SOPHOS
Security made simple.

SafeGuard Enterprise
Erste Schritte und Praxistipps

Produktversion: 8
Stand: Juli 2016

Inhalt

1 Einleitung

Dieses Handbuch besteht aus zwei Teilen:

- Der Abschnitt Einführung in Synchronized Encryption (Seite 4) hilft Ihnen beim Einstieg in das neue Synchronized Encryption Modul.

  Er enthält einen Überblick über die neuen Funktionen und wie Sie das Modul in Ihrer Umgebung implementieren. Weiterführende Informationen zum Synchronized Encryption Modul finden Sie in der SafeGuard Enterprise Administratorhilfe.

- Der Abschnitt Praxistipps und Empfehlungen (Seite 13) enthält Tipps und Empfehlungen für eine reibungslose Bereitstellung (Rollout), Administration und Verwendung von SafeGuard Enterprise.

  Es handelt sich hierbei um keine umfassende Installationsanleitung, sondern richtet sich hauptsächlich an Benutzer, die bereits mit dem Produkt vertraut sind. Weitere Informationen zu Installation und Administration finden Sie in der SafeGuard Enterprise Administratorhilfe.

2 Einführung in Synchronized Encryption

Synchronized Encryption ist das neue Modul zur Dateiverschlüsselung in Sophos SafeGuard Enterprise. Die zentralen Veränderungen gegenüber der Dateiverschlüsselung in älteren Versionen von SafeGuard Enterprise sind:

- Automatische Verschlüsselung von Dateien, die mit definierten Anwendungen (In-Apps) erzeugt oder bearbeitet wurden.
- Nur definierte Anwendungen können Dateien entschlüsseln.
- Die Verschlüsselung ist nicht vom Speicherort der Datei abhängig.
- Schlüssel können mit mobilen Geräten (iOS oder Android) ausgetauscht werden.

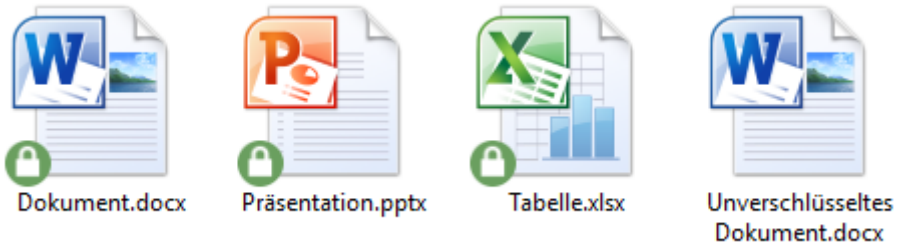
  Hinweis: Sie müssen die Sophos Mobile Control Umgebung so einrichten, dass eine Kommunikation mit SafeGuard Enterprise möglich ist.
- Schlüssel können automatisch von den Geräten der Benutzer entfernt werden, wenn eine Bedrohung der Sicherheit erkannt wurde.

  Hinweis: Dieses Feature ist nur verfügbar, wenn Sie web-basierte Sophos Central Endpoint Protection gemeinsam mit SafeGuard Enterprise verwenden. Sie benötigen eine SafeGuard Enterprise Richtlinie um Schlüssel entfernen zu können. Dieses Feature ist sowohl für Windows als auch für Mac Endpoints verfügbar.
- Benutzer können den Recovery-Schlüssel für die volume-basierende Verschlüsselung (BitLocker Drive Encryption bei Windows Geräten oder FileVault2 bei Mac OS X Geräten) über ihre mobilen Geräte beziehen.

2.1 Arbeiten mit Standardanwendungen

Mit Synchronized Encryption können Sie wie gewohnt arbeiten und brauchen sich nicht um Verschlüsselung zu sorgen. Nur wenn Sie Informationen mit Empfängern außerhalb Ihres Unternehmens teilen, müssen Sie einschätzen, welches Sicherheitsniveau angebracht ist.

Zum Beispiel: Sie erstellen wie gewohnt Inhalte in Excel oder PowerPoint. Beim Speichern werden die Dateien automatisch verschlüsselt. Verschlüsselte Dokumente werden mit einem kleinen Vorhängeschloss-Symbol am Dateisymbol gekennzeichnet.



2.2 Informationen innerhalb des Unternehmens teilen

In dieser Version von SafeGuard Enterprise (SGN 8) wird nur ein Schlüssel für die Dateiverschlüsselung verwendet. Das erleichtert das interne Teilen von Informationen. Alle Benutzer von SafeGuard Enterprise können die Informationen lesen.

Sie können mit den verschlüsselten Dateien in gewohnter Weise verfahren: per E-Mail senden, auf eine Netzwerkfreigabe stellen oder auf einen Wechseldatenträger kopieren.

Sie müssen Synchronized Encryption auf den Rechnern aller Benutzer installieren, die Zugriff auf die innerhalb des Unternehmens geteilten Informationen benötigen.

Hinweis: Stellen Sie sicher, dass Sie SafeGuard Enterprise sowohl für Windows als auch für Mac Benutzer installieren.

2.3 Informationen mit externen Parteien austauschen

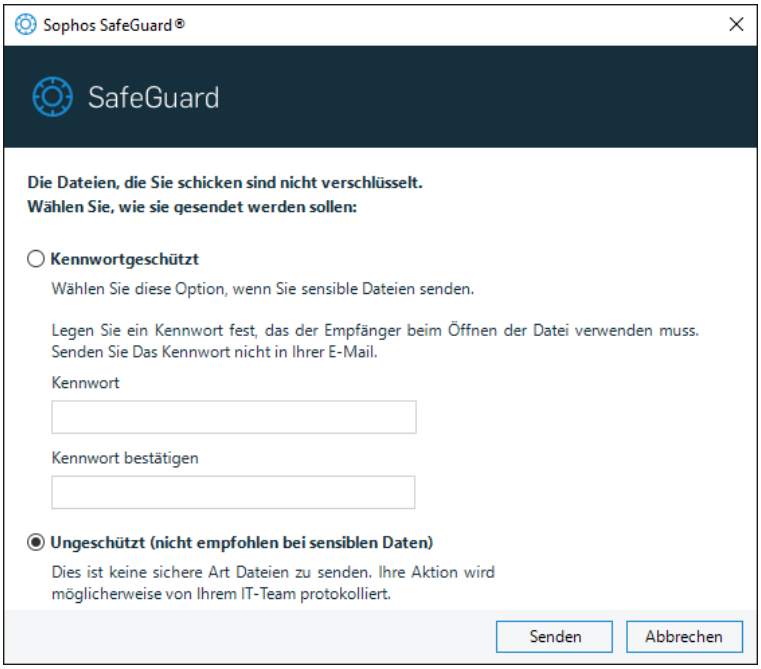
Die Verschlüsselung von Daten dient dazu, den Zugang zu sensiblen Daten einzuschränken. Dokumente mit Finanzdaten oder neuestem geistigen Eigentum sind üblicherweise nicht für die Öffentlichkeit gedacht. Dennoch gibt es oft Fälle, wo Sie derartige Informationen mit jemandem außerhalb Ihres Unternehmens teilen möchten. Manchmal sollen die Dokumente weiterhin verschlüsselt sein, manchmal handelt es sich auch nicht um vertrauliche Daten.

Für Benutzer von Outlook gelten andere Arbeitsabläufe wie für Benutzer anderer Mail-Clients.

Tipp: Geben Sie Ihren Benutzern Zugriff auf die SafeGuard Enterprise Benutzerhilfe.

Outlook-Benutzer

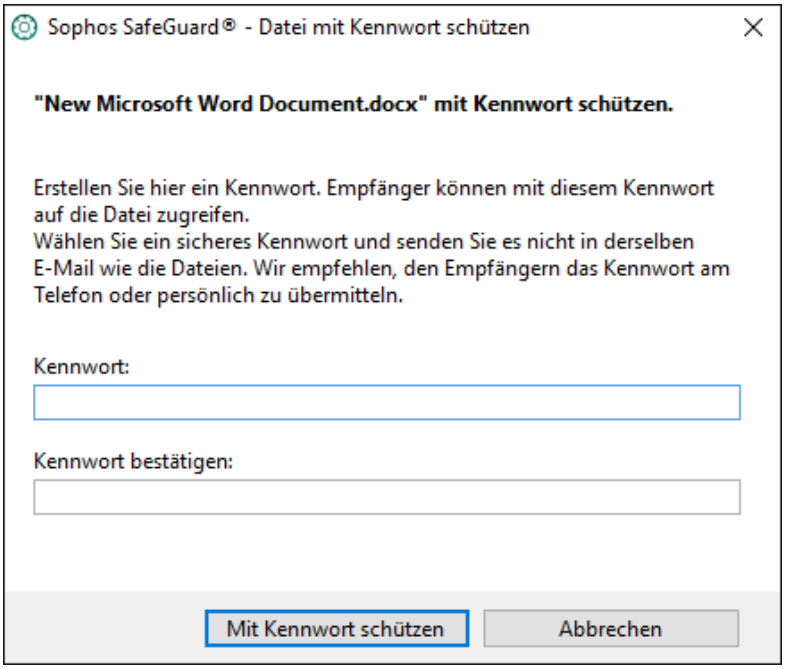
Benutzer mit einem Windows Computer mit Microsoft Outlook (32-Bit-Version von Office) müssen sich nicht weiter um Verschlüsselung kümmern. Sie können Synchronized Encryption so konfigurieren, dass immer wenn eine E-Mail mit einem Anhang an einen externen Empfänger gesendet wird, Benutzer mittels Pop-up gefragt werden, wie mit dem Anhang verfahren werden soll.



Andere Benutzer

Windows und Mac Benutzer können eine Datei entweder entschlüsseln, um sie unverschlüsselt zu versenden, oder eine kennwortgeschützte Datei erzeugen, um Inhalte sicher zu teilen.

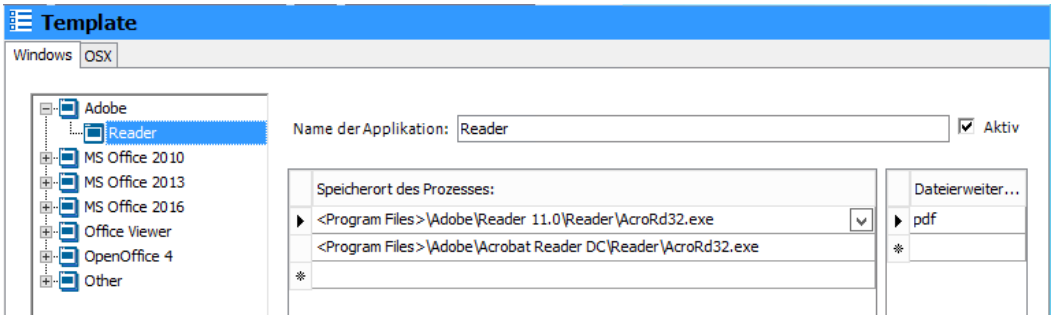
Sie können mit der rechten Maustaste auf eine Datei klicken und **SafeGuard Dateiverschlüsselung** > **Ausgewählte Datei entschlüsseln** wählen. Oder sie wählen **SafeGuard Dateiverschlüsselung** > **Kennwortgeschützte Datei erstellen**. In diesem Fall wird eine neue Datei mit der Endung HTML erzeugt und der Empfänger kann mit dem vom Sender definierten Kennwort auf die Datei zugreifen.

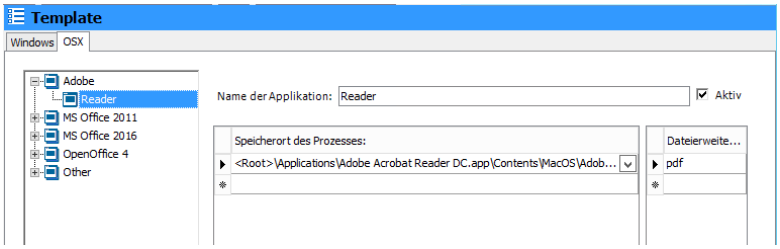


Weitere Informationen finden Sie in der SafeGuard Enterprise Benutzerhilfe im Kapitel Mailanhänge sicher versenden.

2.4 Definieren von In-Apps

In-Apps sind Anwendungen, die verschlüsselte Inhalte erzeugen und lesen können. Diese Anwendungen werden von einem Sicherheitsbeauftragten anhand von vollständigen Pfaden sowohl für Windows als auch für Mac OS X definiert.





Tipp: Stellen Sie sicher, dass die Anwendungen auf allen Computern am selben Ort installiert sind oder beziehen Sie alle möglichen Installationsverzeichnisse in die Definition der In-Apps mit ein.

2.4.1 Welche Anwendungen soll ich als In-App definieren?

In-Apps sind die einzigen Anwendungen, die verschlüsselte Inhalte erzeugen und lesen können. Sie müssen alle Anwendungen einbeziehen, die Sie zum Erstellen oder Lesen von verschlüsselten Dateien verwenden möchten.

Typische Anwendungen für die Erstellung von Inhalten:

- Office Suites (Microsoft Office, OpenOffice, FreeOffice, ...)
- Design Suites (Adobe Creative Suite, ...)

Typische Anwendung zum Betrachten von Inhalten:

- Office-Betrachter
- PDF-Betrachter
- Bildbetrachter

  Hinweis: Sie können keine Windows Store-Apps zur In-App-Liste hinzufügen.

Tipp: Berücksichtigen Sie alle Dateitypen, die von Anwendungen zum Erstellen von Inhalten verwendet werden. So müssen Sie zum Beispiel für Microsoft Word neben .docx auch .rtf, .odt etc. einbeziehen.

In einigen Fällen müssen Sie auch Anwendungen einbeziehen, die nur von einzelnen Benutzern verwendet werden. Das bedeutet aber nicht, dass Sie die entsprechende Richtlinie nur bestimmten Benutzern zuweisen müssen; wenn Benutzer eine Richtlinie für eine Anwendung erhalten, die sie nicht haben, so wird dieser Teil der Richtlinie ignoriert.

2.4.2 Welche Anwendungen soll ich NICHT als In-App definieren?

Verschlüsselung verhindert, dass sensible Informationen nach außen dringen; daher sollen Anwendungen, die dazu dienen, Informationen zu versenden, niemals als In-Apps definiert werden. Andernfalls würden alle Inhalte vor dem Senden entschlüsselt und es bestünde keinerlei Schutz der Daten.

Definieren Sie daher nie Anwendungen wie E-Mail-Clients, Internet Browser, Backup-Software und dergleichen als In-Apps.

Hinweis: Für Mac OS X kann es jedoch sinnvoll sein, E-Mail-Programme einzubeziehen, da kein Outlook Add-In verfügbar ist, siehe Richtlinien für Mac OS X Endpoints (Seite 16).

2.5 Aspekte, die vor der Bereitstellung beachtet werden müssen

Stellen Sie Synchronized Encryption vorerst nur einer eingeschränkten Anzahl von Personen (Testgruppe) zur Verfügung. Statten Sie alle anderen Benutzer mit einer Richtlinie aus, mit der sie keine verschlüsselten Inhalte erzeugen, jedoch auf die verschlüsselten Dateien ihrer Kollegen zugreifen können, siehe Erstellen von Lesezugriff-Richtlinien (Seite 9).

Beachten Sie außerdem vor der Bereitstellung von Synchronized Encryption die folgenden Aspekte.

2.5.1 Öffnen von Dateien in einer anderen App als der mit der sie erstellt wurden

Viele Anwendungen können Dateien in unterschiedlichen Formaten erzeugen. Bedenken Sie deshalb, mit welchen Anwendungen eine Datei geöffnet werden kann. Zum Beispiel kann Microsoft Word auch PDF-Dateien erzeugen. Ist Microsoft Word als In-App (Anwendung, die Dateien verschlüsselt) definiert, werden die erzeugten PDF-Dateien verschlüsselt. Dies ist erwartetes Verhalten, da es sich um sensiblen Inhalt handeln könnte.

Jedoch müssen Sie auch die Anwendung berücksichtigen, mit der die Datei geöffnet und gelesen werden soll. In unserem Beispiel ist dies wahrscheinlich ein PDF-Betrachter, und obwohl PDF-Betrachter normalerweise nicht zum Erstellen von Dateien verwendet werden, müssen sie doch als In-Apps definiert werden. Andernfalls können die Dateien nicht mit dem PDF-Betrachter gelesen werden. Aus diesem Grund haben wir die häufigsten PDF-Betrachter schon in die Applikationenlisten-Vorlage aufgenommen, die im SafeGuard Management Center zur Verfügung steht.

Andere Beispiele:

- In-Apps, die Bilder exportieren
- In-Apps, die Text in unterschiedlichen Formaten exportieren, zum Beispiel .txt, .rtf oder .csv.

Tipp: Berücksichtigen Sie für alle Dateien, die Sie mit den definierten In-Apps erzeugen können, Anwendungen zum standardmäßigen Öffnen der Dateien. Stellen Sie sicher, dass diese Anwendungen auf allen Computern installiert sind und definieren Sie sie ebenfalls als In-Apps, um auf die verschlüsselten Inhalte zugreifen können.

2.5.1.1 Windows 10 PDF

Der standardmäßige PDF-Betrachter für Windows 10 ist der neue Internet-Browser Edge. Sie könnten Edge als In-App definieren. Jedoch würde das bedeuten, dass alle Dateien, die mit Edge ins Internet hochgeladen werden, entschlüsselt werden.

Wichtig: Statten Sie daher Ihre Windows 10 Geräte mit einem anderen PDF-Betrachter als Edge aus, zum Beispiel Adobe Acrobat Reader oder Foxit Reader.

2.5.2 Java-Anwendungen

Java-Anwendungen verwenden häufig dieselbe ausführbare Datei `java.exe` gemeinsam. Es ist nicht möglich, zwischen unterschiedlichen Java-Anwendungen über den Pfad der laufenden `java.exe` zu unterscheiden.

Wenn Sie java.exe als In-App definieren, müssen Sie bedenken, dass alle Anwendungen, die diese ausführbare Datei verwenden, verschlüsselte Inhalte erstellen und darauf zugreifen können.

2.5.3 Webbasierte Anwendungen

Benutzer müssen häufig mit Dokumenten arbeiten und sie dann in eine webbasierte Anwendung hochladen. Verschlüsselte Dateien bleiben verschlüsselt und können vom zugrunde liegenden System nicht gelesen werden. Das bedeutet:

- Die Dateien können nicht aufgrund ihres Inhalts indexiert werden.
- Werden Dateien von außen aufgerufen, sind sie nicht lesbar.

Möglicherweise benötigen Sie extern Zugriff auf diese Dateien. Benutzer können dazu die Dateien vor dem Hochladen entschlüsseln. Alternativ können Sie einen Ordner erstellen, wo Dateien unverschlüsselt gespeichert werden.

Dieser von der Verschlüsselung ausgenommene Ordner sollte nur für diesen Zweck verwendet werden. Stellen Sie sicher, dass Ihre Benutzer darüber informiert werden.

Tipp: Erstellen Sie eine Ausnahme für die Dateiverschlüsselung; entweder über einen direkten Pfad wie **`c:\unencrypted`**, oder definieren Sie einen relativen Pfad (nur auf Windows Endpoints möglich). Wenn Sie einen relativen Pfad verwenden, müssen Benutzer einen Ordner mit einem vereinbarten Namen anlegen. Lautet der Name des Ordners beispielsweise **`\unencrypted`**, so werden Dateien und Unterordner in allen Ordnern mit dem Namen **`\unencrypted`** auf dem Computer nicht verschlüsselt.

2.5.4 Austausch von Informationen mit Plattformen, die nicht über SafeGuard Verschlüsselung verfügen

Zuweilen erstellen Benutzer Dateien, die zur Verwendung in einer anderen Umgebung gedacht sind. Zum Beispiel können Dateien auf einem Windows oder Mac Endpoint erstellt werden aber in einer Terminal Server Umgebung verwendet werden. Da SafeGuard Enterprise in Terminal Server Umgebungen nicht unterstützt wird, bleiben verschlüsselte Dateien dort verschlüsselt und können von keiner Anwendung gelesen werden.

Die Lösung besteht darin, den gewünschten Speicherort per Verschlüsselungsrichtlinie von der Verschlüsselung auszuschließen.

2.5.5 Was passiert mit meinen Vorschauen?

Dateibrowser (Windows Explorer oder Finder) können Vorschauen für unterschiedliche Dateitypen wie Bilder, Textdokumente, Tabellenkalkulationen und PDF-Dateien anzeigen. Diese Vorschauen werden üblicherweise beim Speichern oder Ändern der Datei erzeugt. Um eine Vorschau erzeugen zu können, muss die entsprechende Anwendung auch Zugriff auf den unverschlüsselten Inhalt der Datei haben. Daher muss die Anwendung zur Liste der In-Apps hinzugefügt werden. Bei Mac OS X handelt es sich um eine separate Anwendung, die standardmäßig in der Liste enthalten ist.

2.6 Erstellen von Lesezugriff-Richtlinien

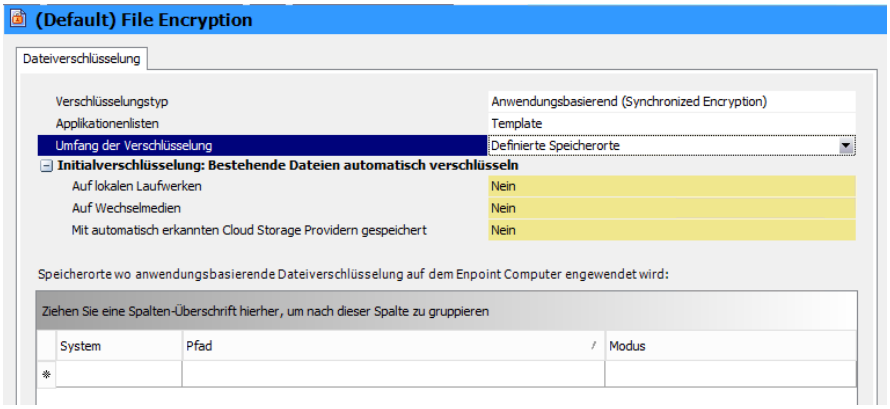
Am Beginn des Rollouts von Synchronized Encryption sollen Benutzer in der Lage sein, verschlüsselte Dokumente zu lesen, aber nicht selbst zu erstellen. Sie können dann nach

und nach die Verschlüsselung für bestimmte Gruppen und schließlich für alle Benutzer aktivieren.

Die erste Richtlinie ist eine Lesezugriff-Richtlinie.

Windows

Für Windows Benutzer erstellen Sie eine Synchronized Encryption Richtlinie mit allen benötigten Anwendungen und **Umfang der Verschlüsselung** > **Definierte Speicherorte**, definieren jedoch keine Speicherorte.



Weitere Informationen finden Sie in der SafeGuard Enterprise Administratorhilfe im Kapitel Erstellen von Lesezugriff-Richtlinien für Windows Endpoints.

Mac OS X

Mac OS X verhält sich anders als Windows. Auf Mac OS X Computern können verschlüsselte Dateien nur in definierten Speicherorten gelesen werden.

Das bedeutet, dass die Lesezugriff-Richtlinie für Windows-Nutzer nicht für Mac-Nutzer verwendet werden kann.

Für Mac-Nutzer erstellen Sie eine Richtlinie vom Typ **Dateiverschlüsselung** und wählen **Pfadbasiert** als Verschlüsselungstyp. Sie müssen zumindest einen Speicherort hinzufügen, ihn von der Verschlüsselung **Ausschließen** und den Pfad den Mac-Nutzern mitteilen. Der Pfad lautet beispielsweise **`<Documents>/Verschlüsselt`**. Benutzer, die ein verschlüsseltes Dokument lesen möchten, müssen das Dokument zuerst an diesen Speicherort kopieren oder verschieben.

Weitere Informationen finden in der SafeGuard Enterprise Administratorhilfe im Kapitel Erstellen von Lesezugriff-Richtlinien für Mac Endpoints.

2.7 Informieren der Endbenutzer

In vielen Fällen ist das Thema Verschlüsselung neu für Benutzer. Wir empfehlen daher, dass Sie Benutzer über Ihre Vorgehensweise und Regeln hinsichtlich Verschlüsselung aufklären. Besonders bei Synchronized Encryption ist es wichtig für Benutzer zu erfahren, was sie zu erwarten haben. Zum Beispiel: Welche Anwendungen werden als In-Apps definiert? Dieses Wissen ermöglicht Benutzern, fehlende Anwendungen zu identifizieren und dem SafeGuard Enterprise Sicherheitsbeauftragten Feedback zu geben. Dieser kann dann die benötigte Anwendung zur Liste der In-Apps hinzufügen.

Empfohlene Vorgehensweise:

- Senden Sie eine E-Mail an alle Benutzer in der Sie erklären, welche Verschlüsselungsregeln implementiert werden und welche Auswirkungen sie haben. Idealerweise stellen Sie einen Link auf eine interne Website bereit, die Sie jederzeit leicht anpassen können wenn beispielsweise neue In-Apps hinzugefügt werden.
- Geben Sie eine Mail-Adresse an, an die Benutzer Feedback senden können.
- Wenn Sie SafeGuard Enterprise bereits auf allen Endpoints ausgerollt haben (eventuell nur Lesezugriff), können Sie ein Dokument anfügen, das mit dem Synchronized Encryption Schlüssel verschlüsselt ist, und ihre Benutzer prüfen lassen, ob sie das Dokument lesen können. Ist dies nicht der Fall, so wissen Sie, dass ein Problem bei der Installation oder bei der Kommunikation zwischen Endpoint und dem SafeGuard Backend vorliegt bevor Sie die Verschlüsselung für alle Benutzer aktivieren.

2.7.1 Beispielnachricht

Dies ist ein Beispiel für eine E-Mail, mit der Sie Ihre Benutzer informieren können. Sie enthält bereits die wichtigsten Informationen, aber Sie können selbstverständlich weitere Punkte hinzufügen, etwa wenn Sie eine Regel zum Ausnehmen von Ordnern mit dem Namen "Unencrypted" verwenden oder wenn Sie andere Anwendungen in Gebrauch haben. Der Text geht von dem Fall aus, dass mit der E-Mail ein mit Synchronized Encryption verschlüsseltes Dokument als Anhang gesendet wird.

= =
=

Sehr geehrte Kolleginnen und Kollegen,

die IT-Abteilung hat nun auf allen Rechnern SafeGuard Enterprise installiert. Dabei handelt es sich um ein Produkt zur Datenverschlüsselung von Sophos, das zukünftig von allen verwendet wird, um unsere Dokumente zu schützen. In der Regel wird dies keinen Einfluss auf Ihre tägliche Arbeitsweise haben, jedoch möchten wir Sie auf einige Ausnahmen hinweisen.

Wir werden Synchronized Encryption nächste Woche aktivieren. Sobald die Software aktiviert ist, werden Sie auf Ihrem Computer verschlüsselte Dateien erzeugen. Wir haben einiges an Informationen für einen leichten Einstieg auf unserer Intranet-Seite unter "Verschlüsselung" zusammengestellt, siehe https://firma.intern/verschluesselung.

Um zu prüfen, ob Ihr Gerät bereit für die Verschlüsselung ist, öffnen Sie bitte die angefügte Datei.

- **Windows und Mac OS X:** Wenn Sie das Dokument öffnen und den Inhalt lesen können, sind Sie startklar. Wenn die Nachricht in der Datei nicht korrekt angezeigt wird, kontaktieren Sie bitte den IT Service Desk.

- **iOS und Android:** Öffnen Sie den Anhang in der Sophos Secure Workspace App auf Ihrem Gerät. Der systemeigene Betrachter kann die Datei nicht öffnen, weil sie verschlüsselt ist. Wenn Sie Sophos Secure Workspace noch nicht auf Ihrem Mobilgerät installiert haben, kontaktieren Sie bitte den IT Service Desk.

Anwendungen

Die folgenden Anwendungen werden automatisch verschlüsselte Inhalte auf Ihrem Gerät erzeugen. Wenn Sie unterschiedliche Anwendungen verwenden, um auf verschlüsselte Dateien zuzugreifen, werden Sie nur den verschlüsselten Inhalt sehen.

Windows:

- Adobe Reader

- MS Office 2010 (Excel, PowerPoint, Word)
- MS Office 2013 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)
- Office-Betrachter
- Foxit Reader für PDF

Mac OS X

- Adobe Reader
- Apple Produktivität (Keynote, Numbers, Pages, Preview)
- MS Office 2011 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)

Wie verhält es sich mit dem Senden von Dateien?

Beachten Sie, dass beim Senden von E-Mails an externe Empfänger die Datei in verschlüsselter Form gesendet wird. Das bedeutet, dass Ihr Empfänger den Inhalt nicht lesen kann. Ist der Inhalt nicht vertraulich, können Sie die Datei vor dem Senden entschlüsseln. Wenn es sich um vertraulichen Inhalt handelt oder Sie nicht sicher sind, erstellen Sie eine kennwortgeschützte Datei. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie "SafeGuard Dateiverschlüsselung". Wählen Sie dann entweder "Ausgewählte Datei entschlüsseln" oder "Kennwortgeschützte Datei erstellen".

Wenn Sie **Windows** verwenden und die Datei über **Microsoft Outlook** versenden, müssen Sie diese Schritte nicht manuell vornehmen. Wenn das System feststellt, dass Sie eine verschlüsselte Datei an einen externen Empfänger versenden, werden Sie zu einer Entscheidung aufgefordert, wie mit der Datei verfahren werden soll.

Was passiert mit Dateien, die auf unsere Web-Anwendungen hochgeladen werden?

Dateien, die Sie verschlüsselt hochladen, werden nicht entschlüsselt. Das bedeutet, sie bleiben sowohl in SharePoint als auch in allen anderen Web-Anwendungen stets verschlüsselt. Eventuell möchten Sie Dateien vor dem Hochladen manuell entschlüsseln. Beachten Sie, dass keine Vorschauen angezeigt werden und dass die Indexierung nicht funktioniert.

Probleme? Vorschläge?

Wenn Sie Probleme mit SafeGuard Enterprise oder generell mit Ihrem Computer haben seit die Verschlüsselung aktiviert wurde, erstellen Sie bitte ein IT-Ticket beim IT Service Desk.

Mit freundlichen Grüßen

3 Praxistipps und Empfehlungen

3.1 Rollout

Hinweis: SafeGuard Enterprise Server und SafeGuard Management Center erfordern .NET 4.5.

Allgemeine Empfehlungen

- Versuchen Sie, einen gemischten Rollout des neuen Synchronized Encryption Moduls und des alten File Encryption Moduls zu vermeiden.
- Ein schrittweiser Rollout erfordert einen Testlauf für jeden Schritt, besonders bei komplexen, verschachtelten AD-Gruppenzugehörigkeiten.
- Eine Schulung der Benutzer ist entscheidend für den reibungslosen Rollout und Betrieb.
- Auch muss klar kommuniziert werden, wer teilnimmt und welche Konsequenzen zu erwarten sind.
- IT- und Support-Abteilungen müssen ausreichend Personal zur Verfügung haben.

Voraussetzungen

- Auf allen Endpoints sollte SafeGuard Enterprise 8 installiert sein. Andernfalls funktioniert das Teilen von verschlüsselten Dateien nicht transparent und der gewohnte Arbeitsablauf ist beeinträchtigt.
- Wenn Sie verschlüsselte Dateien auch auf mobilen Geräten lesen möchten (eine neue Funktion von SafeGuard Enterprise 8), müssen Sie auch die Sophos Secure Workspace App ausrollen.

  Hinweis: Um verschlüsselte Dateien auf mobilen Geräten zu lesen, müssen Sie Sophos Secure Workspace verwenden und über Sophos Mobile Control verwalten.
- Stellen Sie sicher, dass sich Benutzer auch auf Reisen regelmäßig mit dem SafeGuard Enterprise Backend über VPN oder "Direct Access" (Windows) verbinden, so dass immer die aktuellsten Verschlüsselungsrichtlinien angewendet werden können.

3.1.1 Vorbereitung von Endpoints für Synchronized Encryption

Für die ordnungsgemäße Funktion von Synchronized Encryption muss die Windows-Runtime **`vstor-redist.exe`** installiert sein. Die Datei installiert Microsoft Visual Studio 2010 Tools für Office-Laufzeit und ist im Installationspaket enthalten.

Wir empfehlen, die Komponenten in folgender Reihenfolge zu installieren:

1. **`vstor-redist.exe`**
2. **`SGNClient.msi`**
3. Konfigurationspaket

Hinweis: Sie können das Installationspaket nicht installieren bevor die Installation von **`vstor-redist.exe`** abgeschlossen ist.

3.1.2 Partieller Rollout

In vielen Situationen kann das neue **Synchronized Encryption** Modul nicht für alle Mitarbeiter gleichzeitig ausgerollt und aktiviert werden. In diesen Fällen ist es wichtig, Benutzern Lesezugriff auf verschlüsselte Dateien zu geben, auch wenn sie SafeGuard Enterprise Endpoints verwenden, bei denen **Synchronized Encryption** noch nicht aktiviert ist. Dazu ist eine Lesezugriff-Richtlinie erforderlich.

Um Benutzern Lesezugriff zu geben brauchen Sie folgendes:

- Den **Synchronized Encryption** Schlüssel.

  Er ist standardmäßig dem Stammknoten im Management Center zugewiesen und alle Benutzer innerhalb eines Unternehmens sollten diesen Schlüssel automatisch erhalten.

- Eine **Applikationenliste** und eine spezifische Lesezugriff-Richtlinie.

  Detaillierte Informationen zum partiellen Rollout von Synchronized Encryption finden Sie in der SafeGuard Enterprise Administratorhilfe, Kapitel Partieller Rollout von Synchronized Encryption.

3.1.3 Synchronized Encryption und SafeGuard Enterprise File Encryption in derselben Umgebung

Hinweis: Wenn Ihre Umgebung sowohl Synchronized Encryption als auch File Encryption erfordert, beachten Sie folgendes um eine reibungslose Integration zu gewährleisten.

Synchronized Encryption unterstützt nur einen Schlüssel für das gesamte Unternehmen. Diese erleichtert Administration und Rollout. Für einige Abteilungen, zum Beispiel Personalwesen oder Finanzwesen, kann die Anforderung einer kryptographischen Abgrenzung zu anderen Abteilungen bestehen um ihre Dokumente nur innerhalb der jeweiligen Abteilung zugänglich zu machen.

In diesem Fall müssen die SafeGuard Enterprise File Encryption Module (File Share, Cloud Storage, Data Exchange) verwendet werden. Diese Module unterstützen die Verwendung unterschiedlicher Schlüssel für die Verschlüsselung. Sie können das Synchronized Encryption Modul und das SafeGuard Enterprise File Encryption Module nicht auf demselben Computer installieren.

Um sowohl Synchronized Encryption als auch SafeGuard Enterprise File Encryption zu verwenden sind einige administrative Schritte erforderlich:

1. Beim Rollout von SafeGuard Enterprise muss berücksichtigt werden, dass in unterschiedlichen Abteilungen unterschiedliche Module installiert werden müssen.
2. Abteilungen mit speziellen Anforderungen benötigen andere Richtlinien als die, die Endpoints mit **Synchronized Encryption** zugewiesen sind. Dazu sollte die importierte AD-Struktur eine einfache Zuweisung dieser Richtlinien zu Benutzern und Computern erlauben.
3. Rollout und Installation der SafeGuard Enterprise Module muss entsprechend der zugewiesenen Richtlinien erfolgen: Die richtigen Computer müssen die richtigen Richtlinien erhalten.

   Hinweis: Das Outlook Add-In ist für SafeGuard Enterprise File Encryption Module nicht verfügbar. Daher können Synchronized Encryption und File Encryption Endpoints verschlüsselte Mailanhänge nicht transparent teilen.

Empfehlungen

- Benutzer von SafeGuard Enterprise File Encryption Modulen müssen den **Synchronized Encryption** Schlüssel erhalten. Dann können Benutzer Dateien transparent lesen, die mit dem **Synchronized Encryption** Schlüssel verschlüsselt sind.
- Teilen von verschlüsselten Dateien:

  Für Benutzer von SafeGuard Enterprise File Encryption Modulen empfehlen wir, eine Richtlinie zu erstellen, die den **Synchronized Encryption** Schlüssel für die Verwendung mit einer "Transfer"-Freigabe definiert. Alle Dateien, die in dieser Freigabe erstellt oder dort hin verschoben werden, werden mit dem **Synchronized Encryption** Schlüssel verschlüsselt. **Synchronized Encryption** Benutzer können diese Dateien lesen.

- Teilen von unverschlüsselten Dateien:

  Für Benutzer von SafeGuard Enterprise File Encryption Modulen kann eine Richtlinie verwendet werden, die einen Ordner von der Verschlüsselung ausschließt (**Verschlüsselungstyp**: **Pfadbasiert**, **Modus**: **Ausschließen**).

- Wenn Benutzer von SafeGuard Enterprise File Encryption Modulen Dateien mit **Synchronized Encryption** Benutzern teilen möchten, müssen sie die Dateien zuerst entschlüsseln. Sie können dann entscheiden, ob sie die Dateien unverschlüsselt senden oder mit dem Synchronized Encryption Schlüssel verschlüsseln möchten.

3.1.4 Überprüfen der Gültigkeit von Benutzerzertifikaten

Die Überprüfung der Gültigkeit von Benutzerzertifikaten ist besonders für Unternehmen wichtig, die bisher nur SafeGuard Enterprise BitLocker verwendet haben und nun zusätzlich das **Synchronized Encryption** Modul verwenden möchten.

Prüfen Sie die Zertifikate im SafeGuard Management Center unter **Schlüssel & Zertifikate** > **Zertifikate** > **Zugewiesene Zertifikate**.

Abgelaufene Zertifikate oder solche, die bald ablaufen werden, sind in der Spalte **Gültig bis** rot markiert. Um ein Zertifikat zu erneuern, aktivieren Sie das Kontrollkästchen in der Spalte **Erneuern**. Benutzer mit bereits abgelaufenen Zertifikaten müssen neue erhalten. Sie müssen die abgelaufenen Zertifikate löschen, dann erhalten die betroffenen Benutzer automatisch neue Zertifikate wenn sie sich das nächste Mal an SafeGuard Enterprise anmelden.

SafeGuard Enterprise enthält das Datenbankskript **`UserCertficateRenewal.vbs`**, mit dem diese Aufgaben automatisiert abgewickelt werden können. Das Skript kann im SafeGuard Enterprise oder Windows **Taskplaner** verwendet werden, um diese Checks regelmäßig durchzuführen und die Zertifikate, wenn nötig, zu erneuern, siehe Sophos Knowledgebase-Artikel 118878.

3.1.5 Überprüfen, ob alle Benutzer bestätigt sind

In SafeGuard Enterprise müssen neue Benutzer im SafeGuard Management Center bestätigt oder über Active Directory authentisiert werden. Benutzer mit Active Directory werden automatisch bestätigt. Manche Benutzer hingegen, zum Beispiel lokale Benutzer, müssen manuell bestätigt werden. Unbestätigte Benutzer sind keine **SGN Benutzer** und erhalten daher keine Schlüssel für Synchronized Encryption. Dies trifft sowohl auf Windows als auch auf Mac Endpoints zu.

Wir empfehlen, die erste Richtlinie als Lesezugriff-Richtlinie auszurollen. Nachdem alle Endpoints/Benutzer ihre Schlüssel erhalten haben, können Sie die Verschlüsselungsrichtlinien

aktivieren. Dadurch stellen Sie sicher, dass alle Benutzer bestätigt wurden bevor sie ihre Verschlüsselungsrichtlinien erhalten. So können Probleme mit unbestätigten Benutzern vermieden werden.

3.1.6 Richtlinien für Mac OS X Endpoints

Für die Dateiverschlüsselung empfehlen wir, eine Richtlinie vom Typ **Anwendungsbasierend (Synchronized Encryption)** mit **Umfang der Verschlüsselung** > **Definierte Speicherorte** zu definieren und zu Beginn nur wenige Speicherorte anzugeben, an denen Dateien automatisch verschlüsselt werden. Auf diesem Weg können die Auswirkungen auf die Arbeitsweise der Benutzer gering gehalten werden.

Für eine einfachere Unterscheidung von Windows und Mac OS X Endpoints bei der Verwaltung von Richtlinien empfehlen wir die Verwendung eines separaten AD oder einer separaten SafeGuard Enterprise Gruppe für Mac OS X Benutzer und Computer. Aktivieren Sie die Mac OS X Richtlinie nur für Mac OS X Benutzer und Computer.

3.1.6.1 Empfehlungen für eine Mac OS X Synchronized Encryption Richtlinie

In-Apps

Anwendungen, die Daten verschlüsseln sollen, zur **Applikationenliste hinzufügen**:

- E-Mail

  Hinweis: Für Mac OS X ist kein Outlook Add-In verfügbar. Sie können jedoch Outlook und Apple Mail zur Applikationenliste hinzufügen, um sicher zu stellen, dass keine verschlüsselten Daten versehentlich an Empfänger versendet werden, die sie nicht öffnen können. Beachten Sie, dass die Mail-Apps, die Sie zur Liste hinzufügen, alle Mailanhänge unverschlüsselt senden, alle verschlüsselten Anhänge verschlüsselt speichern und alle unverschlüsselten Anhänge unverschlüsselt speichern.

  - /Applications/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - /Applications/Microsoft Office 2011/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - Applications/Mail.app/Contents/MacOS/Mail

- Um die Vorschau im Mac OS X Finder und in Apple Mail zu aktivieren, müssen folgende Prozesse hinzugefügt werden:
  - /Applications/Preview.app/Contents/MacOS/Preview
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite
  - /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/Resources/QuickLookUIHelper.app/Contents/MacOS/QuickLookUIHelper
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/MacOS/quicklookd

Pfade für Umfang der Verschlüsselung: Definierte Speicherorte

- Verschlüsseln:
  - <Documents>\Encrypted
- Wenn Sie möchten, dass Benutzer verschlüsselte Dokumente mit Doppelklick über den Mail Client öffnen können, müssen Sie diese Anwendungen (zum Beispiel Apple Mail) zur Applikationenliste hinzufügen und die dazugehörenden temporären Ordner zur Liste der definierten Speicherorte hinzufügen.

  Die Orte, die Sie für Mail-Clients auf Mac definieren müssen, sind folgende:
  - <%TMPDIR%>\com.apple.mail\com.apple.mail
  - <User Profile>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads

  Fügen Sie folgende Orte für Outlook für Mac OS X hinzu:
  - <User Profile>\Library\Caches\TemporaryItems\Outlook Temp\
  - <%TMPDIR%>com.microsoft.Outlook\Outlook Temp\

3.2 Backend

3.2.1 Lesezugriff-Benutzer für Active Directory Synchronisierung

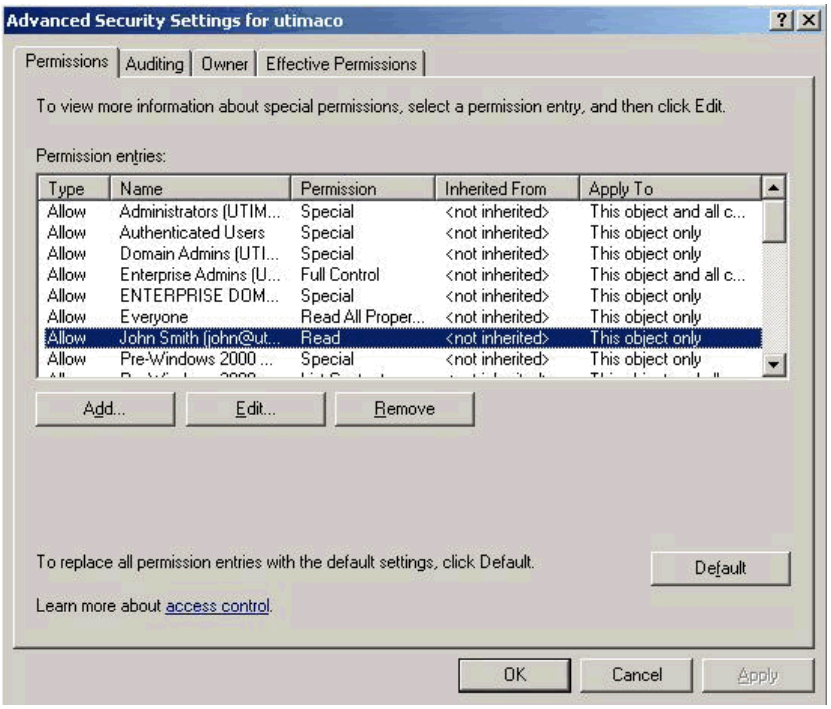
Hinweis: Um die Sicherheit der Verbindung zu erhöhen, empfehlen wir die Verwendung einer SSL-Verschlüsselung für die Active Directory-Synchronisierung.

Das Konto, das für den Import und die Synchronisierung von Active Directory verwendet wird, sollte ein Lesezugriff-Benutzer sein. Der Benutzer benötigt Lesezugriff auf die Domäne und alle untergeordneten Objekte.

So weisen Sie Rechte zu:

1. Öffnen Sie das Fenster **Active Directory-Benutzer und -Computer** und wählen Sie **Erweiterte Funktionen**.
2. Klicken Sie mit der rechten Maustaste auf die Domäne und dann auf **Eigenschaften**.
3. Fügen Sie einen Benutzer oder eine Gruppe hinzu und aktivieren Sie das Kontrollkästchen **Zulassen** um **Lese**-Rechte zuzuweisen.
4. Klicken Sie auf **Erweitert**, wählen Sie den Benutzer oder die Gruppe und klicken Sie auf **Bearbeiten**.
5. Wählen Sie im Dialog **Berechtigungseintrag für <Domäne>** den Eintrag **Dieses und alle untergeordneten Objekte** aus der **Übernehmen für:** Auswahlliste.

   Das Ergebnis sollte so aussehen:



3.2.2 Benutzer, die mit "#" im Management Center gekennzeichnet sind

Benutzer, die sich in SafeGuard Enterprise registriert haben als kein Domain Controller verfügbar war, werden im Management Center mit "#" gekennzeichnet.

3.3 Richtlinien

3.3.1 Ordner, die von der Verschlüsselung ausgenommen werden müssen

Stellen Sie sicher, dass Sie die folgenden Verzeichnisse von der Verschlüsselung ausschließen, wenn Sie **Synchronized Encryption** verwenden:

Windows

- **`<Local Application Data\Temp>`**

  Grund: Manche Anwendungen erzeugen viele kleine temporäre Dateien. Werden sie nicht ausgenommen, werden alle diese temporären Dateien gemäß Richtlinie verschlüsselt. Schließen Sie daher den Ordner aus, um Performance-Probleme zu vermeiden.

- **`<Local Application Data>\Microsoft (und Unterverzeichnisse)`**

  Grund: Einige Anwendungen rufen andere Anwendungen auf (zum Beispiel in Microsoft PowerPoint eingebettete Videos). Ist die aufrufende Anwendung eine Anwendung, die Dateien verschlüsselt, dann wird auch die temporäre Datei (in diesem Beispiel die Video-Datei) verschlüsselt. Ist die aufgerufene Anwendung (zum Beispiel ein Browser) eine Anwendung, die keine Dateien verschlüsselt (weil sie nicht auf der Applikationenliste steht), kann sie die verschlüsselte Datei nicht lesen.

- **`<Program Files>`**

Grund: Um auf diesen Ordner zugreifen zu können sind Administratorrechte erforderlich. SafeGuard Initial Encryption kann diese Dateien aufgrund von fehlenden Zugriffsrechten nicht verschlüsseln. Schließen Sie diesen Ordner aus, um zu vermeiden, dass die SafeGuard Datenbank mit Benachrichtigungen über fehlgeschlagene Dateiverschlüsselungen überfüllt wird.

Alle Systeme

- **`<!cloud storage providers!>`**

  Generell empfehlen wir, Cloud Storage zu verschlüsseln, jedoch können Sie einzelne Cloud Storage Anbieter ausschließen, die zum Austauschen von Dateien mit externen Partnern verwendet werden. Dies verhindert, dass Dateien in bekannten lokalen Cloud Storage Synchronisierungsordnern verschlüsselt werden. So können Probleme beim Austauschen von Dateien mit externen Partnern über Cloud-Synchronisierung vermieden werden. Wenn Sie keine Cloud-Ordner für den Datenaustausch mit externen Partnern nutzen, müssen Sie keine Ordner ausschließen.

- **`<Music>`**, **`<Pictures>`**

  Grund: Normalerweise müssen Sie diese Dateien nicht verschlüsseln. Wenn Sie nicht wollen, dass diese Ordner von der Verschlüsselung ausgenommen sind, müssen die Anwendungen, mit denen diese Dateien geöffnet werden, Teil der **Applikationenliste** sein.

  Hinweis: Auf Mac OS X können Sie die Photos App und Bibliothek nicht verwenden, wenn Sie die Dateien in **`<Pictures>`** verschlüsseln.

- **`<User Profile>\AppData\Roaming\AppleComputer`**

  Grund: Dies ist der lokale Synchronisierungsordner für Apple iCloud auf Windows Endpoints. Er sollte aus demselben Grund ausgenommen werden wie **`<!cloud storage providers!>`**.

3.3.2 Empfehlungen für Richtlinieneinstellungen

Definieren Sie einen Ordner "Unencrypted".

Dieser Ordner kann zum Teilen von unverschlüsselten Dateien verwendet werden, beispielsweise mit Linux Benutzern innerhalb des Unternehmens oder im Rahmen eines partiellen Rollouts, siehe Erstellen von Richtlinien für anwendungsbasierte Dateiverschlüsselung.

- **Windows**

  Um den Ordner "Unencrypted" von der Verschlüsselung auszunehmen müssen Sie den Ordner **`Unencrypted`** (relativer Pfad) als Ausnahme in einer Richtlinie mit **Umfang der Verschlüsselung** > **Überall** definieren. Wenn Sie das tun, werden alle Dateien in Ordnern mit diesem Namen nicht verschlüsselt, egal wo sich der Ordner befindet.

- **Mac OS X**

  Unter Mac OS X werden keine relativen Pfade unterstützt. Wir empfehlen daher, den Pfad **`<Documents>\Unencrypted`** als Ausnahme in einer Richtlinie mit **Umfang der Verschlüsselung** > **Überall** zu definieren.

Outlook Add-In

Wir empfehlen, die Option **Verschlüsselungsmethode für Domains auf Whitelists** in einer Richtlinie vom Typ **Allgemeine Einstellungen** auf **Unverändert** zu setzen.

Schlüssel auf gefährdeten Computern entziehen

SafeGuard Enterprise **Synchronized Encryption** Endpoints werden von Sophos Central Endpoint Protection informiert, wenn der Computer einen gefährdeten Status erreicht.

Wir empfehlen, die Option **Schlüssel auf gefährdeten Computern entziehen** auf **Nein** zu setzen. Überprüfen Sie das Feedback zu betroffenen Endpoints unter **Berichte** im SafeGuard Management Center hinsichtlich rotem Systemzustand. Als nächstes sollten Sie die Endpoints überprüfen und gegebenenfalls bereinigen. Schließlich sollten Sie die Option **Schlüssel auf gefährdeten Computern entziehen** auf **Ja** setzen.

3.3.3 Gastbenutzer

Auf Endpoints, die nur SafeGuard Enterprise BitLocker-Verwaltung installiert haben, könnte die Option **Registrieren von neuen SGN-Benutzern erlauben** auf **Besitzer** gesetzt sein.

Jedoch muss auf Endpoints ohne SafeGuard Enterprise POA, die BitLocker-Verwaltung oder Dateiverschlüsselungsmodule installiert haben, die Option **Registrieren von neuen SGN-Benutzern erlauben** auf **Jeder** gesetzt sein. Wenn Sie diese Option nicht auf **Jeder** setzen, erhalten zukünftige Benutzer nur den Status **SGN-Gast**. Sie erhalten keine Zertifikate und können nach der Installation eines Moduls zur Dateiverschlüsselung wie **Synchronized Encryption** keine Dateien verschlüsseln.

3.3.4 Richtlinien für Mac OSX und RSOP

Unter Mac OS X werden nur Richtlinien berücksichtigt, die Benutzern zugewiesen sind. Wenn Sie die Richtlinien Computern zuweisen, erhalten Mac OS X Endpoints keine Richtlinien.

Das RSOP im Management Center zeigt zwar die aktuell zugewiesene Richtlinie an, jedoch wird sie nicht aktiv.

3.3.5 Datei-Tracking

Beachten Sie, dass die Funktionalität des Datei-Tracking von SafeGuard Enterprise nationalen Gesetzen unterliegt. Vergewissern Sie sich, ob Sie gesetzlich zum Datei-Tracking befugt sind.

3.3.6 Kennwort ändern

Wenn Sie den SafeGuard Enterprise Credential Provider verwenden, wird der Windows-Dialog, der Benutzer daran erinnert, ihr Kennwort zu ändern, nicht mehr angezeigt.

Um Benutzer daran zu erinnern ihr Kennwort zu ändern, müssen Sie eine SafeGuard Enterprise Richtlinie vom Typ **Kennwort** mit den erforderlichen Einstellungen definieren und zuweisen, siehe Syntaxregeln für Kennwörter.

3.4 Endpoints - alle Plattformen

3.4.1 Sicherer Systemzustand kann nicht hergestellt werden - Bereinigung fehlgeschlagen

Next-Generation Data Protection ermöglicht die Kommunikation zwischen Sophos SafeGuard und Sophos Endpoint Protection, wenn verfügbar. Dies ist eine Erweiterung der Synchronized Security Nachricht. SafeGuard und Endpoint tauschen sich mittels "Heartbeat" über den Systemzustand (Health-Status) aus.

Ist ein System mit Malware infiziert, wird es gesperrt (Lockdown), um sensible Daten zu schützen.

Wenn das passiert, werden Benutzer von Sophos Endpoint Protection informiert, dass Ihr Systemzustand rot (unsicher) ist. Außerdem werden sie von Sophos SafeGuard darüber informiert, dass sie nicht mehr in der Lage sind, auf verschlüsselte Dateien zuzugreifen. Dies bleibt aufrecht, bis der Systemzustand wieder sicher (grün) ist. Sobald das System wieder einen grünen Health-Status erlangt, synchronisiert sich Sophos SafeGuard mit dem Backend und Benutzer können wieder auf verschlüsselte Dateien zugreifen.

Falls Benutzer zwar eine entsprechende Benachrichtigung erhalten, aber ihr System binnen kurzer Zeit keinen sicheren Status erlangt, sollten sie die IT-Abteilung um Hilfe bitten.

Wenn ein Endpoint nicht in der Lage ist, einen sicheren Status zu erlangen, bedeutet das, dass die Sophos Anti-Virus Bereinigung fehlgeschlagen ist (Bereinigung in Sophos Central auf automatisch). Schlägt die Bereinigung fehl, so sind zusätzliche Maßnahmen seitens IT nötig, um die Malware zu entfernen, siehe https://www.sophos.com/de-de/support/knowledgebase/112129.aspx.

3.5 Windows Endpoints

3.5.1 Dateien manuell verschlüsseln/entschlüsseln

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

- **Status der Verschlüsselung anzeigen**: Zeigt an, ob die Datei verschlüsselt ist und welcher Schlüssel verwendet wurde.
- **Gemäß Richtlinie verschlüsseln** Verschlüsselt Ihre Datei mit dem Synchronized Encryption Schlüssel sofern der Dateityp in der Applikationenliste enthalten ist und der Speicherort nicht von der Verschlüsselung ausgenommen wurde.
- **Ausgewählte Datei entschlüsseln** (nur für verschlüsselte Dateien): 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 unverschlüsselte Dateien): Sie können Dateien manuell mit dem Synchronized Encryption-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 teilen möchten, der nicht über den Synchronized Encryption-Schlüssel Ihres Unternehmens verfügt. Ihre Datei wird verschlüsselt und als HTML-Datei gespeichert.

Empfänger können die Datei mit ihrem Browser öffnen sobald Sie ihnen das Kennwort mitteilen.

Hinweis: Diese Funktion ist nur für Dateien verfügbar, die entweder unverschlüsselt oder mit einem Schlüssel in Ihrem Schlüsselring verschlüsselt sind. Bereits verschlüsselte Dateien werden entschlüsselt bevor sie kennwortgeschützt werden.

Hinweis: Der Kennwortschutz verwendet Base64-Codierung, daher ist das Ergebnis größer als die Originaldatei. Die maximal unterstützte Dateigröße beträgt 50 MB.

Hinweis: Es können nur einzelne Dateien kennwortgeschützt werden, nicht ganze Ordner oder Pfade. Jedoch können Sie mehrere Dateien markieren, um sie zu verschlüsseln, entschlüsseln oder ihren Verschlüsselungsstatus anzuzeigen.

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

- **Status der Verschlüsselung anzeigen**: Zeigt eine Liste der enthaltenen Dateien, deren Verschlüsselungsstatus und die verwendeten Schlüssel an.
- **Gemäß Richtlinie verschlüsseln** Das System erkennt automatisch alle unverschlüsselten Dateien und verschlüsselt sie mit dem Synchronized Encryption Schlüssel sofern der Dateityp in der Applikationenliste enthalten ist und der Speicherort nicht von der Verschlüsselung ausgenommen wurde. Abhängig von Ihrer Richtlinie werden auch Dateien, die mit einem anderen Schlüssel verschlüsselt sind, mit dem Synchronized Encryption-Schlüssel wiederverschlüsselt.

3.5.2 E-Mails, die mit einer automatischen Weiterleitungs-Regel gesendet werden

Wenn Sie **am Endpoint** eine Regel zum automatischen Weiterleiten von E-Mails definieren, werden automatisch weitergeleiteten E-Mails nicht protokolliert.

3.6 Mac OS X Endpoints

3.6.1 Position der Icons auf dem Desktop

Wenn Sie SafeGuard Enterprise für Mac verwenden, werden die Positionen der Icons auf Ihrem Desktop möglicherweise nicht richtig gespeichert. Wenn Sie die Position eines Icons verändern, wird es nach einem Neustart oder Logon wieder an seiner alten Position angezeigt.

Um die Positionen Ihrer Icons zu dauerhaft zu speichern, gehen Sie wie folgt vor:

1. Starten Sie die Terminal-Anwendung auf Ihrem Mac.
2. Geben Sie folgendes Kommando ein:

   ```
   defaults write com.sophos.encryption MountDesktopAsNetworkVolume 1
   ```

3. Melden Sie sich ab und wieder an.

Das System ist nun in der Lage, die Positionen Ihrer Desktop-Icons zu speichern.

Wichtig: Wenn Sie dieses Kommando ausführen, verändert sich die Funktionsweise des Papierkorbs. Wenn Sie eine Datei löschen, wird sie nicht mehr in den Papierkorb gelegt, sondern permanent gelöscht. Um die Einstellung zurückzusetzen, geben Sie folgendes Kommando in der Terminal-Anwendung ein:

defaults remove com.sophos.encryption MountDesktopAsNetworkVolume.

4 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support Knowledgebase unter http://www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation/ herunter.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/support/contact-support/support-query.aspx.

5 Rechtliche Hinweise