SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise für Mac

Benutzerhilfe

Produktversion: 8.3

Inhalt

1 Über SafeGuard Enterprise für Mac

Sophos SafeGuard wird auf Macs ausgeführt, um diese zu schützen. Es enthält zwei Module:

- SafeGuard Native Device Encryption (Seite 1) schützt Ihren Computer mithilfe der FileVault Verschlüsselungs-Technologie.
- SafeGuard File Encryption (Seite 2) ermöglicht Ihnen, Dateien mit einem Schlüssel oder mit einem Kennwort zu verschlüsseln.

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. Nähere Informationen zum Verwalten von Sophos SafeGuard Enterprise finden Sie auf der Sophos Website.

Allgemeine Informationen zu Ihrer Installation von Sophos SafeGuard erhalten Sie über das Sophos SafeGuard-Symbol in der Menüleiste in den Sophos SafeGuard Einstellungsbereich (Seite 5).

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

Wichtig
Prüfen Sie vor dem Aktualisieren Ihres Betriebssystems, ob Ihre Version von Sophos SafeGuard die neueste Version des Betriebssystems unterstützt, siehe SafeGuard Enterprise Versionsinfo. Wenn Sie Ihr Betriebssystem zuerst aktualisieren, verlieren Sie möglicherweise den Zugriff auf Ihre Daten.

1.1 SafeGuard Native Device Encryption

Sophos SafeGuard Native Device Encryption baut auf der in Ihrem Betriebssystem enthaltenen FileVault Festplatten-Verschlüsselungstechnologie auf. Es verschlüsselt Ihre gesamte Festplatte, so dass Ihre Daten sogar dann sicher sind, wenn der Computer verloren oder gestohlen wird.

SafeGuard Native Device Encryption arbeitet im Hintergrund. Sie werden beim Öffnen, Bearbeiten und Speichern von Dateien nicht zur Verschlüsselung oder Entschlüsselung aufgefordert.

Nähere Informationen zu Ihrer Installation finden Sie auf der Registerkarte Disk Encryption (Seite 7) im Sophos SafeGuard Einstellungsbereich.

Mit SafeGuard Native Device Encryption können Sie:

- Computer verschlüsseln (Seite 9)
- Computer entschlüsseln (Seite 9)
- SafeGuard Native Device Encryption und SafeGuard File Encryption (Seite 10)
- Überprüfen der Verbindung zum SafeGuard Enterprise Server (Seite 16)

1.2 SafeGuard File Encryption

SafeGuard File Encryption ermöglicht Ihrem Sicherheitsbeauftragten zu definieren, welche Dateien auf Ihrem Computer verschlüsselt werden und wer sie lesen kann. Welche Dateien verschlüsselt werden, kann auf zwei Arten festgelegt werden:

- Pfadbasierte Dateiverschlüsselung (Seite 3)
- Anwendungsbasierte Dateiverschlüsselung (Seite 3)

Dateiverschlüsselungsrichtlinien werden immer Benutzern zugewiesen, nicht Computern. Üblicherweise geben File Encryption-Richtlinien vor, dass Dateien in Ihren Benutzer-Ordnern, wie zum Beispiel **Dokumente**, verschlüsselt werden. Ihr Sicherheitsbeauftragter kann aber Ordner definieren, wo Dateien unverschlüsselt bleiben. Auf der Registerkarte Richtlinien (Seite 6) im Einstellungsbereich können Sie sehen, an welchen Orten auf Ihrem Computer verschlüsselt wird.

Im Finder sind verschlüsselte Dateien mit einem grünen Schloss-Symbol gekennzeichnet. Dateien ohne Symbol sind normalerweise unverschlüsselt.

Hinweis
Wenn Sie eine Datei als Bundle oder Paket speichern, werden möglicherweise keine Overlay-Symbole angezeigt obwohl die Datei verschlüsselt ist. Beispiel: Wenn Sie in TextEdit eine verschlüsselte Bild-Datei in eine verschlüsselte Text-Datei einfügen und als RTF-Dokument mit Anhängen speichern, scheint diese Datei unverschlüsselt. Sie ist dennoch verschlüsselt.

Nachdem die Verschlüsselungssoftware installiert wurde und die Kommunikation mit dem SafeGuard Enterprise Server hergestellt wurde, werden Sie aufgefordert, ihr macOS Passwort einzugeben. Außerdem brauchen Sie ein persönliches Zertifikat. Dieses Zertifikat wird am SafeGuard Enterprise Server erzeugt, sobald Sie Ihr Kennwort eingeben. Dieser Vorgang ist nur nach Produktinstallation, erster Anmeldung oder dem Kennwort-Zurücksetzen erforderlich.

Stellen Sie gleich nach der Installation von SafeGuard File Encryption sicher, dass alle Richtlinien angewendet werden, die Ihnen vom Sicherheitsbeauftragten zugewiesen wurden, siehe Dateien gemäß Richtlinie verschlüsseln (Seite 11).

Mit SafeGuard File Encryption können Sie:

- Dateien gemäß Richtlinie verschlüsseln (Seite 11)
- Dateien manuell verschlüsseln/entschlüsseln (Seite 12)
- Verschlüsselte Dateien per E-Mail senden (Seite 12)
- Datei mit Kennwort schützen (Seite 13)
- Dateien auf Wechselmedien verschlüsseln (Seite 14)
- Recovery von verschlüsselten Dateien (Seite 15)

Benutzereinverständnis auf macOS 10.14

Ab macOS 10.14 müssen Anwendungen die Zustimmung des Benutzers einholen, wenn sie andere Anwendungen steuern wollen. Nach der Installation zeigt macOS einen Dialog mit der Meldung **"Sophos SafeGuard" möchte Zugriffsrechte um "Finder" zu steuern“** und fordert Sie auf, das zu erlauben oder zu verweigern. Klicken Sie auf **OK**, da die Finder-Funktionalität erforderlich ist, damit SafeGuard File Encryption ordnungsgemäß funktioniert.

Dadurch wird ein Eintrag im Bereich **Automatisierung** Ihrer Einstellungen zum **Datenschutz** hinzugefügt, sodass SafeGuard File Encryption Finder automatisch starten kann.

Wenn Sie auf **Nicht erlauben** klicken, wird dieser Dialog nicht mehr angezeigt und SafeGuard File Encryption kann die Finder-Funktionalität nicht verwenden.

Wenn Sie die Einstellungen zu einem späteren Zeitpunkt ändern möchten, gehen Sie in den Einstellungen zum **Datenschutze** zum Abschnitt **Automation** und wählen Sie unter **Sophos SafeGuard** die Option **Finder**, damit SafeGuard File Encryption den Finder steuern kann.

1.2.1 Pfadbasierte Dateiverschlüsselung

Pfadbasierte Dateiverschlüsselung ermöglicht Ihrem Sicherheitsbeauftragten, Speicherorte zu definieren, wo Dateien verschlüsselt werden. Diese Speicherorte nennen wir Sichere Ordner (Seite 4). Auf der Registerkarte Richtlinien (Seite 6) im Einstellungsbereich können Sie sehen, an welchen Orten auf Ihrem Computer verschlüsselt wird.

- Neue Dateien an Speicherorten, an denen verschlüsselt wird, werden automatisch verschlüsselt.
- Wenn Sie eine unverschlüsselte Datei an einen Ort verschieben, an dem verschlüsselt wird, wird sie verschlüsselt.
- Wenn Sie eine verschlüsselte Datei an einen Ort verschieben, der von der Verschlüsselung ausgenommen ist, wird sie entschlüsselt.
- 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 weder den Inhalt lesen noch können Sie sie an einen anderen Ort verschieben.
- Wenn Sie auf einem Computer, auf dem File Encryption nicht installiert ist, auf eine verschlüsselte Datei zugreifen, können Sie den Inhalt nicht lesen.

1.2.2 Anwendungsbasierte Dateiverschlüsselung

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. Anwendungsbasierte Dateiverschlüsselung wirkt sich auf alle Sichere Ordner (Seite 4) aus. Zusätzlich kann Ihr Sicherheitsbeauftragter bestimmte Speicherorte von der Verschlüsselung ausnehmen. Auf der Registerkarte Richtlinien (Seite 6) im Einstellungsbereich können Sie sehen, an welchen Orten auf Ihrem Computer verschlüsselt wird.

- Neue Dateien, die mit bestimmten Anwendungen erstellt wurden, werden automatisch verschlüsselt.
- Dateien, die mit bestimmten Anwendungen geändert wurden, 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.
- Wenn Sie auf eine verschlüsselte Datei mit einer Anwendung zugreifen, die nicht in Ihrer Richtlinie definiert ist, können Sie den Inhalt nicht lesen.

1.2.3 Sichere Ordner

Sichere Ordner sind Speicherorte auf Ihrem Mac, auf Netzwerkfreigaben oder auf Wechselmedien, wo Dateien verschlüsselt werden. Sie werden von Ihrem Sicherheitsbeauftragten in einer Richtlinie definiert. Üblicherweise sind dies Ordner wie Dokumente und temporäre Ordner, wo Microsoft Outlook oder Apple Mail E-Mail-Anhänge speichern.

Ab macOS Catalina benötigt SafeGuard Enterprise Ihre Erlaubnis für den Zugriff auf Ordner wie Dokumente, Desktop, Bilder und Apple Mail.

Führen Sie folgende Schritte aus, damit SafeGuard Enterprise auf diese Ordner zugreifen kann:

1. Öffnen Sie **Sicherheit**.
2. Klicken Sie zum Bearbeiten auf das Schloss.
3. Wählen Sie **Vollzugriff auf Festplatte** aus.
4. Klicken Sie auf die Schaltfläche +, um diese beiden SafeGuard-Apps dem Bereich **Vollzugriff auf Festplatte** hinzuzufügen:
   - sgd aus dem Ordner `/usr/local/bin/`
   - Sophos SafeGuard aus dem Ordner `/Library/Sophos SafeGuard FS`

Einschränkungen

- **Verschlüsselte Dateien nur in sicheren Ordnern lesbar**

  Auf eine verschlüsselte Datei, die sich außerhalb eines sicheren Ordners befindet, können Sie nicht zugreifen. Sie müssen sie entweder in einen sicheren Ordner verschieben oder sie zuerst manuell entschlüsseln.

- **Permanente Versionsspeicherung in sicheren Ordnern nicht verfügbar**

  Für Dateien in sicheren Ordnern ist die Standardfunktionalität **Alle Versionen durchsuchen...** nicht verfügbar.

- **Nach Dateien suchen**

  — Standardmäßig ist die Spotlight-Suche nach Dateien in sicheren Ordnern nicht möglich. Informationen zum Aktivieren von Spotlight finden Sie unter Verschlüsselte Dateien suchen (Seite 15).

  — Die Suche nach Dateien mit Etikett funktioniert nicht in sicheren Ordnern.

- **Sichere Ordner freigeben**

  Ein sicherer Ordner kann nicht über das Netzwerk freigegeben werden.

2 Sophos SafeGuard Einstellungsbereich

Nach der Installation von Sophos SafeGuard Enterprise für Mac erscheint das Sophos SafeGuard Symbol in den **Systemeinstellungen**.

Klicken Sie auf das Symbol um den Sophos SafeGuard Einstellungsbereich zu öffnen.

Die Registerkarte **Über** wird angezeigt. Hier finden Sie Informationen zu der auf Ihrem Mac installierten Produktversion.

2.1 Registerkarte Server

Die Registerkarte **Server** enthält folgende Informationen und Funktionen im Zusammenhang mit dem SafeGuard Enterprise Server:

Serverinfo

- **Kontaktintervall**: Zeit zwischen den Synchronisierungen mit dem Server.
- **Letzter Kontakt**: Datum der letzten Synchronisierung mit dem Server.
- **URL Primärer Server**: URL der Haupt-Serververbindung
- **URL Sekundärer Server**: URL der sekundären Serververbindung.
- **Server-Verifizierung**: Zeigt, ob die SSL-Server-Verifizierung zur Kommunikation mit dem Server aktiviert ist.

Konfigurationsdatei hierhin ziehen

Ziehen Sie die Konfigurations-Zip-Datei in diesen Bereich, um die Konfigurationsinformation vom SafeGuard Enterprise Server auf dem Mac zu übernehmen.

Synchronisieren

Mit dieser Schaltfläche starten Sie manuell eine Synchronisierung mit dem SafeGuard Enterprise Server.

Verbindung prüfen

Mit dieser Schaltfläche prüfen Sie die Verbindung mit dem SafeGuard Enterprise Server.

Unternehmenszertifikat

- **Gültig ab:** ist das Datum, an dem das Zertifikat gültig wurde.
- **Gültig bis:** ist das Datum, an dem das Zertifikat ungültig wird.
- **Herausgeber:** ist die Instanz, die das Zertifikat herausgegeben hat.
- **Seriennummer:** zeigt die Seriennummer des Unternehmenszertifikats an.

2.2 Registerkarte Benutzer

Die Registerkarte **Benutzer** enthält folgende Informationen:

- **Benutzername**
- Die **Domäne**, zu der Ihr Mac gehört. Für lokale Benutzer wird hier der lokale Computername angezeigt.

- Die **SafeGuard Benutzer-GUID**, die bei Ihrer ersten Anmeldung generiert wurde.
- Der **SafeGuard-Benutzerstatus** zeigt an, ob Sie ein **SGN-Benutzer** oder ein **Unbestätigter Benutzer** sind. Als unbestätigter Benutzer können Sie keine verschlüsselten Dateien öffnen oder erstellen. Bitten Sie in diesem Fall Ihren Sicherheitsbeauftragten, Ihr Konto zu bestätigen.

Im zweiten Fensterbereich wird Information über das **Benutzerzertifikat** angezeigt. Dies ist nur für File Encryption relevant.

- **Gültig ab:** ist das Datum, an dem das Zertifikat gültig wurde.
- **Gültig bis:** ist das Datum, an dem das Zertifikat ungültig wird.
- **Herausgeber:** ist die Instanz, die das Zertifikat herausgegeben hat.
- **Seriennummer:** zeigt die Seriennummer des Zertifikats an.

Im dritten Fensterbereich können Sie definieren, ob ein Symbol für jede Komponente im Systemmenü angezeigt wird. Diese Optionen sind nur verfügbar, wenn die entsprechende Komponente installiert ist.

- **System Menü für Native Device Encryption anzeigen**
- **System Menü für File Encryption anzeigen**

2.3 Registerkarte Schlüssel

Diese Registerkarte wir nur angezeigt, wenn Sie SafeGuard File Encryption installiert haben.

Die Registerkarte **Schlüssel** zeigt die Namen aller existierenden Schlüssel in einer Liste an.

Klicken Sie auf das Listensymbol unten rechts neben **Anzahl Schlüssel**, um die GUID-Informationen der betreffenden Schlüssel aus- oder einzublenden.

Sie können Schlüssel anzeigen und sortieren, indem Sie auf eines der Überschriftenelemente **Schlüsselname** oder **Schlüssel-GUID** klicken.

Wenn ein Schlüssel in blau angezeigt wird, handelt es sich um Ihren persönlichen Schlüssel. Lokale Schlüssel werden grün dargestellt (siehe Lokale Schlüssel verwenden (Seite 15)). Alle anderen (Standard-)Schlüssel werden schwarz dargestellt.

2.4 Registerkarte Richtlinien

Diese Registerkarte wir nur angezeigt, wenn Sie SafeGuard File Encryption installiert haben.

Klicken Sie in der Registerkarte **Richtlinien** auf eines der Symbole in der unteren rechten Ecke, um zwischen der Ansicht **Lokal übersetzter Pfad** und **Empfangene Richtlinien** hin- und herzuschalten.

- Die Ansicht **Lokal übersetzter Pfad** zeigt nur diejenigen Richtlinien an, die dem gegenwärtig angemeldeten Benutzer an einem bestimmten Mac zugewiesen sind. Die Spalten in der Tabelle enthalten folgende Informationen:
  - @: Während der Initialverschlüsselung oder wenn größere Dateien verschlüsselt werden sehen Sie ein sich drehendes Rad in der ersten Spalte.
  - **Lokal übersetzter Pfad**: Zeigt den Speicherort auf Ihrem Mac.
  - **Modus**: Zeigt an, ob ein Speicherort verschlüsselt wird oder von der Verschlüsselung ausgenommen ist.
  - **Anwendungsbereich**: Zeigt an, ob Unterordner eines Speicherorts in die Verschlüsselung einbezogen sind.

- **Schlüsselname**: Zeigt den Namen des Schlüssels an, der dem angegebenen Speicherort zugewiesen ist.

  Ihr persönlicher Schlüssel wird blau angezeigt.

  Ein orangefarbener Schlüssel wurde in einer Richtlinie konfiguriert, die Ihnen zugewiesen wurde. Sie besitzen den Schlüssel jedoch nicht, weil er nicht Ihrem Schlüsselring zugewiesen wurde. Das kann beim Zugriff auf Daten Probleme verursachen. Wenden Sie sich in diesem Fall an Ihren Sicherheitsbeauftragten.

- Die Ansicht **Empfangene Richtlinien** zeigt alle Richtlinien an, die vom Server empfangen wurden. Die Übersicht enthält folgende Informationen:
  - **Empfangene Richtlinien**: Legt fest, welche Dateien oder Ordner verschlüsselt werden.
  - Alle anderen Spalten enthalten die oben beschriebenen Informationen für die Ansicht **Lokal übersetzter Pfad**.

Richtlinien in der Ansicht Lokal übersetzter Pfad erzwingen

- Wenn keine Richtlinie ausgewählt ist, können Sie über die Schaltfläche **Erzwinge alle Richtlinien** die Initialverschlüsselung starten. Weitere Informationen finden Sie unter Dateien gemäß Richtlinie verschlüsseln (Seite 11).
- Wenn Sie eine Richtlinie auswählen, können Sie über die Schaltfläche **Erzwinge Richtlinie** die ausgewählte Richtlinie anwenden.
- Wenn Sie eine Richtlinie auswählen, können Sie über die Schaltfläche **Im Finder anzeigen** den ausgewählten sicheren Ordner im Finder anzeigen.

Mögliche Ergebnisse beim Erzwingen von Richtlinien

- Unverschlüsselte Dateien werden mit dem Schlüssel verschlüsselt, der von einer Richtlinie zugewiesen wurde.
- Dateien, die bereits mit dem in der Richtlinie vorgegebenen Schlüssel verschlüsselt sind, bleiben verschlüsselt.
- Dateien, die bereits mit einem anderen Schlüssel verschlüsselt sind, werden entweder
  - nicht verändert, wenn der Benutzer den entsprechenden Schlüssel nicht in seinem Schlüsselring hat, oder
  - mit dem per Richtlinie zugewiesenen Schlüssel neu verschlüsselt, wenn der Benutzer diesen Schlüssel in seinem Schlüsselring hat.
- Dateien in Ordnern, die von der Verschlüsselung ausgenommen sind, werden entschlüsselt.
- Dateien, die aufgrund fehlender Berechtigungen (schreibgeschützt) nicht zugänglich sind, bleiben unverändert.

2.5 Registerkarte Disk Encryption

Diese Registerkarte wir nur angezeigt, wenn Sie SafeGuard Native Device Encryption installiert haben.

Die Registerkarte **Disk Encryption** enthält Informationen über die aktuellen Richtlinien und den Verschlüsselungsstatus Ihres Macs.

Im ersten Fensterteil wird angezeigt, ob das Systemlaufwerk gemäß der Richtlinie, die der Sicherheitsbeauftragte gesetzt hat, verschlüsselt werden soll.

Im zweiten Fensterteil wird der Status des Macs angezeigt. Es gibt folgende Möglichkeiten:

- Das Systemlaufwerk ist verschlüsselt und ein zentral gespeicherter Wiederherstellungsschlüssel ist verfügbar.
- Das Systemlaufwerk ist verschlüsselt, aber es ist kein zentral gespeicherter Wiederherstellungsschlüssel verfügbar.
- Das Systemlaufwerk ist nicht verschlüsselt.

Darunter wird die Schaltfläche **Systemlaufwerk entschlüsseln** angezeigt. Sie ist verfügbar, wenn der Sicherheitsbeauftragte eine Richtlinie definiert, die keine Verschlüsselung für den Endpoint vorsieht.

3 Hinweise zur Vorgehensweise

3.1 Computer verschlüsseln

Wenn Ihr Sicherheitsbeauftragter Ihnen eine Device Encryption-Richtlinie zuweist, werden Sie aufgefordert, Ihr macOS-Passwort einzugeben. Danach startet die Verschlüsselung Ihres Computers.

1. Geben Sie Ihr macOS Passwort ein.
2. Klicken Sie auf **Aktivieren** oder **Aktivieren und Neustart**.

   Macs, die das Apple File System (APFS) verwenden, benötigen keinen Neustart, sodass nur die Option **Aktivieren** angezeigt wird.

Die Initialverschlüsselung läuft im Hintergrund und Sie können weiterhin mit Ihrem Computer arbeiten. Weitere Informationen finden Sie unter SafeGuard Native Device Encryption (Seite 1).

Kontaktieren Sie Ihren Administrator, wenn das Aktivieren der Verschlüsselung fehlschlägt.

3.2 Computer entschlüsseln

Normalerweise ist keine Entschlüsselung notwendig. Wenn der Sicherheitsbeauftragte eine Richtlinie setzt, die keine Verschlüsselung für Ihren bereits verschlüsselten Mac vorsieht, bleibt der Mac verschlüsselt. In diesem Fall können Sie allerdings auch entschlüsseln. Verwenden Sie die entsprechende Schaltfläche in den Systemeinstellungen. Siehe Registerkarte Disk Encryption (Seite 7).

3.3 Vergessenes Kennwort zurücksetzen

Wie Sie ein vergessenes Kennwort zurücksetzen, hängt davon ab, welch Art der Verschlüsselung auf Ihrem Mac installiert ist:

- SafeGuard Native Device Encryption (Seite 9)
- SafeGuard Native Device Encryption und SafeGuard File Encryption (Seite 10)

3.3.1 SafeGuard Native Device Encryption

Wenn Sie Ihr macOS Passwort vergessen haben, gehen Sie wie folgt vor:

1. Schalten Sie Ihren Mac ein.
2. Klicken Sie auf das Fragezeichen im Feld **Passwort**.
   Ihre Merkhilfe für Ihr Kennwort wird angezeigt und Sie werden gefragt, ob Sie Ihr Kennwort mithilfe des Wiederherstellungsschlüssels zurücksetzen wollen.
3. Klicken Sie auf das Pfeilsymbol neben der Meldung, um zum Feld Wiederherstellungsschlüssel zu wechseln.
4. Kontaktieren Sie Ihren Sicherheitsbeauftragten und erfragen Sie Ihren Wiederherstellungsschlüssel.

5. Geben Sie Ihren Wiederherstellungsschlüssel in das entsprechende Feld ein und klicken Sie auf das Pfeil-Symbol auf der rechten Seite.
   Der Mac startet und der Dialog **Passwort zurücksetzen** wird angezeigt.
6. Wenn Sie ein Active Directory Benutzer sind, bitten Sie Ihren Administrator, Ihr Kennwort zurückzusetzen, und fordern Sie ein neues Kennwort an.
   a) Stellen Sie sicher, dass Ihr Computer mit Active Directory Domain Services verbunden ist.
   b) Klicken Sie im Dialog **Passwort zurücksetzen** auf **Abbrechen** und geben Sie Ihr neues Kennwort ein.
   c) Ändern Sie Ihr Passwort erneut, falls erforderlich.
7. Wenn Sie ein lokaler macOS Benutzer sind, definieren Sie ein neues Kennwort und eine Merkhilfe und klicken Sie auf **Passwort zurücksetzen**
8. Wenn das System Ihren Anmeldeschlüsselbund nicht entsperren kann, klicken Sie auf **Neuen Schlüsselbund erstellen**.
9. Ein Mac mit Mac OS 10.13 und APFS formatiertem Systemlaufwerk benötigt möglicherweise das neue Kennwort, um ein neues Wiederherstellungskennwort zu erstellen. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort ein.

   Der Dialog wird nur angezeigt, wenn Sie mit dem SafeGuard Enterprise Server verbunden sind. Wenn keine Verbindung besteht, wird dieser beim nächsten Verbindungsaufbau angezeigt.

3.3.2 SafeGuard Native Device Encryption und SafeGuard File Encryption

Diese Anleitung geht davon aus, dass Sie sowohl SafeGuard Native Device Encryption als auch SafeGuard File Encryption auf Ihrem Mac installiert haben. Wenn Sie nur eines der genannten Module verwenden, können die erforderlichen Schritte abweichen.

Wenn Sie Ihr macOS Passwort vergessen haben, gehen Sie wie folgt vor:

1. Schalten Sie Ihren Mac ein.
2. Klicken Sie auf das Fragezeichen im Feld **Passwort**.
   Ihre Merkhilfe für Ihr Kennwort wird angezeigt und Sie werden gefragt, ob Sie Ihr Kennwort mithilfe des Wiederherstellungsschlüssels zurücksetzen wollen.
3. Klicken Sie auf das Pfeilsymbol neben der Meldung, um zum Feld Wiederherstellungsschlüssel zu wechseln.
4. Kontaktieren Sie Ihren Sicherheitsbeauftragten und erfragen Sie Ihren Wiederherstellungsschlüssel. Ihr Sicherheitsbeauftragter muss außerdem im SafeGuard Management Center Ihr Benutzerzertifikat entfernen.
5. Geben Sie Ihren Wiederherstellungsschlüssel in das entsprechende Feld ein und klicken Sie auf das Pfeil-Symbol auf der rechten Seite.
   Der Mac startet und der Dialog **Passwort zurücksetzen** wird angezeigt.
6. Wenn Sie ein Active Directory Benutzer sind, bitten Sie Ihren Administrator, Ihr Kennwort zurückzusetzen, und fordern Sie ein neues Kennwort an.
   a) Stellen Sie sicher, dass Ihr Computer mit Active Directory Domain Services verbunden ist.
   b) Klicken Sie im Dialog **Passwort zurücksetzen** auf **Abbrechen** und geben Sie Ihr neues Kennwort ein.
   c) Ändern Sie Ihr Passwort erneut, falls erforderlich.
7. Wenn Sie ein lokaler macOS Benutzer sind, definieren Sie ein neues Kennwort und eine Merkhilfe und klicken Sie auf **Passwort zurücksetzen**
8. Klicken Sie auf **Neuen Schlüsselbund erstellen**.

Ein neuer Anmeldeschlüsselbund wird erstellt. Bestehende Einträge in Ihrem Schlüsselbund bleiben dabei gültig.

9. Ein Mac mit Mac OS 10.13 und APFS formatiertem Systemlaufwerk benötigt möglicherweise das neue Kennwort, um ein neues Wiederherstellungskennwort zu erstellen. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort ein.

   Der Dialog wird nur angezeigt, wenn Sie mit dem SafeGuard Enterprise Server verbunden sind. Wenn keine Verbindung besteht, wird dieser beim nächsten Verbindungsaufbau angezeigt.
10. Geben Sie Ihr neues Kennwort ein, um Ihr SafeGuard Benutzerzertifikat zu erstellen. Wenn Sie ein Active Directory-Benutzer sind, werden Ihre Schlüssel automatisch in den SafeGuard Enterprise Schlüsselring geladen. Sie können wie gewohnt auf Ihre Dokumente zugreifen.
11. Wenn Sie ein lokaler Benutzer sind, bitten Sie Ihren Sicherheitsbeauftragten, Ihre Benutzerregistrierung zu bestätigen.
12. Öffnen Sie die Registerkarte **Server** im Einstellungsbereich und klicken Sie auf **Synchronisieren**.

Ihre Schlüssel werden wiederhergestellt und Sie können wieder auf Ihre verschlüsselten Dokumente zugreifen.

3.4 Device Encryption Wiederherstellungsschlüssel zentral speichern

Wenn kein zentral gespeicherter Wiederherstellungsschlüssel verfügbar ist, kann Ihnen der Helpdesk nicht bei der Kennwort-Wiederherstellung behilflich sein. Um den Wiederherstellungsschlüssel zentral verfügbar zu machen, importieren Sie ihn mit dem Kommandozeilen-Tool: `sgdeadmin --import-recoverykey`. Dann kann Ihnen der Sicherheitsbeauftragte den Wiederherstellungsschlüssel zur Verfügung stellen, wenn Sie ihn brauchen.

Wenn Sie den Wiederherstellungsschlüssel nicht kennen, kontaktieren Sie Ihren Sicherheitsbeauftragten. Wenn Sie Ihr Kennwort vergessen und kein Wiederherstellungsschlüssel verfügbar ist, dann sind alle auf dem verschlüsselten Laufwerk gespeicherten Daten verloren.

3.5 Dateien gemäß Richtlinie verschlüsseln

Ihr Sicherheitsbeauftragter definiert mittels Richtlinien, welche Dateien verschlüsselt werden und welcher Schlüssel dafür verwendetet wird. Um sicherzustellen, dass vertrauliche Dateien auf Ihrem Computer verschlüsselt sind, empfehlen wir eine initiale Verschlüsslung. Das bedeutet, dass alle Richtlinien angewendet werden, die Sie von Ihrem Sicherheitsbeauftragen zugewiesen bekommen haben. So starten Sie eine initiale Verschlüsselung:

1. Öffnen Sie die **Systemeinstellungen**.
2. Klicken Sie auf das Sophos SafeGuard Symbol.
3. Wählen Sie das Register **Richtlinien**.
4. Wechseln Sie zur Ansicht **Lokal übersetzter Pfad** und klicken Sie auf **Erzwinge alle Richtlinien**.

Alle Dateien in sicheren Ordnern werden mit dem in der Richtlinie definierten Schlüssel verschlüsselt oder neu verschlüsselt, siehe Sichere Ordner (Seite 4).

Wenn Sie eine einzelne Richtlinie erzwingen wollen, so wählen Sie diese aus und klicken Sie auf **Erzwinge Richtlinie**.

Wenn Sie einzelne Dateien oder Ordner gemäß Richtlinie verschlüsseln möchten, klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner und wählen Sie **Gemäß Richtlinie verschlüsseln**.

3.6 Dateien manuell verschlüsseln/entschlüsseln

SafeGuard File Encryption ermöglicht Ihnen, einzelne Dateien manuell zu verschlüsseln oder entschlüsseln. Kicken Sie mit der rechten Maustaste auf eine Datei und wählen Sie eine der folgenden Optionen:

- **Verschlüsselungsstatus anzeigen**: Zeigt an, ob die Datei verschlüsselt ist und welcher Schlüssel verwendet wurde.
- **Gemäß Richtlinie verschlüsseln**: Die ausgewählten Dateien werden mit dem in der Richtlinie definierten Schlüssel verschlüsselt oder neu verschlüsselt.
- **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 Datei mit Kennwort schützen (Seite 13). Diese Funktion ist nur für Dateien verfügbar, die entweder unverschlüsselt oder mit einem Schlüssel in Ihrem Schlüsselring verschlüsselt sind.

3.7 Prüfen, wo Dateien verschlüsselt sind

Ihr Sicherheitsbeauftragter legt mittels Richtlinien fest, an welchen Speicherorten auf Ihrem Computer Dateien verschlüsselt werden und wo nicht. So können Sie Ihre Richtlinien ansehen:

1. Öffnen Sie die **Systemeinstellungen**.
2. Klicken Sie auf das Sophos SafeGuard Symbol.
3. Öffnen Sie die Registerkarte **Richtlinien**, siehe Registerkarte Richtlinien (Seite 6).

3.8 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.

Wenn Sie E-Mails an Empfänger außerhalb Ihres Firmennetzwerks senden, empfehlen wir, die Datei mit einem Kennwort zu verschlüsseln, siehe Datei mit Kennwort schützen (Seite 13).

Wenn Sie Dateien an Empfänger außerhalb Ihres Firmennetzwerks versenden und Sie keinen Kennwortschutz verwenden möchten, stellen Sie sicher, dass Sie die betreffende Datei zuerst entschlüsseln. Andernfalls können Empfänger die verschlüsselten Dateien nicht lesen.

3.9 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 dazu mit der rechten Maustaste auf die Datei, die Sie versenden möchten, und wählen Sie **Kennwortgeschützte Datei erstellen**.
   Wenn eine Fehlermeldung angezeigt wird, wählen Sie im Finder **Darstellung > Vorschau ausblenden** und versuchen Sie es erneut.
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.

3.10 Dateien in der Cloud verschlüsseln

Sophos SafeGuard verschlüsselt Ihre Dateien in der Cloud automatisch, wenn folgende Voraussetzungen erfüllt sind:

- Ihr Administrator hat spezifiziert, dass Dateien in Cloud-Ordnern verschlüsselt werden.

- Der Cloud-Ordner befindet sich außerhalb eines Secured Folder (siehe Sichere Ordner (Seite 4)).
- Sie verwenden einen der unterstützen Cloud-Anbieter:
  - Box
  - Dropbox
  - Google Drive
  - Microsoft OneDrive
  - Microsoft OneDrive for Business

Ob Ihr Cloud-Ordner verschlüsselt ist, sehen Sie auf der Registerkarte **Richtlinien** im Einstellungsbereich, siehe Registerkarte Richtlinien (Seite 6).

Hinweis

- Verschlüsselte Dateien werden mit dem Sophos SafeGuard Overlay-Symbol statt mit dem Symbol des Cloud-Anbieters angezeigt.
- Sie können verschlüsselte Dateien in der Cloud nicht gleichzeitig mit anderen Benutzern ansehen oder bearbeiten.

3.11 Dateien auf Wechselmedien verschlüsseln

Wenn Sie ein Wechselmedium mit Ihrem Mac verbinden, werden Sie gefragt, wie Sie mit den darauf befindlichen Dateien verfahren möchten. Sie haben folgende Möglichkeiten:

1. Wählen Sie **Einstellung speichern und diesen Dialog nicht mehr anzeigen** und klicken Sie auf **Nein**.
   Es werden niemals Dateien auf diesem Medium verschlüsselt.
2. Wählen Sie **Einstellung speichern und diesen Dialog nicht mehr anzeigen** und klicken Sie auf **Ja**.
   Immer wenn Sie eine Datei auf diesem Medium speichern, wird sie automatisch verschlüsselt.
3. Wählen Sie **Vorhandene Dateien verschlüsseln** und klicken Sie auf **Ja**.
   Bestehende Dateien auf dem Wechselmedium werden verschlüsselt und neue Dateien werden verschlüsselt solange das Medium mit Ihrem Mac verbunden ist.
4. Wählen Sie **Einstellung speichern und diesen Dialog nicht mehr anzeigen** und **Vorhandene Dateien verschlüsseln** und klicken Sie auf **Ja**.
   Sowohl bestehende als auch neue Dateien auf dem Speichermedium werden immer automatisch verschlüsselt.

3.12 Verschlüsselte Dateien auf Wechselmedien austauschen

Sie können Wechselmedien wie USB-Speichersticks oder externe Festplatten verwenden, um verschlüsselte Dateien auszutauschen.

Um Daten auf einem Wechselmedium zwischen zwei Parteien austauschen und bearbeiten zu können, müssen beide Parteien über die zugehörige Richtlinie und den zugewiesenen Schlüssel verfügen.

Für den Austausch zwischen Windows- und macOS-Endpoints müssen Wechselmedien mit FAT32 formatiert sein. Andere Dateisysteme funktionieren möglicherweise mit eingeschränktem Funktionsumfang. Da das Dateisystem im Finder nicht angezeigt werden kann, müssen Sie das Festplattendienstprogramm (Disk Utility) verwenden.

Wenn Sie größere Datenmengen auf Wechselmedien austauschen stellen Sie sicher, dass Sie mehr als doppelt so viel freien Speicherplatz zur Verfügung haben, wie die größte auszutauschende Datei benötigt.

Auf Wechselmedien, die auch für Time Machine-Backups verwendet werden, wird das Verzeichnis `Backups.backupdb` automatisch von der Verschlüsselung ausgenommen.

3.13 Lokale Schlüssel verwenden

Lokale Schlüsse sind nur für Pfadbasierte Dateiverschlüsselung (Seite 3) verfügbar.

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

So erzeugen Sie einen lokalen Schlüssel:

1. Stellen Sie sicher, dass Ihr Endpoint eine Verbindung zum SafeGuard Enterprise Server hat, siehe Registerkarte Server (Seite 5).
2. Klicken Sie mit der rechten Maustaste auf eine oder mehrere Dateien und wählen Sie **Neuen Schlüssel erzeugen**.
3. Wählen Sie einen Namen und eine Passphrase für Ihren Schlüssel und klicken Sie auf **OK**.

   Der Schlüsselname wird mit dem Präfix "Local_" sowie mit Datum und Zeit versehen.

Der lokale Schlüssel wird erzeugt und zu Ihrem Schlüsselring hinzugefügt. Sie können nun den lokalen Schlüssel auf ein Wechselmedium oder einen Cloud Storage Ordner anwenden.

3.14 Verschlüsselte Dateien suchen

Wenn Sie nach verschlüsselten Dateien suchen möchten, müssen Sie Spotlight manuell aktivieren.

1. Mit folgendem Terminal-Befehl können Sie die Spotlight-Suche aktivieren:

   ```
   sgfsadmin --enable-spotlight
   ```
2. Mit folgendem Terminal-Befehl können Sie die Spotlight-Suche deaktivieren:

   ```
   sgfsadmin --disable-spotlight
   ```

Hinweis
Die Verwendung von Spotlight zusammen mit Sophos SafeGuard kann die Suchgeschwindigkeit verlangsamen.

3.15 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. Rechtsklicken Sie auf die Datei und wählen Sie **Verschlüsselungsstatus anzeigen** aus dem Kontextmenü.
   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, wählen Sie **Systemeinstellungen > Sophos SafeGuard > Server**.
5. Klicken Sie auf die Schaltfläche **Synchronisieren**.
6. Öffnen Sie die Registerkarte **Schlüssel** und überprüfen Sie, ob der erforderliche Schlüssel in der Liste angezeigt wird.

Wenn der Schlüssel, mit dem die betreffende Datei verschlüsselt wurde, in der Registerkarte **Schlüssel** angezeigt wird, können Sie nun auf den Inhalt der Datei zugreifen.

3.16 Überprüfen der Verbindung zum SafeGuard Enterprise Server

Wenn Sie Schwierigkeiten bei der Synchronisierung Ihres Endpoints mit dem SafeGuard Enterprise Server haben, gehen Sie wie folgt vor:

1. Öffnen Sie den Sophos SafeGuard Einstellungsbereich (Seite 5) und öffnen Sie die Registerkarte Server (Seite 5).
2. Klicken Sie **Verbindung prüfen**.
   Das Fenster **Prüfe SafeGuard Enterprise Client-Server-Verbindung** wird geöffnet.
3. Klicken Sie **Ausführen**.
   Das System überprüft die Verbindung zum SafeGuard Enterprise Server.
4. Klicken Sie die Schaltfläche **Exportieren** im unteren Fensterbereich, um die Ergebnisse als Textdatei zu speichern.
5. Wenden Sie sich an Ihren Administrator, falls die Verbindung zum SafeGuard Enterprise Server fehlschlägt.

4 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.

5 Rechtliche Hinweise