SOPHOS

Cybersecurity made simple.

# SafeGuard Enterprise

## Benutzerhilfe

Produktversion: 8.3

# Inhalt

# 1 Über SafeGuard Enterprise

Sophos SafeGuard wird auf Windows Endpoints ausgeführt, um diese zu schützen. Es besteht aus mehreren Modulen.

Unter Umständen stehen Ihnen nicht alle in dieser Hilfe beschriebenen Funktionen zur Verfügung. Das ist abhängig von Ihrer Lizenz und den Richtlinien, die Sie von Ihrem Sicherheitsbeauftragten erhalten haben.

Sophos SafeGuard wird zentral im Sophos SafeGuard Management Center verwaltet und konfiguriert.

Allgemeine Informationen zu Ihrer Installation von Sophos SafeGuard erhalten Sie über das Sophos SafeGuard Taskleistensymbol (Seite 8).

Die wichtigsten Funktionen zum Verschlüsseln und Entschlüsseln von Dateien sind über das Kontextmenü im Windows Explorer verfügbar.

Dieses Dokument bezieht sich nur auf Windows Endpoints. Informationen zu Mac Endpoints finden Sie in der SafeGuard Enterprise für Windows Benutzerhilfe.

**Module:**

**Full Disk Encryption**

- **Festplattenverschlüsselung mit BitLocker (Seite 2)**

**Synchronized Encryption**

- **SafeGuard File Encryption (anwendungsbasiert) (Seite 2)**

**File Encryption**

- **SafeGuard File Encryption (pfadbasiert) (Seite 3)**
- **SafeGuard Cloud Storage (Seite 4)**
- **SafeGuard Data Exchange (Seite 4)**

# 2 Module

## 2.1 Festplattenverschlüsselung mit BitLocker

Die Festplattenverschlüsselung mit BitLocker baut auf der BitLocker-Laufwerkverschlüsselungstechnologie auf, die in Ihrem Betriebssystem enthalten ist. Sie verschlüsselt Ihre gesamte Festplatte, so dass Ihre Daten sogar dann sicher sind, wenn der Computer verloren geht oder gestohlen wird.

Wenn Sie sich an Ihren Endpoint anmelden, müssen Sie Anmeldeinformationen eingeben, um BitLocker zu entsperren. Für weitere Informationen, siehe Einen Computer mit BitLocker verschlüsseln (Seite 11).

Mit Sophos SafeGuard können Sie BitLocker auf Endpoints mit einem der folgenden Betriebssysteme verwalten:

- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise

## 2.2 SafeGuard File Encryption (anwendungsbasiert)

Anwendungsbasierte Dateiverschlüsselung verschlüsselt Dateien, die mit bestimmten Anwendungen (z.B. Microsoft Word) erzeugt oder geändert wurden. Eine Richtlinie definiert eine Liste von Anwendungen, für die die Dateiverschlüsselung automatisch durchgeführt wird. Die Verschlüsselung ist persistent, das bedeutet, Ihre Daten sind auch dann sicher, wenn sie an einen anderen Ort verschoben, in die Cloud hochgeladen oder per E-Mail versandt werden.

Wenn Ihr Sicherheitsbeauftragter die Dateiverschlüsselung für Microsoft Word aktiviert hat, wird jede Datei, die Sie mit Word erstellen und/oder speichern automatisch mit einem vordefinierten Schlüssel verschlüsselt. Jeder, der diesen Schlüssel in seinem Schlüsselring hat, kann auf diese Datei zugreifen.

- Neue Dateien, die mit definierten Anwendungen erstellt wurden oder Dateien mit bestimmten definierten Dateierweiterungen, werden automatisch verschlüsselt.
- Wenn Sie den Schlüssel für eine verschlüsselte Datei haben, können Sie den Inhalt lesen und ändern.
- Wenn Sie den Schlüssel für eine verschlüsselte Datei nicht haben, können Sie den Inhalt nicht lesen.
- Wenn Sie auf einem Computer, auf dem File Encryption nicht installiert ist, auf eine verschlüsselte Datei zugreifen, können Sie den Inhalt nicht lesen.
- Dateien, die von einem unverschlüsselten Ordner in einen Ordner mit Verschlüsselungsregel verschoben oder kopiert werden, werden verschlüsselt.
- Dateien, die von einem verschlüsselten Ordner in einen unverschlüsselten Ordner verschoben oder kopiert werden, werden entschlüsselt.

- Dateien, die von einem verschlüsselten Ordner in einen Ordner mit einer anderen Verschlüsselungsregel verschoben oder kopiert werden, werden gemäß der Richtlinie des Zielordners verschlüsselt.
- Wenn Dateien mit Applikationen erstellt werden, für die Dateiverschlüsselung nicht aktiv ist aber die Dateiendung der Datei ist in einer Applikationenliste definiert, wird die Datei verschlüsselt und kann nicht mit der Applikation geöffnet werden, mit der sie erstellt wurde. Zum Beispiel, wenn Sie mit OpenOffice eine .doc-Datei erstellen und OpenOffice ist nicht in einer **Applikationenliste** angegeben.

**Wichtig**
Wird das Kopieren oder Verschieben von Dateien unterbrochen, z.B. durch einen Neustart, wird der Vorgang nicht automatisch fortgesetzt. Dies kann dazu führen, dass Dateien unbeabsichtigterweise unverschlüsselt sind. Um sicherzustellen, dass Dateien immer korrekt verschlüsselt sind, siehe Dateien gemäß Richtlinie verschlüsseln (Seite 13).

Um festzustellen, an welchen Orten auf einem Computer verschlüsselt wird, siehe Prüfen, wo Dateien verschlüsselt sind (Seite 16).

Um den Verschlüsselungsstatus einer oder mehrerer Dateien festzustellen, rechtsklicken Sie die Datei/die Dateien und wählen Sie **SafeGuard Dateiverschlüsselung > Verschlüsselungsstatus anzeigen**.

Im Windows Explorer sind verschlüsselte Dateien mit einem grünen Schloss-Symbol gekennzeichnet. Wird kein Schloss-Symbol angezeigt, obwohl die Datei verschlüsselt ist, siehe Sophos knowledgebase article 108784.

# 2.3 SafeGuard File Encryption (pfadbasiert)

Pfadbasierte Dateiverschlüsselung ermöglicht Ihrem Sicherheitsbeauftragten, Speicherorte zu definieren, wo Dateien verschlüsselt werden. z.B. **Dokumente**.

Wenn für Ihren Computer eine **File Encryption**-Richtlinie vom Typ **Pfadbasiert** gilt, werden die Dateien in den von der Richtlinie abgedeckten Speicherorten ohne Benutzerinteraktion transparent verschlüsselt:

- Neue Dateien an Speicherorten, an denen verschlüsselt wird, werden automatisch verschlüsselt.
- Wenn Sie den Schlüssel für eine verschlüsselte Datei haben, können Sie den Inhalt lesen und ändern.
- Wenn Sie den Schlüssel für eine verschlüsselte Datei nicht haben, können Sie den Inhalt nicht lesen.
- Wenn Sie auf einem Computer, auf dem File Encryption nicht installiert ist, auf eine verschlüsselte Datei zugreifen, können Sie den Inhalt nicht lesen.

Um festzustellen, an welchen Orten auf Ihrem Computer verschlüsselt wird, siehe Prüfen, wo Dateien verschlüsselt sind (Seite 16).

Um den Verschlüsselungsstatus einer oder mehrerer Dateien festzustellen, rechtsklicken Sie die Datei/die Dateien und wählen Sie **SafeGuard File Encryption > Verschlüsselungsstatus anzeigen**.

Im Windows Explorer sind verschlüsselte Dateien mit einem grünen Schloss-Symbol gekennzeichnet. Wird kein Schloss-Symbol angezeigt, obwohl die Datei verschlüsselt ist, siehe Sophos knowledgebase article 108784.

# 2.4 SafeGuard Cloud Storage

SafeGuard Cloud Storage bietet pfadbasierte Verschlüsselung von in der Cloud gespeicherten Dateien. Es beeinflusst nicht die Art und Weise, wie Sie mit Ihren Dateien arbeiten, sondern stellt sicher, dass die lokalen Kopien Ihrer Cloud-Daten transparent verschlüsselt werden und auch verschlüsselt bleiben, wenn sie in der Cloud gespeichert werden.

SafeGuard Cloud Storage erkennt automatisch Ihren Cloud Storage Provider (falls dieser unterstützt wird) und wendet die Verschlüsselungsrichtlinie auf den Synchronisierungsordner an.

SafeGuard Cloud Storage führt keine Initialverschlüsselung Ihrer Daten durch. Dateien, die vor der Installation oder Aktivierung von SafeGuard Cloud Storage per Richtlinie gespeichert wurden, bleiben unverschlüsselt. Wenn Sie solche Daten verschlüsseln möchten, müssen Sie sie zunächst aus der Cloud entfernen und sie dann wieder hinzufügen.

**Hinweis**
Fügen Sie keine Dateien zu Ihrem Dropbox Ordner hinzu, indem Sie sie auf das Dropbox Symbol am Windows Schreibtisch ziehen. Diese Dateien werden im Klartext in Ihren Dropbox Ordner kopiert. Um sicherzustellen, dass Dateien verschlüsselt sind, kopieren Sie sie direkt in Ihren Dropbox Ordner.

**Wichtig**
Beim Extrahieren eines ZIP-Archivs mit dem integrierten Archivprogramm von Microsoft Windows wird der Vorgang angehalten, sobald eine verschlüsselte Datei entdeckt wird, für die kein Schlüssel verfügbar ist. Der Benutzer erhält eine Nachricht, dass der Zugriff verweigert wurde, aber er wird nicht darüber informiert, dass Dateien vorhanden sind, die nicht verarbeitet wurden und somit fehlen. Andere Archivierprogramme wie z. B. 7-Zip eignen sich sehr gut für ZIP-Archive, die verschlüsselte Dateien enthalten.

# 2.5 SafeGuard Data Exchange

Das Modul SafeGuard Data Exchange bietet pfadbasierte Verschlüsselung von Dateien auf Wechselmedien, so können Sie sie mit anderen Benutzern austauschen. Nur Benutzer, die über die entsprechenden Schlüssel verfügen, können den Inhalt der verschlüsselten Daten lesen. Alle Ver- und Entschlüsselungsprozesse laufen transparent und mit minimaler Benutzerinteraktion ab.

Während Ihrer täglichen Arbeit merken Sie nicht, dass es sich um verschlüsselte Daten handelt. Entfernen Sie das wechselbare Speichermedium, bleiben die Daten jedoch verschlüsselt und sind gegen unbefugten Zugriff geschützt. Unbefugte Benutzer können zwar physikalisch auf die Daten zugreifen, jedoch können sie ohne SafeGuard Data Exchange und den richtigen Schlüssel die Daten nicht lesen.

Ihr Sicherheitsbeauftragter legt fest, wie mit Daten auf Wechselmedien umgegangen werden soll. Er kann z. B. festlegen, dass ausschließlich verschlüsselte Dateien auf den Medien zugelassen sind. In diesem Fall werden alle bereits auf dem Medium bestehenden Dateien initial verschlüsselt. Außerdem werden alle neuen Dateien, die auf dem Medium gespeichert werden, verschlüsselt. Sollen bereits existierende Dateien nicht verschlüsselt werden, kann der Zugriff auf die bereits auf dem Medium vorhandenen unverschlüsselten Dateien gestattet werden. In diesem Fall verschlüsselt SafeGuard Data Exchange die bereits vorhandenen unverschlüsselten Dateien nicht. Die neu hinzugekommen Dateien werden jedoch verschlüsselt. Somit können Sie die vorhandenen unverschlüsselten Dateien lesen und auch bearbeiten. Solche Daten werden erst verschlüsselt,

wenn der Name der Datei geändert wird. Der Sicherheitsbeauftragte kann auch festlegen dass Sie nicht dazu berechtigt sind, auf unverschlüsselte Dateien zuzugreifen, und die Dateien bleiben unverschlüsselt.

Für den Austausch von auf dem Medium vorhandenen verschlüsselten Dateien haben Sie folgende Möglichkeiten:

- **Der Empfänger der Dateien hat SafeGuard Enterprise installiert:** Sie können für den Datenaustausch gemeinsame Schlüssel verwenden, oder einen neuen Schlüssel erzeugen. Wenn Sie einen Schlüssel erzeugen, müssen Sie dem Empfänger der Daten eine Passphrase mitteilen.
- **Der Empfänger der Dateien hat SafeGuard Enterprise *nicht* installiert:** SafeGuard Enterprise bietet SafeGuard Portable. SafeGuard Portable lässt sich zusätzlich zu den verschlüsselten Dateien auf das Wechselmedium kopieren. Mit Hilfe von SafeGuard Portable und der entsprechenden Passphrase kann der Empfänger die verschlüsselten Dateien entschlüsseln und wieder verschlüsseln, ohne dafür SafeGuard Data Exchange installiert haben zu müssen.

**Wichtig**
Beim Extrahieren eines ZIP-Archivs mit dem integrierten Archivprogramm von Microsoft Windows wird der Vorgang angehalten, sobald eine verschlüsselte Datei entdeckt wird, für die kein Schlüssel verfügbar ist. Der Benutzer erhält eine Nachricht, dass der Zugriff verweigert wurde, aber er wird nicht darüber informiert, dass Dateien vorhanden sind, die nicht verarbeitet wurden und somit fehlen. Andere Archivierprogramme wie z. B. 7-Zip eignen sich sehr gut für ZIP-Archive, die verschlüsselte Dateien enthalten.

## 2.5.1 Overlay-Symbole

Overlay-Symbole sind kleine Symbole, die über Elementen im Windows Explorer angezeigt werden. Sie geben Auskunft über den Verschlüsselungsstatus von Dateien. Das Erscheinungsbild der Symbole hängt davon ab, welche Module auf Ihrem Endpoint installiert sind.

Die Data Exchange Overlay-Symbole werden nur bei Dateien und Volumes angezeigt.

- Der rote Schlüssel zeigt an, dass zum Entschlüsseln einer Datei keinen Schlüssel besitzen. Dieses Symbol wird nur bei Dateien angezeigt.
- Der grüne Schlüssel wird angezeigt, wenn eine Datei verschlüsselt ist und sich deren Schlüssel in Ihrem Schlüsselring befindet. Dieses Symbol wird nur bei Dateien angezeigt.
- Der graue Schlüssel wird angezeigt, wenn eine Datei nicht verschlüsselt ist, aber eine Verschlüsselungsregel für diese Datei verfügbar ist. Dieses Symbol wird nur bei Dateien angezeigt.
- Der gelbe Schlüssel wird angezeigt, wenn für ein Laufwerk eine Verschlüsselungsrichtlinie festgelegt wurde. Dieses Symbol wird nur bei Laufwerken angezeigt.

Overlay-Symbole werden nur bei Datenlaufwerken, Wechseldatenträgern und CDs/DVDs angezeigt. Overlay-Symbole für Boot-Laufwerke werden im Staging-Ordner angezeigt (der Ordner, in dem Windows die Dateien speichert, bevor sie auf CD/DVD gebrannt werden). Wenn Sie einen unverschlüsselten Ordner angeben, wird bei den unverschlüsselten Dateien in diesem Ordner und seinen Unterordnern kein grauer Schlüssel angezeigt. Generell gilt, dass kein grauer Schlüssel angezeigt wird, wenn auf eine Datei keine Verschlüsselungsregel angewendet wurde.

**Hinweis**
Werden keine Overlay-Symbole angezeigt, finden Sie nähere Informationen im Sophos Knowledgebase-Artikel 108784.

## 2.5.2 Transparente Verschlüsselung

Ist auf ihrem Computer festgelegt, dass Dateien auf Wechselmedien verschlüsselt werden sollen, laufen alle Ver- und Entschlüsselungsvorgänge vollständig transparent ab.

Die Dateien werden verschlüsselt, wenn sie auf die Wechselmedien geschrieben werden und entschlüsselt, wenn sie vom Wechselmedium an einen anderen Ort kopiert oder verschoben werden.

Die Daten werden in diesem Fall nur entschlüsselt, wenn Sie an einen Ort kopiert oder verschoben werden, für den keine andere Verschlüsselungsrichtlinie gilt. Sie liegen dort dann in Klartext vor. Gilt am neuen Speicherort eine andere Verschlüsselungsrichtlinie, werden die Daten dort entsprechend verschlüsselt.

## 2.5.3 Medien-Passphrase für Wechselmedien

SafeGuard Data Exchange unterstützt das Festlegen einer einzelnen Medien-Passphrase, mit der Sie auf alle mit Ihrem Computer verbundenen Wechseldatenträger zugreifen können. Dies ist unabhängig von dem für die Verschlüsselung der einzelnen Dateien verwendeten Schlüssel.

Ist diese Passphrase festgelegt, so kann der Zugriff auf verschlüsselte Dateien einfach durch Eingabe der Medien-Passphrase erlangt werden. Die Medien-Passphrase ist an die Computer, an denen Sie sich anmelden dürfen, gebunden. Somit verwenden Sie auf jedem Computer, an den Sie sich anmelden dürfen, die gleiche Medien-Passphrase.

Anweisungen zum Festlegen einer Medien-Passphrase finden Sie unter Eine Medien-Passphrase verwenden (Seite 21).

Die Medien-Passphrase kann geändert werden und wird automatisch auf jedem Computer, mit dem Sie arbeiten, synchronisiert, sobald Sie ein Wechselmedium mit diesem Computer verbinden.

Eine Medien-Passphrase ist in den folgenden Situationen nützlich:

- Sie möchten verschlüsselte Daten auf Wechselmedien auf Computern benutzen, auf denen SafeGuard Enterprise nicht installiert ist (SafeGuard Data Exchange in Kombination mit SafeGuard Portable).
- Sie möchten Daten mit externen Benutzern austauschen: Wenn Sie den externen Benutzern die Medien-Passphrase mitteilen, können Sie Ihnen den Zugriff auf alle Dateien auf dem Wechselmedium gewähren, unabhängig davon, welcher Schlüssel für die Verschlüsselung der einzelnen Dateien verwendet wurde.

Sie können auch den Zugriff auf alle Dateien einschränken, indem Sie dem externen Benutzer nur die Passphrase eines spezifischen Schlüssels (eines so genannten lokalen Schlüssels, der von einem SafeGuard Data Exchange Benutzer erzeugt werden kann) mitteilen. In diesem Fall hat der externe Benutzer nur Zugriff auf die Dateien, die mit diesem spezifischen Schlüssel verschlüsselt sind. Alle anderen Dateien sind für den externen Benutzer nicht lesbar.

Wenn Sie SafeGuard Enterprise Gruppenschlüssel für den Austausch von Daten auf Wechselmedien verwenden, ist innerhalb einer Arbeitsgruppe, deren Mitglieder alle den gleichen Gruppenschlüssel verwenden, keine Medien-Passphrase notwendig. In diesem Fall ist der Zugriff auf verschlüsselte Dateien auf Wechselmedien - falls so von Ihrem Sicherheitsbeauftragten definiert - voll transparent. Sie müssen keine Passphrase und kein Kennwort eingeben. Dies resultiert daraus, dass Gruppenschlüssel und Medien-Passphrasen für Wechselmedien gleichzeitig verwendet werden können. Da das System einen verfügbaren Gruppenschlüssel automatisch erkennt, ist der Zugriff für Benutzer, die diesen Schlüssel verwenden, voll transparent. Wenn kein Gruppenschlüssel erkannt wird, zeigt SafeGuard Data Exchange einen Dialog an, der den Benutzer zur Eingabe einer Medien-Passphrase oder einer Passphrase für einen lokalen Schlüssel auffordert.

## Unterstützte Medien

SafeGuard Data Exchange unterstützt folgende Wechselmedien:

- Systemstartschlüssel
- Externe Festplatten, die über USB oder FireWire angeschlossen sind.
- CD-RW-Laufwerke (UDF)
- DVD-RW-Laufwerke (UDF)
- Speicherkarten in USB-Kartenlesern

Blu-ray Discs und Dual-Layer DVDs werden nicht unterstützt.

# 3 Sophos SafeGuard Taskleistensymbol

Über das Sophos SafeGuard Taskleistensymbol in der Windows Taskleiste können Sie auf alle Funktionen von Sophos SafeGuard auf Ihrem Endpoint zugreifen. Die Verfügbarkeit der verschiedenen Funktionen hängt davon ab, welche Module installiert sind.

Rechtsklicken Sie auf das Sophos SafeGuard Taskleistensymbol um Folgendes anzuzeigen:

- **Anzeigen**:
  - **Schlüsselring**: Zeigt alle für Sie verfügbaren Schlüssel an.

    **Hinweis**
    Wenn Ihr Endpoint von einem Standalone-Endpoint zu einem zentral verwalteten Endpoint migriert wurde, kann eine zweite Anmeldung an SafeGuard Enterprise notwendig sein um Ihre benutzerdefinierten lokalen Schlüssel anzuzeigen.

  - **Benutzerzertifikat**: Zeigt Informationen zu Ihrem Zertifikat an.
  - **Unternehmenszertifikat**: Zeigt Informationen zu Ihrem Unternehmenszertifikat an.
- **BitLocker Anmeldeinformationen zurücksetzen**: Öffnet einen Dialog zum Zurücksetzen Ihrer BitLocker-PIN.
- **Neuen Schlüssel erzeugen**: Öffnet einen Dialog zum Erzeugen eines neuen Schlüssels für die Verwendung zum Datenaustausch über SafeGuard Data Exchange (Seite 4) oder SafeGuard Cloud Storage (Seite 4). Nur verfügbar, wenn eines der beiden Module auf Ihrem Computer installiert ist.
- **Medien-Passphrase ändern**: Öffnet einen Dialog zum Ändern der Medien-Passphrase, siehe SafeGuard Data Exchange (Seite 4).
- **Daten abgleichen**: Stößt den Datenabgleich mit dem SafeGuard Enterprise Server an. Das System informiert Sie über den Fortschritt und das Ergebnis des Datenabgleichs. Sie können den Datenabgleich auch durch Doppelklicken auf das Sophos SafeGuard Taskleistensymbol anstoßen.
- **Status**: Informationen über den Status des durch SafeGuard Enterprise geschützten Computers:

| Feld | Information |
|---|---|
| **Letzte erhaltene Richtlinie** | Datum und Uhrzeit wann der Computer zuletzt eine neue Richtlinie empfangen hat. |
| **Letzter Schlüsselempfang** | Datum und Uhrzeit wann der Computer zuletzt einen neuen Schlüssel empfangen hat. |
| **Letzter Zertifikatsempfang** | Datum und Uhrzeit wann der Computer zuletzt ein neues Zertifikat empfangen hat. |
| **Letzter Server-Kontakt** | Datum und Uhrzeit des letzten Kontakts zum Server. |

| Feld | Information |
| --- | --- |
| **SGN-Benutzerstatus** | Status des Benutzers, der am Computer angemeldet ist (Windows-Anmeldung):<br>— **ausstehend**<br>Die Replikation des Benutzers in der SGN-Datenbank ist ausstehend. Das bedeutet, dass der initiale Benutzerabgleich noch nicht abgeschlossen ist. Diese Information ist vor allem nach Ihrer ersten Anmeldung an SafeGuard Enterprise wichtig, da Sie sich erst an der SafeGuard Power-on Authentication anmelden können, wenn der initiale Benutzerabgleich abgeschlossen ist.<br>— **SGN-Benutzer**<br>Der in Windows angemeldete Benutzer gilt als SafeGuard Enterprise-Benutzer. Ein SGN-Benutzer kann sich bei der SafeGuard Power-on Authentication anmelden, wird der UMA (User Machine Assignment - Benutzer-Computer Zuordnung) hinzugefügt und erhält ein Benutzerzertifikat und einen Schlüsselring für den Zugriff auf verschlüsselte Daten.<br>— **SGN-Benutzer (Besitzer)**<br>Sofern die Standardeinstellungen nicht geändert wurden, kann der Besitzer es anderen Benutzern ermöglichen, sich an dem Endpoint anzumelden und SGN-Benutzer zu werden.<br>— **SGN-Gast**<br>SGN-Gastbenutzer werden nicht der UMA hinzugefügt, erhalten keine Berechtigungen zum Anmelden bei der SafeGuard POA, bekommen kein Zertifikat und keinen Schlüsselring zugewiesen und werden nicht in der Datenbank gespeichert.<br>— **SGN-Gast (Service Account)**<br>Der an Windows angemeldete Benutzer ist ein SafeGuard Enterprise Gastbenutzer, der sich mit einem Service Account für administrative Aufgaben angemeldet hat.<br>— **SGN Windows-Benutzer**<br>Ein SafeGuard Enterprise Windows-Benutzer wird nicht zur SafeGuard POA hinzugefügt, verfügt jedoch über einen Schlüsselring, mit dem er auf verschlüsselte Dateien zugreifen kann wie ein SafeGuard Enterprise-Benutzer. Die Benutzer werden der UMA hinzugefügt, d. h. sie dürfen sich auf diesem Endpoint bei Windows anmelden.<br>— **Unbestätigter Benutzer**<br>Unbestätigte Benutzer haben aus einem der folgenden Gründe keinen Zugriff zum Schlüsselring:<br>– Benutzer hat falschen Anmeldeinformationen eingegeben.<br>– Benutzer ist ein lokaler Benutzer.<br>– AD-Authentifizierungsserver ist nicht erreichbar.<br>– Authentisierung fehlgeschlagen.<br>Siehe Sophos Knowledgebase Artikel 124328 |

| Feld | Information |
|---|---|
| **SGN Endpoint-Status** | Zeigt den Sicherheitsstatus des Computers.<br>— **Nicht anwendbar**<br>Die entsprechende Funktion ist inaktiv.<br>— **Endpoint ist sicher**<br>Der Health-Status des Computers ist sicher.<br>— **Endpoint ist gefährdet**<br>Der Health-Status des Computers ist unsicher. Deshalb wurden Ihre Schlüssel entzogen und Sie haben keinen Zugriff auf verschlüsselte Dateien. |
| **Policy Cache Status**<br>**Zu versendende Datenpakete** | Gibt an, ob Datenpakete vorhanden sind, die an den SafeGuard Enterprise Server geschickt werden sollen. |
| **Local Self Help (LSH) Status**<br>**Aktiviert**<br>**Aktiv** | Gibt an, ob Local Self Help per Richtlinie freigeschaltet ist, und vom Benutzer auf dem Computer aktiviert wurde. |
| **Bereit zum Zertifikatwechsel** | Dieser Text wird angezeigt, wenn der Sicherheitsbeauftragte ein neues Zertifikat für die Anmeldung mit Token an Ihren Computer zugewiesen hat. Sie können das Zertifikat für die Anmeldung mit Token nun ändern. Weitere Informationen hierzu finden Sie in der SafeGuard Enterprise 8.0 Benutzerhilfe. |

- **Hilfe**: Öffnet die SafeGuard Enterprise Benutzerhilfe.
- **Über SafeGuard Enterprise**: Zeigt Informationen über Ihre SafeGuard Enterprise Version.

# 4 Hinweise zur Vorgehensweise

## 4.1 Einen Computer mit BitLocker verschlüsseln

Abhängig von dem Anmeldemodus, den der Sicherheitsbeauftragte für Ihren Endpoint eingerichtet hat, kann das Verhalten der SafeGuard Enterprise BitLocker-Unterstützung leicht abweichen.

Es wird in jedem Fall ein Dialog angezeigt, auf dem Sie auswählen können, ob Sie mit der Verschlüsselung fortfahren oder diese auf einen späteren Zeitpunkt verschieben möchten.

Wenn Sie das Speichern, Neustarten und/oder Verschlüsseln bestätigen, beginnt die Verschlüsselung trotzdem nicht sofort. Es wird ein Hardware-Test durchgeführt, um sicherzustellen, dass Ihr Endpoint die Voraussetzungen für die SafeGuard Enterprise BitLocker-Verschlüsselung erfüllt. Das System führt einen Neustart durch und überprüft, ob alle Hardware-Voraussetzungen erfüllt werden. Wenn z.B. TPM oder USB Stick nicht verfügbar oder zugänglich sind, werden Sie nach einem anderen Speichermedium zum Speichern des externen Schlüssels gefragt. Das System überprüft auch, ob Sie die Anmeldeinformationen korrekt eingeben können. Wenn Sie Ihre Anmeldeinformationen nicht eingeben können, startet der Computer dennoch, nicht aber die Verschlüsselung. Sie werden erneut nach Ihrer PIN oder dem Kennwort gefragt. Nach einem erfolgreichen Hardware-Test beginnt die BitLocker-Verschlüsselung.

Wenn Sie **Später erinnern** auswählen, startet die Verschlüsselung nicht und Sie werden erst wieder aufgefordert, dieses Volume zu verschlüsseln, wenn:

- eine neue Richtlinie eingeführt wird,
- sich der BitLocker-Verschlüsselungsstatus eines Volume ändert oder
- Sie sich erneut am System anmelden.

### 4.1.1 Systemstartschlüssel speichern

Wenn Ihr Sicherheitsbeauftragter **TPM + Systemstartschlüssel** oder **Systemstartschlüssel** als Anmeldemodus definiert hat, müssen Sie angeben, wo der Systemstartschlüssel gespeichert werden soll. Wir empfehlen zum Speichern des Schlüssels einen unverschlüsselten USB Stick zu verwenden. Die gültigen Ziellaufwerke für den Systemstartschlüssel sind in dem Dialog angegeben. Später müssen Sie den Stick immer dann einstecken, wenn Sie den Computer starten.

Wählen Sie das Ziellaufwerk aus und klicken Sie auf **Speichern und neu starten**.

### 4.1.2 Kennwort setzen

Wenn Ihr Sicherheitsbeauftragter **Kennwort** als Anmeldemodus eingerichtet hat, werden Sie aufgefordert, Ihr neues Kennwort einzugeben und zu wiederholen. Später benötigen Sie dieses Kennwort immer dann, wenn Sie Ihren Computer starten. Die erforderliche Länge und Komplexitiät des Kennworts hängen von den Gruppenrichtlinienobjekten ab, die Ihr Sicherheitsbeauftragter eingerichtet hat. Sie werden in dem Dialog über die Kennwortanforderungen informiert.

**Hinweis**
Beim Festlegen einer PIN oder eines Kennworts sind einige Dinge zu beachten. Die Pre-Boot-Umgebung unterstützt nur das US-Tastaturlayout. Wenn Sie jetzt eine PIN oder ein Kennwort mit Sonderzeichen festlegen, müssen Sie später bei der Anmeldung möglicherweise andere Tasten für die Eingabe verwenden.

### 4.1.3 PIN setzen

Wenn Ihr Sicherheitsbeauftragter **TPM + PIN** als Anmeldemodus eingerichtet hat, werden Sie aufgefordert, Ihre neue PIN einzugeben und zu wiederholen. Sie brauchen diese PIN in Zukunft immer wenn Sie ihren Computer starten. Die erforderliche Länge und Komplexität hängen von den Gruppenrichtlinienobjekten ab, die Ihr Sicherheitsbeauftragter eingerichtet hat. Sie werden in dem Dialog über die PIN-Anforderungen informiert.

**Hinweis**
Beim Festlegen einer PIN oder eines Kennworts sind einige Dinge zu beachten. Die Pro-Boot-Umgebung unterstützt nur das US-Tastaturlayout. Wenn Sie jetzt eine PIN oder ein Kennwort mit Sonderzeichen festlegen, müssen Sie später bei der Anmeldung möglicherweise andere Tasten für die Eingabe verwenden.

### 4.1.4 Dialog für TPM-only

Wenn Ihr Sicherheitsbeauftragter **TPM** als Anmeldemodus eingerichtet hat, müssen Sie lediglich den Neustart und die Verschlüsselung Ihres Endpoints bestätigen.

## 4.2 Eine vergessene BitLocker PIN/Kennwort zurücksetzen

Wenn Sie sich nicht bei Ihrem Computer anmelden können, weil Sie PIN, Kennwort oder USB-Schlüssel vergessen haben, benötigen Sie einen Wiederherstellungsschlüssel. So fordern Sie einen Wiederherstellungsschlüssel an:

1. Starten Sie den Computer neu und drücken Sie die **Esc**-Taste, wenn der **BitLocker**-Anmeldebildschirm erscheint.
2. Auf dem Bildschirm **BitLocker-Wiederherstellung** wird die **Wiederherstellungsschlüssel-ID** angezeigt.
   Die **Wiederherstellungsschlüssel-ID** wird nur für kurze Zeit angezeigt. Um sie erneut anzuzeigen, müssen Sie den Computer neu starten.
3. Wenden Sie sich an Ihren Administrator und teilen Sie ihm die **Wiederherstellungsschlüssel-ID** mit.
   Ihr Administrator muss den Wiederherstellungsschlüssel für Ihren Computer im Sophos SafeGuard Management Center suchen und Ihnen den Schlüssel mitteilen.
4. Geben Sie im Bildschirm **BitLocker-Wiederherstellung** den Wiederherstellungsschlüssel ein.
   Sie können jetzt Ihren Computer starten.

Sobald Sie am System angemeldet sind, geben Sie die neuen BitLocker-Anmeldeinformationen ein. Abhängig vom Betriebssystem wird ein Dialog zum Zurücksetzen der Anmeldeinformationen angezeigt. Wenn dieser Dialog nicht automatisch angezeigt wird, klicken Sie mit der rechten Maustaste auf das

SafeGuard Enterprise-Symbol in der Taskleiste, wählen Sie **Bit Locker Anmeldeinformationen zurücksetzen** aus und folgen Sie den Anweisungen auf dem Bildschirm.

# 4.3 Eine vergessene BitLocker-PIN/ein BitLocker-Kennwort mit Challenge/Response zurücksetzen

## Challenge/Response-Verfahren

Wenn Sie einen BitLocker Recovery-Schlüssel benötigen, gehen Sie wie folgt vor:

1. Starten Sie den PC neu. Nach dem Neustart wird eine Meldung mit gelbem Text auf schwarzem Grund angezeigt. Drücken Sie innerhalb der nächsten drei Sekunden eine beliebige Taste.
2. Der Challenge/Response-Bildschirm wird angezeigt.
3. Im zweiten Schritt erhalten Sie die Informationen, die Sie benötigen, um sich an den Helpdesk zu wenden.
4. Teilen Sie dem Helpdesk die folgenden Informationen mit:
   - **Computer**, zum Beispiel Sophos\<Computername>
   - **Challenge**-Code, z. B. ABC12-3DEF4-56GHO-892UT-Z654K-LM321. Bewegen Sie den Mauszeiger über die einzelnen Zeichen, um eine Buchstabierhilfe einzublenden, oder drücken Sie mehrmals **F1** um diese Hilfe einzublenden. Der Code wird nach 30 Minuten ungültig. Dann wird der PC automatisch heruntergefahren.
5. Geben Sie dann den vom Helpdesk erhaltenen **Response-Code** (sechs Blöcke mit jeweils zwei Text-Feldern, pro Feld sind 5 Zeichen erforderlich) ein.
   - Sobald ein Textfeld vollständig ausgefüllt ist springt der Fokus automatisch auf das nächste Textfeld.
   - Wenn Sie in einem Block ein falsches Zeichen angeben, wird der entsprechende Block rot markiert.
6. Klicken Sie nach erfolgreicher Eingabe des Response-Code auf **Weiter** oder drücken Sie **Enter**, um die Challenge/Response-Aktion abzuschließen.

## BitLocker-Anmeldeinformationen zurücksetzen

Geben Sie die neuen BitLocker-Anmeldeinformationen ein, sobald Sie am System angemeldet sind, Abhängig vom Betriebssystem wird ein Dialog zum Zurücksetzen der Anmeldeinformationen angezeigt. Wenn dieser Dialog nicht automatisch angezeigt wird, klicken Sie mit der rechten Maustaste auf das SafeGuard Enterprise-Symbol in der Taskleiste, wählen Sie **Bit Locker Anmeldeinformationen zurücksetzen** aus und folgen Sie den Anweisungen auf dem Bildschirm.

# 4.4 Dateien gemäß Richtlinie verschlüsseln

Nachdem auf Ihren Computer eine **File Encryption** Richtlinie angewendet wurde, werden vorhandene Dateien in den von der Richtlinie abgedeckten Speicherorten nicht automatisch verschlüsselt. Es muss eine initiale Verschlüsselung durchgeführt werden.

Wir empfehlen, diese Initialverschlüsselung durchzuführen, sobald auf Ihrem Endpoint eine File Encryption Richtlinie eingeht, obwohl Ihr Sicherheitsbeauftragter diesen Verschlüsselungsvorgang auch automatisch starten kann.

Um die Verschlüsselung manuell zu starten, klicken Sie mit der rechten Maustaste auf den Knoten **Dieser PC** im Windows Explorer und wählen Sie **SafeGuard Dateiverschlüsselung > Gemäß Richtlinie verschlüsseln**. Der SafeGuard Assistent für Dateiverschlüsselung (Seite 14) verschlüsselt alle Dateien in Ordnern und Unterordnern, die in den definierten Verschlüsselungsrichtlinien enthalten sind.

## 4.4.1 SafeGuard Assistent für Dateiverschlüsselung

Um den SafeGuard Assistenten für Dateiverschlüsselung zu starten, klicken Sie mit der rechten Maustaste auf den Knoten **Dieser PC** oder auf einen Ordner im Windows Explorer und wählen Sie **SafeGuard Dateiverschlüsselung > Gemäß Richtlinie verschlüsseln**.

Die Anwendung überprüft alle Ordner, die in einer Verschlüsselungsregel für den Benutzer definiert sind:

- Unverschlüsselte Dateien, die verschlüsselt werden sollen, werden mit dem in der Regel definierten Schlüssel verschlüsselt.
- Verschlüsselte Dateien, die mit einem anderen Schlüssel verschlüsselt werden sollen, werden mit dem in der Regel definierten Schlüssel neu verschlüsselt.
- Wenn der Benutzer den aktuellen Schlüssel nicht hat, wird eine Fehlermeldung angezeigt.
- Verschlüsselte Dateien, die laut Verschlüsselungsrichtlinie unverschlüsselt sein sollten, bleiben verschlüsselt.

Ein Status-Bild zeigt den Gesamtstatus des Vorgangs:

- **Grün:** Der Vorgang wurde erfolgreich abgeschlossen.
- **Rot:** Der Vorgang wurde mit Fehlern abgeschlossen.
- **Gelb:** Der Vorgang dauert an.

In drei Registerkarten werden detaillierte Informationen zu den verarbeiteten Dateien angezeigt:

- Die Registerkarte **Übersicht** zeigt Zähler zu den gefundenen/verschlüsselten/neu verschlüsselten usw. Dateien an. Mit der **Exportieren...** Schaltfläche können Sie Berichte zu den verarbeiteten Dateien mit den entsprechenden Ergebnissen in XML-Format erstellen.
- Die Registerkarte **Fehler** zeigt die Dateien, die nicht wie gewünscht verarbeitet werden konnten.
- Die Registerkarte **Geändert** zeigt die Dateien, die erfolgreich geändert werden konnten.
- Die Registerkarte **Alle** zeigt alle verarbeiteten Dateien und die entsprechenden Ergebnisse.

Klicken Sie auf die Schaltfläche **Beenden** in der oberen rechten Ecke, um den Vorgang abzubrechen. Daraufhin wird anstelle der Schaltfläche **Beenden** die Schaltfläche **Neu starten** angezeigt, mit der Sie den Vorgang erneut starten können.

Wird der Vorgang mit Fehlern abgeschlossen, wird anstelle der Schaltfläche **Beenden** die Schaltfläche **Erneut versuchen** angezeigt. Wenn Sie auf **Erneut versuchen** klicken, wird der Vorgang nur für die Dateien, die nicht verarbeitet werden konnten, neu gestartet.

# 4.5 Dateien manuell verschlüsseln/entschlüsseln

SafeGuard File Encryption ermöglicht Ihnen, einzelne Dateien manuell zu verschlüsseln oder zu entschlüsseln. Klicken Sie mit der rechten Maustaste auf eine Datei und wählen Sie **SafeGuard Dateiverschlüsselung**. Folgende Funktionen stehen zur Verfügung:

- **Verschlüsselungsstatus anzeigen**: Zeigt an, ob die Datei verschlüsselt ist und welcher Schlüssel verwendet wurde.
- **Gemäß Richtlinie verschlüsseln** Mehr dazu erfahren Sie unter Dateien gemäß Richtlinie verschlüsseln (Seite 13).
- **Entschlüsseln**: (Nur für pfadbasierte Dateiverschlüsselung): Ermöglicht das Entschlüsseln einer Datei, für die keine Dateiverschlüsselungsregel gilt.
- **Ausgewählte Datei entschlüsseln** (nur für anwendungsbasierte Dateiverschlüsselung): Sie können Dateien entschlüsseln und unverschlüsselt speichern. Wir empfehlen, Ihre Datei nur dann zu entschlüsseln, wenn sie keine sensiblen Informationen enthält.
- **Ausgewählte Datei verschlüsseln** (nur für anwendungsbasierte Dateiverschlüsselung): Sie können Dateien manuell mit dem in Ihrer Richtlinie definierten Schlüssel verschlüsseln.
- **Kennwortgeschützte Datei erstellen**: Hier können Sie ein Kennwort zum manuellen Verschlüsseln Ihrer Datei definieren. Dies ist sinnvoll, wenn Sie eine vertrauliche Datei mit jemandem außerhalb Ihres Unternehmens teilen möchten, siehe Verschlüsselte Dateien per E-Mail senden (Seite 17).

Wenn Sie mit der rechten Maustaste auf Ordner oder Laufwerke klicken, sind folgende Funktionen verfügbar:

- **Verschlüsselungsstatus anzeigen**: Zeigt eine Liste der enthaltenen Dateien, deren Verschlüsselungsstatus und die verwendeten Schlüssel an.
- **Gemäß Richtlinie verschlüsseln** Mehr dazu erfahren Sie unter Dateien gemäß Richtlinie verschlüsseln (Seite 13).

Die folgenden Optionen sind nur für Cloud Storage und Data Exchange verfügbar:

- **Standardschlüssel**: Zeigt den derzeit für auf dem Laufwerk neu angelegte Dateien (durch Speichern, Kopieren, Verschieben) verwendeten Schlüssel an. Die Standardschlüssel können für jedes Volume oder Wechselmedium getrennt festgelegt werden.
- **Standardschlüssel festlegen**: Öffnet einen Dialog, in dem ein anderer Standardschlüssel ausgewählt werden kann.
- **Neuen Schlüssel erzeugen**: Öffnet den Dialog zum Erzeugen von benutzerdefinierten lokalen Schlüsseln.
- **Verschlüsselung wieder aktivieren:** Ihr Sicherheitsbeauftragter kann Sie dazu berechtigen zu entscheiden, ob Dateien auf mit Ihrem Computer verbundenen Wechselmedien verschlüsselt werden sollen. Wenn Sie Wechselmedien mit Ihrem Computer verbinden, wird eine Meldung angezeigt, die Sie dazu auffordert zu entscheiden, ob die Dateien auf dem angesteckten Medium verschlüsselt werden sollen. Darüber hinaus kann Sie Ihr Sicherheitsbeauftragter dazu berechtigen festzulegen, ob Ihre Entscheidung für das relevante Medium gespeichert werden soll. Wenn Sie **Einstellung speichern und Dialog nicht mehr anzeigen** wählen, wird die Meldung für das relevante Medium nicht mehr angezeigt. In diesem Fall steht der neue Befehl **Verschlüsselung wieder aktivieren** im Kontextmenü des relevanten Mediums im Windows Explorer zur Verfügung. Wählen Sie diesen Befehl, um Ihre Entscheidung über die Verschlüsselung für das relevante Medium rückgängig zu machen. Ist dies nicht möglich, weil Sie zum Beispiel nicht über die notwendigen Rechte für das Medium verfügen, so wird eine Fehlermeldung angezeigt. Nachdem

 

Sie Ihre Entscheidung rückgängig gemacht haben, werden Sie wieder dazu aufgefordert zu entscheiden, ob die Dateien auf dem relevanten Medium verschlüsselt werden sollen.

# 4.6 Prüfen, wo Dateien verschlüsselt sind

Wenn Sie überprüfen möchten, wo Dateien auf Ihrem Computer verschlüsselt sind und welche Schlüssel zum Schutz Ihrer Dateien verwendet werden, können Sie das SafeGuard Enterprise `FETool` verwenden.

Um das SafeGuard Enterprise `FETool` zu starten, öffnen Sie eine Eingabeaufforderung, gehen Sie zu `C:\Programme (x86)\Sophos\SafeGuard Enterprise\FileEncryption` und geben Sie `fetool rli -a`ein.

Dieser Befehl listet alle Verschlüsselungsregeln auf, die für Ihren Computer gelten. Die Liste enthält den Verschlüsselungsmodus, den vollständigen Pfad zu den entsprechenden Ordnern und die verwendeten Schlüssel.

# 4.7 Datei mit Kennwort schützen

Wenn Sie E-Mails an Empfänger außerhalb Ihres Firmennetzwerks senden, empfehlen wir, die Datei mit einem Kennwort zu verschlüsseln. Das erlaubt den Empfängern ohne SafeGuard Enterprise auf verschlüsselte Dateien zuzugreifen.

Gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei, die Sie versenden möchten, und wählen Sie **Kennwortgeschützte Datei erstellen**.
2. Folgen Sie den Anweisungen auf dem Bildschirm und erzeugen Sie ein Kennwort. Wählen Sie ein sicheres Kennwort und senden Sie es nicht in derselben E-Mail wie die Dateien.
   Ihre Datei wird verschlüsselt und als HTML-Datei gespeichert. Sie können die HTML-Datei nun sicher per E-Mail versenden.

   **Hinweis**
   - Für die Verschlüsselung benötigen Sie freien Platz auf der Festplatte.
   - Die verschlüsselte HTML-Datei ist größer als die Originaldatei.
   - Die maximal unterstützte Dateigröße beträgt 50 MB.
   - Um mehrere Dateien auf einmal zu verschlüsseln, können Sie sie in eine .zip-Datei packen und die .zip-Datei verschlüsseln.

3. Übermitteln Sie Ihren Empfängern das Kennwort am Telefon oder persönlich.
   Empfänger können einen der folgenden Browser verwenden, um den kennwortgeschützten Anhang zu öffnen:
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Internet Explorer 11
   - Microsoft Edge
4. Weisen Sie Ihre Empfänger an, auf die Datei doppelzuklicken und den Anweisungen auf dem Bildschirm zu folgen, um Folgendes zu tun:
   - Das Kennwort eingeben und auf **Entschlüsseln** klicken, um auf die Datei zuzugreifen

- Auf **Neue Datei mit Kennwort schützen** klicken, um eine andere Datei mit einem Kennwort zu schützen.

Empfänger können die Datei öffnen, die Sie mit einem Kennwort geschützt haben. Sie können die Datei mit einem Kennwort schützen, bevor sie sie an Sie zurücksenden. Dabei können sie dasselbe oder ein neues Kennwort verwenden. Sie können sogar eine neue Datei mit einem Kennwort schützen.

# 4.8 Verschlüsselte Dateien per E-Mail senden

Wenn Sie verschlüsselte Dateien an Empfänger innerhalb Ihres Firmennetzwerks senden, brauchen Sie sich nicht um die Verschlüsselung und Entschlüsselung zu kümmern. Empfänger, die den erforderlichen Schlüssel haben, können die Datei lesen.

Zum Senden von E-Mails an Empfänger außerhalb Ihres Firmennetzwerks bietet SafeGuard Enterprise ein Add-In für Microsoft Outlook, mit dem E-Mail-Anhänge einfach verschlüsselt werden können. Wenn Sie eine E-Mail mit einem oder mehreren Anhängen versenden, werden Sie gefragt, wie Sie mit Ihren Dateien verfahren möchten. Die verfügbaren Optionen hängen vom Verschlüsselungsstatus der Datei(en) ab, die Sie an die Mail anhängen.

**Hinweis**
Wenn Sie eingebettete Elemente wie Kontakte (.vcf) oder E-Mails (.msg) als Anlagen senden, werden Sie nicht zur Verschlüsselung aufgefordert. Sie werden unverschlüsselt gesendet.

- **Kennwortgeschützt**

  Wählen Sie diese Option, wenn Sie sensible Dateien an Empfänger außerhalb Ihrer Organisation senden.

  Nachdem Sie ein Kennwort definiert und auf Senden gedrückt haben wird Ihre Datei verschlüsselt und als HTML-Datei gespeichert. Wenn Sie mehrere Dateien gleichzeitig versenden wird jede Datei einzeln mit demselben Kennwort geschützt. Bereits verschlüsselte Dateien werden entschlüsselt bevor sie kennwortgeschützt werden.

  Empfänger können die Datei mit ihrem Browser öffnen sobald Sie ihnen das Kennwort mitteilen. Wählen Sie ein sicheres Kennwort und senden Sie es nicht in derselben E-Mail wie die Dateien. Wir empfehlen, den Empfängern das Kennwort am Telefon oder persönlich zu übermitteln.

  Empfänger können einen der folgenden Browser verwenden, um den kennwortgeschützten Anhang zu öffnen:

  — Mozilla Firefox

  — Google Chrome

  — Microsoft Internet Explorer 11

  — Microsoft Edge

  Die Entschlüsselung mit anderen Browsern, z. B. mobilen Browsern, funktioniert möglicherweise, wird jedoch nicht aktiv unterstützt.

  Empfänger können die erhaltene Datei bearbeiten und sie mit demselben Kennwort oder mit einem neuen Kennwort verschlüsselt zurücksenden. Sie können sogar eine neue Datei mit einem Kennwort schützen. Ein Assistent im Browser führt durch den Prozess. Weitere Informationen finden Sie im Sophos Knowledgebase-Artikel 124440.

  Sie können Dateien auch manuell mit einem Kennwort schützen, siehe Datei mit Kennwort schützen (Seite 16).

- **Ungeschützt**

 

Wählen Sie diese Option nur wenn Ihr Mailanhang keine sensiblen Daten enthält. Wenn Sie eine E-Mail mit ungeschützten Anhängen senden kann Ihre Aktion protokolliert und von Ihrem Sicherheitsbeauftragten überwacht werden.

- **Anhänge, die unverändert gesendet werden**

  Wenn die E-Mail Anhänge enthält, die nicht kennwortgeschützt werden können, können Sie diese Anhänge entweder unverändert senden oder aus der E-Mail entfernen. Der Dialog enthält eine Liste von Dateien, die aus einem der folgenden Gründe nicht geschützt werden können:

  — Die Datei ist bereits kennwortgeschützt. Sie können die Datei entweder zuerst entschlüsseln und dann ein neues Kennwort verwenden, oder Sie senden die Datei unverändert und teilen das erforderliche Kennwort Ihrem Empfänger mit.

  — Die Datei wurde mit einem Schlüssel verschlüsselt, der sich derzeit nicht in Ihrem Schlüsselbund befindet. Der Schlüssel wurde möglicherweise aus Sicherheitsgründen vorübergehend entzogen oder Sie verfügen nicht über den zum Verschlüsseln der Datei verwendeten Schlüssel. Wenden Sie sich in diesem Fall an Ihren Sicherheitsbeauftragten.

E-Mails, die Sie gleichzeitig an interne und externe Empfänger senden, werden wie externe E-Mails behandelt.

# 4.9 Einen lokalen Schlüssel erzeugen

Sie können lokale Schlüssel zum Verschlüsseln von Dateien an bestimmten Speicherorten auf Wechselmedien oder in der Cloud verwenden. Diese Speicherorte müssen bereits in einer Dateiverschlüsselungsrichtlinie enthalten sein.

So erzeugen Sie einen lokalen Schlüssel:

1. Klicken Sie mit der rechten Maustaste auf das Sophos SafeGuard Taskleistensymbol in der Windows Taskleiste oder auf ein Volume, ein Verzeichnis oder eine Datei.
2. Klicken Sie auf **Neuen Schlüssel erzeugen**.
3. Geben Sie im Dialog **Schlüssel erzeugen** einen Namen und eine **Passphrase** für den Schlüssel ein.

   Der interne Name des Schlüssels wird im Feld darunter angezeigt.
4. Bestätigen Sie die Passphrase.

   Wenn Sie eine unsichere Passphrase eingeben, wird ein Hinweis angezeigt. Zur Erhöhung des Sicherheitsniveaus ist die Verwendung von komplexen Passphrasen empfehlenswert. Sie können selbst entscheiden, ob Sie die unsichere Passphrase dennoch verwenden wollen. Die Passphrase muss außerdem den Unternehmensrichtlinien entsprechen. Ist dies nicht der Fall, so wird eine Warnung angezeigt.
5. Wenn Sie den Dialog über ein Kontextmenü geöffnet haben, enthält dieses die Option **Als neuen Standardschlüssel für Pfad verwenden**. Mit der Option **Als neuen Standardschlüssel für Pfad verwenden** können Sie diesen Schlüssel als Standardschlüssel für ein Volume oder einen Cloud Storage-Synchronisierungsordner festlegen.

   Der Standardschlüssel, den Sie hier angeben, wird im laufenden Betrieb für die Verschlüsselung verwendet. Dieser Standardschlüssel wird solange verwendet, bis ein anderer gesetzt wird.
6. Klicken Sie auf **OK**.

   Der Schlüssel wird erzeugt und steht zur Verfügung, wenn die Daten erfolgreich mit dem SafeGuard Enterprise Server synchronisiert wurden.

   Wenn Sie diesen Schlüssel als Standardschlüssel festlegen, werden alle Daten, die ab diesem Zeitpunkt auf ein Wechselmedium oder in einen Cloud Storage Synchronisierungsordner kopiert werden, mit diesem Schlüssel verschlüsselt.

Damit ein Empfänger alle Daten auf dem Wechselmedium entschlüsseln kann, müssen Sie gegebenenfalls die Daten auf dem Medium mit dem lokal erzeugten Schlüssel neu verschlüsseln. Wählen Sie das Medium im Windows Explorer aus und klicken Sie im Kontextmenü **SafeGuard Dateiverschlüsselung > Gemäß Richtlinie verschlüsseln**. Wählen Sie dann den gewünschten lokalen Schlüssel aus und verschlüsseln Sie die Daten. Wenn Sie eine Medien-Passphrase benutzen, ist dies nicht notwendig.

### 4.9.1 Import von Schlüsseln aus einer Datei

Wenn Sie ein Wechselmedium mit verschlüsselten Daten erhalten haben oder auf Cloud Storage Daten in einem freigegebenen Ordner zugreifen möchten und diese Daten mit benutzerdefinierten lokalen Schlüsseln verschlüsselt sind, können Sie den zur Entschlüsselung notwendigen Schlüssel in Ihren privaten Schlüsselring importieren.

Dazu benötigen Sie die Passphrase für diesen Schlüssel. Diese muss Ihnen von der Person, die die Daten verschlüsselt hat, mitgeteilt werden.

1. Wählen Sie die Datei auf dem Wechselmedium und klicken Sie auf **SafeGuard Dateiverschlüsselung > Schlüssel aus Datei importieren**.
2. Geben Sie im nun angezeigten Dialog die Passphrase ein.

Der Schlüssel wird importiert und Sie können auf die Datei zugreifen.

## 4.10 Daten mit SafeGuard Data Exchange austauschen

Typische Anwendungsfälle für den sicheren Datenaustausch mit SafeGuard Data Exchange sind:

- Austausch von Daten mit SafeGuard Enterprise Benutzern, die zumindest über einen Schlüssel verfügen, der sich auch in Ihrem Schlüsselring befindet.

  In diesem Fall verschlüsseln Sie die Daten auf dem Wechselmedium mit einem Schlüssel, den auch der Empfänger (z. B. auf seinem Notebook) in seinem Schlüsselring hat. Da er den Schlüssel besitzt, kann er auf die verschlüsselten Daten transparent zugreifen.

- Austausch von Daten mit SafeGuard Enterprise Benutzern, die nicht den gleichen Schlüssel besitzen wie Sie selbst.

  Dazu erzeugen Sie einen lokalen Schlüssel und verschlüsseln die Daten damit. Lokal erzeugte Schlüssel sind mit einer Passphrase abgesichert und können von SafeGuard Enterprise importiert werden. Sie teilen dem Empfänger der Daten die Passphrase mit. Damit kann er den Schlüssel importieren und dann auf die Daten zugreifen.

- Austausch von Daten mit Benutzern ohne SafeGuard Enterprise

  Benutzer, die SafeGuard Enterprise nicht auf ihrem Computer installiert haben, können mit SafeGuard Portable auf verschlüsselte Dateien zugreifen. SafeGuard Portable wird nicht auf Macs unterstützt. Weitere Informationen finden Sie unter:

  — Austauschen von Daten auf Wechselmedien ohne SafeGuard Enterprise (Seite 21)

  — Dateien mit SafeGuard Portable bearbeiten (Seite 25)

 

## 4.10.1 Wechselmedien mit SafeGuard Data Exchange verschlüsseln

Die Verschlüsselung von unverschlüsselten Daten auf einem Wechselmedium startet entweder automatisch, wenn Sie das Wechselmedium mit dem System verbinden, oder Sie muss von Ihnen angestoßen werden. Wenn Sie dazu berechtigt sind zu entscheiden, ob Dateien auf Wechselmedien verschlüsselt werden sollen, werden Sie dazu aufgefordert, sobald Sie Wechselmedien an Ihren Computer anschließen.

So starten Sie den Verschlüsselungsvorgang manuell:

1. Wählen Sie im Windows Explorer im Kontextmenü **SafeGuard Dateiverschlüsselung > Gemäß Richtlinie verschlüsseln**. Ist kein bestimmter Schlüssel festgelegt worden, wird ein Dialog angezeigt, in dem Sie einen Schlüssel auswählen können.
2. Wählen Sie einen Schlüssel und klicken Sie auf **OK**. Alle Daten, die sich auf dem Wechselmedium befinden, werden verschlüsselt.

   Der Standardschlüssel wird benutzt, solange kein anderer Schlüssel als Standard definiert wird. Wenn Sie den Standardschlüssel ändern, wird der neue Schlüssel für die Initialverschlüsselung der Wechselmedien verwendet, die nach der Änderung mit dem Computer verbunden werden.

**Hinweis**
Benutzergenerierte lokale Schlüssel werden zum Datenaustausch mit Benutzern benötigt, die SafeGuard Enterprise zwar installiert haben, aber nicht dieselben Schlüssel wie Sie verwenden. Darüber hinaus sind lokale Schlüssel für den sicheren Datenaustausch mit Benutzern, die SafeGuard Enterprise nicht einsetzen, erforderlich. Lokale Schlüssel sind am Präfix Local_ zu erkennen.

Wird die Option **Unverschlüsselte Dateien verschlüsseln und verschlüsselte Dateien umschlüsseln** ausgewählt, werden bereits verschlüsselte Dateien, für die der Schlüssel vorhanden ist, entschlüsselt und anschließend mit dem neuen Schlüssel verschlüsselt.

**Initialverschlüsselung abbrechen**

Wenn die Initialverschlüsselung per Konfiguration automatisch startet, sind Sie möglicherweise dazu berechtigt, die Initialverschlüsselung abzubrechen. In diesem Fall ist die Schaltfläche **Abbrechen** aktiv, eine **Start**-Schaltfläche wird angezeigt und der Beginn des Verschlüsselungsvorgangs hat eine Verzögerung von 30 Sekunden. Wenn Sie in diesem Zeitraum nicht auf **Abbrechen** klicken, startet die Initialverschlüsselung nach 30 Sekunden automatisch. Wenn Sie auf **Start** klicken, wird die Initialverschlüsselung sofort gestartet.

### Initialverschlüsselung für Benutzer mit einer Medien-Passphrase

Wenn die Verwendung einer Medien-Passphrase per Richtlinie definiert wurde, werden Sie vor der Initialverschlüsselung aufgefordert, die Medien-Passphrase einzugeben. Die Medien-Passphrase gilt für alle von Ihnen verwendeten Wechselmedien und ist an Ihren Computer bzw. an alle Computer, an denen Sie sich anmelden dürfen, gebunden.

Die Initialverschlüsselung wird automatisch gestartet, wenn Sie die Medien-Passphrase eingegeben haben.

Wenn Sie die Medien-Passphrase einmal eingegeben haben, startet die Initialverschlüsselung jeweils automatisch, wenn Sie ein neues Wechselmedium mit dem Computer verbinden.

Auf Computern, auf denen Ihre Medien-Passphrase nicht eingestellt ist, wird die Initialverschlüsselung nicht gestartet.

## 4.10.2 Eine Medien-Passphrase verwenden

Falls die Verwendung einer Medien-Passphrase per Richtlinie definiert ist, werden Sie aufgefordert, die Medien-Passphrase einzugeben, wenn Sie nach der Installation von SafeGuard Data Exchange zum ersten Mal ein Wechselmedium mit dem Computer verbinden.

Wenn der Dialog angezeigt wird, geben Sie eine Medien-Passphrase ein. Mit dieser Medien-Passphrase können Sie auf alle verschlüsselten Dateien auf Ihren Wechselmedien zugreifen, unabhängig davon, welcher Schlüssel für die Verschlüsselung verwendet wurde.

Die Medien-Passphrase gilt für alle Wechselmedien, die Sie mit Ihrem Computer verbinden, sowie auf allen Computern, an denen Sie sich anmelden dürfen. Die Medien-Passphrase kann auch mit SafeGuard Portable verwendet werden und ermöglicht auch hier den Zugriff auf alle Dateien, unabhängig davon, mit welchem Schlüssel sie verschlüsselt wurden.

Beachten Sie, dass Sie auf Macs keine Medien-Passphrase verwenden können.

### Ändern/Zurücksetzen der Medien-Passphrase

Sie können Ihre Medien-Passphrase jederzeit mit dem Befehl **Medien-Passphrase ändern** im Menü des Taskleistensymbols ändern. Es wird ein Dialog angezeigt, in dem Sie die alte und die neue Medien-Passphrase eingeben und die neue bestätigen.

Wenn Sie Ihre Medien-Passphrase vergessen haben, können Sie sie in diesem Dialog auch zurücksetzen. Wenn Sie die Option **Medien-Passphrase zurücksetzen** auswählen und auf **OK** klicken, werden Sie darüber informiert, dass Ihre Medien-Passphrase bei der nächsten Anmeldung zurückgesetzt wird.

Melden Sie sich nun sofort ab und danach wieder an. Sie werden darüber informiert, dass keine Medien-Passphrase vorhanden ist, und dazu aufgefordert, eine neue einzugeben.

### Eine Medien-Passphrase synchronisieren

Die Medien-Passphrasen auf Ihren Wechselmedien und Ihrem Computer werden automatisch synchronisiert. Wenn Sie die Medien-Passphrase auf Ihrem Computer ändern und dann ein Wechselmedium mit dem Computer verbinden, das noch die alte Version der Medien-Passphrase verwendet, werden Sie darüber informiert, dass die Medien-Passphrasen synchronisiert wurden. Dies trifft auf alle Computer zu, an denen Sie sich anmelden dürfen. Beachten Sie, dass Sie keine Medien-Passphrase auf Macs verwenden können.

Nach einem Wechsel der Medien-Passphrase sollten Sie alle Ihre Wechselmedien einmal mit dem Computer verbinden. Dadurch stellen Sie sicher, dass die neue Medien-Passphrase auf allen Geräten verwendet wird (Synchronisierung).

## 4.10.3 Austauschen von Daten auf Wechselmedien ohne SafeGuard Enterprise

SafeGuard Portable ermöglicht Ihnen verschlüsselte Daten auf Wechselmedien mit Benutzern, die SafeGuard Enterprise nicht installiert haben, auszutauschen.

**Hinweis**

Daten, die mit SafeGuard Data Exchange verschlüsselt wurden, können mit Hilfe von SafeGuard Portable ent- bzw. verschlüsselt werden. Dies wird durch ein eigenes Programm (SGPortable.exe) erreicht, das automatisch auf das Wechselmedium kopiert wird.

Mit SafeGuard Portable in Verbindung mit der relevanten Medien-Passphrase erhalten Sie Zugriff auf alle verschlüsselten Dateien. Dabei spielt es keine Rolle, welcher lokale Schlüssel für die Verschlüsselung verwendet wurde. Mit der Passphrase eines lokalen Schlüssels hingegen erhalten Sie lediglich Zugriff auf die Dateien, die mit diesem spezifischen Schlüssel verschlüsselt wurden.

Empfänger können die verschlüsselten Daten entschlüsseln und sie auch wieder verschlüsseln, wenn Sie Ihnen die Medien-Passphrase oder die Passphrase eines lokalen Schlüssels mitteilen. Sie haben die Wahl, ob sie bereits vorhandene Schlüssel, die mit SafeGuard Data Exchange erzeugt wurden, für die Verschlüsselung wählen oder ob sie (z. B. bei neuen Dateien) einen neuen Schlüssel mit SafeGuard Portable erzeugen und diesen zur Verschlüsselung der Daten verwenden.

SafeGuard Portable muss dabei nicht auf den Computern der Empfänger installiert sein. Es verbleibt auf dem Wechselmedium.

Für weitere Informationen, siehe Dateien mit SafeGuard Portable bearbeiten (Seite 25).

## 4.10.4 Dateien mit SafeGuard Data Exchange auf CDs / DVDs schreiben

Mit SafeGuard Data Exchange können Sie verschlüsselte Dateien über den im Windows Explorer integrierten Assistenten zum Schreiben von CDs auf CDs/DVDs brennen. Ihr Sicherheitsbeauftragter muss eine Verschlüsselungsregel für das CD-Laufwerk definieren. Wenn für das optische Medium keine Verschlüsselungsregel festgelegt ist, werden die Dateien immer in Klartext auf das Medium geschrieben.

Die SafeGuard Disc Burning Erweiterung für den Assistenten für das Schreiben auf CDs steht nur beim Brennen von CDs/DVDs im **Mastered** Format zur Verfügung. Für das Livedateisystem ist kein Assistent notwendig. Das optische Laufwerk wird in diesem Fall wie jedes andere Wechselmedium behandelt. Dateien werden automatisch beim Kopieren auf die CD/DVD verschlüsselt, wenn eine entsprechende Verschlüsselungsregel existiert.

Im Assistenten zum Schreiben von CDs können Sie festlegen, wie die Dateien auf CD gebrannt werden sollen (verschlüsselt oder in Klartext). Nachdem Sie einen Namen für die zu brennende CD eingegeben haben, wird die SafeGuard Data Exchange Disc Burning Erweiterung angezeigt.

Im Abschnitt **Statistik** wird angezeigt,

- wie viele Dateien zum Brennen ausgewählt sind
- wie viele der ausgewählten Dateien verschlüsselt sind
- wie viele der ausgewählten Dateien in Klartext gespeichert sind

Unter **Status** wird angezeigt, welche Schlüssel für die bereits verschlüsselten Dateien verwendet wurden.

SafeGuard Data Exchange verwendet zur Verschlüsselung beim Brennen auf CD immer den Schlüssel, der beim Festlegen der Verschlüsselungsregel für das optische Laufwerk ausgewählt wurde.

Die Situation, dass zu brennende Dateien mit verschiedenen Schlüsseln verschlüsselt sind, kann dann entstehen, wenn die Verschlüsselungsregel für das optische Laufwerk geändert wurde.

Unverschlüsselte Dateien befinden sich dann im Ordner für zu brennende Dateien, wenn die Verschlüsselungsregel deaktiviert war, als diese hinzugefügt wurden.

### Dateien verschlüsselt auf CD brennen

Wenn Sie die Dateien verschlüsselt auf CD brennen möchten, klicken Sie auf die Schaltfläche **Um-/Verschlüsseln aller Dateien**.

Bei Bedarf werden verschlüsselte Dateien neu verschlüsselt und in Klartext vorliegende Dateien verschlüsselt. Die Dateien auf der gebrannten CD sind mit dem Schlüssel, der für die Verschlüsselungsregel für das optische Laufwerk ausgewählt wurde, verschlüsselt.

### Dateien in Klartext auf CD brennen

Wenn Sie auf **Alle Dateien entschlüsseln** klicken, werden die Dateien entschlüsselt und dann auf CD gebrannt.

### SafeGuard Portable auf das optische Speichermedium kopieren

Wenn Sie diese Option auswählen, wird auch SafeGuard Portable auf das Medium gebrannt. Dies ermöglicht das Lesen und Bearbeiten von mit SafeGuard Data Exchange verschlüsselten Dateien auf Computern, auf denen SafeGuard Data Exchange nicht installiert ist.

## 4.11 Austauschen von Daten in der Cloud ohne SafeGuard Enterprise

SafeGuard Portable ermöglicht Ihnen in der Cloud verschlüsselte Daten mit Benutzern, die SafeGuard Enterprise nicht installiert haben, auszutauschen.

SafeGuard Portable ermöglicht Ihnen auch von Computern, auf denen SafeGuard Enterprise nicht installiert ist, auf verschlüsselten Daten in Ihrem Cloud Storage zuzugreifen. Daten, die mit SafeGuard Cloud Storage verschlüsselt wurden, können mit Hilfe von SafeGuard Portable ent- bzw. verschlüsselt werden. Dies wird durch ein eigenes Programm (SGPortable.exe) erreicht, das automatisch in Ihren Synchronisierungsordner kopiert wird.

Mit der Passphrase eines lokalen Schlüssels erhalten Sie lediglich Zugriff auf die Dateien, die mit diesem spezifischen Schlüssel verschlüsselt wurden. Sie oder andere Empfänger können jeweils die verschlüsselten Daten entschlüsseln und sie auch wieder verschlüsseln. Die Passphrase für einen lokalen Schlüssel muss dem Empfänger zuvor mitgeteilt werden.

Der Empfänger hat die Wahl, ob er bereits vorhandene Schlüssel verwendet, oder ob er (z. B. bei neuen Dateien) einen neuen Schlüssel mit SafeGuard Portable erzeugt.

SafeGuard Portable muss dabei nicht auf dem Computer Ihres Kommunikationspartners installiert oder kopiert werden. Das Programm verbleibt im Cloud Storage.

Für eine detaillierte Beschreibung von SafeGuard Portable, siehe Dateien mit SafeGuard Portable bearbeiten (Seite 25).

Wenn Sie auf eine Datei doppelklicken oder den Befehl zum Öffnen auswählen, wird die Datei nicht direkt entschlüsselt. Dies liegt daran, dass entschlüsselte Dateien in Cloud Storage Synchronisierungsordnern automatisch mit der Cloud synchronisiert werden. In diesem Fall wird ein Dialog angezeigt, der Sie dazu auffordert, einen sicheren Speicherplatz für die Datei auszuwählen.

Entschlüsselte Dateien werden nicht automatisch gelöscht, wenn SafeGuard Portable geschlossen wird. Änderungen, die in mit SafeGuard Portable für Cloud Storage entschlüsselten Dateien vorgenommen werden, werden nicht in die verschlüsselten Original-Dateien übernommen.

**Hinweis**
Speichern Sie Cloud Storage Synchronisierungsordner nicht auf Wechselmedien oder auf dem Netzwerk. Wenn Sie dies tun, erzeugt SafeGuard Portable unverschlüsselte Dateien in diesen Ordnern.

# 4.12 Standardschlüssel verwenden

Welcher Schlüssel zur Verschlüsselung im laufenden Betrieb von SafeGuard Data Exchange oder SafeGuard Cloud Storage verwendet wird, bestimmen Sie durch das Festlegen eines Standardschlüssels.

Ihr Sicherheitsbeauftragter muss die Anwendung von Standardschlüsseln für Cloud Storage explizit zulassen. Wenn dies zulässig ist, können Sie einen Standardschlüssel aus einem vordefinierten Schlüssel-Set auswählen und ihn für die Verschlüsselung von Ordnern in der Cloud verwenden.

Sie können einen Standardschlüssel über das Kontextmenü an folgenden Stellen definieren:

- Wechselmedien
- Dateien auf Wechselmedien
- Cloud Storage Synchronisierungsordnern oder eines Unterordners
- Dateien in einem Cloud Storage Synchronisierungsordner oder eines Unterordners
- Sie können einen Schlüssel auch unmittelbar beim Anlegen eines neuen lokalen Schlüssels im Dialog **Schlüssel erzeugen** als Standardschlüssel auswählen.

Um einen Standardschlüssel zu definieren, wählen Sie **SafeGuard Dateiverschlüsselung > Standardschlüssel festlegen**.

Der Schlüssel, den Sie hier auswählen, wird für alle nachfolgenden Verschlüsselungsoperationen auf dem Wechselmedium oder in Ihrem Cloud Storage Synchronisierungsordner verwendet. Wollen Sie einen anderen Schlüssel verwenden, müssen Sie einen neuen Standardschlüssel festlegen.

Wird für die Cloud Storage Verschlüsselung ein lokaler Schlüssel ausgewählt, wird SafeGuard Portable in den Cloud Storage Synchronisierungsordner kopiert.

Wenn Sie verschlüsselte Dateien auf Android- und iOS-Geräten mit Sophos Secure Workspace lesen möchten, müssen Sie für die Verschlüsselung lokale Schlüssel verwenden. Weitere Informationen hierzu finden Sie in der Sophos Secure Workspace Benutzerhilfe.

**Beispiel**

Sie möchten Dropbox verwenden, um gesicherte Daten für mehrere Partner bereitzustellen und jedem Partner Zugriff auf nur einen Unterordner zu gewähren. Legen Sie dazu einfach einen separaten Standardschlüssel für jeden Unterordner fest. SafeGuard Enterprise fügt automatisch eine Kopie von SafeGuard Portable hinzu. SafeGuard Portable ermöglicht Partnern ohne SafeGuard Cloud Storage Zugriff auf die verschlüsselten Daten in den Unterordnern. Sie teilen Ihren Partnern dann die jeweiligen Passphrasen für die Schlüssel mit. Mit SafeGuard Portable und den Passphrasen können Ihre Partner die Daten in den für sie erstellten Ordnern entschlüsseln. Sie haben jedoch keinen Zugriff auf die Daten in anderen Unterordnern, da diese mit einem anderen Schlüssel verschlüsselt sind.

# 4.13 Recovery von verschlüsselten Dateien

Dateien, die mit einem Schlüssel verschlüsselt sind, der nicht in Ihrem Schlüsselring enthalten ist, können nicht geöffnet werden. Das kann der Fall sein, weil eine Firmenrichtlinie vorsieht, dass Sie keinen Zugriff auf diese Dateien haben. Es kann allerdings auch sein, dass Sie die Datei zwar öffnen dürfen, aber nicht über den benötigten Schlüssel verfügen. In diesem Fall müssen Sie herausfinden, mit welchem Schlüssel die Datei verschlüsselt ist und Ihren Sicherheitsbeauftragten bitten, den Schlüssel Ihrem Schlüsselring zuzuweisen. Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **SafeGuard Dateiverschlüsselung > Verschlüsselungsstatus anzeigen**.
   Der Schlüssel mit dem die Datei verschlüsselt wurde wird angezeigt.
2. Kontaktieren Sie Ihren Sicherheitsbeauftragten und nennen Sie den Schlüsselnamen.
3. Bitten Sie Ihren Sicherheitsbeauftragten, den Schlüssel Ihrem Schlüsselring zuzuweisen.
4. Sobald Ihr Sicherheitsbeauftragter bestätigt, dass Ihre Richtlinie aktualisiert wurde, klicken Sie mit der rechten Maustaste auf das Taskleistensymbol.
5. Klicken Sie auf **Daten abgleichen**.
6. Klicken Sie erneut mit der rechten Maustaste auf das Taskleistensymbol und klicken Sie dann auf **Status**.
   Ein Dialog zeigt das Datum an, wann zuletzt ein Schlüssel an Ihren Computer übermittelt wurde. Unter **Letzter Schlüsselempfang** wird das aktuelle Datum angezeigt sobald der angeforderte Schlüssel zu Ihrem Schlüsselring hinzugefügt wurde.

Sie können nun auf die Datei zugreifen.

# 4.14 Überprüfen der Verbindung zum SafeGuard Enterprise Server

Wenn Sie Schwierigkeiten bei der Synchronisierung eines Endpoints mit dem Server haben, können Sie das Client/Server Connectivity Check Tool verwenden um festzustellen, warum die Kommunikation zwischen Endpoint und SafeGuard Enterprise Server fehlschlägt.

Um das SafeGuard Enterprise Client/Server Connectivity Check Tool zu starten öffnen Sie den Pfad `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client` und führen Sie die Anwendung `SGNCSCC.exe` aus.

Nähere Informationen entnehmen Sie bitte dem Sophos Support-Artikel 109662.

# 4.15 Dateien mit SafeGuard Portable bearbeiten

Als SafeGuard Enterprise Benutzer benötigen Sie SafeGuard Portable nicht. Die folgende Beschreibung erfolgt aus der Sicht eines Benutzers, der nicht über Sophos SafeGuard verfügt und darum die verschlüsselten Daten nur mit SafeGuard Portable bearbeiten kann.

Sie haben mit SafeGuard Data Exchange verschlüsselte Dateien zusammen mit einem Ordner `SGPortable` erhalten. In diesem Ordner befindet sich die Datei `SGPortable.exe`.

1. Starten Sie SafeGuard Portable mit einem Doppelklick auf `SGPortable.exe`.

   Mit Hilfe von SafeGuard Portable können Sie die verschlüsselten Dateien ent- und auch wieder verschlüsseln.

Zusätzlich zu den Dateieigenschaften zeigt SafeGuard Portable die Spalte **Schlüssel** an. Diese Spalte gibt an, ob die Daten verschlüsselt sind. Ist die Datei verschlüsselt, wird der Name des verwendeten Schlüssels angezeigt. Sie können nur Dateien entschlüsseln, für deren Schlüssel Sie die entsprechende Passphrase wissen.

2. Wenn Sie eine Datei bearbeiten wollen, rechtsklicken Sie auf die Datei und wählen Sie einen der folgenden Befehle:

| | |
|---|---|
| **Verschlüsselungsschlüssel setzen** | Öffnet den Dialog **Schlüssel eingeben**. Hier können Sie einen Schlüssel für die Verschlüsselung mit Hilfe von SafeGuard Portable generieren. |
| **Verschlüsseln** | Verschlüsselt die Datei mit dem zuletzt verwendeten Schlüssel. |
| **Entschlüsseln** | Öffnet den Dialog **Passphrase eingeben** zum Eingeben einer Passphrase um die ausgewählte Datei zu entschlüsseln. |
| **Verschlüsselungsstatus** | Zeigt den Verschlüsselungsstatus an. |
| **Kopieren nach** | Kopiert die Datei in den Ordner Ihrer Wahl und entschlüsselt diese. |
| **Löschen** | Löscht die markierte Datei. |

Die Kommandos **Öffnen**, **Löschen**, **Verschlüsseln**, **Entschlüsseln** und **Kopieren** können auch über Symbole in der Symbolleiste aufgerufen werden.

## 4.15.1 Einen Verschlüsselungsschlüssel für SafeGuard Portable setzen

Zum Setzen eines Verschlüsselungsschlüssels für SafeGuard Portable gehen Sie folgendermaßen vor:

1. Wählen Sie über das Kontextmenü der rechten Maustaste oder über das Menü **Datei** den Befehl **Verschlüsselungsschlüssel setzen**.

   Der Dialog **Schlüssel eingeben** wird angezeigt.
2. Geben Sie einen **Namen** und eine **Passphrase** für den Schlüssel ein.
3. Bestätigen Sie die Passphrase und klicken Sie auf **OK**.

   Die Passphrase muss den Unternehmensrichtlinien entsprechen. Ist dies nicht der Fall, so wird eine Warnung angezeigt.

Der Schlüssel wird erzeugt und ab diesem Zeitpunkt zur Verschlüsselung verwendet.

## 4.15.2 Dateien mit SafeGuard Portable verschlüsseln

1. Rechtsklicken Sie in SafeGuard Portable auf die Datei und wählen Sie **Verschlüsseln**.

   Die Datei wird dann mit dem zuletzt von SafeGuard Portable verwendeten Schlüssel verschlüsselt.

   Wenn Sie per Drag & Drop neue Dateien speichern, werden Sie gefragt, ob Sie diese Dateien verschlüsseln wollen.

   Wenn kein Standardschlüssel angegeben ist, wird ein Dialog zum Festlegen eines Standardschlüssels geöffnet. Geben Sie den Namen des Schlüssels und eine Passphrase ein, bestätigen Sie die Passphrase und klicken Sie auf **OK**.

2. Um weitere Dateien mit dem soeben festgelegten Schlüssel zu verschlüsseln, wählen Sie **Verschlüsseln** aus dem Kontextmenü oder aus dem Menü **Datei**.
   Alle weiteren Verschlüsselungen, die Sie mit SafeGuard Portable vornehmen, werden ab jetzt mit dem zuletzt verwendeten und von SafeGuard Portable gesetzten Schlüssel vorgenommen. Es sei denn, Sie setzen einen neuen Schlüssel.

## 4.15.3 Dateien mit SafeGuard Portable entschlüsseln

1. Rechtsklicken Sie in SafeGuard Portable auf die Datei und wählen Sie **Entschlüsseln**.

   Der Dialog zur Eingabe der Medien-Passphrase oder der Passphrase eines lokalen Schlüssels wird angezeigt.
2. Geben Sie dort die entsprechende Passphrase ein (die Passphrase muss Ihnen vom Absender der Daten mitgeteilt werden) und klicken Sie auf **OK**.

   Die Datei wird entschlüsselt.

Über die Medien-Passphrase erhalten Sie Zugriff auf alle verschlüsselten Dateien. Dabei spielt es keine Rolle, welcher lokale Schlüssel für die Verschlüsselung benutzt wurde. Mit der Passphrase eines lokalen Schlüssels hingegen erhalten Sie lediglich Zugriff auf die Dateien, die mit diesem Schlüssel verschlüsselt wurden.

Wenn Sie eine Datei entschlüsseln, die mit einem von Ihnen in SafeGuard Portable erzeugten Schlüssel verschlüsselt worden ist, wird diese Datei automatisch entschlüsselt.

Haben Sie einmal Dateien entschlüsselt und die Passphrase des Schlüssels eingegeben, dann müssen Sie diese beim nächsten Entschlüsseln und Verschlüsseln nicht mehr eingeben, wenn die Dateien mit dem gleichen Schlüssel verschlüsselt worden sind.

SafeGuard Portable „merkt“ sich die Schlüssel so lange die Applikation läuft. Beim Verschlüsseln wird immer der zuletzt von SafeGuard Portable verwendete Schlüssel benutzt.

Entschlüsselte Dateien werden wieder verschlüsselt, wenn Sie SafeGuard Portable schließen.

# 5 Support

## Vollständiger Release

Technische Unterstützung zu Sophos-Produkten erhalten Sie auf folgende Weise:

- Tauschen Sie sich in der Sophos Community unter community.sophos.com/ mit anderen Benutzern aus, die dasselbe Problem haben.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Lesen Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation.aspx.
- Stellen Sie eine Support-Anfrage unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

# 6 Rechtliche Hinweise