



Versionshinweise zu Symantec™ Encryption Desktop Version 10.3 für Windows Maintenance Pack

Vielen Dank, dass Sie sich für dieses Produkt der Symantec Corporation entschieden haben. Diese Versionshinweise enthalten wichtige Informationen zu dieser Version von Symantec Encryption Desktop. Wir empfehlen, das gesamte Dokument zu lesen.

Wir sind für alle Kommentare und Anregungen dankbar. Im Abschnitt "Weitere Informationen" erfahren Sie, wie Sie sich an uns wenden können.

Produkt: Symantec Encryption Desktop

Version: 10.3.2 MP5

Warnung: Der Export dieser Software wurde eventuell von der US-Regierung eingeschränkt.

Hinweis: Sie finden die neueste Version dieses Dokuments [im Abschnitt "Produkte" der Website der Symantec Corporation](#).

Inhalt

- Infos zu Symantec Encryption Desktop
- Änderungen in dieser Version
- Installieren des Maintenance Pack
- Technischer Support
- Copyright und Marken

Infos zu Symantec Encryption Desktop

Symantec™ Encryption Desktop Powered by PGP Technology ist ein Sicherheitstool, das mithilfe von Kryptografie Daten vor nicht autorisiertem Zugriff schützt.

Symantec Encryption Desktop schützt Ihre Daten, wenn sie per E-Mail gesendet werden. Sie können die gesamte Festplatte verschlüsseln, damit alle Daten ständig geschützt sind, oder nur einen Teil der Festplatte mit Hilfe eines virtuellen Laufwerks, um Ihre wichtigsten Daten sicher zu speichern. Sie können Ihre Dateien und Ordner sicher mit anderen Benutzern im Netzwerk gemeinsam nutzen. Eine beliebige Kombination von Dateien und Ordnern kann zur einfachen Verteilung oder Sicherung in einem verschlüsselten Paket komprimiert werden. Darüber hinaus können Sie mit Symantec Encryption Desktop vertrauliche Dateien sicher löschen, damit niemand mehr auf sie zugreifen kann, sowie den freien Speicherplatz auf der Festplatte überschreiben, damit keine ungesicherten Dateifragmente zurückbleiben.

Mit Symantec Encryption Desktop können Sie PGP-Schlüsselpaare erstellen sowie Ihre privaten Schlüsselpaare und die öffentlichen Schlüssel anderer Benutzer verwalten.

Änderungen in dieser Version

Hier finden Sie die Änderungen an Symantec Encryption Desktop.

Eine aktualisierte Liste der Systemanforderungen für Symantec Encryption Desktop finden Sie unter <http://www.symantec.com/docs/TECH224415>.

Änderungen in diesem Maintenance Pack

Änderungen in Symantec Encryption Desktop für Windows 10.3.2 MP5

E-Mail

- Ein Problem mit der Unterstützung von Microsoft Outlook/MAPI in Symantec Encryption Desktop wurde behoben: Offline-E-Mail-Richtlinien verursachen jetzt keine doppelten E-Mails mehr. [3547567]
- Ist in Microsoft Outlook der Cache-Modus deaktiviert, werden in RTF formatierte E-Mails unter Microsoft Exchange Server 2013 jetzt ordnungsgemäß dargestellt. [3456553]

Symantec Drive Encryption

- Laden Sie zum Aktivieren der Kompatibilität mit der Funktion "Sicherer Start" auf Microsoft Surface Pro 1 und Surface Pro 2 das Tool "Microsoft Surface Pro UEFI CA OEM PK" herunter. Dieses Tool und entsprechende Anweisungen finden Sie unter <http://www.microsoft.com/en-us/download/details.aspx?id=41666>. Beachten Sie, dass Sie dieses Tool nur ausführen können, wenn der Computer verschlüsselt und "Sicherer Start" aktiviert ist. [3319192]
- Der Broadcom-Smartcard-Reader in Computern der Reihe Dell Latitude E6530 funktioniert jetzt ordnungsgemäß mit PGP BootGuard. [3529298]
- Eine aktuelle Liste der aktuellen SmartCards und Token für Symantec Drive Encryption-Administratorschlüssel finden Sie im folgenden Artikel der Symantec-Supportdatenbank: [TECH149099](http://www.symantec.com/docs/TECH149099). [3583553]

Symantec Encryption Desktop

- In Symantec Encryption Desktop werden jetzt token-basierte Fehler beim Anmelden von Benutzern protokolliert, wenn das Stammzertifikat nicht in der Symantec Encryption Management Server-Konsole auf der Registerkarte **Schlüssel > Vertrauenswürdige Schlüssel** angezeigt wird. [3493890]

Symantec File Share Encryption

- In Symantec File Share Encryption können Benutzer jetzt auf die Pfad- und Benutzerverwaltungsfunktionen für bereitgestellte Unterordner freigegebener, verschlüsselter verteilter DFS-Ordner zugreifen. [3402457]

- In Symantec File Share Encryption können Benutzer von Symantec Encryption Desktop jetzt den Namen des Gruppenschlüssels sehen, der zum Verschlüsseln eines freigegebenen Ordners verwendet wurde. [3555340, 3572636]
- In Symantec File Share Encryption sind jetzt die Funktionen zum Hinzufügen und Entfernen von Benutzern sowie zum Ändern von Benutzerrollen für Gruppenadministratoren verfügbar. [3467664]

Änderungen in Symantec Encryption Desktop für Windows 10.3.2 MP4

Allgemein

- Funktionsprobleme wurden behoben und die Gesamtsicherheit der Anwendung wurde verbessert.

Änderungen in Symantec Encryption Desktop für Windows 10.3.2 MP3

Symantec Encryption Desktop

- Die Sicherheitslücke "CVE-2014-3436" wurde behoben und Symantec Encryption Desktop schränkt die Dekomprimierung beim Dekodieren großer verschlüsselter E-Mail-Dateien ein. Denial-of-Service-Angriffe werden so verhindert. Symantec möchte sich bei Alexander Klink von n.runs professionals GmbH für den Hinweis und seine Zusammenarbeit bei der Lösung des Problems bedanken. [3493711]

Symantec File Share Encryption

- Ein Kompatibilitätsproblem mit Double-Take Availability 7.0.1 wurde behoben. Mit Symantec File Share Encryption verschlüsselte Microsoft Access-Dateien werden nicht mehr beschädigt. Dies gilt für alle unterstützten Versionen von Microsoft Windows, außer Windows 8 (32 Bit). [3523815]
- Benutzer können jetzt TXT-Dateien in gemeinsam genutzten Ordnern, die mit Symantec File Share Encryption verschlüsselt wurden, ändern, ohne dass Daten beschädigt werden, wenn der gemeinsam genutzte Ordner gleichzeitig auf dem Remote-Dateiserver angezeigt wird. Dies gilt für alle unterstützten Versionen von Microsoft Windows, außer Windows 8 (32 Bit). [3523820]
- Von DFS gemeinsam genutzte TXT-Dateien, die mit Symantec File Share Encryption verschlüsselt wurden, enthalten nach Änderung keine unleserlichen Daten mehr. [3523825]

Änderungen in Symantec Encryption Desktop für Windows 10.3.2 MP2

Symantec Drive Encryption

- Folgende Smartcards sind jetzt mit Symantec Encryption Desktop bei der Preboot-Authentifizierung kompatibel [3508102]:
 - ID-One Cosmo v7.0 mit 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

- Der Symantec Encryption Desktop-Client zeigt jetzt die Speicherkapazität von Laufwerken, die größer als 2 TB sind, korrekt an. [3272070]

Änderungen in Symantec Encryption Desktop für Windows 10.3.2 MP1

E-Mail

- Benutzer können jetzt mit S/MIME verschlüsselte E-Mails aus Symantec Encryption Desktop senden, wenn im Zertifikat nur die Kennzeichnung "keyEncipherment" aktiviert ist. [3250866]

Symantec Encryption Desktop

- Der Prozess "lsass.exe" wird jetzt nicht mehr mit einer Fehlermeldung zur Datei PGPpsdk.dll abrupt beendet. [2898169]
- Symantec Encryption Desktop protokolliert jetzt nur ein Ereignis, wenn auch Symantec Endpoint Encryption Removable Storage auf demselben Computer installiert ist. [3153572]
- PGP Zip öffnet und entschlüsselt jetzt Dateien, deren Name das Wort "E-Mail" oder "Anhang" enthält. [3193714, 3206141]
- Der Prozess "PGPTray" wird nicht unerwartet bei der Benutzeranmeldung unter Windows 7 beendet, wenn die Ordnerumleitung aktiviert ist. [3243735]
- Die Sicherheitslücke "CVE" (CVE-2014-1646) wurde behoben. Dabei trat eine Speicherlesezugriffsverletzung beim Versuch auf, bestimmte unvollständige Dateien zu verarbeiten. Dies konnte zum Absturz der Anwendung oder einer potenziell beliebige Code-Ausführung mit Anwendungsberechtigungen führen. Symantec möchte sich bei Jeremy Brown (jerbrown) von ReSP in Zusammenarbeit mit Microsoft Vulnerability bedanken, dass er dieses Problem gemeldet und dann mit uns zusammengearbeitet hat, um es zu beheben. [3452808]

Symantec Drive Encryption

- Benutzer können jetzt neu erstellte Benutzerschlüssel einem externen Speichergerät mit Additional Decryption Key (ADK) hinzufügen. [3076950]
- In Symantec Encryption Desktop werden jetzt Passphrases für das Einmalige Anmelden unter Microsoft Windows 7 beim Einloggen synchronisiert, wenn Benutzer eine Domain Name System(DNS)- oder User Principal Name(UPN)-Domäne angeben müssen. [3299738]
- Benutzer können jetzt PGP BootGuard nicht mehr umgehen, wenn die Bypass-Funktion deaktiviert ist. [3304044]
- Die Software ist jetzt mit Smartcards von Giesecke und Devrient Sm@rt Café Expert 5.0 für die Authentifizierung vor dem Systemstart kompatibel. [3407936]

Zusätzliche Informationen

Berichtigungen an der Dokumentation

- Die Dokumentation zu Symantec Encryption Desktop 10.3.2 enthielt einen Tipp, die Wörter "Anhang" bzw. "E-Mail" nicht in den Namen von PGP Zip-Dateien zu verwenden.

Dieses Problem wurde in Symantec Encryption Desktop 10.3.2 MP1 behoben und PGP Zip öffnet jetzt Dateien mit diesen Wörtern im Namen ordnungsgemäß.

Bekannte Probleme

- **Software-Inkompatibilität mit Symantec Drive Encryption:** HP ProtectTools Suite Drive Encryption blockiert die Verschlüsselung des Datenträgers mit Symantec Drive Encryption oder verursacht einen Systemabsturz mit einem blauen Bildschirm, je nach Reihenfolge, in der die Anwendungen installiert wurden. Details zu bekannten Softwarekompatibilitätsproblemen mit Symantec Encryption Desktop finden Sie in der Symantec-Supportdatenbank im Artikel [TECH223625](#). [3406884]

Installieren des Maintenance Pack

So installieren Sie Symantec Encryption Desktop unter Windows

Hinweis: Sie müssen über Administratorrechte verfügen, um Symantec Encryption Desktop installieren zu können.

1. Doppelklicken Sie auf das Installationsprogramm für Symantec Encryption Desktop.
2. Folgen Sie den Anweisungen auf dem Bildschirm.
3. Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.

Weitere Informationen, inklusive Anweisungen zum Aktualisieren finden Sie im *Benutzerhandbuch zu Symantec Encryption Desktop für Windows*.

Technischer Support

Der technische Support von Symantec unterhält mehrere Supportcenter weltweit. Die Hauptaufgabe ist das Beantworten spezifischer Fragen zu Produktfunktionen. Die Mitarbeiter des technischen Support erstellen auch die Inhalte unserer Online-Supportdatenbank. Der technische Support arbeitet mit den anderen Bereichen von Symantec zusammen, um Fragen schnell zu beantworten. Beispielsweise erarbeitet der technische Support mit Product Engineering und Symantec Security Response Warnservices und Virendefinitions-Updates.

Symantec Support bietet Folgendes:

- Eine Reihe von Optionen, aus denen Sie die für die Größe Ihres Unternehmens passende wählen können
- Telefon bzw. webbasierter Support mit schneller Reaktion und aktuellen Informationen
- Software-Upgrades durch Upgrade-Versicherung
- Globaler Support auf Basis örtlicher Geschäftsstunden oder rund um die Uhr verfügbar
- Premium-Angebote, u. a. Account Management Services

Informationen zu Symantecs Support-Angeboten finden Sie auf unserer Website unter:

www.symantec.com/business/support/

Alle Support-Dienste werden im Rahmen Ihres Supportvertrags und der entsprechenden Unternehmensrichtlinie für technischen Support zur Verfügung gestellt.

Aufrufen des technischen Support

Kunden mit einem aktuellen Supportvertrag können Informationen unter folgender URL abrufen:

www.symantec.com/business/support/

Bevor Sie sich an den technischen Support wenden, prüfen Sie, ob die in der Produktdokumentation aufgeführten Systemanforderungen erfüllt sind. Außerdem sollten Sie auf den Computer zugreifen können, auf dem das Problem auftrat, falls es nötig ist, das Problem erneut zu provozieren.

Halten Sie folgende Informationen bereit:

- Produktversion
- Hardware
- Arbeitsspeicher, Speicherplatz und NIC
- Betriebssystem
- Version von Software und Patch
- Netzwerktopologie
- Router, Gateway und IP-Adresse
- Problembeschreibung:
 - Fehlermeldungen und Protokolldateien
 - Problemlösungsschritte, die vor der Kontaktaufnahme zu Symantec durchgeführt wurden
 - Änderungen an Softwarekonfiguration und Netzwerk

Lizenzierung und Registrierung

Wenn Sie das Symantec-Produkt registrieren müssen oder ein Lizenzschlüssel erforderlich ist, können Sie auf den technischen Support unter folgender URL zugreifen:

www.symantec.com/business/support/

Kundenservice

Informationen zum Kundenservice finden Sie unter folgender URL:

www.symantec.com/business/support/

Der Kundenservice ist für nichttechnische Fragen zuständig, beispielsweise:

- Fragen zu Lizenzen oder Seriennummern
- Aktualisieren von Registrierungsinfos (Änderung von Anschrift oder Name)
- Allgemeine Produktinformationen (Funktionen, verfügbare Sprachen, lokale Händler)
- Neueste Informationen zu Produkt-Updates
- Informationen zu Upgrade-Versicherung und Supportverträgen
- Informationen zu den Symantec Buying Programs
- Ratschläge zu den Optionen des technischen Support von Symantec
- Nichttechnische Fragen vor dem Kauf
- Probleme mit Datenträgern oder Handbüchern

Ressourcen zu Supportverträgen

Wenn Sie Fragen zu einem vorhandenen Supportvertrag haben, wenden Sie sich an das entsprechende Verwaltungsteam in Ihrer Region:

Asien/Pazifik und Japan customercare_apac@symantec.com

Europa, Naher Osten, Afrika semea@symantec.com

Nord- und Lateinamerika supportsolutions@symantec.com

Copyright und Marken

Copyright (c) 2014 Symantec Corporation. Alle Rechte vorbehalten. Symantec, das Symantec-Logo, das Häkchen-Logo, PGP, Pretty Good Privacy und das PGP-Logo sind Marken bzw. eingetragene Marken der Symantec Corporation bzw. Ihrer Tochterunternehmen in den USA und anderen Ländern. Andere Namen können Marken ihrer Eigentümer sein.