



Symantec™ Encryption Desktop Version 10.3 for Windows Maintenance Pack Release Notes

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

Symantec Corporation welcomes your comments and suggestions. You can use the information in Getting Assistance to contact us.

Product: Symantec Encryption Desktop

Version: 10.3.2 MP5

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

Note: To view the most recent version of this document, go to the [Products section on the Symantec Corporation website](#).

What's Included in This File

- About Symantec Encryption Desktop
- Changes in this release
- Installing this Maintenance Pack
- Technical Support
- Copyright and Trademarks

About Symantec Encryption Desktop

Symantec™ Encryption Desktop, Powered by PGP Technology is a security tool that uses cryptography to protect your data against unauthorized access.

Symantec Encryption Desktop protects your data while being sent by email. It lets you encrypt your entire hard drive—so everything is protected all the time—or just a portion of your hard drive, via a virtual disk on which you can securely store your most sensitive data. You can use it to share your files and folders securely with others over a network. It lets you put any combination of files and folders into an encrypted, compressed package for easy distribution or backup. Finally, use Symantec Encryption Desktop to shred (securely delete) sensitive files—so that no one can retrieve them—and shred free space on your hard drive, so there are no unsecured remains of any files.

Use Symantec Encryption Desktop to create PGP keypairs and manage both your personal keypairs and the public keys of others.

Changes in This Release

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

For an updated list of system requirements for Symantec Encryption Desktop, see <http://www.symantec.com/docs/TECH224415>.

What's Changed in This Maintenance Pack

What's Changed in Symantec Encryption Desktop for Windows 10.3.2 MP5

Messaging

- Resolved an issue with Microsoft Outlook/MAPI support in Symantec Encryption Desktop so that offline email policies no longer cause email duplication. [3547567]
- Resolved an issue so that Microsoft Outlook with cached mode disabled now properly displays the rich text format content of an email for Microsoft Exchange Server 2013 users. [3456553]

Symantec Drive Encryption

- 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. [3319192]
- Resolved a compatibility issue so that the integrated Broadcom smartcard reader in Dell Latitude E6530 systems now works as expected with PGP BootGuard. [3529298]
- For details on the updated list of the supported smart cards and tokens for the Symantec Drive Encryption administrator keys, refer to the Symantec Knowledgebase article [TECH149099](#). [3583553]

Symantec Encryption Desktop

- Resolved an issue with Symantec Encryption Desktop so that token-based user enrollment failures are logged when the root Certificate Authority (CA) certificate is not present in the **Keys > Trusted Keys** tab of the Symantec Encryption Management Server console. [3493890]

Symantec File Share Encryption

- Resolved an issue with Symantec File Share Encryption so that users can now access the path and user management functions for mounted subfolders of shared, encrypted distributed file system (DFS) folders. [3402457]
- Resolved an issue with Symantec File Share Encryption so that Symantec Encryption Desktop users can now see the name of the group key that was used to encrypt a shared folder. [3555340, 3572636]
- Resolved an issue with Symantec File Share Encryption so that the options for adding and deleting users, and for changing users' roles, are now correctly enabled for group administrators. [3467664]

What's Changed in Symantec Encryption Desktop for Windows 10.3.2 MP4

General

- Improved some functionality issues and further enhanced the overall security of the application.

What's Changed in Symantec Encryption Desktop for Windows 10.3.2 MP3

Symantec Encryption Desktop

- Resolved the CVE-2014-3436 vulnerability so that Symantec Encryption Desktop limits decompression while decoding large encrypted email files, which could have led to a denial-of-service attack. Symantec would like to thank Alexander Klink with n.runs professionals GmbH for reporting this issue and working with Symantec as we addressed it. [3493711]

Symantec File Share Encryption

- Resolved a compatibility issue with Double-Take Availability 7.0.1 so that Microsoft Access files that are encrypted using Symantec File Share Encryption do not become corrupted. This applies to all supported Microsoft Windows platforms, except Windows 8 (32-bit). [3523815]
- Resolved an issue so that users can now modify .txt files in shared folders that are encrypted using Symantec File Share Encryption without causing data corruption when the shared folder is viewed simultaneously on the remote file server. This applies to all supported Microsoft Windows platforms, except Windows 8 (32-bit). [3523820]
- Resolved an issue so that DFS-shared .txt files that are encrypted with Symantec File Share Encryption no longer display garbled data after being modified. [3523825]

What's Changed in Symantec Encryption Desktop for Windows 10.3.2 MP2

Symantec Drive Encryption

- Added compatibility with the following smart cards so that they work properly with Symantec Encryption Desktop at preboot authentication [3508102]:
 - ID-One Cosmo v7.0 with Oberthur PIV Applet Suite 2.3.2
 - Giesecke & Devrient SmartCafe Expert 80K DI v3.2
 - Giesecke & Devrient SmartCafe Expert 144K DI v3.2
 - Gemalto TOP DL GX4 144K FIPS
- Resolved an issue so that the Symantec Encryption Desktop client now correctly displays the storage capacity of a drive when it is greater than 2 TB. [3272070]

What's Changed in Symantec Encryption Desktop for Windows 10.3.2 MP1

Messaging

- Resolved an issue so that users can now send S/MIME encrypted email messages from Symantec Encryption Desktop when only the keyEncipherment flag is enabled in the certificate. [3250866]

Symantec Encryption Desktop

- Resolved an issue so that the lsass.exe process does not terminate abruptly with an error message about the PGP sdk .dll file. [2898169]
- Resolved an issue so that Symantec Encryption Desktop now logs only one event when Symantec Endpoint Encryption Removable Storage is also installed on the same computer. [3153572]
- Resolved an issue so that PGP Zip now successfully opens and decrypts files when the word "message" or "attachment" is included in the file name. [3193714, 3206141]
- Resolved an issue so that the PGPTray process does not terminate unexpectedly at user enrollment on Microsoft Windows 7 systems when folder redirection is enabled. [3243735]
- Resolved the CVE vulnerability (CVE-2014-1646) with a memory read access violation when attempting to parse certain malformed files that could result in an application crash or potential arbitrary code execution with application privileges. Symantec thanks Jeremy Brown (jerbrown) of ReSP working through Microsoft Vulnerability for reporting this and working with us as we addressed it. [3452808]

Symantec Drive Encryption

- Resolved an issue so that users can now add newly created user keys to an external storage device that has an Additional Decryption Key (ADK). [3076950]
- Resolved an issue with Symantec Encryption Desktop so that single sign-on (SSO) passphrases on Microsoft Windows 7 computers are now synchronized at log on, if users are required to specify a Domain Name System (DNS) or User Principal Name (UPN) domain. [3299738]
- Resolved an issue so that users cannot bypass PGP BootGuard when the bypass feature is disabled. [3304044]
- Added compatibility with Giesecke and Devrient Sm@rt Café Expert 5.0 smart card for pre-boot authentication. [3407936]

Additional Information

Documentation Errata

- The Symantec Encryption Desktop documentation for version 10.3.2 included a tip that advised you not to include the word "attachment" or "message" in the file names of PGP Zip files. This issue has been resolved in Symantec Encryption Desktop 10.3.2 MP1, and PGP Zip now correctly opens files using these words in the file name.

Known Issues

- **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](#). [3406884]

Installing this Maintenance Pack

To install Symantec Encryption Desktop on your Windows system

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

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*.

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:

www.symantec.com/business/support/

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 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_apac@symantec.com

Europe, Middle-East, Africa semea@symantec.com

North America, Latin America supportsolutions@symantec.com

Copyright and Trademarks

Copyright (c) 2014 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. Other names may be trademarks of their respective owners.