Symantec™ Encryption Desktop Version 10.3 for Windows Release Notes

Thank you for using this Symantec Corporation product. These Release Notes contain important information regarding this release of Symantec Encryption Desktop for Windows. 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 for Windows

Version: 10.3.0

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 Web site.

What's Included in This File

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 or by instant messaging (IM). 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.

What's New in Symantec Encryption Desktop Version 10.3 for Windows

Building on Symantec Corporation's proven technology, Symantec Encryption Desktop 10.3 for Windows includes numerous improvements and the following new features.

What's New in 10.3 Win

What's New in Symantec Encryption Desktop 10.3

- **Symantec identity branding**

  The PGP product line has been renamed. For a detailed map of old product names to new ones, refer to the

Symantec Knowledgebase article TECH197084.

- **Integration with Symantec File Share Encryption and Dropbox on Apple iOS devices**

  The integration of Symantec File Share Encryption, formerly known as PGP NetShare, with Dropbox brings protection to files copied from a Dropbox Windows client to cloud-based storage. You can then view these encrypted Dropbox files on your iOS device. This integration allows protected files to move among Dropbox locations, to be read, edited, and saved by you or a collaborative group. Files and folders are encrypted or decrypted transparently, as needed.

- **Microsoft Windows PE (WinPE) 64-bit Support**

  Symantec Drive Encryption, formerly known as PGP Whole Disk Encryption, now provides WinPE recovery for both 32-bit and 64-bit Microsoft Windows 7 environments.

Resolved Issues

For a list of issues that have been resolved in this release, please go to the Symantec Knowledgebase 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 XP Professional 32-bit (Service Pack 2 or 3), Windows XP Professional 64-bit (Service Pack 2), Windows XP Home Edition (Service Pack 2 or 3), Microsoft Windows XP Tablet PC Edition 2005 SP2, Windows Vista (all 32- and 64-bit editions, including Service Pack 2), Windows 7 (all 32- and 64-bit editions, including Service Pack 1), Windows Server 2003 (Service Pack 1 and 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 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.

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 2003 SP 2 (32- and 64-bit editions); Windows Server 2008 64-bit SP 1 and 2; Windows Server 2008 R2 64-bit
- VMWare ESXi4 (supported Microsoft Windows Servers operating in a virtual environment)

For additional system requirements and best practices information, go to the Symantec Knowledgebase and search for TECH149613, "PGP Whole Disk Encryption on Windows Servers".

Symantec Drive Encryption on Tablet PCs

Symantec Drive Encryption is supported on Tablet PCs that meet the following additional requirements:

- Dell Latitude XT1 and XT2 Tablet PC Touch Screen Laptops (undocked)
- 1024 x 768 x 16 screen display running SVGA mode
- Optional physical keyboard

Hardware Requirements

- 512 MB of RAM
- 64 MB hard disk space

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 Corporation, however, does not support the use of other clients.

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

- Microsoft Outlook 2010 (32- and 64-bit)/Exchange Server 2010 (on-premise only)
- Microsoft Outlook 2007 SP2(Outlook 12)/Exchange Server 2007 SP2
- Microsoft Outlook 2003 SP3/Exchange Server 2003 SP3
- Microsoft Windows Mail 6.0.600.16386
- Microsoft Outlook Express 6 SP1
- Microsoft Windows Live Mail
- Mozilla Thunderbird 3.0
- Lotus Notes/Domino Server 7.04 FP1
- Lotus Notes/Domino Server8.02 FP3
- Lotus Notes/Domino Server8.5.1 FP2
- Lotus Notes/Domino Server8.5.2
- Novell GroupWise 6.5.3

Instant Messaging Client Compatibility

Symantec Encryption Desktop is compatible with the following instant messaging clients when encrypting AIM instant messages, file transfers, and direct connections:

- AOL AIM 6.5.5
    - To encrypt instant messages with AIM 6.5, you must change the default port that AIM uses from 493 to 5190.
    - Audio and video connections are not encrypted by Symantec Encryption Desktop.
    - Continued interoperability with the AIM service may be affected by changes made to the underlying AIM protocols after Symantec Encryption Desktop version 10.3 is released.
- Trillian 3.1 (Basic and Pro)

Other instant messaging clients may work for basic instant messaging, but have not been certified for use.

Anti-Virus and other Protection Software Compatibility for Windows

Symantec Encryption Desktop has been tested with the following anti-virus products and no issues have been identified:

- AVG 2012.0.2197
- Trend Titanium Antivirus 2012
- McAfee Internet Security Version 5.6.119.0
- Sophos Anti-Virus version 10.0 and Sophos Web Protection software

Some incompatibilities have been identified with anti-virus products listed in the following sections.

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.

McAfee Host Intrusion Prevention

- Symantec Encryption Desktop is compatible with McAfee Host Intrusion Prevention software when the following conditions are met: [2497804]
    - Symantec Encryption Desktop and McAfee are installed on Windows 7 systems.
    - McAfee HIPS IPS policy settings are disabled.
    - Symantec Encryption Desktop SSO is not used.
    - Always wait for network within a GPO.

McAfee VirusScan Enterprise, AntiSpyware Enterprise 8.8

- An Access Protection Rule prevents Symantec Encryption Desktop from being installed or uninstalled (various error messages appear). To work around this issue, refer to the McAfee Knowledgebase article KB52624.

Symantec Norton AntiVirus 11.x through 12.x, Symantec Norton Internet Security 2005, Symantec Norton Internet Security 2006

- No special configuration required for MAPI email.
- When using POP email, enable **Auto-Protect** and disable the **Anti-Spam** and **Email Scanning** options. **Auto-Protect**, which is enabled by default, provides protection against viruses in email messages when the message is opened.
- Disable SSL/TLS in Server Settings in Symantec Encryption Desktop or Symantec Encryption Satellite. (In Symantec Encryption Desktop, select the PGP Messaging Control Box and then choose **Messaging > Edit Server Settings**. For **SSL/TLS**, select **Do Not Attempt**. In Symantec Encryption Satellite, on the **Policies** tab, select **Ignore SSL/TLS**.) These versions of Norton AntiVirus prevent all mail clients from using SSL/TLS, regardless of the use of Symantec Encryption software.

Personal Firewall Compatibility

Symantec Encryption Desktop for Windows has been tested with the following personal firewall software:

- **Zone Alarm:** The Zone Alarm firewall, by default, restricts access to localhost. Because Symantec Encryption Desktop redirects connections to localhost, this stops Symantec Encryption Desktop from working correctly. To fix this, add localhost (127.0.0.1) as a trusted IP address in Zone Alarm (on the Firewall/Zones screen). Email proxying by Symantec Encryption Desktop will work normally once this is accomplished. [6446]
- **CyberArmor Personal Firewall:** Symantec Encryption Desktop 10.3 is not compatible with InfoExpress CyberArmor Personal Firewall versions 2.6.050802 or 3.2.050802 or prior. Before you install Symantec Encryption Desktop, you must upgrade these versions: contact your helpline or the vendor (InfoExpress at support@infoexpress.com) for more information. [7010]
- **Webroot Desktop Firewall**: Symantec Encryption Desktop is compatible with Webroot Desktop Firewall Version 5.8 only. Earlier versions of Webroot software are not compatible with Symantec Encryption Desktop.

Citrix and Terminal Services Compatibility

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

- Citrix Presentation Server 4.0
- Citrix Metaframe XP
- Windows 2003 Terminal Services
- Windows 2008 Terminal Services (SP1 and SP 2)
- Windows 2008 Terminal Services R2 (SP 1)

The following features of Symantec Encryption Desktop for Windows are available in these environments, as specified:

- Email encryption is fully supported.
- PGP Zip functionality is fully supported.
- PGP Shredder functionality is fully supported.
- Symantec File Share Encryption is fully supported.
- PGP Virtual Disks cannot be mounted at a drive letter over Citrix/TS, but can be mounted at directory mount points on NTFS volumes.
- Symantec Drive Encryption is not supported.

For information on how to install Symantec Encryption Desktop on a Citrix server, go to the Symantec Knowledgebase and search for TECH149081, "Installing PGP Desktop 9.5.x or above on Citrix Server".

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

- Athena ASEDrive IIIe USB reader (0dc3:0802)

Embedded smart card readers

- Dell D430 embedded reader
- Dell D630 embedded reader
- Dell D830 embedded reader
- Dell E6410 embedded reader (Broadcom)
- Dell E6510 embedded reader (Broadcom)

Compatible Smart Cards or Tokens for Symantec Drive Encryption Authentication

Symantec Drive Encryption is compatible with the following smart cards for pre-boot authentication:

- ActiveIdentity ActivClient CAC cards, 2005 model
- *ActiveIdentity ActivClient CAC cards, 2005 and older*
- Aladdin eToken PRO 64K, 2048 bit RSA capable *(4253)*
- Aladdin eToken PRO USB Key 32K, 2048 bit RSA capable
- Aladdin eToken PRO without 2048 bit capability (older smart cards) *(4151)*
- Aladdin eToken PRO Java 72K
- Aladdin eToken NG-OTP 32K

  Note: Other Aladdin eTokens, such as tokens with flash, should work provided they are APDU compatible with the compatible tokens. OEM versions of Aladdin eTokens, such as those issued by VeriSign, should work provided they are APDU compatible with the compatible tokens.

- Athena ASEKey Crypto USB Token
- Athena ASECard Crypto Smart Card

  Note: The Athena tokens are compatible only for credential storage.

- Axalto Cyberflex Access 32K V2
- Charismathics CryptoIdentity plug 'n' crypt Smart Card only stick
- EMC RSA SecurID 800 Rev A, B, and D

  Note: This token is compatible only for key storage. SecurID is not compatible.

- EMC RSA Smart Card 5200
- Marx CrypToken USB token

- Rainbow iKey 3000
- S-Trust StarCOS smart card

  Note: S-Trust SECCOS cards are not compatible.

- SafeNet iKey 2032 USB token
- SafeNet 330 smart card
- T-Systems Telesec NetKey 3.0 smart card
- T-Systems TCOS 3.0 IEI smart card

Personal Identity Verification (PIV) cards

- Oberthur ID-One Cosmo V5.2D personal identity verification cards using ActivClient version 6.1 client software.
- Giesecke and Devrient Sm@rtCafe Expert 3.2 personal identity verification cards using ActivClient version 6.1 client software.

Installation Instructions

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*.

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.

The Symantec Encryption Desktop features that will be active on your system depend on the type of license you have:

- Symantec Encryption Desktop Professional 10.3 includes Symantec Desktop Email and Symantec Drive Encryption.
- Symantec Encryption Desktop Storage 10.3 includes Symantec Drive Encryption and Symantec File Share Encryption.
- Symantec Encryption Desktop Enterprise 10.3 includes Symantec Desktop Email, Symantec Drive Encryption and Symantec File Share Encryption.

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

Additional Information

Documentation Errata

- The user documentation states that a file that Symantec File Share Encryption encrypts typically displays a lock icon. It also states that in the Dropbox folder no lock icon appears. This is incorrect. The lock icon now appears as expected on files that are encrypted using Symantec File Share Encryption. The Dropbox icon is displayed on files in the Dropbox folder that are not encrypted.

General

- **Japanese characters and Current Window/Clipboard processing**: The Current Window/Clipboard encryption and decryption features do not support ISO-2022-JP. [7489/2452667]
- **Compatibility with Oracle applications**: If you encounter problems with Oracle application using Oracle JInitiator you may be able to use the latest version of the Sun Java Runtime Environment to run your Oracle applications. [15543/2460732]
- **Compatibility with Google Desktop**: Symantec Encryption Desktop is compatible with Google Desktop installed if you disable the option in Google Desktop to index mail. For more information, see the Symantec Knowledgebase and search for TECH149154, "Encrypted message content displayed in Google Desktop Indexing". [16286/2461476, 18499/2463691]
- **Windows XP Password Changes**: Symantec Encryption Desktop relies on the Microsoft Data Protection API (DPAPI) to secure user enrollment data. Windows XP SP2 users may lose access to this enrollment information due to a known issue in SP2. Users affected by this Microsoft issue should upgrade to Windows XP SP3 and re-enroll. For more information, see Microsoft KB article 890951. [20852/2465792]
- **Windows Password Changes**: To ensure proper operation for a variety of PGP functions, including SSO and SKM keys, Windows passwords should never be changed using the "net user" command in Windows command prompt. [22825/2467771]
- **PGP Log**: By default, Symantec Encryption Desktop now saves log files in Unicode format. If you cannot open the PGP Log file after you have saved it, save the log as another file type. [30408/2475365]
- **Upgrading when multiple Symantec encryption client products are installed:** If Symantec Encryption Desktop and PGP Command Line are installed on the same system and those versions are earlier than 10.2, you must upgrade both products at the same time. If only one product is updated to version 10.2 or later, then the other product will not function correctly until it is also updated. [31379/2476336]
- **The PGP SDK Service**: Beginning with PGP Desktop 10.2.0, the PGP SDK service (PGPServ.exe) is no longer needed as it is now efficiently referenced in memory. Therefore, the PGPServ.exe is no longer listed under Services (in Computer Management). [2628949]

PGP Keys

- **RSA SecurID SID800**: The RSA SecurID SID800 only supports SHA-1. When generating a key on the RSA SecurID SID800, modify the key properties by clicking **Advanced**, and under **Hashes** select only SHA-1. If a key has already been generated, view the Key Properties, edit the set of supported Hashes, and select only SHA-1. [14861/2460050]
- **GemPlus Smart Cards**: GemPlus smart cards only support SHA-1. When generating a key on GemPlus smart cards, modify the key properties by clicking the Advanced button, and under Hashes select only SHA-1. If a key has already been generated, get the Key Properties, edit the set of supported Hashes, and select only SHA-1. [15681/2460870, 16603/2461793]
- **Athena Tokens**: When creating 2048-bit PGP keys to be used with Athena tokens, you cannot copy the PGP key to the token. You can, however, create the 2048-bit key directly on the token. [24861/2469813]
- **Interoperability with older versions of PGP Desktop**: PGP Desktop 9.0.X does not have support for DSA key sizes greater than 1024 bits. Users of PGP Desktop 9.0.X cannot properly view the properties of such keys, or create signatures with them, or verify signatures made by them. If interoperability with this version is important, use RSA keys, or DSA keys of 1024 bits. [27905/2472860]
- **Adding an ADK to a keypair**: When adding an Additional Decryption Key (ADK) to a keypair, do not then create another ADK and add the second ADK to the first keypair. [28420/2473376]
- **Using the Rainbow/SafeNet iKey 2032**: The PKCS#11 driver dkck232.dll ver 4.7.20.35 can cause Symantec Encryption Desktop to stop working and PGP Tray to halt. This driver is included in the iKey 2000 Series Software from SafeNet. [30829/2475786]
- **Using local keyrings**: While you can create additional keyrings in Symantec Encryption Desktop, Symantec recommends that you use only the default keyring created during installation of the product. Only the default keyring is used by Symantec Encryption Desktop and keys stored in other keyrings are not used. [2577064]

PGP Messaging

- **Thunderbird Email Sent to BlackBerry Users**: If your Thunderbird email client is set to send email in HTML-only format, and the message is encrypted by either Symantec Encryption Management Server or Symantec Encryption Desktop before it arrives at the BES gateway, the recipient will be unable to view the email message on his or her

BlackBerry. To work around this issue, configure your Thunderbird email client so that it does not send HTML-only messages. [16273/2461463]

- **MAPI and Message policies:** Policies based on the condition "Message is <x>" are not currently supported with MAPI. [9448/2454628]
- **Adding comments to secured messages**: To ensure proper display of comments added to secured messages using the **Add a comment to secured messages** option, Symantec Corporation recommends using ASCII text in the Comment field. [11127/2456310]
- **Encrypt Current Window functionality in Microsoft Windows 7:** Due to increased security provisions in Microsoft Windows 7, some applications do not allow encrypted text to be automatically pasted when using the **Encrypt Current Window** functionality in Symantec Encryption Desktop. You will have to manually paste the encrypted text into the message. [27144/2472099]
- **S/MIME Messages**:
  - **S/MIME-signed email messages**: PGP may not process S/MIME signed emails if the signing X.509 certificate is not included in the email. The certificate is almost always included with the email unless the sender turns off this option. [9489/2454670, 9491/2454672]
  - **S/MIME and MAPI:** S/MIME users who intend to use S/MIME with MAPI should ensure that they have an X.509 certificate attached to their keys; otherwise, it is possible that these messages when saved in the Sent Items folder cannot be processed by Symantec Encryption Desktop. [9858/2455040]
- **Microsoft Outlook**:
  - **Using rules to move messages to a mail folder in Microsoft Outlook**: Messages that have been stored in Outlook 2003 or 2007 as encrypted are unencrypted when moved to a mail folder when a message rule is created and applied. To work around this issue, either create the message rule before messages are received in your inbox, or manually drag the messages to the folder. [27255/2472210]
  - **Microsoft Outlook**: Messages that have been processed by Symantec Encryption Desktop cannot be modified from the Microsoft Outlook Outbox. [20269/2465208]
  - **Microsoft Outlook and ESET Antivirus**: When using Microsoft Outlook on a system on which ESET Antivirus is installed, you may encounter a delay when opening Outlook. [22192/2467137]
  - **MAPI/Exchange users and inline objects**: If you are a MAPI/Exchange user, and you are sending messages containing embedded content in a proprietary format (inline objects), Symantec Encryption Desktop will secure the complete message. This causes inline objects to be readable/viewable only by recipients in a MAPI/Exchange environment. [5530/2450704]
  - **Outlook MAPI**: If you are using Outlook in a MAPI environment, use the PGP Log to confirm the validity of PGP signature annotations in message bodies unless the message was decrypted by your Symantec Encryption Management Server, which will do this for you. [6819/2451994, 7304/2452482]
  - **Outlook Connector for Notes**: The Outlook Connector for Notes that allows an Outlook client to emulate a Lotus Notes client is not supported. [7567/2452745]
  - **MAPI Email on Windows Vista**: After upgrading from Windows XP to Windows Vista without reinstalling Symantec Encryption Desktop, MAPI messages are sent in the clear and existing encrypted messages are not decrypted. When you upgrade your operating system to Windows Vista, Symantec Corporation recommends that you first uninstall Symantec Encryption Desktop, upgrade your operating system, and then reinstall Symantec Encryption Desktop. [13119/2458307]
  - **Advanced formatting in messages**: When composing an email in the RTF format using Microsoft Outlook and securing the message with Encryption Desktop in the PGP/MIME format, some advanced formatting such as tables may be removed. [2788848]
- **Lotus Notes**:
  - **Lotus Notes and users who have been disabled**: When a user has been disabled, email sent by the user is initially blocked. To work around this issue, send the email again and email is sent in the clear, as expected. [12234/2457420]
  - **Lotus Notes and users who have been disabled**: When a user has been disabled, and then re-enabled, the user must restart Lotus Notes to send encrypted email. [12236/2457422]
  - **Japanese Notes IDs**: Due to the way that Lotus Notes creates SMTP addresses from the user ID, accounts with Japanese user IDs may display incorrectly or be truncated in some dialog boxes in Symantec Encryption Desktop. This does not interfere with the operation of Symantec Encryption Desktop or delivery of the user's email. [12913/2458100]
  - **Lotus Notes Text Size Increases**: When using Lotus Notes 8.5.1 or earlier, the text size appears to

increase in size when replying to email messages. This issue relates to CD-MIME conversion and IBM Lotus has resolved the issue in Notes version 8.5.2. Other workarounds to resolve the issue are to change the format preference for incoming mail to "Prefers MIME" or change the preferred encoding of the mail policy to "PGP Partition". [29150/2474106]

- **Lotus Notes and the PGP-EML format**: When encoding PGP-EML message, PGP Lotus failed to convert the "From" header to the RFC822 format. Instead of RFC822 format, the "From" header is encoded in the Lotus Notes abbreviated format such as test user1/acme. [2918338]

- **POP**: Verizon POP accounts return an incorrect response when connecting to the POPS/SMTPS ports if you have not purchased Verizon's Silver/Gold services. In this situation you must set the ports manually to 110/25 in the Policy user interface for the account, respectively, to avoid connecting to the normal ports. [NBN]
- **SMTP**: Activate SMTP AUTH in your email client if it is not currently active. [NBN]
- **Instant Messaging**:
  - **Multiple AIM connections**: If your system has multiple ways to access the AIM service (LAN and wireless network accesses, for example), and you lose your connection to AIM but the AIM server doesn't see the connection as lost, and your IM client accesses the AIM service again using the other network access, the AIM server will see you as signed in to the same AIM account from two locations. This will cause Symantec Encryption Desktop to disable the AIM proxy because of the error condition and the AIM server will display a message telling you that your account is logged in from two different locations. To solve this problem, simply reply to the message from the AIM server with a 1. The old AIM session will be discontinued and Symantec Encryption Desktop will encrypt the remaining AIM session. [NBN]

Symantec File Share Encryption

- **Compatibility with SmartFTP**: SmartFTP from SmartSoft Ltd. cannot be used to download files into a folder protected by Symantec File Share Encryption. Use the built-in Windows FTP client instead. [17942/2463133]
- **Windows Links**: Symantec File Share Encryption does not follow Windows links (.lnk files), including such links as "My Network Places". Adding a folder to Symantec File Share Encryption that is actually a link will protect the link file and not the desired location. [13339/2458527]
- **Using Symantec File Share Encryption with Windows Vista**: On Windows Vista systems, adding new folders to a Symantec File Share Encryption Protected Folder using the drag-and-drop method is not supported in this release. This issue does not occur with Windows Vista SP1. [12506/2457693]
- **Software incompatibility with the Symantec File Share Encryption feature**: The following programs are incompatible with Symantec File Share Encryption:
  - Securewave Sanctuary Device Control 3.0.3. To use Symantec Encryption Desktop with Sanctuary Device Control, it is necessary to upgrade the Securewave software to version 4.1 or later. [12850/2458037]
  - CommVault System Data Migrator. To use Symantec Encryption Desktop with Data Migrator, it is necessary to unregister the Symantec File Share Encryption DLL (at the command prompt, type `regsvr32 /u PGPfsshl.dll`). [12016/2457201]
- **Whitelisted Applications**: Application whitelists are applications that your Symantec Encryption Management Server administrator has defined so that all files created by the application are forced to be encrypted. Files created by these whitelisted applications are locked (requiring authentication to access) after you log off or shut down your system. [17491/2462682]
- **Using Symantec File Share Encryption and SharePoint with Windows Vista 64-bit**: The Symantec File Share Encryption shortcut menu is not available on 64-bit versions Windows Vista systems when viewing a folder within SharePoint. To access the shortcut menu, view the folder using Windows Explorer. [19421/2464523]
- **Accessing newly protected Symantec File Share Encryption protected folders**: On Microsoft Windows 7 64-bit systems, you may encounter an error when you attempt to access a protected folder on a WebDav system. To work around this issue, clear the message dialog box and try again. [24301/2469253]
- **Mapped local drives**: Do not map a local drive on Microsoft Windows Vista, Windows 7, or Windows Server 2008 and then encrypt the contents of a folder on the mapped drive. Doing so could cause your data to become corrupted. [27680/2472635]
- **Symbols in Active Directory groups**: Certain characters that are allowed when creating Active Directory groups can cause Symantec File Share Encryption to fail on encryption or re-encryption, or searches. Do not use the pound, percent, or left/right parentheses -- #, %, (, or) -- when creating Active Directory groups. [26336/2471290]
- **Microsoft Office 2010 with Sharepoint 2010**: Symantec File Share Encryption is not compatible with Microsoft Office 2010 and Sharepoint 2010. If you use Office 2010 with Sharepoint 2010, any files that were protected by

Symantec File Share Encryption could lose their protection if the file is opened/edited/saved after being encrypted. [30828/2475785]

- **Restoring protected folders from the Recycle Bin**: If you delete a Symantec File Share Encryption-protected folder (send it to the Windows Recycle Bin), and then restore that folder, the files inside the folder retain their protection but the folder is no longer protected. This issue occurs only on systems running Microsoft Windows 7 SP 1. [2623979]
- **Single file encryption**: Symantec File Share Encryption encrypts single files only if they are Microsoft Office files and text files. For example, you will lose Symantec File Share Encryption protection if you protect a single PDF file, edit the file, and then save it. To work around this issue, place the file into a folder and encrypt the folder.
- **Zip files lose Symantec File Share Encryption protection**: If you open a Symantec File Share Encryption-protected zipped file (.zip) from within Windows Explorer, edit the file (delete, modify, or add files), then save and close the zipped file, you will lose the Symantec File Share Encryption protection. To work around this issue, re-encrypt the zipped file after modifying it. [2718378]
- **PDF files lose Symantec File Share Encryption protection**: If you open a Symantec File Share Encryption-protected PDF file (.PDF), edit the file, then save and close the zipped file, you will lose the Symantec File Share Encryption protection. To work around this issue, re-encrypt the PDF file after modifying it. [2718381]
- **Symantec File Share Encryption and Dropbox**: Symantec File Share Encryption automatically encrypts new files in your Dropbox folder, but not existing files. If you have an existing Microsoft Office file, when you open that file, Symantec File Share Encryption encrypts the file, even if it was not modified. This is because Office creates "shadow" files and though you did not change the file, the file is saved and is considered to be a changed file. [2831395]
- **Symantec File Share Encryption and Dropbox**: Symantec File Share Encryption still protects the files and folders in your Dropbox folder, even if you have uninstalled the Dropbox application. To remove the protection of these files, decrypt the files and folders. [2801162]

PGP Portable

- **PGP Portable and Microsoft Office 2003**: PGP Portable is compatible with Microsoft Office 2003 when Office Service Pack 3 is installed. [21854/2466798]
- **PGP Portable and Microsoft Office 2003**: Microsoft Office 2003 documents cannot currently be added to a PGP Portable Disk when the disk is being created on a Windows Vista system. [21697/2466640]
- **Accessing Data on Windows XP systems**: Mounting a PGP Portable Disk on Windows XP will fail with a "Not Connected" error if another process is already using port 80. [21869/2466813]
- **Creating new Word documents on a PGP Portable Disk**: When creating a new Microsoft Word file on a mounted PGP Portable Disk on Windows XP (right-clicking the mounted PGP Portable Disk and selecting **New > File > Microsoft Word Document)**, the resulting zero-byte Word file is read-only. To edit the file, save it as a new name (on the PGP Portable Disk). [21680/2466623]
- **Adding Data on Windows XP Systems**: In order to add data to a PGP Portable Disk on a Windows XP system, set the local security policy for **Allowed to format and eject removable media** to **Administrator and Interactive Users**. [21975/2466919]
- **Disk Space Requirements**: When copying large files to a PGP Portable disk, ensure that you have sufficient space available on your local drive. The amount of space needed is equivalent to the amount of data being copied to the PGP Portable disk. [21595/2466538]
- **PGP Portable Passphrases**: Japanese characters are not currently supported for passphrases when creating a new PGP Portable Disk or changing the passphrase on an existing disk. [21717/2466660]
- **PGP Portable Disk File Names**: When creating a PGP Portable Disk, the combination of file name and folder name(s) cannot exceed 240 characters. [21816/2466759]
- **PGP Portable and Trend Micro Antivirus**: To create a PGP Portable Disk on Windows XP systems where Trend Micro Antivirus is installed, stop or disable all Trend Micro services before creating the PGP Portable Disk. You can start or re-enable the services after the disk has been created. This issue does not occur on Windows 7 64-bit systems. [26091/2471044]
- **Copying large files**: On Microsoft Windows XP systems, there is a known limitation with the Microsoft WebDav redirector so that you can only copy files that are smaller than 2GB in size. Files larger than 2GB appear to be copied but result in a zero-byte file. On Windows Vista and Windows 7 systems, you may need to adjust the file limits for temporary files in **Sync Center > Manage Offline Files and Folders** to match the size of the files you are copying. [27501/2472456]

PGP Shredder

- **Shredding (wiping small files)**: Shredding small files (under 1 K) on some NTFS-formatted disks can leave remnants of the file behind due to an NTFS optimization that stores file data in internal data structures for very small files. These structures are not considered free space even after deleting a file, and thus they also will not be shredded using Symantec Encryption Desktop's Shred Free Space feature. In addition, NTFS supports Journaling, which can save shredded file data in an internal operating system cache. For the highest security shredding on NTFS disks, we recommend starting your system from an OS on a different partition and using Symantec Encryption Desktop's option in the Shred Free Space feature to overwrite these NTFS data structures (the **Shred NTFS internal data structures** checkbox). This does not affect FAT32 or other supported file systems. [NBN]
- **Shredding sparse files**: Sparse files, commonly used for disk images, database snapshots, log files and in scientific applications, cannot be securely deleted using PGP Shredder. [21255/2466198]
- **Automatic shredding**: Automatically shred when emptying the Recycle Bin/Trash is not compatible with the Windows built-in CD burning software. [22794/2467740]
- **Shredding files on systems running Microsoft Windows 7**: Depending on where the files are located, you may not be able to shred more than 16 files at a time. To shred more than 16 files, either move them to a folder (then right-click the folder and select **Symantec Encryption Desktop > PGP Shredder [folder name]**, or shred the files in multiple operations. [26835/2471789]

PGP Viewer

- **Lotus Notes**: Due to the Lotus Notes architecture, an encrypted message cannot be dragged from Lotus Notes email client and dropped into PGP Viewer to be decrypted. [23384/2468331]
- **Viewing Sign-Only Emails with Shift-JIS**: Outlook Express or Windows Mail messages signed using Shift-JIS cannot be verified using PGP Viewer. This issue does not occur if the message was encrypted and signed. [22870/2467816]
- **S/MIME Messages**: S/MIME-encrypted messages cannot be decrypted by PGP Viewer in this release. [22022/2466966]
- **Displaying Decrypted Messages**: If you drag an item to PGP Viewer and the message does not appear, restart PGP Viewer and drag the item again. [22215/2467160]
- **Copying Email Messages to Inbox**: When copying a Microsoft Outlook 2003 email message to your inbox using PGP Viewer, the date/time stamp on the message is changed to the current date/time. [24355]
- **Viewing MAPI Email**: Microsoft Outlook messages opened within PGP Viewer will display Unmatched Address in the From: field. [24703/2469655]
- **Cancelling the passphrase prompt**: If you drag an item to PGP Viewer and then click **Cancel** when prompted to enter your passphrase, you will need to restart PGP Viewer again. This is required so that you can then enter your passphrase in order to decrypt messages. [25390/2470342]
- **PGP Viewer with Outlook Express on Microsoft Windows XP 64-bit systems**: On Microsoft Windows XP 64-bit systems, you cannot use the **Copy to Inbox** option after dragging and dropping a message onto PGP Viewer when your default mail program is Outlook Express. [23815/2468765]
- **Microsoft Outlook 2010 64-bit support**: This version of PGP Viewer does not support decrypting messages from the 64-bit version of Outlook 2010. [28145/2473100]

PGP Virtual Disk

- **Using with Personal Certificate-based Keys**: In order to mount a PGP Virtual Disk that is secured with a personal certificate-based key, note that you should not enter a passphrase when prompted in the PGP Enter Passphrase dialog box, but instead click **Enter**. [14762/2459951]
- **Existing NTFS PGP Virtual Disks and Windows Vista**: NTFS disks created under Windows XP may not be properly handled by Windows Vista. For best results, create NTFS disks in Windows Vista. A future Microsoft update is expected to resolve this Windows issue. [12644/2457831]

Symantec Drive Encryption

- **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, 27274/2472229]

- **Backwards compatibility**. Disks encrypted with this version of Symantec Drive Encryption can only be accessed with this same version of Symantec Drive Encryption for Mac OS X or versions 10.0 and up for Windows. [19875/2464814]
- **Symantec Drive Encryption Evaluation Licenses**. If you are using Symantec Drive Encryption with an evaluation license in a managed Symantec Encryption Management Server environment, please ensure you obtain a valid license *prior to* the expiration of your evaluation license. This will prevent the automatic decryption of your disk upon expiration of the evaluation license. [16445/2461635]
- **Symantec Drive Encryption Authentication**: The ActiveIdentity ActivClientCAC model 2002 smart card is not compatible in this release. To use the ActiveClient CAC card, use model 2005. [16259/2461449]
- **Passphrase Recovery**: Token users who use passphrase recovery when authenticating at PGP BootGuard will be prompted to change their passphrase. This prompt can be ignored as your PIN will not be changed even if you enter text in the dialog or click **Cancel**. [24335/2469287]
- **Passphrase Recovery**: Passphrase recovery is only available for encrypted boot disks. [24510]
- **Passphrase Recovery**: If you use the **Forgot Passphrase** option at the PGP BootGuard screen and enter an incorrect user name, you will need to click **Cancel** to return to the PGP BootGuard screen and then select **Forgot Passphrase** again. [24825/2469777]
- **Symantec Drive Encryption and Smart Card Readers**: When using a smart card reader with a built-in PIN pad, the correct PIN may not be accepted the first time it is entered on the pad, and you will be prompted to provide the PIN again. When this message appears, click OK without entering the anything. This will either allow the PIN to be accepted or will transfer control to the PIN pad of the smart card reader, where you can enter the PIN again. [16143/2461333]
- **Symantec Drive Encryption and Smart Card Readers**: Pre-boot authentication using a smart card reader is not currently supported on Panasonic Toughbook and Sony Vaio P-Series Mini systems. [20638/2465578]
- **Symantec Drive Encryption and GemXpresso**: Symantec Encryption Desktop is not compatible with the GemXpresso family of smart cards. Keys on the GemXpresso smart card can be used for encrypting PGP Virtual Disks and Symantec File Share Encryption protected folders, but cannot be used to encrypt a disk or removable disk. [16415/2461605]
- **Symantec Drive Encryption and SSO**: When you add an SSO user to Symantec Drive Encryption, be sure that there are no leading spaces in the user's name (for example, " acameron"). If the SSO user's name has a leading space, you will receive an error message that there was a login failure. [26995/2471950]
- **Symantec Drive Encryption and SSO**: If you encounter problems with synchronizing a Windows password change on a Windows XP system, follow the steps below to correct the issue: [17269/2462459]
  1. On your Windows Desktop, right-click My Network Places and select **Properties** from the shortcut menu.
  2. Select **Advanced > Advanced Settings**.
  3. Select the **Provider Order** tab.
  4. Rearrange the order of the providers so `PGPpwflt` is listed above the Intel card.
  5. Click **OK**.

  You can also modify the .msi installation file. Use the `PGP_SET_HWORDER=1` command to place PGPpwflt in the first of the list. For example, run the .msi installation file using the following command:

  ```
  msiexec /i pgpdesktop.msi PGP_SET_HWORDER=1
  ```

- **Symantec Drive Encryption SSO on Novell Networks**: The Single Sign-On feature of Symantec Drive Encryption does not work on Windows Vista systems running Novell Network Client. Once you have authenticated at the PGP Bootguard screen you will need to enter your password again to start Windows Vista. [16688/2461878]
- **Symantec Drive Encryption SSO on Novell Networks**: When using the Single Sign-On feature of Symantec Drive Encryption on Windows Vista systems running Novell Network Client, offline users receive a Novell Security Message stating the "tree or server cannot be found." To continue logging in to Windows, click Yes, and the login proceeds normally. [16995/2462185]
- **TPM Support**: We are in the process of validating many different TPM implementations.We are interested in your test results on any additional TPM systems. [14666/2459855]

  TPM authentication with Symantec Drive Encryption works on Windows XP systems only. [2469217]

- **Token Authentication**: Token authentication in PGP BootGuard requires pressing CTRL+ENTER instead of just Enter. Users may also experience some delay during the authentication of tokens in PGP BootGuard. [14792/2459981, 16466/2461656]
- **Aladdin Smartcards**: Aladdin Smartcards do not properly generate 2048-bit keys using Aladdin software version 4.5.52, and such keys cannot be used for Symantec Drive Encryption pre-boot authentication. Symantec Corporation is working with Aladdin to correct this issue. Note that Aladdin tokens do not have this issue. [16699/2461889]
- **Athena ASECard Crypto Cards:** The Athena ASECard Crypto Card is not compatible with OmniKey readers for pre-boot authentication. Use a different compatible reader with Athena smart cards for pre-boot authentication. [18283/2463475]
- **Upgrading**: The PGP BootGuard screen is not updated immediately after you upgrade to Symantec Encryption Desktop 10.3. To display the updated PGP BootGuard screen (containing new login and keyboard options), reboot your system a second time. [NBN]
- **Removable drive encryption:** Certain types of removable flash devices cannot be encrypted with the vendor-supplied format. They must be formatted within Windows prior to encrypting. [12362]
- **Removable drive encryption**: If both **Automatically Encrypt Boot Disk Upon Installation** and **Force Encryption of Removable Disk** are enabled by policy, you may encounter an error when inserting a USB disk while a fixed disk is being encrypted. To work around this issue, wait until the encryption process has completed on the fixed disk. [12167/2457353]
- **Symantec Drive Encryption and Hibernation:** When resuming from Hibernation, an extra domain password prompt may appear even if Single Sign-on is active. [9935/2455117]
- **Disk Recovery:** As a best practice, if you need to perform any disk recovery activities on a disk protected with Symantec Drive Encryption, Symantec Corporation recommends that you first decrypt the disk (by using the **Symantec Encryption Desktop Disk > Decrypt** option, your prepared Symantec Drive Encryption Recovery Disk, or by connecting the hard disk via a USB cable to a second system and decrypting from that system's Symantec Encryption Desktop software). Once the disk is decrypted, proceed with your recovery activities. [NBN]
- **Using Symantec Drive Encryption with Norton Ghost 9 or 10:** Ghost is compatible with fully encrypted disks. Ghost sometimes exhibits errors when used to make backups within the Windows OS of partially encrypted disks. To recover from an error like this, reboot the system and perform a Windows chkdsk when the system restarts. Ghost should be functional again. [13004/2458192]
- **Compatibility of older-version recovery disks:** Symantec Drive Encryption recovery disks are compatible only with the version of Symantec Encryption Desktop that created the recovery CD. For example, if you attempt to use a 9.10 recovery disk to decrypt a disk protected with Symantec Drive Encryption version 10.3 or later, it will render the Symantec Drive Encryption disk inoperable. [10556/2455738]
- **Preparing for disk encryption:** Errors when attempting to encrypt your disk are often caused by bad sectors on a hard disk. These can frequently be corrected with third-party products which repair and ensure the health of your disk. The Windows CHKDSK program may resolve the issue in some instances, but more comprehensive programs such as SpinRite from Gibson Research Corporation (http://www.grc.com) are often required. Additionally, if your disk is seriously fragmented, Symantec Corporation recommends that you defragment your disk prior to encryption using the Windows Disk Defragmenter. [10561/2455743]
- **Symantec Drive Encryption and Dell systems boot diagnostics:** (Dell systems only) Advanced boot diagnostics that are normally accessible by pressing F12 during the boot process are not available on disks encrypted with Symantec Drive Encryption. To run advanced boot diagnostics using F12, first decrypt the disk, and then run diagnostics. [12120/2457306]
- **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]

- **IBM Fingerprint Software:** Symantec Encryption Desktop is compatible with the IBM ThinkVantage fingerprint software version 5.6.1 or later. [13786/2458975]
- **Symantec Drive Encryption SSO**: When using Symantec Drive Encryption SSO, Symantec Corporation recommends that organizations enable the Microsoft Group Policy option **Always wait for the network at computer startup and logon**. This ensures that password expiration and forced changes happen as soon as possible. For more information regarding this setting, see the following Microsoft Knowledgebase articles. [14142/2459331]
  - http://technet.microsoft.com/en-us/library/bb456994.aspx
  - http://support.microsoft.com/kb/305293
- **Modifying the system partition**: Do not make any changes to the system partition on a boot disk that has been encrypted by Symantec Drive Encryption; it will fail to boot properly on the next startup. If you must make changes to the partitioning of an encrypted disk, decrypt the disk first and then make the partition changes.
- **Using CHKDSK**: CHKDSK may report errors in a file called PGPWDE01 when checking a disk that has been encrypted with Symantec Drive Encryption. This file is protected by Symantec Drive Encryption and such errors can be ignored. [20197/2465136]
- **Using Maximum CPU Usage to encrypt removable disks**: Removable disks cannot be encrypted using the Maximum CPU Usage option, even though this option can be selected. [24286/2469238]
- **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]
- **Entering Full Width Japanese Alphabet Characters For Passphrase Recovery**: When you have forgotten your passphrase and you have answered the questions in order to enable passphrase recovery, you can now enter full-width Japanese Alphabet characters. To do this, at the PGP BootGuard, select **Forgot Passphrase**. The first character must be entered as an uppercase character to begin. Enter the uppercase character and then either press Enter (to accept the character) or press the spacebar two times to select the lowercase character. (When creating the questions in Symantec Encryption Desktop, be sure that you have enabled Full Width in the Japanese IME.) [26228/2471182]
- **Using numeric keypads**. Numeric keypads are not supported when creating and/or entering PGP BootGuard passphrases. [25673/2470626]
- **Using Symantec Drive Encryption on Dell XT2 Tablet PCs**:
  - EISA recovery partitions existing on the Dell Latitude XT2 Tablet PCs are displayed as an **Unknown** partition when viewed in Symantec Encryption Management Server. [26669/2471623]
  - Use of the **CTRL**, **Rotate Screen**, and **Tool/Settings** buttons on the Dell Latitude XT2 Tablet PC while the PGP BootGuard screen is displayed results in PGP BootGuard halting unexpectedly. [26564/2471518]
  - Use of the Symantec Drive Encryption Recovery CD with a virtual keyboard is not supported in this release. A physical keyboard is supported. [26614/2471568]
- **Authenticating at PGP BootGuard on Dell XT Tablets**: To authenticate at the PGP BootGuard screen when using Dell XT tablets, use the built-in keyboard on the tablet. You cannot use a pen, stylus, USB keyboards, or eTokens when authenticating on these tablets. [2636340]
- **Encrypting Mac OS X formatted external drives with Symantec Drive Encryption for Windows.** A drive that is created under Mac OS X using GPT (GUID Partition Table) can be mounted and used on Microsoft Windows systems, but the drive cannot be encrypted using Symantec Drive Encryption for Windows. To work around this issue, either format the disk using MBR Partition or encrypt the disk under Mac OS X. [26460/2471414]
- **Using child domains and the AutoLogin feature of Microsoft Windows**. The AutoLogin feature fails if you modify the Windows Registry to change the child domain user to the autologin user and use the FQDN as the "DefaultDomainName." To use the child domain in the "DefaultDomainName" value, use the WINS name, rather than the FQDN. This is a limitation of the AutoLogin feature of Windows. [29869/2474825]
- **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]
- **USB 3.0 host controller ports**. This release of Symantec Encryption Desktop does not support the use of tokens inserted in USB 3.0 host controller ports. [28299/2473255]
- Aladdin eToken and SSO. The Aladdin eToken PRO Java 72K token is not compatible with Symantec Drive

Encryption and single sign-on in this release. [29896/2474852]

- **T-Systems TCOS smart card**. The T-Systems TCOS 3.0 IEI smart card is not compatible with Symantec Drive Encryption in this release. [31111/2476068]
- Incomplete encryption of disks that are partitioned with Acronis. Symantec Encryption Desktop does not encrypt external disks that are formatted and partitioned with Acronis Disk Director. [30827/2475784]
- **PGP WDE Command Line**:
  - **Passphrase required for PGP WDE command line stop command**: The `--stop` command now requires a passphrase. Scripts that use this command without providing a passphrase will fail. [29822/2474778]
  - **Domain required for PGP WDE command line recovery-configure command**: The `--recovery-configure` command now requires a domain for in a Symantec Encryption Management Server-managed environment. It also requires one for users that have a domain. In these situations, scripts that use this command without providing a domain will fail. [28656/2473612]
  - **Unable to change user's domain**: In this release, the `--change-userdomain` command does not change the specified user's domain. To change a user's domain, use Symantec Encryption Desktop and not PGP WDE Command Line. [28605/2473561]
  - **Unable to check status without enrolling to a Symantec Encryption Management Server**: Previous versions of PGP WDE command line allowed the use of pgpwde.exe for specific functions, such as `--status` and `--list-users`, for clients that were not enrolled to a server. Use the `--admin-authorization` or `--aa` flag with the command line. For example, run `pgpwde.exe --status --disk 0 --aa)`. [2701384]
- **Compatibility with Symantec Endpoint Encryption Full Disk**. Symantec Drive Encryption is not compatible with SEE Full Disk and should not be installed on the same system.
- **RSA token authentication fails at PGP BootGuard**. RSA token authentication fails at preboot when the firmware version for RSA is 3.01. This issue has been resolved by RSA. To resolve this issue, upgrade the RSA firmware to version 3.5. [2493913]
- **Authenticating using a card reader**. To authenticate at PGP BootGuard using a smart card, be sure the card reader is connected directly to the computer and not through the docking station. If the card reader is connected to the docking station, you will not be able to authenticate using the smart card. [2729258]
- **Keys on USB tokens and Smartcards**. Keys with spaces in the user name cannot be used for authentication at PGP BootGaurd. [2611446]
- **Integrated Smart Card readers**. Smart card readers built-in to Dell laptops do not work. To work around this issue, use an external smart card reader. [2932848, 2644692]

PGP Zip

- **PGP Zip and Symantec File Share Encryption**: On Windows Vista, creating a PGP Zip archive of a folder added to Symantec File Share Encryption is not supported. [17058]
- **Self-decrypting archives:** When the recipient of a self-decrypting archive (SDA) decrypts it, all dialog boxes that Symantec Encryption Desktop displays are in English, regardless of what version of Symantec Encryption Desktop—English, German, or Japanese—was used to create the SDA and regardless of what language your system is currently running. This applies only to the dialog boxes that appear; file names and the content of the SDA are not affected. [7144]
- **Compatibility with AVG Anti-Virus**: To create a PGP Zip SDA on systems running AVG Anti-Virus software, you must be using AVG Anti-Virus version 8.0 or later. If you are using an earlier version of AVG Anti-Virus, disable heuristic analysis in the RESIDENT SHIELD if you want to create PGP Zip SDAs. [16488]

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 Web site 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