SOPHOS

Security made simple.

Sophos SafeGuard Native Device Encryption für Mac

Administratorhilfe

Produktversion: 7

Stand: Dezember 2014

Inhalt

1 Über SafeGuard Native Device Encryption für Mac

Sophos SafeGuard Native Device Encryption für Mac bietet Mac Benutzern denselben Schutz ihrer Daten wie das die Funktionalität zur Festplattenverschlüsselung in SafeGuard Enterprise für Windows Benutzer tut.

SafeGuard Native Device Encryption für Mac baut auf der in Mac OS X eingebauten Verschlüsselungstechnologie FileVault 2 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. Darüber hinaus ermöglicht es Ihnen, Festplattenverschlüsselung in Ihrem gesamten Netzwerk zur Verfügung zu stellen und zu verwalten.

Die Verschlüsselung arbeitet transparent. Der Benutzer wird beim Öffnen, Bearbeiten und Speichern von Dateien nicht zur Verschlüsselung oder Entschlüsselung aufgefordert.

Im Management Center von SafeGuard Enterprise können Sie angeben, welche Computer (Windows Computer genauso wie Macs) zu verschlüsseln sind, können deren Verschlüsselungsstatus überprüfen und Benutzern behilflich sein, die ihr Passwort vergessen haben.

1.1 Über dieses Dokument

Dieses Dokument beschreibt, wie Sophos SafeGuard Native Device Encryption für Mac installiert, konfiguriert und verwaltet wird.

Mehr zum Arbeiten mit dem Management Center und zu Richtlinien finden Sie in der *SafeGuard Enterprise Administratorhilfe*.

Benutzerrelevante Informationen finden Sie in der *Schnellstartanleitung für Sophos SafeGuard Native Device Encryption für Mac* .

1.2 Fachbegriffe und Akronyme

Die folgenden Fachbegriffe und Akronyme werden in diesem Dokument verwendet:

Fachbegriff oder Akronym	Bedeutung oder Erläuterung
GUID	Ein Globally Unique Identifier (GUID) ist eine global eindeutige Zahl, die in verteilten Computersystemen zum Einsatz kommt
POA	Die Power-on Authentication (POA) (synonym: "Pre-Boot Authentisierung")
SGN	SafeGuard Enterprise
SSL	Secure Sockets Layer: Netzwerkprotokoll zur sicheren Übertragung von Daten über das Internet.

2 Installation

Das folgende Kapitel beschreibt die Installation von SafeGuard native Device Encryption auf Mac OS X Client-Rechnern. Eine Beschreibung zur Installation der Administrationsumgebung (Backend) finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

Zwei Installationsarten für Mac OS X Client-Rechner gibt es:

- manuelle (beaufsichtigte) Installation
- automatisierte (unbeaufsichtigte) Installation

Wenn Sie SafeGuard File Encryption und SafeGuard Native Device Encryption (hieß bis Version 6.10 SafeGuard Disk Encryption) verwenden möchten, muss es sich in beiden Fällen um Version 7 handeln. Die Verwendung unterschiedlicher Versionen dieser Produkte auf demselben Mac wird nicht unterstützt.

Hinweis: Wenn Sie SafeGuard Disk Encryption 6.01 oder älter installiert haben, müssen Sie diese Version vor der Installation von SafeGuard File Encryption für Mac Version 7 deinstallieren.

Das Installer Package ist signiert und OS X versucht, diese Signatur zu validieren. Ist die Internetverbindung langsam oder nicht richtig konfiguriert, kann es eventuell zu Verzögerungen beim Installationsvorgang von bis zu 20 Minuten kommen.

2.1 Installationsvoraussetzungen

Stellen Sie vor dem Beginn der Installation sicher, dass das SafeGuard Enterprise-SSL-Serverzertifikat in den Systemschlüsselbund importiert wurde und für SSL auf **Immer vertrauen** gesetzt ist.

1. Bitten Sie Ihren SafeGuard Server-Administrator, Ihnen das SafeGuard Enterprise-Serverzertifikat (Datei <Zertifikatsname>.cer).zur Verfügung zu stellen.
2. Importieren Sie die Datei *Zertifikatsname>.cer*) in Ihre Schlüsselbundverwaltung. Wählen Sie dazu **Programme** - **Dienstprogramme** und doppelklicken Sie **Schlüsselbundverwaltung.app**.
3. Wählen Sie im linken Fensterteil **System**.
4. Öffnen Sie einen Finder und wählen Sie die Datei *<Zertifikatsname>.cer* von oben.
5. Ziehen Sie die Zertifikatsdatei in die Schlüsselbundverwaltung.
6. Sie werden aufgefordert, Ihr Mac-OS X-Kennwort einzugeben.
7. Klicken Sie nach der Kennworteingabe auf **Schlüsselbund ändern**, um den Vorgang zu bestätigen.
8. Doppelklicken Sie dann auf die Datei *<Zertifikatsname>.cer* . Klicken Sie auf den Pfeil neben **Vertrauen**, um die Vertrauenseinstellungen anzuzeigen.
9. Für **Secure Sockets Layer (SSL)** wählen Sie die Option **Immer vertrauen**.
10. Schließen Sie den Dialog. Sie werden erneut aufgefordert, Ihr Mac-OS X-Kennwort einzugeben.
11. Geben Sie das Kennwort ein und bestätigen Sie mit ein Klick auf **Einstellungen aktualisieren**. Ein blaues Plus-Zeichen in der unteren rechten Ecke des Zertifikats-Symbols zeigt Ihnen, dass dieses Zertifikat als vertrauenswürdig für alle Benutzer eingestuft ist.

12. Öffnen Sie einen Webbrowser und stellen Sie sicher, dass Ihr SafeGuard Enterprise Server unter **`https://<Servername>//SGNSRV`** verfügbar ist.

Nun können Sie mit der Installation beginnen.

Hinweis:

Das Zertifikat kann auch importiert werden, indem der folgende Befehl ausgeführt wird: **`sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.keychain -r trustAsRoot -p ssl "/<Ordner>/<Zertifikatsname>.cer"`**. Dieser Befehl kann auch für eine automatisierte Installation mittels Skript verwendet werden. Ändern Sie die Namen des Ordners und des Zertifikats entsprechend Ihren Anforderungen.

Hinweis:

Wenn Sie den oben beschriebenen Vorgang umgehen wollen, so können Sie den Befehl **`sgdeadmin --disable-server-verify`** mit sudo-Rechten wie hier beschrieben ausführen: Kommandozeilen-Optionen (Seite 14). Wir empfehlen nicht, diese Option zu verwenden, da dadurch eine Sicherheits-Schwachstelle entstehen kann.

2.2 Manuelle (beaufsichtigte) Installation

Eine manuelle (oder beaufsichtigte) Installation ermöglicht Ihnen, die Installation Schritt-für-Schritt zu steuern und zu testen. Sie wird auf Mac-Einzelplatzrechnern durchgeführt.

Hinweis:

Stellen Sie sicher, dass der Server wie unter Installationsvoraussetzungen (Seite 4) beschrieben korrekt aufgesetzt wurde.

1. Öffnen Sie *Sophos SafeGuard DE.dmg*.
2. Nachdem Sie die Readme-Datei gelesen haben, doppelklicken Sie auf *Sophos SafeGuard DE.pkg* und folgen Sie den Anweisungen des Installationsassistenten. Sie werden nach Ihrem Kennwort gefragt, um die Installation neuer Software zu erlauben. Das Produkt wird im Ordner */Library/Sophos SafeGuard DE/* installiert.
3. Klicken Sie auf **Schließen**, um die Installation abzuschließen.
4. Nach einem Neustart melden Sie sich mit Ihrem Kennwort an.
5. Öffnen Sie die **Systemeinstellungen** und klicken Sie auf das Sophos Encryption-Symbol, um die Produkteinstellungen anzuzeigen.

6. Klicken Sie auf die Registerkarte **Server**.
7. Werden Server und Zertifikatsdetails angezeigt, so überspringen Sie die nächsten Schritte, gehen zu Schritt 11 und klicken **Synchronisieren**. Wird keine Information angezeigt, so fahren Sie mit dem nächsten Schritt fort.
8. Nehmen Sie die Konfigurations-Zipdatei (Eine Beschreibung, wie Sie ein Konfigurationspaket erstellen, entnehmen Sie der*SafeGuard Enterprise Administratorhilfe* version 7.0, *Mit Konfigurationspaketen arbeiten > Erzeugen eines Konfigurationspakets für Macs*).
9. Ziehen Sie die Zip-Datei in den **Server**-Dialog und lassen Sie sie in der Dropzone los.
10. Sie werden aufgefordert, Ihr Mac-Administratorkennwort einzugeben. Geben Sie das Kennwort ein und klicken Sie zur Bestätigung auf **OK**.

11. Überprüfen Sie die Verbindung zum SafeGuard Enterprise Server. Details zum Unternehmenszertifikat werden im unteren Teil des **Server**dialogs angezeigt. Klicken Sie dann auf **Synchronisieren**. Eine erfolgreichen Verbindung erkennen Sie an einem aktualisierten Zeitstempel (Registerkarte **Server**, **Serverinfo**-Bereich, **Letzter Serverkontakt:**). Bei einer unterbrochenen Verbindung erscheint das folgende Symbol:

    

    Mehr Information finden Sie in der System-Logdatei.

    Mehr Informationen zur Synchronisation und zur Serververbindung finden Sie auch in Registerkarte Server (Seite 11).

2.3 Automatisierte (unbeaufsichtigte) Installation über Remote Management Software

Eine automatisierte (unbeaufsichtigte) Installation erfordert keinen Benutzereingriff während des Installationsprozesses.

Der folgende Abschnitt beschreibt die grundsätzlichen Schritte einer automatisierten (unbeaufsichtigten) Installation von SafeGuard Native Device Encryption für Mac. Verwenden Sie die Managementsoftware, die auf Ihrem System installiert ist. Je nach Managementsoftware-Lösung, die Sie verwenden, können die tatsächlichen Schritte von der Beschreibung abweichen.

Hinweis:

Um SafeGuard Native Device Encryption für Mac auf Client-Rechnern zu installieren, gehen Sie wie folgt vor:

1. Laden Sie die Installationsdatei *Sophos SafeGuard DE.dmg* herunter.
2. Kopieren Sie die Datei auf die Zielrechner.
3. Installieren Sie die Datei auf den Zielrechnern. Wenn Sie Apple Remote Desktop verwenden, sind die Schritte 2 und 3 zu einem einzelnen Schritt zusammengefasst.
4. Nehmen Sie die Konfigurations-Zipdatei (Eine Beschreibung, wie Sie ein Konfigurationspaket erstellen, entnehmen Sie der*SafeGuard Enterprise Administratorhilfe* version 7.0, *Mit Konfigurationspaketen arbeiten > Erzeugen eines Konfigurationspakets für Macs*) und kopieren Sie sie auf die Zielrechner.
5. Führen Sie auf den Zielrechnern das folgende Kommando aus:

    `/usr/bin/sgdeadmin --import-config /Pfad/zur/Datei.zip`

    Passen Sie */Pfad/zur/Datei* auf Ihre Einstellungen an. Dieses Kommando muss mit Administratorrechten ausgeführt werden. Wenn Sie Apple Remote Desktop verwenden, geben Sie **`root`** in das Feld **Benutzername** ein um festzulegen, welcher Benutzer das Kommando oben ausführt.

3 Konfiguration

Sophos SafeGuard Native Device Encryption für Mac OS X wird über das SafeGuard Management Center verwaltet. Das folgende Kapitel beschreibt ausschließlich die Mac-spezifischen Konfigurationseinstellungen. Alle Management Center-Standardfunktionen sind in der *SafeGuard Enterprise Administrator-Hilfe* beschrieben.

Hinweis:

SafeGuard Native Device Encryption für Mac wendet nur Richtlinien vom Typ **Geräteschutz** und **Allgemeine Einstellungen** an und ignoriert alle Richtlinieneinstellungen außer **Ziel**, **Verschlüsselungsmodus für Medien** und **Server-Verbindungsintervall (Min)**.

3.1 Zentral verwaltete Konfigurationsoptionen

Die folgenden Optionen werden zentral im Management Center konfiguriert:

Richtlinien

Richtlinien werden im SafeGuard Management Center zentral verwaltet. Um die Festplattenverschlüsselung zu starten, müssen die Einstellungen wie folgt vorgenommen werden:

1. Erzeugen Sie eine neue Richtlinie vom Typ **Geräteschutz**. Als **Ziel des Geräteschutzes** wählen Sie **Lokale Datenträger**, **Interner Speicher** oder **Boot-Laufwerke**. Geben Sie einen Namen für die Richtlinie ein und klicken Sie auf **OK**.
2. Wählen Sie für die Option **Verschlüsselungsmodus für Medien** die Einstellung **Volume-basierend**.

Eine neue Richtlinie für Geräteschutz wurde erstellt und für Festplattenverschlüsselung für Macs konfiguriert.

Hinweis: Stellen Sie sicher, dass die Richtlinie den Clients, die verschlüsselt werden sollen, zugewiesen ist. Wenn alle Endpoints zu verschlüsseln sind, können Sie die Richtlinie der obersten Ebene Ihrer Domäne oder Arbeitsgruppe zuweisen. Wenn sich IT-Mitarbeiter um die Installation der Endpoints kümmern, weisen Sie die Richtlinie erst zu, wenn die Clients den Endbenutzern übergeben wurden. Sonst besteht die Gefahr, dass die Endpoints zu bald verschlüsselt und IT-Mitarbeiter anstatt der eigentlichen Benutzer für FileVault 2 aktiviert werden.

Server-Verbindungsintervall

Mehr Informationen zu Richtlinien und zum Server-Verbindungsintervall finden Sie in der *SafeGuard Enterprise Administrator-Hilfe*.

3.2 Lokal verwaltete Konfigurationsoptionen

Die folgenden Optionen werden lokal auf dem Mac Client-Rechner konfiguriert:

- **Datenbankinformation synchronisieren**

  Verwenden Sie den Befehl **`sgdeadmin --synchronize`**, um das Synchronisieren von Datenbankinformation aus dem Management Center wie z.B. von Richtlinien und Schlüsseln etc. zu starten.

- **System Menü aktivieren oder deaktivieren**

  Verwenden Sie den Befehl **`sgdeadmin --enable-systemmenu`**, um das System-Menü in der rechten oberen Bildschirmecke zu aktivieren.

  Verwenden Sie den Befehl **`sgdeadmin --disable-systemmenu`**, um das System-Menü in der rechten oberen Bildschirmecke zu deaktivieren.

  Hinweis: Die Standardeinstellung nach der Installation von SafeGuard Native Device Encryption ist "deaktiviert".

  Weitere Informationen zum System-Menü finden Sie unter Sophos SafeGuard native Device Encryption System-Menü (Seite 13).

Eine vollständige Übersicht aller Kommandozeilen-Optionen (Seite 14) finden Sie in .

4 Arbeiten mit SafeGuard Native Device Encryption für Mac

In der separaten Schnellstart-Anleitung für SafeGuard Native Device Encryption werden die benutzerrelevanten Aspekte der Anwendung erklärt. Sie finden die aktuelle Version der Produktdokumentation auf unserer Dokumentations-Webseite unter http://www.sophos.com/de-de/support/documentation.aspx.

In den folgenden Abschnitten finden Sie Informationen zum Arbeiten mit SafeGuard Native Device Encryption for Mac aus der Sicht eines Administrators.

4.1 Wie funktioniert Verschlüsselung?

FileVault 2 schützt alle Daten mit XTS-AES-128 Datenverschlüsselung auf Laufwerksebene. Der Algorithmus wurde für 512-Byte Blöcke optimiert. Die Konvertierung von Klartext zu Chiffretext und umgekehrt hat kaum Auswirkungen auf das Benutzererlebnis, weil ihr vom System eine entsprechend niedrige Priorität zugewiesen wird.

Arbeitete man früher mit einer Festplattenverschlüsselung, war es notwendig, sich nach dem Start des Computers zweimal zu identifizieren: Einmal, um das verschlüsselte Startvolume zu entsperren (POA), und ein zweites Mal, um sich am Schreibtisch anzumelden.

Das ist jedoch nicht mehr notwendig. Benutzer geben ihr Kennwort bei der Pre-Boot Anmeldung ein und es wird automatisch auch an das Betriebssystem weitergegeben, sobald dieses hochgefahren ist und Anmeldeinformationen benötigt. Durch die Kennwort-Weiterleitung ist es nicht notwendig, dass sich Benutzer nach einem Neustart zweimal anmelden müssen.

Benutzer können ihr Kennwort jederzeit zurücksetzen, ohne dass deshalb eine neuerliche Verschlüsselung notwendig wäre. Der Grund ist ein mehrstufiges Verschlüsselungsschlüssel-System. Die Schlüssel, die von Benutzern verwendet werden (z.B. Kennwörter für die Anmeldung oder Wiederherstellungsschlüssel) sind abgeleitete Verschlüsselungsschlüssel. Der wirkliche Laufwerksverschlüsselungsschlüssel wird niemals einem Benutzer offengelegt.

Weiter Informationen zu FileVault 2 finden Sie in: *Apple Technical White Paper - Best Practices for Deploying FileVault 2 (Aug. 2012)*. Es kann von der Apple Website heruntergeladen werden.

4.2 Initialverschlüsselung

Wenn eine laufwerksbasierende Verschlüsselung des Systemlaufwerks in der Richtlinie definiert ist, dann wird die Verschlüsselung für den momentan angemeldeten Benutzer aktiviert. Gehen Sie auf Client-Seite wie folgt vor:

1. Bevor die Verschlüsselung beginnt, wird ein Dialog zur Eingabe von Benutzernamen und Passwort angezeigt. Geben Sie das Mac OS X Anmeldekennwort ein.

   Wenn der Dialog wackelt, ist das Passwort nicht korrekt. Versuchen Sie es erneut.

   Hinweis: Wenn das 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. Nähere Informationen finden Sie in den Logdateien. Der Standardspeicherort ist `/var/log/system.log`.

3. Die Festplattenverschlüsselung startet und wird im Hintergrund ausgeführt. Der Benutzer kann seine Arbeit fortsetzen.

Der Benutzer wird als der erste FileVault 2 Benutzer des Endpoints hinzugefügt.

4.3 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. Sie finden die entsprechende Schaltfläche im Einstellungsbereich, siehe Registerkarte Disk Encryption (Seite 13).

Benutzer mit lokalen Administrator-Rechnten können nicht daran gehindert werden, mithilfe der eingebauten FileVault 2 Funktionalität manuell zu versuchen, ihre Festplatte zu entschlüsseln. Jedoch werden sie zu einem Neustart aufgefordert, um die Entschlüsselung fertigzustellen. Sobald der Mac den Neustart abgeschlossen hat, wird SafeGuard native Device Encryption für Mac erneut die Verschlüsselung erzwingen, sofern eine entsprechende Richtlinie gesetzt ist.

4.4 FileVault 2 Benutzer hinzufügen

Nur Benutzer, die auf einem Endpoint für FileVault 2 registriert sind, können sich nach einem Neustart am System anmelden. Um einen Benutzer zu FileVault 2 hinzuzufügen, gehen Sie folgendermaßen vor:

1. Melden Sie sich mit dem Benutzer an, den Sie für FileVault 2 aktivieren wollen, während der Mac eingeschaltet bleibt.
2. Geben Sie im Dialog **Aktivieren Sie Ihren Benutzeraccount** den Benutzernamen und das OS X Anmeldekennwort dieses Benutzers ein. Wenn Sie Mac OS X Version 10.8 benutzen, werden nicht nur die Anmeldeinformationen dieses Benutzers abgefragt, sondern auch die eines anderen Benutzers, der bereits für FileVault 2 aktiviert ist. Unter Mac OS X Version 10.9 ist das nicht mehr notwendig.

Deshalb können sich, mit der Ausnahme von Mac OS X Version 10.8, Benutzer so einfach anmelden als würde keine Festplattenverschlüsselung verwendet.

4.5 FileVault 2 Benutzer löschen

Ein Benutzer kann im SafeGuard Management Center von der Liste der Benutzer, die einem Mac zugeordnet sind, gelöscht werden. Nach dem nächsten Synchronisieren wird der Benutzer auch am Endpoint von der Liste der FileVault 2 Benutzer gelöscht. Das bedeutet allerdings nicht, dass sich dieser Benutzer an diesem Mac nicht mehr anmelden kann. Um wieder für FileVault 2 aktiviert zu werden ist es ist lediglich notwendig, sich einmal anzumelden während der Mac läuft.

Wenn Sie verhindern wollen, dass ein bestimmter Benutzer einen Mac startet, dann markieren Sie ihn im Management Center als gesperrt. Dann wird er von der Liste der FileVault 2 Benutzer am Client gelöscht und es ist keine neuerliche Autorisierung möglich.

Alle FileVault 2 Benutzer können gelöscht werden bis auf den letzten. Wird der Besitzer gelöscht, wird der nächste Benutzer in der Liste als Besitzer markiert. In SafeGuard Native Device Encryption für Mac macht es keinen Unterschied, ob ein Benutzer Besitzer ist oder nicht.

4.6 Synchronisierung mit dem Backend

Während der Synchronisierung wird der Status der Clients an das SafeGuard Enterprise Backend gemeldet, Richtlinien werden aktualisiert und die Benutzer-Computer Zuordnung wird geprüft.

Die folgenden Informationen werden von den Clients gesendet und im SafeGuard Management Center angezeigt:

- Sobald ein Endpoint verschlüsselt ist, ist "POA" angehakt. Weitere Informationen, die angezeigt werden, umfassen Laufwerksname, Label, Typ, Status, Algorithmus und Betriebssystem.
- Neue FileVault 2 Benutzer werden auch im Management Center angezeigt.

Hinweis: Falls die SafeGuard Enterprise Client Software von einem Endpoint entfernt wird, sind der Endpoint und seine Benutzer im SafeGuard Management Center immer noch sichtbar. Aber der Zeitstempel des letzten Serverkontakts ändert sich nicht mehr.

Auf Client-Seite wird Folgendes aktualisiert:

- Richtlinien, die im Management Center geändert wurden, werden am Client nachgezogen.
- Benutzer, die im Management Center gelöscht oder gesperrt wurden, werden auch von der Liste der FileVault 2 Benutzer des Clients gelöscht.

4.7 Einstellungsbereich

Der Einstellungsbereich ermöglicht Ihnen, Einstellungen für spezifische Anwendungen oder für das System vorzunehmen. Nachdem Sie Sophos SafeGuard Native Device Encryption (oder Sophos SafeGuard File Encryption) auf einem Mac-Client installiert haben, erscheint das folgende Symbol in den Systemeinstellungen:

Klicken Sie auf das Symbol um den Einstellungsbereich zu öffnen. Der Inhalt der Registerkarte **Über** wird angezeigt.

Die Menüleiste ermöglicht Ihnen die folgenden Menü-Informationsfenster zu öffnen:

4.7.1 Registerkarte Über

In der Registerkarte **Über** erhalten Sie Informationen zur installierten Produktversion auf Ihrem Mac und zu Copyrights und eingetragenen Warenzeichen. Wenn SafeGuard File Encryption installiert ist, wird es ebenfalls aufgelistet.

Klicken Sie auf den Link im unteren Fensterbereich, um die Sophos-Webseite zu öffnen.

4.7.2 Registerkarte Server

Klicken Sie auf **Server**, um ein Fenster mit den folgenden Informationen und Funktionalitäten zu öffnen:

Serverinfo

- **Kontaktintervall:** zeigt das Intervall an, in dem die Synchronisation gestartet wird. Informationen darüber, wie dieses Intervall festgelegt wird, finden Sie unter *SafeGuard Enterprise Administrator-Hilfe > Richtlinieneinstellungen > Allgemeine Einstellungen*.
- **Letzter Serverkontakt:** zeigt Datum und Uhrzeit, 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. Eine Beschreibung, wie Sie diese Option ändern können, finden Sie unter Kommandozeilen-Optionen (Seite 14) (Befehl **`sgdeadmin --enable-server-verify`** oder **`sgdeadmin --disable-server-verify`**).

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. Siehe auch Manuelle (beaufsichtigte) Installation (Seite 5).

Synchronisieren

Klicken Sie diese Schaltfläche, um Datenbankinformationen, wie z.B. Richtlinien, manuell zu synchronisieren. Dies kann z.B. erforderlich sein, wenn Änderungen im SafeGuard Management-Center vorgenommen wurden.

Ist die Netzwerkverbindung unterbrochen, so erscheint das folgende Symbol:

Öffnen Sie die Logdatei, um Informationen über mögliche Ursachen zu erhalten.

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.

4.7.3 Registerkarte Benutzer

Klicken Sie auf **Benutzer**, um sich Information zu folgenden Punkten anzeigen zu lassen:

- Den **Benutzernamen** des momentan angemeldeten Benutzers.
- Die **Domäne**, die das Domänenverzeichnis auflistet, zu dem der Client gehört. Für lokale Benutzer wird hier der lokale Computername angezeigt.
- Die **SafeGuard Benutzer-GUID**, die die GUID wiedergibt, die für den Benutzer nach dem ersten Anmelden generiert wurde.

Im zweiten Fensterteil können Sie die folgende Option aktivieren oder deaktivieren:

- **System Menü für Native Device Encryption anzeigen**: Wenn aktiviert, wird das Sophos SafeGuard Native Device Encryption Symbol in der Menüleiste angezeigt. Siehe auch Sophos SafeGuard native Device Encryption System-Menü (Seite 13).

Im dritten Fensterteil werden Informationen über das **Benutzerzertifikat** angezeigt (sofern ein Benutzerzertifikat im SafeGuard Management Center zugewiesen wurde):

- **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.

4.7.4 Registerkarte Disk Encryption

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 eine Schaltfläche **Systemlaufwerk entschlüsseln** angezeigt. Sie kann betätigt werden, wenn FileVault 2 aktiviert ist, der momentan angemeldete Benutzer in FileVault 2 aktiv ist und der Sicherheitsbeauftragte eine Richtlinie gesetzt hat, die besagt, dass für den Client keine Verschlüsselung notwendig ist.

Hinweis: Wenn kein zentral gespeicherter Wiederherstellungsschlüssel verfügbar ist, kann der Helpdesk nicht bei der Kennwort-Wiederherstellung behilflich sein. Deshalb sollte der Wiederherstellungsschlüssel importiert werden. Dazu wird das Kommandozeilen-Tool verwendet: **`sgdeadmin --import-recoverykey`**. Wenn der Wiederherstellungsschlüssel weder dem Benutzer noch dem Sicherheitsbeauftragten bekannt ist, wird eine Entschlüsselung und neue Verschlüsselung des Laufwerks notwendig sein, um einen neuen Wiederherstellungsschlüssel zu erzeugen.

4.8 Sophos 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).

4.9 Kommandozeilen-Optionen

Terminal erlaubt Ihnen, Kommandos und Kommandozeilen-Optionen einzugeben. Folgende Kommandozeilen-Optionen stehen zur Verfügung:

Kommando-Name	Definition	Zusätzliche Parameter (optional)
`sgdeadmin`	Listet die verfügbaren Kommandos zusammen mit einer Kurzhilfe auf.	**`--help`**
`sgdeadmin --version`	Zeigt Version und Copyright des installierten Produkts an.	
`sgdeadmin --status`	Zeigt Systemstatusinformationen wie Versions-, Server- und Zertifikatsinformation an.	
`sgdeadmin --list-user-details`	Zeigt Informationen zum momentan angemeldeten Benutzer an.	**`--all`** zeigt Information für alle Benutzer an (sudo erforderlich). **`--xml`** zeigt Ausgabe im xml-Format an.
`sgdeadmin --list-policies`	Zeigt Richtlinien-spezifische Informationen an. Schlüssel-GUIDS werden wenn möglich in Schlüsselnamen aufgelöst. Fett ausgezeichnete Elemente zeigen einen persönlichen Schlüssel an.	**`--all`** zeigt Information für alle Benutzer an (sudo erforderlich). **`--xml`** zeigt Ausgabe im xml-Format an.
`sgdeadmin --synchronize`	Erzwingt den sofortigen Kontakt mit dem Server (erfordert eine funktionierende Serververbindung).	

Kommando-Name	Definition	Zusätzliche Parameter (optional)
sgdeadmin --import-recoverykey ["recoverykey"]	Importiert den FileVault 2 Wiederherstellungsschlüssel, überschreibt den bestehenden Wiederherstellungsschlüssel.	**--force** Der bestehende Wiederherstellungsschlüssel wird ohne nochmalige Bestätigung überschrieben. **"recoverykey"** Wenn der Wiederherstellungsschlüssel nicht sofort eingegeben wird, wird der Benutzer danach gefragt.
sgdeadmin --import-config "/Pfad/zur/Zieldatei"	Importiert die angegebene Konfigurations-Zipdatei Siehe auch Manuelle (beaufsichtigte) Installation (Seite 5). Das Kommando braucht Administrator-Rechte (sudo). **Hinweis:** Ziehen Sie komplette Pfade mit der Maus z.B. aus dem Finder in die Terminal-Anwendung.	
sgdeadmin --enable-server-verify	Schaltet die SSL-Serververifizierung für die Kommunikation mit dem SafeGuard Enterprise-Server ein. Nach der Installation ist die SSL-Serververifizierung standardmäßig aktiviert. Das Kommando braucht Administrator-Rechte (sudo).	
sgdeadmin --disable-server-verify	Schaltet die SSL-Serververifizierung für die Kommunikation mit dem SafeGuard Enterprise-Server aus. Das Kommando braucht Administrator-Rechte (sudo). **Hinweis:** Wir empfehlen nicht, diese Option zu verwenden, da dadurch eine Sicherheits-Schwachstelle entstehen kann.	
sgdeadmin --update-machine-info [--domain "domain"]	Aktualisiert die aktuell gespeicherten Computerinformationen, die verwendet werden, um diesen Client auf dem SafeGuard Enterprise Server zu registrieren. Das Kommando braucht Administrator-Rechte (sudo).	**--domain "domain"** Die Domain, die der Client für die Registrierung auf dem SafeGuard Enterprise Server verwenden sollte. Dieser Parameter ist nur erforderlich, wenn der Computer zu mehreren Domains gehört. Der Computer muss dieser Domain

Kommando-Name	Definition	Zusätzliche Parameter (optional)
	Hinweis: Verwenden Sie diesen Befehl erst nach dem Ändern der Domain oder Arbeitsgruppe, zu welcher der Computer gehört. Gehört der Computer zu mehreren Domains oder Arbeitsgruppen und führen Sie diesen Befehl aus, kann dies zu einer Änderung der Domain-Registrierung und Entfernung von persönlichen Schlüsseln und/oder FileVault 2 Benutzern führen.	hinzugefügt werden, ansonsten schlägt der Befehl fehl.

Die folgenden Befehle sind ausführlich in Abschnitt Lokal verwaltete Konfigurationsoptionen (Seite 7) beschrieben:

- **`sgdeadmin --enable-systemmenu`**
- **`sgdeadmin --disable-systemmenu`**
- **`sgdeadmin --synchronize`**

5 Wiederherstellung (Recovery)

Die Wiederherstellung bietet einen Weg, auf ein verschlüsseltes Laufwerk mittels eines zentral gespeicherten Wiederherstellungsschlüssels zuzugreifen. Dies ist notwendig, weil ein Benutzer sein Mac OS X Anmeldekennwort vergessen und keine weitere gültige Benutzer/Kennwort-Kombination vorhanden sein könnte.

5.1 Management der Wiederherstellungsschlüssel

Wenn alle für FileVault 2 aktivierten Benutzer eines Systems ihre Kennwörter vergessen, keine Anmeldeinformationen verfügbar sind und kein Wiederherstellungsschlüssel verfügbar ist, kann das verschlüsselte Laufwerk nicht entsperrt werden und es besteht kein Zugriff auf die Daten. Daten könnten unwiederbringlich verloren werden, deshalb ist es wesentlich, die Wiederherstellung entsprechend zu planen.

Ein neuer Wiederherstellungsschlüssel wird jeweils bei der Aktivierung der Festplattenverschlüsselung generiert. Wenn Sophos SafeGuard Native Device Encryption zum Zeitpunkt der Verschlüsselung noch nicht installiert ist, dann wird er dem Benutzer angezeigt, der in der Folge auch dafür verantwortlich ist, ihn gegen Verlust zu schützen. Ist Sophos SafeGuard Native Device Encryption installiert, dann wird er sicher an das SafeGuard Enterprise übermittelt und dort zentral gespeichert. Der Sicherheitsbeauftragte kann den Wiederherstellungsschlüssel jederzeit abfragen, wenn er benötigt wird. Weitere Informationen über den Wiederherstellungsvorgang finden Sie unter Mac OS X Anmeldekennwort vergessen (Seite 17).

Aber selbst wenn SafeGuard Native Device Encryption zum Zeitpunkt der Verschlüsselung nicht installiert war, kann der Wiederherstellungsschlüssel zentral verwaltet werden. Dafür ist es notwendig, ihn zu importieren. Der entsprechende Kommandozeilenbefehl ist **`sgdeadmin --import-recoverykey`**, siehe auch Kommandozeilen-Optionen (Seite 14). Der Wiederherstellungsschlüssel wird in Großbuchstaben gesendet.

Hinweis:

- Mac OS X 10.8: Der Wiederherstellungsschlüssel wird nicht überprüft, der Benutzer ist dafür verantwortlich, ihn korrekt einzugeben. Nur wenn das Format ungültig ist, wird ein Fehler angezeigt.
- Mac OS X 10.9: Der Wiederherstellungsschlüssel wird auf seine Gültigkeit geprüft.

Nähere Informationen, wie Sie überprüfen, ob für einen Client-Rechner ein Wiederherstellungsschlüssel vorhanden ist, finden Sie unter Registerkarte Disk Encryption (Seite 13).

Ein eventuell vorhandener institutioneller Wiederherstellungsschlüssel kann ebenfalls verwendet werden. Mehr Information dazu finden Sie auch in: OS X: How to create and deploy a recovery key for FileVault 2 unter support.apple.com/kb/HT5077

5.2 Mac OS X-Anmeldekennwort vergessen

Wenn ein Benutzer sein Mac OS X Anmeldekennwort vergisst und keine weitere gültige Benutzer/Kennwort-Kombination vorhanden ist, gehen Sie wie folgt vor:

1. Der Benutzer schaltet den Mac ein.

2. Der Benutzer klickt auf **?** im Anmeldedialog. (Alternativ könnte der Benutzer auch dreimal ein falsches Kennwort eingeben.)

   Die Merkhilfe für das Kennwort wird angezeigt und der Benutzer wird gefragt, ob er oder sie das Kennwort mithilfe des Recovery-Schlüssels zurücksetzen will.

3. Der Benutzer klickt auf das Dreieck neben dem Text, um zum nächsten Schritt (der Eingabe des Recovery-Schlüssels) zu gelangen:

   

4. Im SafeGuard Management Center öffnen Sie den Recovery-Assistenten indem Sie **Extras** > **Recovery** wählen und zeigen Sie den Recovery-Schlüssel für den konkreten Client-Rechner an.
5. Teilen Sie dem Benutzer den Recovery-Schlüssel zur Eingabe am Mac mit.

   Der Mac startet und der Benutzer wird gebeten, ein neues Kennwort und eine Merkhilfe einzugeben.

Nur Mac OS X 10.9: Der Recovery-Schlüssel wird erneuert, sobald er einmal zum Starten des Systems verwendet wurde. Der neue Recovery-Schlüssel wird automatisch erzeugt und an das SafeGuard Enterprise Backend gesendet, wo er gespeichert wird, um für das nächste Recovery verfügbar zu sein.

Hinweis: Seien Sie bei der Weitergabe von Recovery-Schlüsseln vorsichtig. Da ein Recovery-Schlüssel immer maschinenspezifisch und nicht benutzerspezifisch ist, könnte er auch mißbraucht werden, um unberechtigt Zugriff auf sensible Daten eines anderen Benutzers zu erhalten, die sich am selben Computer befinden.

6 Deinstallation auf dem Client-Rechner

Wenn Sie die Software von einem Client deinstallieren müssen, gehen Sie wie folgt vor:

1. Wechseln Sie auf dem Mac Client zu */Library*.
2. Wählen Sie den Ordner */Sophos SafeGuard DE*.
3. Wählen und doppelklicken Sie die Datei *Sophos SafeGuard DE Uninstaller.pkg*
4. Ein Assistent führt Sie durch die Deinstallation.

Hinweis: Es ist nicht notwendig, die Festplatte zu entschlüsseln, bevor Sie die Software deinstallieren.

Hinweis: Ein Benutzer mit Administrator-Rechten kann nicht daran gehindert werden, die Software zu deinstallieren. (Eine Richtlinie, die das bei Windows Clients verhindert, hat keine Auswirkung bei Mac Clients)

Hinweis: Das Uninstaller Package ist signiert und OS X versucht, diese Signatur zu validieren. Ist die Internetverbindung langsam oder nicht richtig konfiguriert, kann es eventuell zu Verzögerungen beim Deinstallationsvorgang von bis zu 20 Minuten kommen.

7 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie die SophosTalk-Community unter community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter 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.

8 Rechtliche Hinweise