enter your Symantec Encryption Desktop license key after installation. If you are in a domain protected by a Symantec Encryption Management Server, your Symantec Encryption Management Server administrator may have configured your Symantec Encryption Desktop installer with a license key.

For more information about Symantec Encryption Desktop licensing and purchase options, go to the Symantec website.

**Known Issues**

This section lists the known issues, any available workarounds, and reference to Symantec Knowledgebase articles for using Symantec Encryption Desktop.

**General**

- **Microsoft Windows 10 systems fail to resume from hibernation:** After upgrading your system to Windows 10, Windows restarts instead of resuming from hibernation. For more information, see the Symantec Knowledgebase article at [https://support.symantec.com/en_US/article.HOWTO119349.html](https://support.symantec.com/en_US/article.HOWTO119349.html). [3818577]

- **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]

**Symantec File Share Encryption**

- **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]

**PGP 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]

**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]

• **Incompatibility with Microsoft Surface Pro laptops when Secure Boot is enabled on Microsoft Windows 8/8.1 UEFI systems.** Symantec Drive Encryption is incompatible with Microsoft Surface Pro laptops when Secure Boot is enabled (a boot failure occurs when restarting your system after encrypting it). To temporarily work around this issue, disable Secure Boot in your system UEFI settings. For more information, refer to the instructions that came with your system. Note that this is an issue with the Microsoft Surface Pro laptop and could be resolved by Microsoft in the future. [3319192]

• **Refreshing or resetting Microsoft Windows 8/8.1 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 and Windows Vista systems.** For systems running Microsoft Windows Vista 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 and Windows Vista 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, 27724/2472229]

• **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. Note that this is a warning and is not a blue screen. This issue does not occur on Windows XP systems. [28625/2473581]

---

**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:

https://support.symantec.com/content/unifiedweb/en_US/contact-support.html

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:

https://support.symantec.com/content/unifiedweb/en_US/contact-support.html

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:

https://support.symantec.com/content/unifiedweb/en_US/contact-support.html

**Customer Support**

Customer support information is available at the following URL:

https://support.symantec.com/content/unifiedweb/en_US/contact-support.html

Customer Support 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 or manuals

Support Agreement Resources
If you want to contact Symantec regarding an existing support agreement, see https://support.symantec.com/content/unifiedweb/en_US/contact-support.html.

Copyright and Trademarks
Copyright (c) 2016 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, the Checkmark Logo, PGP, Pretty Good Privacy, and the PGP logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. Export of this software may be restricted by the U.S. government.