



## **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:** 10.3.0 MP3

**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 provides your enterprise with secure messaging by transparently protecting your messages without user interaction. It automatically creates and maintains a Self-Managing Security Architecture (SMSA) by monitoring authenticated users and their email traffic. You can also send protected messages to addresses that are not part of the SMSA.

The Symantec Encryption Desktop encrypts, decrypts, signs, verifies messages, and provides strong security through policies you control. Symantec Encryption Satellite provides security for email messages up to the email user's computer, allows external users to become part of the SMSA, and provides end users the option to create and manage their keys on their computers.

Symantec Encryption Desktop is a security tool that uses cryptography to protect your data against unauthorized access.

# Changes in This Release

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

## What's Changed in This Maintenance Pack

### What's Changed in Symantec Encryption Desktop for Windows 10.3.0 MP3

#### Symantec File Share Encryption

- Resolved an issue with Symantec File Share Encryption so that an encrypted Microsoft Access file can now be opened on a Hitachi NAS Platform 3090-G2 system. [3073225]
- Files encrypted by Symantec File Share Encryption now correctly appear in the Windows Explorer Preview Pane, and pictures now open successfully with Windows Photo Viewer. [3114548, 3132843]
- Resolved an issue with Symantec File Share Encryption where Windows Photo Viewer no longer fails to open an encrypted JPG file stored on a network share. [3119590]

#### Symantec Encryption Desktop

- Resolved an issue so that attaching Microsoft Debug Diagnostic Tool (DebugDiag) to the Symantec Encryption Desktop executable now works correctly. [3151181]

#### PGP Whole Disk Encryption Command Line

- Resolved an issue with PGP Whole Disk Encryption Command Line so that the output to the command “pgpwde --status --xml” now returns the full text and not just the first character of the cause for interrupted encryption. [3089624]

### What's Changed in Symantec Encryption Desktop for Windows 10.3.0 MP2

#### Compatibility with Microsoft Outlook 2013

Symantec Encryption Desktop 10.3 MP2 for Windows supports the use of the Symantec™ Desktop Email Encryption, Powered by PGP Technology component for Microsoft Outlook 2013 (32-bit) with Windows 8 and Exchange 2010.

#### Symantec File Share Encryption

- Resolved a Symantec File Share Encryption interoperability issue with PC Tools so that PC Tools now successfully launches from the PGP Tray, following the sudden removal of a USB drive. [3178561]
- Resolved the issue with Symantec File Share Encryption when accessing Microsoft's Distributed File System-Replication (DFS-R) share. Blue-screen errors no longer intermittently occur when a user decrypts files on their local physical Windows client or within a Microsoft Remote Desktop Services session. [3178699]
- Resolved an issue with Symantec File Share Encryption so that a Group Admin is no longer able to delete the key—even if it is an unknown key—associated with the Admin role. [3178807]

- Resolved an issue with Symantec File Share Encryption where Windows Photo Viewer no longer fails to open an encrypted picture file (JPG, PNG, BMP, TIFF, GIF) stored on a network share. [3197212]
- Files encrypted by Symantec File Share Encryption now correctly appear in the Windows Explorer Preview Pane, and pictures now open successfully with Windows Photo Viewer. [3212643, 3212649]

### **Symantec Encryption Desktop**

- Resolved an issue so that the Symantec Encryption Desktop Assistant window does not appear while upgrading from PGP Desktop 10.1.x. [3112377]
- Resolved an issue with Symantec Encryption Desktop where the embedded policy to automatically set up key reconstruction no longer fails. [3178761]
- Resolved an issue with Symantec Encryption Desktop so that a Remote Desktop Protocol (RDP) connection now requests the password for a Single Sign-On user of one machine when connecting through RDP from a second machine. [3179584]

### **Symantec Drive Encryption**

- Resolved an issue with Symantec Drive Encryption where a user is now prompted for their passphrase if the option 'Do not save my passphrase' is set, when inserting an encrypted USB flash drive. [3178744]
- Resolved an issue with PGP Whole Disk Encryption Command Line where a member of the WDE-ADMIN group can now successfully run the boot bypass command using Microsoft System Center Configuration Manager (SCCM) on a Microsoft Windows XP computer, while PGP Tray is running. [3178821]
- Resolved an issue with Symantec Drive Encryption where the PGP Desktop (or PGP Command Line) becomes unresponsive, after a user who has an active 'Encrypt or lock USB device' policy, locks the USB device and then tries to encrypt it. [3179089]
- Resolved an issue with Symantec Encryption Desktop where access is denied to an encrypted second external hard disk drive, when the system is powered off then rebooted with multiple drives still connected. [3179112]
- Resolved the issue with Symantec Drive Encryption so that after the PGP Tray restarts, the log file no longer states that the user authenticated using a whole disk recovery token (WDRT). [3179122, 3179128]

### **Messaging**

- Revised the text on the landing page of PGP Viewer to indicate that you can decrypt mail by dragging the entire message onto PGP Viewer instead of dragging an individual attachment from the message. [3178723]
- Resolved the issue with PGP Messaging so that the user name is now displayed on sent mail in Outlook 2010 with Symantec Encryption Desktop installed. [3178795]

## **What's Changed in Symantec Encryption Desktop for Windows 10.3.0 MP1**

### **Symantec Encryption Desktop**

- Resolved an issue with Symantec Encryption Desktop where users with a very large number of email accounts experienced screen drawing issues and system lockups. Now, when the number of accounts reaches 100, warnings begin to appear that the user has exceeded the maximum number of supported accounts and to delete unused accounts. [2464546]

- In the French version of PGP Bootguard authentication, the User Name field label (*Nome D'utilisateur*) is no longer truncated. [2978716]
- Upgrading Symantec Encryption Desktop no longer results in an error on Lenovo systems running the latest BIOS version. [2710313]
- Resolved an issue with Symantec Encryption Desktop so that when Invisible Silent Enrollment configuration is enabled, the Windows roaming user profile now functions correctly. [2935313]
- Resolved an issue where PGP Desktop 10.2 failed to encrypt removable media if Symantec Endpoint Encryption Removable Storage were also installed. Now, Symantec Encryption Desktop 10.3 issues a message in this case that encryption of removable media is not allowed; Symantec Endpoint Encryption Removable Storage takes precedence. [2950616]
- Resolved an issue related to Symantec Drive Encryption that uses an auto-encrypt policy and has an initial user enrolled, where additional users are enrolling. These additional users are no longer prompted for the initial user's Symantec Drive Encryption passphrase in order to be added as a Symantec Drive Encryption user. [2991768]
- Resolved an issue where using an Aladdin eToken to authenticate at PGP Bootguard on a Dell Latitude E6320 would cause the system to freeze. [2708645]
- Resolved an issue where the failure of Internet Explorer 8 to properly handle Proxy Auto Configuration (.pac) files was causing PGP modules (for example, PGP Tray) to stop responding when communicating with key servers or Symantec Encryption Management Server(s). [2961450]
- Resolved an issue where Symantec Encryption Desktop issues an error and fails to decrypt certain S/MIME messages that lack signedAttributes. [2991730]
- Resolved an interoperability and file corruption issue between Symantec Encryption Desktop, Symantec Endpoint Encryption Removable Storage Edition and Windows Defrag. [3040634/3023117/3044544]

### **Symantec Drive Encryption**

- Resolved an issue with Symantec Encryption Desktop so that super-silent enrollment (no prompt for user name/password) now behaves like silent enrollment (prompts for user name/password), rather than failing, when Symantec Drive Encryption is disabled. [2591144]
- Resolved an issue with Symantec Drive Encryption where encryption immediately pauses on a Dell Latitude E6420, if the OS has been installed from the Windows CD shipped by Dell with the hardware. [2740496]
- For the French version of PGP Bootguard authentication, the User Name field label ("Nome D'utilisateur") is no longer truncated. [2978716]
- Resolved an issue where some commands issued from PGP Whole Disk Encryption Command Line caused Symantec Drive Encryption to stop responding. [3032890]
- Resolved an issue with a potential buffer overflow in Symantec Drive Encryption running on Microsoft Windows XP or Microsoft Windows Server 2003 systems. For more information, see the Symantec Knowledgebase article TECH201455 (<http://www.symantec.com/docs/TECH201455>). [3039558, 3043664]
- Smart card readers built-in to Dell laptops now work as expected. [3062440]
- Resolved an issue with Symantec Encryption Desktop where access is denied to an encrypted second external hard disk drive, when the system is powered off then rebooted with multiple drives still connected. [2877378]

## Messaging

- Resolved an issue where attachments to plain text emails were being stripped from the email when forwarded to Microsoft Outlook from external devices such as printers. [2803618]

## 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/](http://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/](http://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/](http://www.symantec.com/business/support/)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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](mailto:customercare_apac@symantec.com)

Europe, Middle-East, Africa              [semea@symantec.com](mailto:semea@symantec.com)

North America, Latin America          [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

## **Copyright and Trademarks**

Copyright (c) 2013 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.