SOPHOS

Security made simple.

SafeGuard Enterprise für Mac

Benutzerhilfe

Produktversion: 8.0

Inhalt

1 Über SafeGuard Enterprise für Mac

SafeGuard Enterprise ist eine modulare Sicherheits-Suite, die plattformübergeifende Sicherheit für Endpoints mittels zentral definierter Richtlinien gewährleistet. SafeGuard Enterprise wird zentral über das SafeGuard Management Center verwaltet.

Die wichtigsten Sicherheitsfunktionen von SafeGuard Enterprise an einem Endpoint sind die Verschlüsselung von Daten und der Schutz vor Angreifern, die einen Rechner mit Hilfe eines externen Mediums starten wollen. SafeGuard Enterprise für Mac beinhaltet **SafeGuard Synchronized Encryption**, **SafeGuard File Encryption** und **SafeGuard Native Device Encryption**. Abhängig von einer Richtlinie kommt für die Dateiverschlüsselung auf Ihrem Endpoint entweder Synchronized Encryption oder File Encryption zum Einsatz. Native Device Encryption dient zur Festplattenverschlüsselung und kann mit beiden genannten Systeme verwendet werden.

Um allgemeine Informationen zu Ihrer Installation von SafeGuard Enterprise für Mac aufzurufen, klicken Sie auf das SafeGuard Icon im Einstellungsbereich (Seite 12). Weitere Informationen sowie grundlegende Funktionen finden Sie im System-Menü. Ab OS X 10.10 ist im Finder auch ein Kontextmenü zum Aufrufen von SafeGuard-Funktionen verfügbar.

Wichtig: Bevor Sie Ihren Mac auf eine neuere Version von OS X aktualisieren, müssen Sie auf die aktuellsten Versionen von SafeGuard File Encryption und Disk Encryption wechseln. Wenn Sie das Betriebssystem zuerst aktualisieren, kann das schwerwiegende Sicherheitsprobleme verursachen und/oder den Zugang zu Ihren Daten einschränken. Weitere Informationen finden Sie im Sophos Knowledgebase-Artikel 122690.

2 SafeGuard Synchronized Encryption

SafeGuard Enterprise Synchronized Encryption ist ein fortschrittliches Dateiverschlüsselungs-System, das Sie alternativ zu SafeGuard File Encryption für Mac (Seite 7) verwenden können. Abhängig von einer Richtlinie kommt auf Ihrem Endpoint entweder das eine oder das andere System zum Einsatz.

SafeGuard Enterprise Synchronized Encryption ermöglicht Ihnen, sensible Dateien anhand der Anwendung, mit der sie erstellt wurden, zu verschlüsseln. Siehe Anwendungsbasierte Dateiverschlüsselung (Seite 4). Die Verschlüsselung ist persistent; das bedeutet, Ihre Daten sind auch dann sicher, wenn sie an einen anderen Ort verschoben (siehe Sichere Ordner (Seite 6)), in die Cloud hochgeladen oder per E-Mail versandt werden (siehe Mailanhänge sicher versenden (Seite 5)).

Abhängig von der Richtlinie, die Ihr Sicherheitsbeauftragter definiert, werden bestimmte Dateitypen automatisch verschlüsselt. In manchen Fällen kann es jedoch erforderlich sein, einzelne Dateien manuell zu verschlüsseln oder entschlüsseln, siehe Dateien manuell verschlüsseln/entschlüsseln (Seite 5).

Um eine initiale Verschlüsselung aller Dateien (bestimmten Typs und an bestimmten Speicherorten) anzustoßen, klicken Sie auf die Schaltfläche **Erzwinge alle Richtlinien** unter Registerkarte Richtlinien (Seite 13) in den Systemeinstellungen. Unverschlüsselte Dateien werden standardmäßig mit dem Synchronized Encryption Schlüssel verschlüsselt. Dateien, die mit einem SafeGuard File Encryption für Mac Schlüssel verschlüsselt sind, werden entschlüsselt und mit dem Synchronized Encryption Schlüssel neu verschlüsselt.

Im Finder werden verschlüsselte Dateien mit einem grünen Schloss-Symbol gekennzeichnet (ab OS X 10.10).

Das SafeGuard-Symbol in der Menüleiste zeigt den Verschlüsselungsstatus einer Datei an. Ist eine verschlüsselte Datei ausgewählt, so ist das Symbol grün. Ist eine unverschlüsselte Datei oder keine Datei ausgewählt, so ist das Symbol schwarz.

2.1 Anwendungsbasierte Dateiverschlüsselung

SafeGuard Enterprise Synchronized Encryption kann jede Datei, die mit einer per Richtlinie definierten Anwendung erstellt oder geändert wurde (zum Beispiel Microsoft Word), verschlüsseln. Eine Richtlinie definiert eine Liste von Anwendungen, für die die Dateiverschlüsselung automatisch durchgeführt wird. Synchronized Encryption erfasst alle Sichere Ordner (Seite 6).

Wenn Ihr Sicherheitsbeauftragter die Dateiverschlüsselung für Microsoft Word aktiviert hat, wird jede Datei, die Sie mit Word erstellen und in einem sicheren Ordner speichern, automatisch mit dem Synchronized Encryption-Schlüssel verschlüsselt. Jeder, der diesen Schlüssel in seinem Schlüsselring hat, kann auf diese Datei zugreifen. Sie können die Datei auf ein Netzlaufwerk oder auf einen USB-Stick kopieren oder per E-Mail versenden - die Dateiverschlüsselung bleibt aufrecht. Weitere Informationen zu E-Mail finden Sie unter Mailanhänge sicher versenden (Seite 5).

Ihr Sicherheitsbeauftragter kann per Richtlinie Ausnahmen für bestimmte Pfade definieren.

Hinweis: Synchronized Encryption Richtlinien sind immer Benutzern zugewiesen, nicht Maschinen.

2.2 Dateien manuell verschlüsseln/entschlüsseln

Synchronized 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:

- **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 entschlüsseln.
- **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. Mit diesem Befehl erstellen Sie eine kennwortgeschützte Kopie Ihrer Datei und speichern diese als HTML-Datei. 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.

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.

2.3 Mailanhänge sicher versenden

Wenn Sie E-Mails mit Anhängen an Empfänger senden, die Synchronized Encryption verwenden, wird automatisch der Synchronized Encryption-Schlüssel verwendet. Sie brauchen sich nicht um die Verschlüsselung und Entschlüsselung zu kümmern.

Wenn Sie E-Mails an Empfänger außerhalb Ihres Firmennetzwerks senden, ist es ratsam, Anhänge zu verschlüsseln um sensible Daten zu schützen. Klicken Sie dazu mit der rechten Maustaste auf die Datei, die Sie versenden möchten, und wählen Sie **Kennwortgeschützte Datei erstellen** (siehe Dateien manuell verschlüsseln/entschlüsseln (Seite 5)). Nachdem Sie ein Kennwort definiert und bestätigt haben wird Ihre Datei verschlüsselt und als HTML-Datei gespeichert. Sie können die Datei nun sicher per E-Mail versenden.

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

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

Hinweis: Diese Software wurde mit den genannten Browsern in der zum Zeitpunkt der Veröffentlichung verfügbaren Version getestet.

Wichtig: 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. Empfänger können Dateien, die mit dem Synchronized Encryption Schlüssel verschlüsselt sind, nicht öffnen und könnten denken, Sie hätten eine fehlerhafte Datei gesendet.

2.4 Sichere Ordner

Wenn Sie Synchronized Encryption verwenden werden alle Dateien, die Sie in sicheren Ordnern ablegen, automatisch verschlüsselt. Ihr Sicherheitsbeauftragter definiert, welche Ordner als sichere Ordner gelten. Üblicherweise sind dies Ordner wie Documents und Downloads sowie temporäre Ordner, wo Microsoft Outlook oder Apple Mail E-Mail-Anhänge speichern.

Um herauszufinden, welche Ordner auf Ihrem Mac sichere Ordner sind, drücken Sie **Alt** und klicken Sie das SafeGuard Symbol in der Menüleiste.

Beachten Sie folgende Einschränkungen:

- **Verschlüsselte Dateien aus sicheren Ordnern verschieben**

  Wenn Sie eine verschlüsselte Datei aus einem sicheren Ordner in einen nicht sicheren Ordner verschieben, so bleibt die Datei zwar verschlüsselt, jedoch können Sie nicht mehr auf ihren Inhalt zugreifen. Sie müssen die Datei zuerst manuell entschlüsseln.

  Wenn Sie eine verschlüsselte Datei in einem sicheren Ordner öffnen und in einen nicht sicheren Ordner speichern, so wird die Datei automatisch entschlüsselt.

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

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

- **Nach Dateien suchen**
  - Die Spotlight-Suche funktioniert nicht bei verschlüsselten Dateien.
  - Die Suche nach Dateien mit Etikett funktioniert nicht in sicheren Ordnern.

- **Sichere Ordner freigeben**

  Ein sicherer Ordner kann nicht über das Netzwerk freigegeben werden.

2.5 Wechselmedien

Wenn Ihr Sicherheitsbeauftragter Ihnen eine Synchronized Encryption Richtlinie zugewiesen hat, werden Wechselmedien als Mount-Points angezeigt und die Verschlüsselung wird aktiviert. Abhängig von der Richtlinie wird die initiale Dateiverschlüsselung automatisch im Hintergrund gestartet.

3 SafeGuard File Encryption für Mac

Sophos SafeGuard File Encryption für Mac erweitert den Sophos SafeGuard Enterprise Datenschutz von Windows auf Mac und ermöglicht eine dateibasierte Verschlüsselung auf lokalen Laufwerken, auf Netzlaufwerken, auf Wechsellaufwerken und in der Cloud. Mit SafeGuard File Encryption für Mac können Sie Dateien sicher ver- und entschlüsseln und diese Dateien mit anderen austauschen.

- Neue Dateien in den relevanten Speicherorten werden automatisch verschlüsselt.
- Wenn Sie den Schlüssel für eine verschlüsselte Datei haben, können Sie den Inhalt lesen und ändern.
- Wenn Sie keinen Schlüssel für eine verschlüsselte Datei haben, können Sie die Datei nicht im Klartext lesen, sondern sehen nur den verschlüsselten Inhalt.
- Wenn Sie auf einem beliebigen Endpoint, auf dem File Encryption nicht installiert ist, auf eine verschlüsselte Datei zugreifen, wird ebenfalls der verschlüsselte Inhalt angezeigt.

SafeGuard File Encryption für Mac ermöglicht Ihrem Sicherheitsbeauftragten festzulegen, ob Dateien in bestimmten Verzeichnissen und/oder Laufwerken verschlüsselt werden oder ob nicht.

Hinweis: Dateiverschlüsselungsrichtlinien werden immer Benutzern zugewiesen, nicht Maschinen.

Die Verschlüsselung selbst ist transparent. Nach der Initialverschlüsselung (Seite 7) stellt das System sicher, dass die Dateien, die sich auf einem Laufwerk oder in einem Verzeichnis befinden, das für die Verschlüsselung festgelegt wurde (sicherer Ordner), verschlüsselt werden.

Nachdem die Verschlüsselungssoftware installiert wurde und die Kommunikation mit dem SafeGuard Enterprise Backend hergestellt wurde, werden Sie aufgefordert, ihr Mac OS X Kennwort einzugeben. Um das Produkt ordnungsgemäß zu verwenden, benötigen Sie ein persönliches Zertifikat. Dieses Zertifikat wird (pro Benutzer) am SafeGuard Enterprise Server erzeugt, sobald Sie Ihr Kennwort eingeben. Dieser Vorgang ist nur nach Produktinstallation, erster Anmeldung oder dem Kennwort-Zurücksetzen erforderlich.

Hinweis: Ohne Verbindung zum SafeGuard Enterprise Server können keine neuen Benutzer registriert werden.

Abhängig von Ihren Sicherheitseinstellungen werden nun ein oder mehrere Laufwerke in Ihrer Finder-Seitenleiste angezeigt.

Hinweis: Die Spotlight-Suche und permanente Versionsspeicherung ("Alle Versionen durchsuchen...") werden nicht unterstützt. Wenn Sie versuchen, ein Laufwerk auszuwerfen, das auf einen lokalen Ordner zeigt, wird es automatisch wieder verbunden.

3.1 Initialverschlüsselung

Starten Sie eine Initialverschlüsselung, bevor Sie mit Ihrer Arbeit beginnen.

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**, um alle Richtlinien anzuwenden.

Alle unverschlüsselten Dateien werden nun verschlüsselt.

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

3.2 SafeGuard File Encryption System-Menü

Das System-Menü stellt Ihnen die folgenden Informationen zur Verfügung:

1. Wenn Sie eine Datei auswählen zeigt das SafeGuard-Symbol in der Menüleiste den Verschlüsselungsstatus und den verwendeten Schlüssel an:

	Grünes Symbol: Die Datei ist verschlüsselt und Sie besitzen den zugehörigen Schlüssel.
	Rotes Symbol: Die Datei ist verschlüsselt, aber Sie besitzen den zugehörigen Schlüssel nicht.
	Graues Symbol: Die Datei sollte verschlüsselt werden. (*)
	Schwarzes Symbol: Die Datei wird ignoriert oder ist von der Verschlüsselung ausgeschlossen.

(*) Mögliches Szenario: Wenn Sie eine unverschlüsselte Datei auswählen, die sich in einem Ordner befindet, wo eine Verschlüsselungsregel angewendet wird, so wird das Symbol grau. Um diese Datei initial zu verschlüsseln, öffnen Sie das Register **Richtlinien**, wählen Sie die zu diesem Ordner gehörende Richtlinie und klicken Sie auf **Erzwinge Richtlinie**.

2. Wird eine Datei verarbeitet, so dreht sich das äußere Rad des Symbols. Dieses Verhalten ist unabhängig vom aktuellen Verschlüsselungsstatus.
3. Abhängig davon, ob Sie Dateien, Ordner oder Laufwerke ausgewählt haben, kann sich der Inhalt des Menüs unterscheiden.
   - Ist eine Datei, ein Ordner oder ein Laufwerk ausgewählt, so werden der Name des erforderlichen Schlüssels sowie Informationen zum aktuellen Verschlüsselungsstatus und zur Verfügbarkeit des Schlüssels angezeigt.
   - Liste der sicheren Ordner (Aktivierungspunkte oder Mount-Points)
   - Klicken Sie auf **Sophos Encryption-Systemeinstellungen öffnen…** um den Einstellungsbereich (Seite 12) zu öffnen.

3.3 Arbeiten mit Wechselmedien

Wenn Ihr Sicherheitsbeauftragter in Ihrer Richtlinie Dateiverschlüsselung für Wechselmedien aktiviert hat können Sie wählen, ob Sie Dateiverschlüsselung anwenden möchten.

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.

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 Mac OS X-Clients muss das Medium mit FAT32 formatiert sein. Da das Dateisystem im Finder nicht angezeigt werden kann, müssen Sie das Festplattendienstprogramm (Disk Utility) verwenden.

Wichtig: 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.

3.4 Lokale Schlüssel

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. Öffnen Sie das System-Menü und wählen Sie **Neuen Schlüssel erzeugen**.
2. 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.

4 SafeGuard Native Device Encryption für Mac

Sophos SafeGuard Native Device Encryption für Mac baut auf der in Mac OS X eingebauten FileVault 2 Festplatten-Verschlüsselungstechnologie auf. Es verwendet FileVault 2 zur Verschlüsselung der gesamten Festplatte, so dass Ihre Daten sogar dann sicher sind, wenn der Computer verloren oder gestohlen wird.

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

Der Sicherheitsbeauftragte definiert im Sophos SafeGuard Management Center, welche Clients zu verschlüsseln sind.

4.1 Initialverschlüsselung durchführen

Wenn eine laufwerksbasierende Verschlüsselung des Systemlaufwerks in der Richtlinie definiert ist, dann wird die Verschlüsselung für den momentan angemeldeten Benutzer aktiviert. Bevor die Verschlüsselung beginnt, werden Sie zur Eingabe von Benutzernamen und Passwort aufgefordert.

1. Geben Sie Ihr Mac OS X Kennwort ein, wenn Sie dazu aufgefordert werden.

   Hinweis: Wenn Ihr Kennwort leer ist, ändern Sie es bitte. Es ist nicht möglich, die Festplattenverschlüsselung zu aktivieren, wenn kein Kennwort gesetzt ist.

2. Warten Sie bis Ihr Mac neu startet.

   Hinweis: Wenn die Aktivierung der Verschlüsselung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenden Sie sich an Ihren Systemadministrator.

Die Initialverschlüsselung läuft im Hintergrund und Sie können weiterhin mit Ihrem Computer arbeiten.

4.2 Entschlüsselung

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 16).

4.3 SafeGuard Native Device Encryption System-Menü

Das System-Menü stellt Ihnen die folgenden Informationen zur Verfügung:

- Das Symbol (links) zeigt den Verschlüsselungsstatus an:

Abbildung 1: System-Menü

	Grünes Symbol: Das Systemlaufwerk ist verschlüsselt.
	Rotes Symbol: Das Systemlaufwerk ist nicht verschlüsselt.

- Der folgende Menübefehl ist verfügbar, wenn Sie auf das Symbol klicken:
  - **Sophos Encryption-Systemeinstellungen öffnen…**

    Öffnet den Sophos Encryption-Einstellungsbereich.

Hinweis: Informationen zum Aktivieren oder Deaktivieren des System-Menüs finden Sie unter Registerkarte Benutzer (Seite 12).

5 Einstellungsbereich

Im Einstellungsbereich können Sie Einstellungen für eine bestimmte Anwendung oder das System festlegen. Nachdem Sie Sophos SafeGuard Enterprise auf einem Mac-Client installiert haben, erscheint das folgende 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.

5.1 Registerkarte Server

Die Registerkarte **Server** enthält folgende Informationen und Funktionen:

Serverinfo

- **Kontaktintervall:** Intervall, in dem die Synchronisation gestartet wird. Es wird zentral vom Sicherheitsbeauftragten festgelegt.
- **Letzter Kontakt:** Datum, an dem der Client zuletzt mit dem Server kommuniziert hat.
- **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 SafeGuard Enterprise-Server aktiviert oder deaktiviert ist.

Konfigurationsdatei hierhin ziehen

Ziehen Sie die Konfigurations-Zip-Datei in diesen Bereich, um die Konfigurationsinformation aus dem SafeGuard Management-Center auf dem Mac-Rechner zu übernehmen.

Synchronisieren

Klicken Sie diese Schaltfläche, um Datenbankinformationen wie z.B. Richtlinien manuell zu synchronisieren.

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.

5.2 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 **SGN-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 mittleren Teil des Fensters werden Informationen über das **Benutzerzertifikat** angezeigt (Nur relevant für File Encryption):

- **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 untersten Fensterteil können Sie folgende Option aktivieren oder deaktivieren:

- **System Menü für Native Device Encryption anzeigen**: Wenn aktiviert, wird das SafeGuard Native Device Encryption System-Menü (Seite 10) Symbol angezeigt.

5.3 Registerkarte Schlüssel

Hinweis: Diese Registerkarte wir nur angezeigt, wenn Sie SafeGuard File Encryption / Synchronized 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.

5.4 Registerkarte Richtlinien

Hinweis: Diese Registerkarte wir nur angezeigt, wenn Sie SafeGuard File Encryption / Synchronized 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.

- Der **Lokal übersetzte Pfad** zeigt nur diejenigen Richtlinien an, die dem zu diesem Zeitpunkt angemeldeten Benutzer an einem spezifischen Mac zugewiesen sind. Die Spalten in der Tabelle enthalten folgende Informationen:
  - **@-Symbol**: während der Initialverschlüsselung oder wenn größere Dateien verschlüsselt werden sehen Sie ein sich drehendes Rad in der ersten Spalte.
  - **Modus**: Es wird entweder **Verschlüsseln** oder **Ausschließen** angezeigt.
  - **Anwendungsbereich**: legt fest, ob Unterordner verschlüsselt werden sollen
  - **Schlüsselname**: Zeigt den Namen des Schlüssels, der dem angegebenen Ablageort zugewiesen ist.

Wenn ein Schlüssel in Blau angezeigt wird, handelt es sich um Ihren persönlichen Schlüssel.

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.

Um zur Ansicht **Empfangene Richtlinien** zu wechseln, klicken Sie auf das rechte Symbol unten rechts.

- Die Ansicht **Empfangene Richtlinien** zeigt alle Richtlinien an, die vom Server empfangen wurden. Diese Ansicht ist identisch zur Ansicht im SafeGuard Management-Center. Die Übersicht enthält folgende Informationen:
  - **Erhaltene Richtlinien**: legt fest, welche Dateien oder Ordner verschlüsselt werden sollen.
  - Alle anderen Spalten enthalten die oben beschriebenen Informationen für die Ansicht **Lokal übersetzter Pfad**.

Sichere Ordner anzeigen und Richtlinien in der Ansicht "Lokal übersetzter Pfad" anzeigen

Wählen Sie in der Tabelle **Lokal übersetzter Pfad** eine Richtlinie aus (1).

- Klicken Sie auf die Schaltfläche **Erzwinge alle Richtlinien** um die initiale Verschlüsselung zu starten. Alle Dateien, die von einer Richtlinie erfasst sind, werden entsprechend verschlüsselt.
- Klicken Sie auf die Schaltfläche **Zeige im Finder** (2), um den ausgewählten sicheren Ordner (Mount-Point) in einem Finder-Fenster zu öffnen.
- Auf **Erzwinge Richtlinie** (3) klicken, um die ausgewählte Richtlinie auf alle erlaubten Dateien anzuwenden. Ein Fortschrittsbalken wird angezeigt. Warten Sie, bis das System die Anwendung der Richtlinie abgeschlossen hat, oder brechen Sie den Vorgang ab, indem Sie auf das Kreuz neben dem Balken klicken.

  Hinweis:

  Dateien, die schreibgeschützt oder aufgrund fehlender Berechtigungen nicht zugänglich sind, werden von der Verschlüsselung ausgenommen.

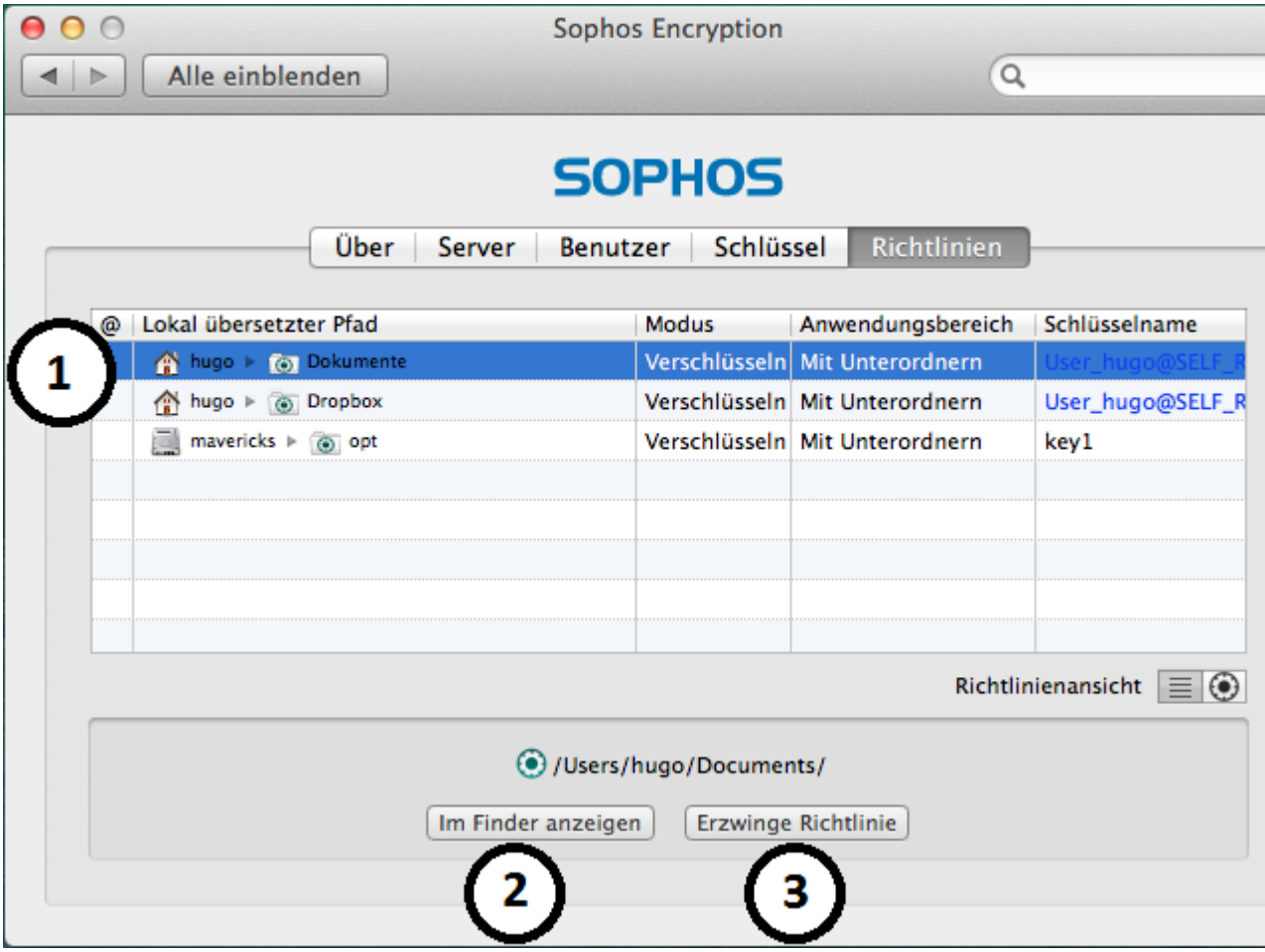

Abbildung 2: Registerkarte Richtlinien - Ansicht Lokal übersetzter Pfad

Mögliche Ergebnisse beim Erzwingen von Richtlinien

- Klartextdateien 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 mit einem anderen Schlüssel verschlüsselt sind,
  - bleiben unverändert, wenn der Benutzer den entsprechenden Schlüssel nicht an seinem Schlüsselring hat.
  - werden mit dem per Richtlinie zugewiesenen Schlüssel neu verschlüsselt, wenn der Benutzer diesen Schlüssel an seinem Schlüsselring hat.
- Dateien, die mehrmals verschlüsselt waren, werden einmal mit dem per Richtlinie zugewiesenen Schlüssel verschlüsselt. Wenn einer der erforderlichen Schlüssel nicht verfügbar ist, werden diese Dateien so weit wie möglich entschlüsselt.

5.5 Registerkarte Disk Encryption

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

Klicken Sie auf **Disk Encryption**, um Informationen über die aktuellen Richtlinien und den Status des Mac-Client anzuzeigen.

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 Mac-Client 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 wird aktiviert wenn der Sicherheitsbeauftragte eine Richtlinie setzt, die besagt, dass für den Client keine Verschlüsselung notwendig ist.

Hinweis: 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.

6 Vergessenes Kennwort zurücksetzen

Hinweis: 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 Mac OS X Anmeldekennwort vergessen haben, gehen Sie wie folgt vor:

1. Schalten Sie Ihren Mac ein.
2. Klicken Sie im Kennwort-Feld auf **?**.

   Ihre Merkhilfe für Ihr Kennwort wird angezeigt und Sie werden gefragt, ob Sie Ihr Kennwort mithilfe des Wiederherstellungsschlüssels zurücksetzen wollen.

3. Falls Sie sich immer noch nicht an Ihr Kennwort erinnern können, klicken Sie auf das Symbol neben dem Text:

   

4. Kontaktieren Sie Ihren Sicherheitsbeauftragten und erfragen Sie Ihren Wiederherstellungsschlüssel. Zusätzlich muss Ihr Sicherheitsbeauftragter 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. Klicken Sie im Dialog **Passwort zurücksetzen** auf **Abbrechen** und geben Sie Ihr neues Kennwort ein. Danach kann noch eine weitere Kennwortänderung erforderlich sein.
7. Wenn Sie ein lokaler Benutzer sind, definieren Sie ein neues Kennwort und eine Merkhilfe und klicken Sie auf **Passwort zurücksetzen**
8. Klicken Sie im folgenden Dialog, der Sie darüber informiert, dass Ihr Schlüsselbund nicht freigegeben werden konnte, auf **Neuen Schlüsselbund erstellen**.

   Ein neuer Anmeldeschlüsselbund wird erstellt.

9. 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, so dass alle Dokumente wie bisher zugänglich sind.

10. Wenn Sie ein lokaler Benutzer sind, bitten Sie Ihren Sicherheitsbeauftragten, Ihre Benutzerregistrierung zu bestätigen.
11. Öffnen Sie die Registerkarte **Server** im Einstellungsbereich und klicken Sie auf **Synchronisieren**.

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

7 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. Wählen Sie die Datei aus und klicken Sie auf das SafeGuard-Symbol in der Menüleiste.

   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.

8 Technischer Support

Technischen Support zu Sophos Produkten finden Sie hier:

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

9 Rechtliche Hinweise