SOPHOS
Security made simple.

SafeGuard Enterprise
Benutzerhilfe

Produktversion: 7
Stand: Dezember 2014

Inhalt

1 Über SafeGuard Enterprise 7.0

Diese Version von SafeGuard Enterprise unterstützt Windows 7 und Windows 8 auf Endpoints mit BIOS oder UEFI.

- Für Systeme mit BIOS können die Administratoren zwischen SafeGuard Enterprise Festplattenverschlüsselung und von SafeGuard Enterprise verwalteter BitLocker Verschlüsselung wählen. Die BIOS Version verwendet den BitLocker-eigenen Wiederherstellungsmechanismus.

  Hinweis: Wenn in diesem Handbuch von SafeGuard Power-on Authentication oder SafeGuard Festplattenverschlüsselung die Rede ist, dann bezieht sich das nur auf Windows 7 BIOS Endpoints.

- Für UEFI Systeme ist die Komponente für Festplattenverschlüsselung die von SafeGuard Enterprise verwaltete BitLocker Verschlüsselung. Für diese Endpoints bietet SafeGuard Enterprise verbesserte Challenge/Response Funktionalitäten. Nähere Informationen zu den unterstützten UEFI-Versionen und Beschränkungen hinsichtlich der Unterstützung von SafeGuard BitLocker Challenge/Response finden Sie in den Versionshinweisen unter http://downloads.sophos.com/readmes/readsgn_7_eng.html.

Hinweis: Wenn sich die Beschreibung nur auf UEFI bezieht, ist das explizit angegeben.

Die Tabelle zeigt, welche Komponenten verfügbar sind.

	SafeGuard Festplattenverschlüsselung mit SafeGuard Power-on Authentication (POA)	BitLocker mit Pre-Boot Authentication (PBA), von SafeGuard verwaltet	SafeGuard C/R Wiederherstellung für BitLocker Pre-Boot Authentication (PBA)
Windows 7 BIOS	**JA**	**JA**	
Windows 7 UEFI		**JA**	**JA**
Windows 8 BIOS		**JA**	
Windows 8 UEFI		**JA**	**JA**
Windows 8.1 BIOS		**JA**	
Windows 8.1 UEFI		**JA**	**JA**

Hinweis: SafeGuard C/R Wiederherstellung für BitLocker Pre-Boot Authentication (PBA) ist nur auf 64 bit Systemen verfügbar.

SafeGuard Festplattenverschlüsselung mit SafeGuard Power-on Authentication (POA) ist das Sophos Modul zur Verschlüsselung von Laufwerken auf Endpoints. Es wird mit einer von Sophos entwickelten Pre-Boot Authentication namens SafeGuard Power On Authentication (POA) geliefert, die Anmeldeoptionen wie Smartcard und Fingerabdruck sowie einen Challenge/Response Mechanismus für die Wiederherstellung unterstützt.

BitLocker mit Pre-Boot Authentication (PBA), von SafeGuard verwaltet, ist die Komponente, die das BitLocker Verschlüsselungsmodul und die BitLocker Pre-Boot Authentication aktiviert und verwaltet.

Sie ist für BIOS und UEFI Plattformen verfügbar:

- Die UEFI Version bietet zusätzlich einen SafeGuard Challenge/Response Mechanismus für die BitLocker Wiederherstellung für den Fall, dass Benutzer ihre Kennwörter vergessen. Die UEFI Version kann verwendet werden, wenn bestimmte Plattform-Anforderungen erfüllt sind. Beispielsweise muss die UEFI Version 2.3.1 sein. Nähere Informationen entnehmen Sie bitte den Versions-Infos.
- Die BIOS Version bietet die Wiederherstellungs-Erweiterungen des SafeGuard Challenge/Response Mechanismus nicht. Sie dient auch als Fallback falls die Anforderungen an die UEFI Version nicht erfüllt sind. Der Sophos Installer prüft, ob die Voraussetzungen erfüllt sind. Falls nicht, installiert er automatisch die BitLocker Version ohne Challenge/Response.

Mac Endpoints

Für Mac Endpoints sind folgende Produkte verfügbar: Sie werden auch von SafeGuard Enterprise verwaltet oder berichten zumindest an das Management Center.

	Sophos SafeGuard File Encryption for Mac 7.0	Sophos SafeGuard Native Device Encryption (FileVault 2-Verwaltung) 7.0
OS X 10.8	**JA**	**JA**
OS X 10.9	**JA**	**JA**
OS X 10.10	**JA**	**JA**

Die Beschreibungen in diesem Handbuch beziehen sich ausschließlich auf Windows. Für die Mac Versionen sehen Sie bitte in den entsprechenden Produkt-Handbüchern nach.

Sophos Mobile Encryption

Mit **Sophos Mobile Encryption** können Sie Dateien lesen, die von den SafeGuard Enterprise-Modulen **SafeGuard Cloud Storage** oder **SafeGuard Data Exchange** verschlüsselt wurden. Sie können Dateien mit einem lokalen Schlüssel verschlüsseln. Diese lokalen Schlüssel sind von einer Passphrase abgeleitet, die vom Benutzer eingegeben wurde. Sie können eine Datei nur entschlüsseln, wenn Sie die Passphrase kennen, die zur Verschlüsselung der Datei verwendet wurde. Nähere Informationen zu Sophos Mobile Encryption finden Sie unter www.sophos.com/de-de.

2 SafeGuard Enterprise auf Windows Endpoints

SafeGuard Enterprise ist eine modulare Sicherheits-Suite, die auf Richtlinien basierende Sicherheit für Endpoints plattformübergeifend mit vom Administrator definierten Richtlinien durchsetzt. SafeGuard Enterprise ist für den Endbenutzer einfach zu bedienen. 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 Module

- **SafeGuard Festplattenverschlüsselung**
  - **Power-on Authentication aktivieren**

    Die Benutzeranmeldung an das Gerät findet unmittelbar nach dem Einschalten statt. Nach erfolgreicher SafeGuard Power On Authentication (POA) erfolgt die Anmeldung am Betriebssystem automatisch. Sie können die SafeGuard POA auch deaktivieren. Die Authentisierung erfolgt dann durch das Betriebssystem.

  - **Volume-basierende Verschlüsselung**

    Alle Daten auf Volumes werden verschlüsselt (inkl. Boot-Dateien, Swapfiles, Datei für den Ruhezustand/Hibernation File, temporäre Dateien, Verzeichnisinformationen etc.) ohne dass sich der Benutzer in seiner Arbeitsweise anpassen oder auf Sicherheit achten muss.

- **BitLocker mit Pre-Boot Authentication, verwaltet durch SafeGuard Enterprise**

  SafeGuard Enterprise verwaltet das Microsoft BitLocker Verschlüsselungsmodul. Auf Systemen mit UEFI gibt es für die BitLocker Pre-Boot Authentication einen Challenge/Response Mechanismus, während auf Systemen mit BIOS der Recovery-Schlüssel vom Management Center abgerufen wird.

- **SafeGuard Data Exchange**
  - SafeGuard Data Exchange bietet einfachen Datenaustausch mit Wechselmedien auf allen Plattformen ohne Neuverschlüsselung.
  - Dateibasierende Verschlüsselung
  - Es werden alle mobilen beschreibbaren Medien, einschließlich externer Festplatten und USB-Sticks, transparent verschlüsselt.

- **SafeGuard File Encryption**
  - SafeGuard File Encryption ermöglicht die dateibasierende Verschlüsselung, hauptsächlich für Arbeitsgruppen zum sicheren Speichern von Daten in Netzwerkfreigaben.

- Dateien in Speicherorten, für die File Encryption Richtlinien gelten, werden direkt und ohne Benutzerinteraktion verschlüsselt.

- **SafeGuard Cloud Storage**

  SafeGuard Cloud Storage bietet dateibasierende Verschlüsselung von in der Cloud gespeicherten Daten. Die lokalen Kopien Ihrer Cloud-Daten werden transparent verschlüsselt und bleiben auch beim Speichern in der Cloud verschlüsselt.

Hinweis: Einige Funktionen, die in dieser Benutzerhilfe beschrieben sind, stehen u. U. auf Ihrem Computer nicht zur Verfügung. Ihr Sicherheitsbeauftragter legt die verfügbaren Funktionen in relevanten Richtlinien fest.

3 Empfohlene Sicherheitsmaßnahmen

Wenn Sie die hier beschriebenen, einfachen Schritte befolgen, sind die Daten auf Ihrem Computer jederzeit sicher und geschützt.

Fahren Sie Ihren Computer vollständig herunter oder versetzen Sie ihn in den Ruhezustand, wenn Sie ihn nicht benutzen.

Wenn sich SafeGuard Enterprise-geschützte Computer in bestimmten Energiesparmodi befinden, in denen das Betriebssystem nicht ordnungsgemäß heruntergefahren und bestimmte Hintergrundprozesse nicht vollständig beendet werden, besteht die Gefahr, dass sich Angreifer Zugriff auf die Verschlüsselungsschlüssel verschaffen. Der Schutz kann erhöht werden, wenn das Betriebssystem immer vollständig heruntergefahren oder in den Ruhezustand versetzt wird.

Wenn Ihr Computer nicht benutzt wird oder unbeaufsichtigt ist:

- Vermeiden Sie alle Arten von Energiesparmodi. Vermeiden Sie den Standbymodus. Der hybride Standbymodus ist eine Mischung aus Energiesparmodus und Standbymodus.
- Sperren Sie nicht einfach den Desktop und schalten den Bildschirm aus (oder schließen den Deckel Ihres mobilen Computers), wenn darauf kein ordnungsgemäßes Herunterfahren oder der Ruhezustand folgt. Die Einstellung einer zusätzlichen Kennwort-Abfrage nach dem Aufwecken des Computers bietet keinen ausreichenden Schutz.
- Fahren Sie den Computer immer ordnungsgemäß herunter oder versetzen Sie ihn in den Ruhezustand.

  Hinweis: Es ist wichtig, dass sich die Ruhezustand-Datei auf einem verschlüsselten Volume befindet. Normalerweise liegt sie auf Laufwerk C:\.

Befolgen Sie diese Schritte insbesondere, wenn Sie einen Laptop an öffentlichen Orten wie Flughäfen nutzen.

Wenn der Computer im Ruhezustand ist oder heruntergefahren wird, wird bei der nächsten Verwendung immer die SafeGuard Power-on Authentication aktiviert. Damit ist der Computer vollständig geschützt.

Stellen Sie sicher, dass allen Volumes ein Laufwerksbuchstabe zugewiesen ist.

Es werden nur Volumes mit zugewiesenem Laufwerksbuchstaben verschlüsselt. Folglich können Volumes ohne Laufwerksbuchstaben missbraucht werden, um an vertrauliche Daten im Klartext zu gelangen.

So wenden Sie diese Bedrohung ab:

- Wenn Sie ein Volume ohne Laufwerksbuchstaben auf Ihrem Computer finden, kontaktieren Sie Ihren Systemadministrator.
- Ändern Sie nicht die Laufwerkbuchstabenzuweisungen.

Wählen Sie sichere Kennwörter.

Sichere Kennwörter sind ein wesentlicher Bestandteil für den Schutz Ihrer Daten. Verwenden Sie sichere Kennwörter vor allem, um die Anmeldung an Ihren Computer zu sichern.

Ein sicheres Kennwort folgt diesen Regeln:

- Es ist lange genug um sicher zu sein: Eine Mindestlänge von 10 Zeichen ist zu empfehlen.
- Es enthält eine Kombination aus Buchstaben (Groß- und Kleinschreibung), Zahlen und Sonderzeichen/Symbolen.
- Es enthält keine allgemein gebräuchlichen Wörter oder Namen.
- Es ist schwer zu erraten, aber es ist leicht, es sich zu merken und korrekt einzutippen.

Ändern Sie Ihre Kennwörter in regelmäßigen Abständen. Teilen Sie sie niemandem mit und bewahren Sie sie nicht schriftlich auf.

4 Power-on Authentication aktivieren

Die SafeGuard Power-on Authentication ist ein Verfahren, bei dem Sie sich authentisieren müssen, bevor das eigentliche Betriebssystem startet. Danach wird Windows gestartet und Sie werden automatisch angemeldet. Analog wird verfahren, wenn sich ein Computer im Ruhezustand (Hibernation, Suspend to Disk) befindet und wieder eingeschaltet wird.

Erscheinungsbild der SafeGuard POA

Das Erscheinungsbild der SafeGuard Power-on Authentication kann an die Anforderungen des Unternehmens angepasst werden. Ein Sicherheitsbeauftragter kann die SafeGuard POA über die relevanten Richtlinieneinstellungen im SafeGuard Management Center anpassen.

Angepasst werden können:

- **Anmeldebild**

  Das Standard-Anmeldebild der SafeGuard Power-on Authentication ist im SafeGuard-Design gehalten. Das Anmeldebild kann durch eine Richtlinieneinstellung ausgetauscht werden. Das ermöglicht z. B. die Anzeige Ihres Unternehmenslogos.

- **Dialogtexte**

  Alle Texte in der SafeGuard Power-on Authentication werden in der Standardsprache, die in den Regions- und Sprachoptionen von Windows eingestellt ist, angezeigt. Sie können die Sprache, die in der SafeGuard POA verwendet wird, ändern, indem Sie die Standardsprache ändern. Die Sprache des Dialogtexts kann auch vom Sicherheitsbeauftragten in einer Richtlinie festgelegt werden.

4.1 Erste Anmeldung nach der Installation von SafeGuard Enterprise

Ist SafeGuard Enterprise mit SafeGuard Power-on Authentication installiert, kommt es beim ersten Systemstart nach der Installation von SafeGuard Enterprise auf einem Computer zu einem veränderten Start-Vorgang. Es erscheinen einige neue Startmeldungen, z. B. der Autologon-Bildschirm, weil sich nun SafeGuard Enterprise in den Startvorgang eingeschaltet hat. Anschließend startet das Windows-Betriebssystem.

Hinweis:

SafeGuard Enterprise arbeitet mit zertifikatsbasierter Anmeldung. Benutzerspezifische Schlüssel und Zertifikate werden jedoch erst nach einer erfolgreichen Windows-Anmeldung erzeugt.

Sie müssen sich bei der ersten Anmeldung nach der Installation zunächst einmal erfolgreich mit Ihren Anmeldedaten wie üblich an Windows anmelden. Danach werden Sie als SafeGuard Enterprise Benutzer registriert. Diese Registrierung ist die Bedingung dafür, dass Ihre Zugangsdaten beim nächsten Systemstart auch in der SafeGuard POA bekannt sind.

Die erfolgreiche Registrierung und der Erhalt aller notwendigen Daten wird als Balloon-Ausgabe angezeigt.

Wenn Sie den Computer neu starten, ist die SafeGuard POA aktiviert. Ab diesem Zeitpunkt geben Sie Ihre Windows-Anmeldedaten in der SafeGuard POA ein. Sie werden dann (wenn

die automatische Anmeldung an Windows aktiviert ist) ohne weitere Kennworteingabe auch an Windows angemeldet.

Die Anmeldung in der SafeGuard POA erfolgt mit Benutzername und Kennwort.

Hinweis: Die Einstellungen für die Computer, auf denen SafeGuard Enterprise installiert ist, werden vom Sicherheitsbeauftragten zentral im SafeGuard Management Center festgelegt und in Richtliniendateien an die Endpoints verteilt.

Ablauf der ersten Anmeldung

Die folgende Beschreibung zeigt den Ablauf der ersten Anmeldung an Ihren Computer, nachdem SafeGuard Enterprise installiert wurde. Voraussetzung dafür, dass die erste Anmeldung wie hier beschrieben abläuft, ist, dass die SafeGuard POA für Ihren Computer installiert und aktiviert ist.

4.1.1 SafeGuard Autologon

1. Der Computer startet und der SafeGuard Autologon Dialog wird angezeigt.
   - Ein SafeGuard Autouser wird angemeldet.
   - Besteht eine Verbindung zum SafeGuard Enterprise Server, so wird der Computer automatisch beim SafeGuard Enterprise Server registriert.
   - Der Maschinenschlüssel wird an den SafeGuard Enterprise Server geschickt und in der SafeGuard Enterprise Datenbank abgelegt.
   - Die Maschinenrichtlinien werden an den Computer geschickt.

4.1.2 Anmeldung an Windows

1. Der Windows-Anmeldedialog wird angezeigt.
2. SafeGuard Enterprise bietet die SafeGuard Enterprise- und die Windows-Authentisierungsmethode. Windows stellt für jede Authentisierungsmethode zwei Symbole zur Verfügung:
   - Klicken Sie auf **Anderer Benutzer**, um einen Dialog zur Eingabe der Anmeldeinformationen zu öffnen.
   - Klicken Sie auf das zweite Symbol (unter dem bereits ein Benutzername angezeigt wird), um einen Dialog zu öffnen, der bereits die Benutzerdaten des zuletzt angemeldeten Benutzers enthält. Es muss nur noch das Kennwort eingegeben werden.

   Wird Ihr Benutzername unter einem SafeGuard Enterprise Symbol angezeigt, klicken Sie auf dieses Symbol. Ist dies nicht der Fall, wählen Sie das SafeGuard Enterprise Symbol, unter dem **Anderer Benutzer** angezeigt wird.

3. Geben Sie wie gewohnt Ihre Windows-Benutzerdaten ein.
   - Ihr Benutzername und ein Hash-Wert Ihrer Anmeldeinformationen werden an den Server geschickt.
   - Benutzerrichtlinien, Zertifikate und Schlüssel werden erzeugt und an den Endpoint geschickt.

   Wenn alle Daten zwischen SafeGuard Enterprise Server und Ihrem Computer erfolgreich abgeglichen worden sind, stehen die Benutzerdaten auch in der SafeGuard Power-on Authentication zur Verfügung.

   Das bedeutet, dass Sie beim **nächsten Systemstart** nur noch in der SafeGuard Power-on Authentication Ihre Windows-Benutzerdaten (Benutzername und Kennwort) eingeben müssen und automatisch angemeldet werden.

Um die SafeGuard Power-on Authentication in vollem Umfang zu aktivieren, starten Sie den Computer neu. Nach dem Neustart schützt die SafeGuard Power-on Authentication Ihren Computer vor unberechtigtem Zugriff.

4.1.3 Anmeldung an der SafeGuard Power-on Authentication nach dem Neustart

1. Beim Neustart des Computers wird der Anmeldedialog der SafeGuard Power-on Authentication angezeigt.

   Die Zertifikate und Schlüssel sind vorhanden, und Sie können sich in der SafeGuard POA mit Ihren Windows-Anmeldeinformationen anmelden.

2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie auf **OK**.

   Ihre Anmeldeinformationen werden überprüft. Nach der Verifizierung Ihrer Anmeldeinformationen werden Sie automatisch an Windows angemeldet.

   Hinweis: Die durchgehende Anmeldung an Windows kann durch eine zentrale Einstellung deaktiviert sein. Ist dies der Fall, wird der Windows-Anmeldedialog angezeigt und Sie müssen die Anmeldeinformationen eingeben.

4.2 Anmeldung an der SafeGuard Power-on Authentication

Nach der vollständigen Aktivierung (initialer Benutzerabgleich und Neustart) der SafeGuard POA melden Sie sich durch Eingabe Ihrer Windows-Benutzerdaten im Anmeldedialog der SafeGuard Power-on Authentication an. Die Anmeldung an Windows erfolgt automatisch.

Hinweis: Durch Klicken auf die **Optionen** Schaltfläche im Anmeldedialog und Deaktivieren des Kontrollkästchens **Durchgehende Anmeldung an Windows** kann die automatische Anmeldung an Windows aufgehoben werden. Dies ist z. B. notwendig, um weiteren Benutzern die Anmeldung an der SafeGuard Power-on Authentication auf diesem Computer zu ermöglichen (siehe Registrieren weiterer SafeGuard Enterprise-Benutzer (Seite 14)). Ob die durchgehende Anmeldung aktiviert oder deaktiviert ist und ob es Ihnen möglich ist, diese Einstellung im Anmeldedialog zu ändern, wird in den für Sie geltenden Richtlinien vom Sicherheitsbeauftragten festgelegt.

Anmeldeverzögerung bei nicht erfolgreicher Anmeldung

Wenn die Anmeldung an der SafeGuard Power-on Authentication fehlschlägt, z. B. wegen eines falsch eingegebenen Kennworts, wird eine Warnmeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Fehlgeschlagene Anmeldeversuche werden protokolliert.

Computersperre

Wenn die eingestellte Anzahl an fehlgeschlagenen Anmeldeversuchen erreicht ist, wird Ihr Computer gesperrt. Um die Computersperre aufzuheben, starten Sie ein Challenge/Response-Verfahren (siehe Recovery über Challenge/Response oder mit Recovery-Schlüssel (Seite 76)).

4.2.1 Recovery für die Anmeldung

Für Recovery-Vorgänge, wenn Sie z. B. ihr Kennwort vergessen haben, bietet SafeGuard Enterprise verschiedene Optionen, die auf unterschiedliche Recovery-Szenarien zugeschnitten sind. Ihr Sicherheitsbeauftragter legt über die relevanten Richtlinieneinstellungen fest, welche Recovery-Methoden auf Ihrem Computer zur Verfügung stehen. Weitere Informationen finden Sie unter Recovery-Optionen (Seite 65).

4.3 Registrieren weiterer SafeGuard Enterprise-Benutzer

So ermöglichen Sie einem anderen Windows-Benutzer die Anmeldung an Ihrem Computer:

1. Schalten Sie den Computer ein.

   Der SafeGuard POA-Anmeldedialog wird angezeigt. Der zweite Windows-Benutzer kann sich nicht an der SafeGuard Power-on Authentication anmelden, es fehlen ihm die notwendigen Schlüssel und Zertifikate.

2. Damit sich der zweite Benutzer an der SafeGuard Power-on Authentication anmelden kann, muss ihm der Besitzer des Computers helfen.

   Hinweis: In den Standardeinstellungen ist festgelegt, dass der erste Benutzer, der sich nach der Installation anmeldet, zum Besitzer des Computers wird. Der Sicherheitsbeauftragte kann den Besitzer des Computers auch über eine Richtlinieneinstellung festlegen.

3. Klicken Sie im SafeGuard POA-Anmeldedialog auf **Optionen** und deaktivieren Sie das **Durchgehende Anmeldung an Windows** Kontrollkästchen. Melden Sie sich mit Ihren Anmeldeinformationen als Besitzer des Computers an.

   Der Windows-Anmeldedialog wird angezeigt.

4. Der zweite Benutzer gibt seine Windows-Anmeldedaten ein.
5. Sind die Benutzerrichtlinien, das Zertifikat und der Schlüssel des zweiten Benutzers auf dem Computer komplett vorhanden (ersichtlich an der entsprechenden Balloon-Ausgabe), wird der zweite Benutzer in SafeGuard Enterprise erzeugt.

   Der zweite Benutzer kann sich beim nächsten Neustart des Computers an der SafeGuard Power-on Authentication anmelden.

Hinweis: Sicherheitsbeauftragte können im SafeGuard Management Center Benutzer zur SafeGuard POA auf einer neuen Maschine hinzufügen. So zugewiesene Benutzer können sich auf diesen Computern im Rahmen der SafeGuard Power-on Authentication anmelden.

4.4 Temporäres Kennwort in der SafeGuard POA

SafeGuard Enterprise bietet Ihnen die Möglichkeit, das Kennwort in der SafeGuard POA vorübergehend zu ändern. Eine vorübergehende Änderung des Kennworts macht dann Sinn, wenn Sie glauben, bei der Eingabe Ihres Kennworts beobachtet worden zu sein.

Beispiel: Sie starten Ihr Notebook an einem öffentlichen Ort, zum Beispiel auf einem Flughafen. Dabei haben Sie das Gefühl, bei der Eingabe des Kennworts in der SafeGuard POA beobachtet worden zu sein. Da Sie keine Verbindung zum Active Directory haben, ist die Änderung des Windows-Kennworts nicht möglich.

Lösung: Sie ändern vorübergehend Ihr Kennwort für die SafeGuard POA und haben dadurch wieder die Gewissheit, dass kein Unbefugter Ihr Kennwort kennt. Wenn Sie wieder Verbindung zum AD haben, werden Sie automatisch aufgefordert, das temporäre Kennwort zu ändern.

1. Geben Sie im Anmeldedialog der SafeGuard POA das bestehende Kennwort ein.
2. Drücken Sie **F8**.

   Hinweis: Wenn Sie das bestehende Kennwort vor dem Drücken der **F8** Taste nicht eingeben, wird das als fehlgeschlagene Anmeldung gewertet und es wird eine entsprechende Meldung angezeigt.

3. Geben Sie im jetzt angezeigten Dialog das neue Kennwort ein und bestätigen Sie es.

   Sie werden darauf hingewiesen, dass die Änderung des Kennworts nur vorübergehend ist.

4. Klicken Sie auf **OK**.

   Hinweis: Wenn Sie diesen Dialog abbrechen, werden Sie mit dem alten Kennwort angemeldet!

   Der Windows-Anmeldedialog wird angezeigt.

   Hinweis: Es findet, auch wenn Ihr System so konfiguriert sein sollte, keine durchgehende Anmeldung an Windows mehr statt. Geben Sie hier das „alte Kennwort“ ein. Das temporäre Kennwort ist ausschließlich für die Anmeldung an der SafeGuard POA gültig!

5. Klicken Sie auf **OK**.

Sie werden an Windows angemeldet.

Zur Anmeldung in der SafeGuard POA können Sie jetzt nur noch das temporär gesetzte Kennwort verwenden. Das temporäre Kennwort gilt solange, bis das Kennwort bei der Windows-Anmeldung geändert wird. Erst dann ist auch wieder eine durchgehende Anmeldung - von der SafeGuard POA bis zu Windows - möglich.

Ändern des temporären Kennworts

Das in der SafeGuard POA temporär geänderte Kennwort muss später wieder geändert werden, damit die Kennwörter wieder synchron sind.

SafeGuard Enterprise fordert Sie automatisch zum Wechseln des Kennworts auf, wenn bei der Anmeldung an Windows wieder eine Verbindung zum Active Directory besteht.

Sie können den Dialog mit der Aufforderung zur Kennwortänderung auch schließen, ohne das Kennwort zu ändern. In diesem Fall wird der Dialog bei jeder Anmeldung angezeigt, bis das Kennwort tatsächlich geändert wird.

Hinweis: Das SafeGuard POA-Kennwort kann auch bei einer bestehenden Verbindung zum Active Directory vorübergehend geändert werden. In diesem Fall wird sofort nach der vorübergehenden Änderung des Kennworts in der SafeGuard POA bei der Anmeldung an Windows der Dialog zum Wechseln des Kennworts angezeigt. Sie können diesen Dialog ohne Änderungen schließen und das "alte Kennwort" zur Anmeldung verwenden. Die Änderung kann dann zu einem späteren Zeitpunkt vorgenommen werden.

4.5 Anmeldung an der SafeGuard Power-on Authentication mit Smartcard oder Token

Bei der Anmeldung mit Smartcard oder Token wird zwischen zwei verschiedenen Anmeldearten unterschieden:

- Die Anmeldung ist *ausschließlich mit Smartcard oder Token* erlaubt.
- Die Anmeldung ist *entweder mit Benutzernamen und Kennwort oder mit Smartcard oder Token* möglich.

Welche Anmeldung erlaubt ist, legt der Sicherheitsbeauftragte in einer Richtlinie fest.

Sie erhalten Ihre Smartcard/Ihren Token von Ihrem Sicherheitsbeauftragten. Dieser stellt die Smartcard/den Token für Sie aus. Sie können Ihre Windows-Anmeldedaten auch selbst auf Ihre Smartcard/Ihren Token aufbringen.

Hinweis: Smartcards und Token werden von SafeGuard Enterprise gleich behandelt. Deshalb werden im Produkt und im Handbuch die Begriffe "Token" und "Smartcard" gleichgesetzt. In den folgenden Abschnitten dieses Handbuchs wird nur noch der Begriff Token verwendet.

4.5.1 Erstmalige Anmeldung mit Token nach der Installation

Die erste Anmeldung mit Token läuft im Prinzip genauso ab, wie für die Anmeldung ohne Token beschrieben.

Haben Sie zu diesem Zeitpunkt bereits einen ausgestellten Token zur Verfügung, können Sie diesen durch Eingabe der PIN des Token zur Anmeldung an Windows verwenden.

Hinweis: Wir empfehlen, Ihren Token mit Ihren Windows-Anmeldeinformationen zu konfigurieren, bevor Sie den Computer neu starten (siehe Speichern von Windows-Anmeldeinformationen auf Ihrem Token (Seite 17)). Denn die für Sie gültigen Sicherheitsrichtlinien könnten eine verpflichtende Anmeldung an die SafeGuard Power-on Authentication mit Token vorschreiben. Befinden sich jedoch Ihre Anmeldeinformationen nicht auf dem Token, können Sie sich in der SafeGuard Power-on Authentication nicht anmelden.

4.5.2 Anmeldung an der SafeGuard POA mit Token

Voraussetzungen: Achten Sie darauf, dass die USB-Unterstützung im BIOS aktiviert ist. Die Token-Unterstützung muss initialisiert und der Token für Sie ausgestellt sein.

1. Stecken Sie den Token ein.

2. Schalten Sie den Computer ein.

   Der Dialog für die Anmeldung mit Token wird angezeigt.

   Hinweis: Wenn die für Sie geltenden Richtlinien eine Anmeldung mit Windows-Benutzerdaten erlauben und Sie entfernen den Token, werden Sie aufgefordert, Ihre Benutzerdaten zur Anmeldung einzugeben. Wird der Dialog für die Anmeldung mit Benutzername und Kennwort nicht angezeigt, können Sie sich in der SafeGuard Power-on Authentication ausschließlich mit Token anmelden.

3. Geben Sie Ihre Token-PIN ein.

   Die Anmeldung an der SafeGuard Power-on Authentication und an Windows (wenn **Durchgehende Anmeldung an Windows** im Anmeldedialog ausgewählt ist) wird ausgeführt.

4.5.3 Ändern der PIN

Sie können die PIN Ihres Token im Windows-Anmeldedialog ändern.

Wenn in der SafeGuard Power-on Authentication **Durchgehende Anmeldung an Windows** aktiviert ist, wird der Windows-Anmeldedialog in der Regel nicht angezeigt. Um den Windows-Anmeldedialog anzeigen zu lassen, deaktivieren Sie dieses Kontrollkästchen bei der SafeGuard POA-Anmeldung.

Hinweis: Eine Aufforderung zum Ändern der PIN wird automatisch angezeigt, wenn Ihr Sicherheitsbeauftragter Regeln vorgegeben hat, die einen Wechsel der PIN (z. B. in bestimmten Zeitintervallen) verlangen.

1. Wählen Sie im **PIN** Dialog zur Anmeldung an Windows das Kontrollkästchen **PIN wechseln**.
2. Geben Sie die PIN Ihres Token ein und klicken Sie auf **OK**.

   Der Dialog **PIN wechseln** wird angezeigt.

3. Geben Sie die neue PIN ein und bestätigen Sie diese.
4. Klicken Sie auf **OK**.

   Die PIN Ihres Token wird geändert und die Anmeldung an Windows wird fortgesetzt.

4.5.4 Speichern von Windows-Anmeldeinformationen auf dem Token

Befinden sich Ihre Windows-Anmeldeinformationen nicht auf Ihrem Token, so können Sie diese selbst auf dem Token speichern.

Hinweis: Wir empfehlen, Ihren Token bei der ersten Anmeldung zu konfigurieren. Denn die für Sie gültigen Sicherheitsrichtlinien könnten eine verpflichtende Anmeldung an der SafeGuard Power-on Authentication mit Token vorschreiben. Befinden sich keine Benutzerinformationen auf dem Token, können Sie sich in der SafeGuard Power-on Authentication nicht anmelden.

1. Verbinden Sie bei Ihrer ersten Anmeldung nach der Installation Ihren Token mit dem System, wenn der Windows-Anmeldedialog angezeigt wird.

   Wird ein leerer Token entdeckt, wird automatisch der **Token ausstellen** Dialog angezeigt.

2. Geben Sie Ihren Windows-Benutzernamen und Ihr Kennwort ein.
3. Bestätigen Sie das Kennwort.

4. Wählen Sie die Domäne aus bzw. geben Sie diese ein und klicken Sie auf **OK**.

   Mit den von Ihnen eingegebenen Daten wird eine Anmeldung an Windows versucht. Ist die Anmeldung erfolgreich, werden die Daten auf den Token geschrieben.

   Sie werden an Windows angemeldet.

Wenn für Sie die Anmeldung mit Token optional ist - Sie haben sich bereits einmal an die SafeGuard POA mit Benutzernamen und Kennwort angemeldet - können Sie Ihren Token auch später ausstellen.

Klicken Sie hierzu im SafeGuard POA-Anmeldedialog auf **Optionen** und deaktivieren Sie das **Durchgehende Anmeldung an Windows** Kontrollkästchen. Dadurch wird der Windows-Anmeldedialog angezeigt und Sie können die Anmeldeinformationen wie beschrieben auf den Token aufbringen.

4.5.5 Recovery für die Anmeldung mit Token

Wenn Sie einen nicht kryptographischen Token benutzen und Ihre PIN vergessen haben, erhalten Sie mit einer der beiden folgenden Recovery-Methoden wieder Zugang zu Ihrem Computer:

- Recovery mit Local Self Help (Seite 66).
- Recovery über Challenge/Response oder mit Recovery-Schlüssel (Seite 76).

Ihr Sicherheitsbeauftragter legt über die relevanten Richtlinieneinstellungen fest, welche Recovery-Methoden auf Ihrem Computer zur Verfügung stehen.

Um ein Recovery-Verfahren zu starten, klicken Sie im Dialog für die Anmeldung mit Token auf **Recovery**.

Hinweis: Diese Recovery-Verfahren sind für kryptographische Token nicht verfügbar. Wenden Sie sich bei Problemen im Rahmen der Anmeldung direkt an Ihren Sicherheitsbeauftragten.

4.5.6 Token entsperren

Wenn Sie die PIN zu oft falsch eingeben, wird Ihr Token gesperrt. Ihr Sicherheitsbeauftragter kann SafeGuard Enterprise so konfigurieren, dass der **Token entsperren** Dialog automatisch angezeigt wird, wenn dieser Fall eintritt.

Ihr Sicherheitsbeauftragter muss Ihnen die Administrator-PIN des Token mitteilen.

1. Geben Sie im **Token entsperren** Dialog die Administrator-PIN ein.
2. Geben Sie eine neue PIN ein und bestätigen Sie diese.

   Welche PIN Sie verwenden können, unterliegt den Regeln, die für PINs festgelegt wurden (z. B. kann festgelegt werden, dass PINs bestimmte Zeichenkombinationen enthalten müssen oder bereits verwendete PINs können verboten sein).

3. Klicken Sie auf **OK**.

Der Token wird entsperrt und die Anmeldung wird fortgesetzt.

Hinweis: Steht diese Funktionalität auf Ihrem Computer nicht zur Verfügung, erhalten Sie mit Challenge/Response wieder Zugriff auf Ihren Computer. Sie können jedoch weder die PIN noch Ihre Benutzeranmeldedaten mit Challenge/Response ändern.

4.5.7 Kryptographische Token - Kerberos

Bei der Verwendung von kryptographischen Token erfolgt die Authentisierung in der SafeGuard POA über das Zertifikat auf dem Token.

Für diese Anmeldeart benötigen Sie einen vollständig ausgestellten Token. Dieser muss Ihnen von Ihrem Sicherheitsbeauftragten bzw. einer anderen autorisierten Person zur Verfügung gestellt werden. Zur Anmeldung müssen Sie nur die PIN des Token eingeben. Ist auf Ihrem Computer ausschließlich diese Anmeldeart vorgesehen, können Sie sich ohne diesen Token nicht anmelden.

Hinweis: Hilfe bei der Anmeldung über Challenge/Response oder Local Self Help ist bei der Verwendung solcher Token nicht möglich. Wenden Sie sich bei Problemen im Rahmen der Anmeldung direkt an Ihren Sicherheitsbeauftragten.

4.5.8 Ändern des Zertifikats für die Anmeldung mit Token

Um das Zertifikat für die Anmeldung mit einem Token zu ändern oder zu erneuern, kann Ihr Sicherheitsbeauftragter ihrem Computer ein neues Zertifikat zuweisen. Nach der Synchronisierung zwischen Ihrem Computer und dem SafeGuard Enterprise Server gibt der Status-Dialog im SafeGuard Enterprise System Tray Icon an, dass Ihr Computer **Bereit für Zertifikatwechsel** ist.

Sie erhalten den neuen Token von Ihrem Sicherheitsbeauftragten.

So ändern Sie das Zertifikat auf Ihrem Computer:

1. Melden Sie sich an der SafeGuard Power-on Authentication mit Ihrem alten Token (Token oder Benutzername/Kennwort) ohne automatische Anmeldung an Windows an.

   Klicken Sie dazu entweder auf **Optionen** und deaktivieren Sie das Kontrollkästchen **Durchgehende Anmeldung an Windows**, oder melden Sie sich nach der automatischen Anmeldung an Windows noch einmal ab.

2. Melden Sie sich mit dem neuen Token an Windows an.

Der neue Token ist für die Anmeldung an der SafeGuard POA gültig. Der alte Token ist für die Anmeldung nicht mehr gültig.

4.6 Automatische Anmeldung an der SafeGuard POA mit Token

Voraussetzungen:

- Die USB-Unterstützung im BIOS ist aktiviert.
- Die Token-Unterstützung muss initialisiert sein und der Token ausgestellt sein.
- Der Sicherheitsbeauftragte hat Ihrem Computer die relevante Richtlinie zugewiesen.

Wurde Ihrem Computer eine entsprechende Richtlinie mit einer festgelegten Default-PIN zugeordnet, so können Sie sich automatisch an der SafeGuard Power-on Authentication mit einem Token anmelden. Sie müssen keine Anmeldeinformationen und auch keine PIN eingeben. Es wird eine durchgehende Anmeldung an der SafeGuard POA durchgeführt. Je nach den für Sie geltenden Richtlinieneinstellungen wird auch eine automatische Anmeldung an Windows durchgeführt.

So melden Sie sich automatisch an der SafeGuard Power-on Authentication mit einem Token an:

1. Stecken Sie den Token ein.
2. Schalten Sie den Computer ein.

Sie werden automatisch an der SafeGuard Power-on Authentication angemeldet. Je nach den für Sie geltenden Richtlinieneinstellungen wird auch eine automatische Anmeldung an Windows durchgeführt.

- Wenn die automatische Anmeldung erfolgreich durchgeführt werden konnte, wird Windows gestartet.
- Schlägt die automatische Anmeldung fehl, so werden Sie dazu aufgefordert, die Token-PIN einzugeben. Dann werden Sie an der SafeGuard Power-on Authentication angemeldet.

4.7 Virtuelle Tastatur

Sie haben die Möglichkeit, sich in der SafeGuard POA eine virtuelle Tastatur anzeigen zu lassen und z. B. Anmeldeinformationen durch Klick auf die am Bildschirm angezeigten Tasten einzugeben.

Voraussetzung: Der Sicherheitsbeauftragte hat die Anzeige der virtuellen Tastatur per Richtlinie aktiviert.

Um die virtuelle Tastatur in der SafeGuard POA einzublenden, klicken Sie im POA-Anmeldedialog auf die Schaltfläche **Optionen** und aktivieren Sie das Kontrollkästchen **Virtuelle Tastatur**.

Für die virtuelle Tastatur werden verschiedene Layouts angeboten. Das Layout kann auch mit denselben Einstellungen wie zum Ändern des SafeGuard POA Tastaturlayouts geändert werden (siehe Ändern des Tastaturlayouts (Seite 20)).

4.8 Tastaturlayout

Beinahe jedes Land hat ein eigenes Tastaturlayout. Das Tastaturlayout in der SafeGuard POA ist sehr wichtig für die Eingabe von Benutzernamen, Kennwort und Response Codes.

SafeGuard Enterprise übernimmt standardmäßig das Tastaturlayout, das in den Regions- und Sprachoptionen von Windows für den Windows-Standardbenutzer zum Zeitpunkt der Installation von SafeGuard Enterprise eingestellt ist.

Die Sprache des verwendeten Tastaturlayouts wird in der SafeGuard POA angezeigt, z. B. „EN“ für Englisch. Neben dem Standard-Tastaturlayout kann das US-Tastaturlayout (Englisch) gewählt werden.

4.8.1 Ändern des Tastaturlayouts

Das normale wie das virtuelle Tastaturlayout der SafeGuard Power-on Authentication kann nachträglich geändert werden.

1. Wählen Sie **Start > Systemsteuerung > Regions- und Sprachoptionen > Erweitert**.
2. Wählen Sie auf der Registerkarte **Regionale Einstellungen** die gewünschte Sprache aus.
3. Wählen Sie dann auf der Registerkarte **Erweitert** unter **Standardeinstellungen für Benutzerkonten** die Option **Alle Einstellungen auf das aktuelle Benutzerkonto und Standardbenutzerprofil anwenden**.

4. Klicken Sie auf **OK**.

Die SafeGuard POA merkt sich das bei der letzten erfolgreichen Anmeldung verwendete Tastaturlayout und aktiviert dieses beim nächsten Anmelden automatisch. Hierfür sind zwei Neustarts erforderlich. Wenn dieses gemerkte Tastaturlayout in den **Regions- und Sprachoptionen** abgewählt wird, bleibt es noch so lange erhalten, bis Sie eine andere Sprache ausgewählt haben.

Hinweis: Zusätzlich ist es notwendig, die Sprache des Tastatur-Layouts für andere, nicht-Unicode-Programme, zu ändern.

Falls die gewünschte Sprache nicht auf Ihrem System vorhanden ist, werden Sie von Windows evtl. aufgefordert, die Sprache zu installieren. Danach müssen Sie Ihren Computer zweimal neu starten, damit das neue Tastaturlayout von der SafeGuard POA eingelesen und dann auch über diese eingestellt werden kann.

Sie können das gewünschte Tastaturlayout der SafeGuard POA mit der Maus oder mit der Tastatur ändern (**Alt+Shift)**.

So ermitteln Sie, welche Sprachen auf dem System installiert und damit verfügbar sind: **Start > Ausführen > regedit**. **`HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`**.

4.9 Unterstützte Hotkeys und Funktionstasten in der SafeGuard Power-on Authentication

Bestimmte Hardware-Funktionalitäten und -Einstellungen können Probleme beim Starten von Computern verursachen, die dazu führen, dass der Rechner im Startvorgang hängen bleibt. Die SafeGuard Power-on Authentication unterstützt eine Reihe von Hotkeys, mit denen sich Hardware-Einstellungen und Funktionalitäten modifizieren lassen. Darüber hinaus sind in die auf dem Computer zu installierende .MSI-Datei Grey Lists integriert, die Funktionen abdecken, von denen ein solches Problemverhalten bekannt ist.

Wir empfehlen, vor jeder größer angelegten SafeGuard Enterprise Installation die aktuelle Version der SafeGuard POA-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung:
http://www.sophos.com/de-de/support/knowledgebase/110285.aspx

Sie können diese Datei anpassen, um die Hardware einer spezifischen Umgebung abzudecken.

Hinweis: Wenn Sie eine angepasste Datei definieren, wird nur diese verwendet, nicht die in der .msi-Datei integrierte Datei. Die Standarddatei wird nur dann verwendet, wenn keine SafeGuard POA-Konfigurationsdatei definiert ist oder gefunden wird.

Um die SafeGuard POA-Konfigurationsdatei zu installieren, geben Sie folgenden Befehl ein:

```
MSIEXEC /i <Client-MSI-Paket> POACFG=<Pfad der
POA-Konfigurationsdatei>
```

Darüber hinaus unterstützt die SafeGuard Power-on Authentication eine Reihe von Funktionstasten.

4.9.1 Hotkeys

Shift - F3 = USB Legacy Unterstützung (aus/an)

Shift - F4 = VESA Grafikmodus (aus/an)

Shift - F5 = USB 1.x und 2.0 Unterstützung (aus/an)

Shift - F6 = ATA Controller (aus/an)

Shift - F7 = nur USB 2.0 Unterstützung (aus/an) USB 1.x bleibt wie über **Shift - F5** gesetzt.

Shift - F9 = ACPI/APIC (aus/an)

Hotkeys Abhängigkeitsmatrix

Shift - F3	Shift - F5	Shift - F7	Legacy	USB 1.x	USB 2.0	Anmerkung
aus	aus	aus	an	an	an	3.
an	aus	aus	aus	an	an	Standard
aus	an	aus	an	aus	aus	1., 2.
an	an	aus	an	aus	aus	1., 2.
aus	aus	an	an	an	aus	3.
an	aus	an	aus	an	aus	
aus	an	an	an	aus	aus	
an	an	an	an	aus	aus	2.

1. **Shift - F5** deaktiviert sowohl die Unterstützung von USB 1.x als auch von USB 2.0.

   Hinweis: Wenn Sie **Shift - F5** drücken, reduziert sich die Wartezeit bis zum Starten der SafeGuard POA erheblich. Beachten Sie jedoch, dass wenn Sie an Ihrem Computer eine USB-Tastatur oder eine USB-Maus benutzen, diese Geräte durch Drücken von **Shift - F5** möglicherweise deaktiviert werden.

   Die POA kann die USB-Tastatur über BIOS SMM nutzen. USB-Token werden nicht unterstützt.

2. Wenn die USB-Unterstützung nicht aktiviert ist, versucht die SafeGuard POA, BIOS SMM zu benutzen anstatt den USB-Controller zu sichern und wiederherzustellen. Der Legacy-Modus kann in diesem Szenario funktionieren.
3. Die Legacy-Unterstützung ist aktiviert, die USB-Unterstützung ist aktiviert. Die SafeGuard POA versucht, den USB-Controller zu sichern und wiederherzustellen. Der Computer kann sich je nach eingesetzter BIOS-Version aufhängen.

Hinweis: Es besteht die Möglichkeit, dass die Änderungen, die über Hotkeys vorgenommen werden können, bereits bei der Installation des SafeGuard Enterprise Client über eine `.mst` Datei vordefiniert wurden.

Nach dem Ändern der Hardware-Einstellungen über die Hotkeys im Rahmen der SafeGuard POA wird ein Dialog angezeigt, der Sie zum Speichern der geänderten Einstellungen auffordert. In diesem Dialog wird eine Übersicht der zu speichernden Konfiguration angezeigt. Klicken Sie auf **Ja**, um die geänderten Einstellungen zu speichern. Sie sind nach dem nächsten Neustart Ihres Computers aktiv. Wenn Sie auf **Nein** klicken, werden die Änderungen nicht gespeichert und die alte Konfiguration bleibt nach dem nächsten Neustart Ihres Computers aktiv.

Wenn Sie in einem SafeGuard POA-Dialog **F5** drücken, wird ein Dialog angezeigt, der die zum Booten der POA verwendete Hotkey-Konfiguration zeigt. Wenn Hotkeys während des Start-Vorgangs geändert wurden, werden die relevanten Tastenstatus blau angezeigt. Die

Farbe Blau bedeutet, dass die Taste in diesem Zustand zum Starten der SafeGuard POA verwendet wurde. Unveränderte Werte werden schwarz angezeigt. Um den Dialog zu schließen, drücken Sie nochmals **F5** oder **Return**.

Nähere Informationen finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/107785.aspx.

4.9.2 Funktionstasten im Anmeldedialog

Hinweis: Die Funktionstasten sind keine Hotkeys!

F2 = Abbrechen des Autologon

F5 = Ruft einen Dialog auf, der die für das Starten der SafeGuard POA verwendete Hotkey-Konfiguration zeigt.

F8 = Ändern des Kennworts in der SafeGuard POA. Drücken Sie statt der **Eingabe**-Taste die Funktionstaste F8, um nach der Anmeldung den Kennwortwechsel in der SafeGuard POA anzustoßen.

ALT+Shift (linke **Alt**- und linke **Shift**-Taste) = Tastatur-Layout wechseln von Deutsch zu Englisch (oder umgekehrt).

Abbrechen und SafeGuard POA auf den Shutdown vorbereiten

Strg+Alt+Entf = Funktioniert auch, wenn nach einer Fehlauthentisierung der Computer sicher heruntergefahren werden soll. Diese Tastenkombination hat die gleiche Funktion wie die Schaltfläche **Herunterfahren**.

Hinweis: Wenn die Anmeldung mit Fingerabdruck aktiviert ist, können Sie durch Drücken von **Strg+Alt+Entf** in den SafeGuard POA-Dialog für die Anmeldung mit Benutzername und Kennwort wechseln. Weitere Informationen finden Sie unter Anmeldung mit Lenovo Fingerabdruck-Leser (Seite 25).

4.10 Kennwortsynchronisierung

SafeGuard Enterprise erkennt automatisch, wenn ein Windows-Kennwort geändert wurde und daher nicht mehr mit dem in der SafeGuard Enterprise Datenbank gespeicherten Kennwort übereinstimmt. Dies ist z. B. dann der Fall, wenn das Windows-Kennwort über VPN oder auf einem anderen Computer oder im Active Directory geändert wurde.

Wenn SafeGuard Enterprise einen solchen Fall erkennt, wird der Benutzer informiert und dazu aufgefordert, das alte Kennwort einzugeben. Danach wird das von SafeGuard Enterprise gespeicherte Kennwort durch das neue Windows-Kennwort aktualisiert.

Die Kennwort-Synchronisierung wird in den folgenden zwei Situationen durchgeführt:

- Während des Anmeldevorgangs
- Während eines Windows Sperren/Entsperren-Vorgangs

5 Anmelden an Windows

SafeGuard Enterprise bietet eine zusätzliche Methode zur Authentisierung.

Wenn Sie im Anmeldedialog der SafeGuard Power-on Authentication das Kontrollkästchen **Durchgehende Anmeldung an Windows** deaktivieren, wird der Windows-Anmeldebildschirm angezeigt. In diesem Dialog können Sie auch eine andere Authentisierungsmethode auswählen.

Hinweis: Das Verwenden einer anderen Authentisierungsmethode bedeutet nicht, dass SafeGuard Enterprise auf dem Computer nicht aktiv ist. Die Anmeldung an SafeGuard Enterprise erfolgt dann nicht im Rahmen der Windows-Anmeldung sondern nach der Anmeldung an Windows.

5.1 Anmeldung mit SafeGuard Enterprise

In der Regel werden Sie nach der Kennworteingabe in der SafeGuard Power-on Authentication (POA) automatisch an Windows angemeldet. Wenn Sie das Kontrollkästchen **durchgehende Anmeldung an Windows** im SafeGuard POA-Anmeldedialog deaktivieren und zur Anmeldung an Windows die SafeGuard Enterprise Methode verwenden, ist SafeGuard Enterprise nach der Anmeldung an Windows in seinem vollen Funktionsumfang einsatzbereit.

Die notwendigen Schlüssel sind vorhanden und alle Daten werden entsprechend den festgelegten Richtlinien ver- und entschlüsselt.

5.2 Anmeldung mit der Windows-Authentisierungsmethode

Sie haben die Möglichkeit, im Windows Anmeldebildschirm eine andere als die SafeGuard Enterprise Authentisierungsmethode zur Anmeldung an Windows zu verwenden.

Wenn Sie die Windows-Authentisierungsmethode verwenden, erfolgt die Anmeldung an SafeGuard Enterprise erst nach der Anmeldung an das Betriebssystem.

Nach der Anmeldung an Windows wird, falls notwendig, automatisch die SafeGuard Enterprise Authentisierungsapplikation gestartet, um die vollständige SafeGuard Enterprise Funktionalität zur Verfügung zu stellen.

Je nach den Anmeldeeinstellungen in der zentralen Verwaltung wird entweder ein Dialog zur Eingabe der Benutzerdaten oder ein PIN-Eingabe-Dialog angezeigt.

1. Geben Sie Ihre Benutzerdaten oder die PIN ein und klicken Sie auf **OK**.

   Erst jetzt steht Ihnen die Funktionalität von SafeGuard Enterprise zur Verfügung und Sie können z. B. auf verschlüsselte Daten zugreifen, wenn Sie den entsprechenden Schlüssel besitzen.

6 Anmeldung mit Lenovo Fingerabdruck-Leser

Hinweis: Die Anmeldung mit dem Lenovo Fingerabdruck-Leser wird nur für Windows 7 (BIOS) Endpoints unterstützt.

Benutzer müssen sich heute unterschiedliche Kennwörter und PINs merken, um Zugang zu Ihren Computern, Anwendungen und Netzwerken zu erhalten. Mit einem Fingerabdruck-Leser genügt es für die Anmeldung, den Finger über den Leser zu führen. Für die Anmeldung ist kein Kennwort oder Token nötig.

Es sind keine Anmeldedaten notwendig, die Sie verlieren oder vergessen könnten. Unberechtigte Personen können sich nicht durch Erraten von Anmeldedaten an Ihrem Computer anmelden. Die Anwendung von Fingerabdruck-Lesern vereinfacht somit die Anmeldung und bietet erhöhte Sicherheit.

SafeGuard Enterprise unterstützt die Anmeldung mit Fingerabdruck in der SafeGuard Power-on Authentication sowie in der Windows-Anmeldephase. So können Sie sich zum Beispiel an einem Lenovo-Notebook anmelden, indem Sie einfach ihren Finger über den im Notebook integrierten Fingerabdruck-Leser führen. Der Anmeldevorgang läuft danach automatisch ab. In Windows können Sie außerdem Ihren Computer per Fingerabdruck sperren und wieder entsperren.

Fingerabdruck-Leser sind direkt in bestimmte Lenovo Notebooks integriert. Die Anmeldung per Fingerabdruck ist auch über externe USB-Tastaturen möglich.

Hinweis:

- Es wird jeweils nur ein angeschlossener Fingerabdruck-Leser an einem Computer akzeptiert.
- Die Anmeldeverfahren Token und Fingerabdruck lassen sich auf einem Computer nicht miteinander kombinieren.
- Die Remote-Anmeldung mit Fingerabdruck wird nicht unterstützt.

6.1 Voraussetzungen

Für die Anmeldung mit Fingerabdruck müssen die folgenden Anforderungen erfüllt sein.

Allgemeine Voraussetzungen

- Lenovo Hardware
- Lenovo Fingerprint Reader in Notebook, USB-Tastatur mit Fingerabdruck-Leser
- Aktuelles BIOS wird empfohlen.
- SafeGuard Enterprise
- Die empfohlene herstellerspezifische Software-Version muss vor SafeGuard Enterprise installiert werden:
  - ThinkVantage Fingerprint for AuthenTec

oder

- ThinkVantage Fingerprint for UPEK.

- Der Sicherheitsbeauftragte muss die Fingerabdruck-Anmeldung per Richtlinie aktiviert haben.

Systemvoraussetzungen

- Windows 7, 32 Bit, 64 Bit
- Windows 8, 32 Bit, 64 Bit

Unterstützte Hardware

Informationen zur unterstützten Hardware für die Fingerabdruck-Anmeldung finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/108789.aspx.

Unterstützte Software

Informationen zur unterstützten Software für die Fingerabdruck-Anmeldung finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/111626.aspx.

6.2 Registrieren von Fingerabdrücken

Damit Sie sich per Fingerabdruck an Ihrem Notebook/Ihrem PC anmelden können, müssen Sie zunächst einen oder mehrere Fingerabdrücke über die empfohlene herstellerspezifische Software registrieren. Der Registrierungsvorgang verknüpft den registrierten Fingerabdruck mit Ihren Anmeldedaten (Benutzername und Kennwort).

Voraussetzungen: In der nachfolgenden Beschreibung wird davon ausgegangen, dass die empfohlene herstellerspezifische Software sowie SafeGuard Enterprise installiert sind.

1. Melden Sie sich an Ihrem Computer in der SafeGuard Power-on Authentication (POA) mit Ihrem Benutzernamen und Ihrem Kennwort an.
2. Registrieren Sie unter Anwendung der installierten herstellerspezifischen Software einen oder mehrere Ihrer Fingerabdrücke. Dieser Registrierungsvorgang verknüpft die Finger mit Ihren Windows-Anmeldedaten.
   a) Informationen dazu, wie Sie einen Fingerabdruck registrieren, finden Sie in der Hilfe zur ThinkVantage Fingerprint Software.
   b) Aktivieren Sie die Option **POA password in BIOS**. (Nur für UPEK. Für AuthenTec ist dieser Schritt nicht notwendig.)
   c) Damit Sie sich auch in der SafeGuard Power-on Authentication mit Fingerabdruck anmelden können, müssen Sie sich mindestens einmal in Windows mit Fingerabdruck anmelden, damit die Anmeldedaten auf den Fingerabdruck-Leser übertragen werden. Für UPEK reicht es aus, einen registrierten Finger über den Fingerabdruck-Leser zu führen. Für AuthenTec müssen Sie bei der ersten Anmeldung mit Fingerabdruck Ihr Windows-Kennwort eingeben.
3. Starten Sie Ihren Computer neu.

4. Um den registrierten Fingerabdruck zu testen, führen Sie nach dem Neustart den registrierten Finger über den Fingerabdruck-Leser.

   Bei Übereinstimmung mit dem registrierten Finger werden Sie nun automatisch an Windows angemeldet.

6.3 Anmeldung an der SafeGuard Power-on Authentication mit Fingerabdruck

Voraussetzungen:

- Der zuständige Sicherheitsbeauftragte hat in der für Sie wirksamen Richtlinie für die **Authentisierung** die Anmeldung mit Fingerabdruck aktiviert.
- Ein oder mehrere Fingerabdrücke sind registriert.

1. Starten Sie Ihren Computer neu.

   Der SafeGuard POA-Anmeldedialog für die Anmeldung mit Fingerabdruck wird angezeigt.

2. Führen Sie einen der registrierten Finger über den Leser.

   Wird der Fingerabdruck erkannt, so liest die SafeGuard Power-on Authentication die Anmeldedaten und überträgt sie an Windows.

   Hinweis: Im Anmeldevorgang werden Symbole mit kurzen Textmeldungen als Aufforderungen, Benachrichtigungen und Warnungen verwendet (siehe Symbole im Anmeldevorgang (Seite 27)).

Sie werden nun automatisch ohne Abfrage weiterer Daten an Windows angemeldet.

Hinweis:

- Sollte die Registrierung in Windows nicht vollständig durchgeführt worden sein - z. B. weil nach der Registrierung der Fingerabdrücke keine Ab-/Anmeldung an Windows vorgenommen wurde - wird in der SafeGuard POA zwar eine Übereinstimmung mit dem registrierten Fingerabdruck gefunden.

  Es sind jedoch keine Anmeldedaten vorhanden. In diesem Fall wird eine Fehlermeldung angezeigt, die Sie dazu auffordert, sich mit Ihrem Benutzernamen und Kennwort, jedoch ohne durchgehende Anmeldung an Windows anzumelden. Dadurch werden die Anmeldedaten auf den Fingerabdruck-Leser übertragen.

- Ob die durchgehende Anmeldung bei Windows aktiviert oder deaktiviert ist und ob es Ihnen möglich ist, diese Einstellungen im SafeGuard POA-Anmeldedialog für die Anmeldung mit Benutzername und Kennwort zu ändern, wird in den für Sie geltenden Richtlinien vom Sicherheitsbeauftragten festgelegt (siehe Anmeldung mit Benutzername und Kennwort (Seite 30)).

6.3.1 Symbole im Anmeldevorgang

Im Rahmen des Anmeldevorgangs mit Fingerabdruck in der SafeGuard Power-on Authentication werden Symbole als Aufforderungen, Benachrichtigungen und Warnungen verwendet. Sie werden im Anmeldevorgang zusammen mit einer kurzen Textmeldung angezeigt.

	Fordert Sie auf, den Finger über den Fingerabdruck-Leser zu führen.
	Gibt an, dass die Anmeldung mit Fingerabdruck im Moment nicht aktiv ist. Dies kann zum Beispiel der Fall sein, wenn das Modul für die Anmeldung mit Fingerabdruck noch nicht initialisiert ist.
	Gibt an, dass der Fingerabdruck-Leser gerade arbeitet und ausgelastet ist.
	Gibt an, dass der Fingerabdruck erfolgreich gelesen und eine Übereinstimmung gefunden wurde.
	Gibt an, dass der Fingerabdruck erfolgreich gelesen, jedoch keine Übereinstimmung gefunden wurde.
	Gibt an, dass der Fingerabdruck nicht eingelesen werden konnte. Führen Sie den Finger erneut über den Fingerabdruck-Leser.
	Gibt an, dass Sie Ihren Finger zu weit links (oder zu weit rechts) positioniert haben. Positionieren Sie Ihren Finger in der Mitte des Fingerabdruck-Lesers.

	Gibt an, dass die Bewegung des Fingers zu schräg ausgeführt wurde. Führen Sie den Finger erneut über den Fingerabdruck-Leser.
	Gibt an, dass Sie die Bewegung zu schnell ausgeführt haben. Führen Sie den Finger erneut über den Fingerabdruck-Leser.
	Gibt an, dass die Bewegung des Fingers zu kurz war. Führen Sie den Finger erneut über den Fingerabdruck-Leser.

6.3.2 Fehlgeschlagene Anmeldeversuche

Kann der Fingerabdruck nach fünf Versuchen nicht gelesen werden, so entspricht das im System einem fehlgeschlagenen Anmeldeversuch, der als Ereignis protokolliert wird. Für die Anmeldung tritt in diesem Fall eine Verzögerung in Kraft.

Wenn der Fingerabdruck zwar gelesen werden konnte, jedoch keine Übereinstimmung mit einem registrierten Fingerabdruck gefunden wird, so entsprechen ebenfalls fünf Versuche einem fehlgeschlagenen Anmeldeversuch, der als Ereignis protokolliert wird. Auch in diesem Fall tritt eine Anmeldeverzögerung in Kraft.

Die Anmeldeverzögerung verlängert sich mit jedem fehlgeschlagenen Anmeldeversuch.

6.3.3 Anmeldung mit Benutzername/Kennwort

Bei aktivierter Anmeldung mit Fingerabdruck können Sie sich trotzdem auch weiterhin mit Ihrem Benutzernamen und Ihrem Kennwort in der SafeGuard Power-on Authentication anmelden, falls zum Beispiel Ihr Fingerabdruck-Leser defekt ist.

1. Drücken Sie die **ESC**-Taste oder die Tastenkombination **Strg+Alt+Entf** im SafeGuard POA-Dialog für die Anmeldung mit Fingerabdruck.

   Daraufhin wird der SafeGuard POA-Dialog für die Anmeldung mit Benutzername und Kennwort angezeigt.

   Hinweis: Wenn Sie im SafeGuard POA-Dialog für die Anmeldung mit Benutzername und Kennwort die Tastenkombination **Strg+Alt+Entf** drücken, wird der Computer heruntergefahren. Die Tastenkombination **Strg+Alt+Entf** entspricht in diesem Dialog der Schaltfläche **Herunterfahren**.

   Der Dialog für die Anmeldung mit Benutzername und Kennwort wird auch dann automatisch angezeigt, wenn kein Fingerabdruck-Leser vorhanden ist, oder keine Benutzerdaten auf dem Fingerabdruck-Leser gefunden werden.

   Hinweis: Im Falle eines beschädigten Local Cache wird die Anmeldung mit Benutzername und Kennwort ebenfalls automatisch aktiviert. In diesem Fall ist der Computer gesperrt und die Anmeldung muss über ein Challenge/Response-Verfahren durchgeführt werden.

2. Um in den SafeGuard POA-Dialog für die Anmeldung mit Fingerabdruck zurückzukehren, drücken Sie nach Wunsch erneut die **Esc** Taste.

   Wenn Sie mit der **Esc**-Taste in den SafeGuard POA-Dialog für die Anmeldung mit Benutzername und Kennwort gewechselt haben, können Sie sich jedoch auch weiterhin durch Führen des Fingers über den Fingerabdruck-Leser anmelden, ohne dass Sie dazu vorher wieder in den SafeGuard POA-Dialog für die Anmeldung mit Fingerabdruck wechseln müssen.

6.4 Ändern des Kennworts

1. Bei aktivierter Anmeldung mit Fingerabdruck in der SafeGuard Power-on Authentication können Sie eine Kennwortänderung in Windows über **Strg+Alt+Entf** vornehmen.

   Bei der Kennwortänderung werden Sie dazu aufgefordert, Ihren Finger über den Fingerabdruck-Leser zu führen, um Ihr neues Kennwort auf den Fingerabdruck-Leser zu übertragen.

   Hinweis: Eine Kennwortänderung gilt jeweils für alle von Ihnen registrierten Finger.

6.4.1 Kennwortsynchronisierung

Sollte Ihr Windows-Kennwort nicht mehr mit dem auf dem Fingerabdruck-Leser gespeicherten Kennwort übereinstimmen, zum Beispiel weil während einer Kennwortänderung das neue Kennwort nicht auf den Fingerabdruck-Leser übertragen wurde, so können Sie Ihr Kennwort aktualisieren:

1. Starten Sie Ihren Computer neu.

2. Drücken Sie die **ESC**-Taste oder die Tastenkombination **Strg+Alt+Entf** im SafeGuard POA-Dialog für die Anmeldung mit Fingerabdruck.

   Daraufhin wird der SafeGuard POA-Dialog für die Anmeldung mit Benutzername und Kennwort angezeigt.

3. Klicken Sie auf **Optionen** und deaktivieren Sie das **Durchgehende Anmeldung an Windows** Kontrollkästchen.

   Hinweis: Ob die durchgehende Anmeldung an Windows aktiviert oder deaktiviert ist und ob es Ihnen möglich ist, diese Einstellungen im SafeGuard POA-Dialog für die Anmeldung mit Benutzername und Kennwort zu ändern, wird in den für Sie geltenden Richtlinien vom Sicherheitsbeauftragten festgelegt.

4. Melden Sie sich mit Ihrem Kennwort an.
5. Der Windows-Anmeldedialog wird angezeigt. Führen Sie einen Ihrer registrierten Finger über den Fingerabdruck-Leser.
6. Das System erkennt den Fingerabdruck, das mit dem Fingerabdruck verknüpfte Kennwort wird jedoch von Windows zurückgewiesen. Dies wird nicht als fehlgeschlagener Anmeldeversuch gewertet, es tritt keine Verzögerung für die Anmeldung in Kraft.

   Eine Meldung wird angezeigt, die auf ein geändertes Kennwort hinweist und Sie auffordert, Ihr aktuelles Windows-Kennwort einzugeben.

7. Geben Sie das korrekte Windows-Kennwort ein.

   Hinweis: Geben Sie hier ein falsches Windows-Kennwort ein, so wird eine fehlgeschlagene Anmeldung protokolliert und eine Anmeldeverzögerung tritt in Kraft. Schließen Sie die Eingabeaufforderung, ohne ein Kennwort einzugeben, so wird ebenfalls eine fehlgeschlagene Anmeldung protokolliert und eine Anmeldeverzögerung tritt in Kraft.

   Nach erfolgreicher Übertragung des Kennworts ist die Kennwortsynchronisierung abgeschlossen und Sie können das Kennwort zur Anmeldung verwenden.

6.5 Recovery für die Anmeldung mit Fingerabdruck

Für den Fall, dass die Anmeldung mit Fingerabdruck nicht funktioniert und Sie das Kennwort für die Anmeldung vergessen haben, bietet SafeGuard Enterprise folgende Recovery-Methoden:

- Recovery mit Local Self Help (Seite 66).
- Recovery über Challenge/Response oder mit Recovery-Schlüssel (Seite 76).

Ihr Sicherheitsbeauftragter legt über die relevanten Richtlinieneinstellungen fest, welche Recovery-Methoden auf Ihrem Computer zur Verfügung stehen.

Um ein Recovery-Verfahren zu starten, klicken Sie im Dialog für die Anmeldung mit Fingerabdruck auf **Recovery**.

Hinweis: Ein Recovery-Verfahren kann dazu führen, dass Sie beim Starten des Computers das Kennwort wechseln müssen, z. B. um ein Recovery-Verfahren zu ermöglichen, wenn Sie Ihr Kennwort vergessen haben. In diesem Fall wird Ihnen auch die Aktualisierung der Daten für die Fingerabdruck-Anmeldung angeboten.

7 Festplattenverschlüsselung

Für die Festplattenverschlüsselung bietet SafeGuard Enterprise folgende Varianten, abhängig vom Betriebssystem, das auf den Endpoints verwendet wird:

- **Windows 7 Endpoints:**
  - Informationen zur SafeGuard Festplattenvollverschlüsselung mit SafeGuard Power-on Authentication finden Sie unter SafeGuard Festplattenverschlüsselung (Seite 32).
  - Informationen zur BitLocker Drive Encryption mit Windows-Anmeldung finden Sie unter BitLocker Drive Encryption (Seite 35)
- **Windows 8 Endpoints:** Informationen zur BitLocker Drive Encryption mit Windows-Anmeldung finden Sie unter BitLocker Drive Encryption (Seite 35)

7.1 SafeGuard Festplattenverschlüsselung

SafeGuard Enterprise bietet transparente, volume-basierende Festplattenverschlüsselung. Welche Volumes (Laufwerke) auf Ihrem Computer verschlüsselt werden, legt Ihr Sicherheitsbeauftragter in den für Sie geltenden Richtlinien fest.

7.1.1 Transparente Verschlüsselung

Die Dateien auf einem verschlüsselten Volume werden transparent verschlüsselt. Sie werden beim Öffnen, Bearbeiten und Speichern von Dateien nicht zur Verschlüsselung oder Entschlüsselung aufgefordert. Wenn Sie die Dateien öffnen, werden sie entschlüsselt und Sie können sie bearbeiten. Beim Speichern werden die Dateien automatisch wieder verschlüsselt.

Wenn Sie Dateien von einem verschlüsselten Laufwerk auf einen unverschlüsselten Speicherort auf Ihrem Computer kopieren oder verschieben (auch mit **Speichern unter**), werden die Dateien entschlüsselt. Die Dateien werden am neuen Speicherort im Klartext abgelegt.

7.1.2 Initialverschlüsselung

Während der initialen Konfiguration von durch SafeGuard Enterprise geschützten Computern können Verschlüsselungsrichtlinien erstellt und in einem Konfigurationspaket an die Computer verteilt werden.

Wenn die erste Verschlüsselungsrichtlinie auf Ihrem Computer wirksam wird, wird die Initialverschlüsselung gemäß den erhaltenen Richtlinieneinstellungen durchgeführt.

7.1.2.1 Initialverschlüsselung bei volume-basierender Verschlüsselung

Nach dem Erhalt einer Richtlinie für die volume-basierende Verschlüsselung nach der Installation von SafeGuard Enterprise auf Ihrem Computer wird die volume-basierende Initialverschlüsselung automatisch gestartet.

Die volume-basierende Verschlüsselung läuft im Hintergrund und Sie können weiterhin mit Ihrem Computer arbeiten.

Hinweis: Versetzen Sie den Computer während der Initialverschlüsselung der System-Partition (d. h. der Partition, auf der sich die Datei hiberfil.sys befindet) nicht in den Ruhezustand. Starten Sie nach Abschluss der Initialverschlüsselung der System-Partition den Computer neu, um sicherzustellen, dass der Ruhezustand wieder problemlos funktioniert.

7.1.2.2 Einschränkungen für die initiale Verschlüsselung von durch SafeGuard Enterprise geschützte Computer

Während der initialen Konfiguration von durch SafeGuard Enterprise geschützten Computern können Verschlüsselungsrichtlinien erstellt und in einem Konfigurationspaket an die Computer verteilt werden. Wenn der SafeGuard Enterprise Client jedoch nicht direkt nach der Installation des Konfigurationspakets eine Verbindung mit dem SafeGuard Enterprise Server herstellt, sondern vorübergehend offline ist, werden nur Verschlüsselungsrichtlinien mit der folgenden spezifischen Einstellung sofort auf dem durch SafeGuard Enterprise geschützten Computer wirksam:

- Geräteschutz vom Typ volume-basierend unter Anwendung des **definierten Computerschlüssels** als Verschlüsselungsschlüssel

Damit alle anderen Richtlinien, die Verschlüsselung mit benutzerdefinierten Schlüsseln umfassen, auf einem durch SafeGuard Enterprise geschützten Computer wirksam werden, muss das entsprechende Konfigurationspaket auch noch einmal der OU des Computers zugewiesen werden. Die benutzerdefinierten Schlüssel werden dann erst erstellt, wenn der SafeGuard Enterprise Client wieder eine Verbindung zum SafeGuard Enterprise Server hergestellt hat.

Die Ursache hierfür ist, dass der **definierte Computerschlüssel** bereits beim ersten Neustart nach der Installation auf dem durch SafeGuard Enterprise geschützten Computer erzeugt wird. Benutzerdefinierte Schlüssel können dagegen erst auf dem Computer erzeugt werden, wenn er beim SafeGuard Enterprise Server registriert ist.

7.1.3 Volume-basierende Festplattenverschlüsselung

Die Volume-basierende Verschlüsselung für ein Volume des durch SafeGuard Enterprise geschützten Computers startet automatisch, wenn dies vom Sicherheitsbeauftragten per Richtlinie festgelegt wurde.

1. Es wird ein Dialog angezeigt und Sie werden aufgefordert, einen Schlüssel auszuwählen, der Ihnen Zugriff auf dieses Volume gibt.

   Hinweis: Jeder Benutzer, der diesen Schlüssel in seinem Schlüsselring hat, kann auf dieses Volume zugreifen. Der Umfang der angebotenen Schlüssel wird von Ihrem Sicherheitsbeauftragten bestimmt. Ist vom Sicherheitsbeauftragten ein bestimmter Schlüssel festgelegt worden, entfällt die Möglichkeit, einen Schlüssel auszuwählen.

2. Nach dem Klicken auf **OK** startet die Verschlüsselung.

   Während des Verschlüsselungsvorgangs zeigt ein Encryption Viewer den Fortschritt der Verschlüsselung des zu verschlüsselnden Volumes an. Falls vorhanden, zeigt der Encryption Viewer auch die bereits vorhandenen verschlüsselten Volumes. Er wird in der Windows Task-Leiste minimiert angezeigt. Ein einfacher Mausklick auf das Symbol zeigt den Encryption Viewer an. Wenn Sie den Encryption Viewer minimieren wollen, können Sie eine Benachrichtigung, dass die Verschlüsselung abgeschlossen ist, anfordern. Wählen Sie dazu die Option **Benachrichtigung anzeigen bevor das Fenster geschlossen wird**. Der Viewer wird automatisch geschlossen, wenn die Verschlüsselung abgeschlossen ist. Sie können das verschlüsselte Volume verwenden wie jedes andere unverschlüsselte Volume Ihres Computers.

   Hinweis:

   - Die Volume-basierende Verschlüsselung/Entschlüsselung wird für Volumes ohne Laufwerksbuchstaben nicht unterstützt.
   - Für Windows 7 Professional, Enterprise und Ultimate wird auf den Endpoints eine Systempartition angelegt, der kein Laufwerksbuchstabe zugeordnet ist. Diese System-Partition kann nicht von SafeGuard Enterprise verschlüsselt werden.
   - Wenn für ein Volume oder einen Volume-Typ eine Verschlüsselungsrichtlinie existiert und die Verschlüsselung des Volumes schlägt fehl, darf der Benutzer nicht auf das Volume zugreifen.
   - Endpoints können während der Verschlüsselung/Entschlüsselung heruntergefahren und neu gestartet werden.
   - Wenn auf die Entschlüsselung die Deinstallation folgt, empfehlen wir, den Endpoint nicht in einen Energiesparmodus oder den Ruhezustand zu versetzen.
   - Wenn nach der volume-basierenden Verschlüsselung eine Richtlinie auf einen Endpoint angewendet wird, die die Entschlüsselung erlaubt, ist Folgendes zu beachten: Nach einer vollständigen volume-basierenden Verschlüsselung muss der Endpoint mindestens einmal neu gestartet werden, bevor die Entschlüsselung gestartet werden kann.

   Hinweis:

   Im Gegensatz zur SafeGuard BitLocker Drive Encryption unterstützt die Volume-basierende SafeGuard-Verschlüsselung keine GUID Partition Table (GPT) Disks. Die Installation wird abgebrochen, wenn eine solche Disk gefunden wird. Wenn dem System später eine GPT Disk hinzugefügt wird, werden Volumes auf der Disk verschlüsselt. Beachten Sie, dass die SafeGuard Recovery-Tools – wie z. B. BE_Restore.exe und recoverkeys.exe – mit solchen Volumes nicht zurechtkommen. Sophos empfiehlt dringend, eine Verschlüsselung von GPT Disks zu vermeiden. Zum Entschlüsseln von Volumes, die unbeabsichtigt verschlüsselt wurden, ändern Sie Ihre SGN-Richtlinien entsprechend und ermöglichen Sie dem Benutzer die Entschlüsselung.

7.1.3.1 Zugriffsrestriktionen

SafeGuard Enterprise verweigert den Zugriff auf Volumes in den folgenden Fällen:

Volumes mit fehlgeschlagener Verschlüsselung

Ist eine Richtlinie vorhanden, die die Verschlüsselung eines Volumes oder eines Volume-Typs definiert, und der Verschlüsselungsvorgang schlägt fehl, so wird der Zugriff auf das Volume verweigert.

Wenn Sie versuchen, auf das Volume zuzugreifen, wird eine entsprechende Meldung angezeigt.

Unidentified File System Objects

Unidentified File System Objects sind Volumes, die von SafeGuard Enterprise nicht eindeutig als verschlüsselt oder unverschlüsselt identifiziert werden können.

Ist eine Richtlinie vorhanden, die die Verschlüsselung eines Volumes dieser Art definiert, so wird der Zugriff auf das Volume verweigert. Wenn Sie versuchen, auf das Volume zuzugreifen, wird eine entsprechende Meldung angezeigt.

Wenn für ein Unidentified File System Object keine Verschlüsselungsrichtlinie vorhanden ist, können Sie auf das Volume zugreifen.

7.2 BitLocker Drive Encryption

Die BitLocker-Laufwerkverschlüsselung ist ein in Windows Betriebssysteme integriertes Feature für die Festplattenverschlüsselung mit Pre-Boot Authentication. BitLocker bietet Datenschutz durch die Verschlüsselung von Boot- sowie Daten-Laufwerken. SafeGuard Enterprise verwaltet BitLocker Drive Encryption und stellt zusätzliche Funktionen bereit.

7.2.1 Verschlüsselungsrichtlinien für BitLocker

Der Sicherheitsbeauftragte kann eine Richtlinie für die Verschlüsselung im SafeGuard Management Center anlegen und diese an die BitLocker Endpoints verteilen. Die Richtlinie wird daraufhin auf den Endpoints ausgeführt.

Die BitLocker-Clients werden transparent im SafeGuard Management Center verwaltet. Es kann ein und dieselbe Verschlüsselungsrichtlinie für Mac, SafeGuard Festplattenvollverschlüsselung und BitLocker-Clients verwendet werden. SafeGuard Enterprise kennt den Status der Clients und wählt die BitLocker-Verschlüsselung entsprechend.

7.2.2 Authentisierung mit BitLocker

BitLocker bietet eine Reihe von Optionen für die Authentisierung. Der Sicherheitsbeauftragte kann die verschiedenen Anmeldemodi in einer Richtlinie im SafeGuard Management Center einstellen und sie an die BitLocker Endpoints verteilen.

Für SafeGuard Enterprise BitLocker-Benutzer sind folgende Anmeldemodi verfügbar:

- TPM
- TPM + PIN
- TPM + Systemstartschlüssel
- Systemstartschlüssel (ohne TPM)
- Kennwort (ohne TPM)

Sie müssen diese Anmeldeinformationen beim Starten Ihres BitLocker-Endpoint angeben.

Trusted Platform Module (TPM)

Das TPM ist ein Modul auf dem Motherboard, das einer Smartcard ähnelt und Verschlüsselungsfunktionen sowie Vorgänge für die digitale Signatur ausführt. Es ist in der

Lage, Benutzerschlüssel anzulegen, zu speichern und zu verwalten. Das TPM ist gegen Angriffe geschützt.

Systemstartschlüssel auf USB-Stick

Die externen Schlüssel können auf einem ungeschützten USB-Stick gespeichert werden. Sie müssen den USB-Stick beim Starten zwecks Authentisierung einstecken.

7.2.3 Verschlüsselung auf einem durch BitLocker geschützten Computer

Wenn die Verschlüsselungsrichtlinie an einen durch BitLocker geschützten Computer gesendet wird, generiert BitLocker die Verschlüsselungsschlüssel, bevor der Computer neu gestartet und die Initialverschlüsselung durchgeführt wird. Abhängig vom System kann das Verhalten leicht abweichen.

Endpoints mit TPM

Ihr Sicherheitsbeauftragter kann TPM, TPM + PIN, TPM + Systemstartschlüssel, Systemstartschlüssel oder Kennwort als Anmeldemodus für BitLocker einrichten. Wenn TPM als Anmeldemodus eingerichtet ist, speichert BitLocker seine eigenen Verschlüsselungsschlüssel in einem Hardwaregerät namens Trusted Platform Module (TPM) Sicherheitshardware. Die Schlüssel werden nicht auf der Festplatte des Computers gespeichert. Während des Startvorgangs muss das BIOS (Basic Input/Output System) auf TPM zugreifen können. Wenn Sie den Computer starten, werden diese Schlüssel automatisch von TPM an BitLocker übergeben.

Endpoints ohne TPM

Wenn Ihr Computer nicht mit TPM ausgestattet ist, werden Sie entweder nach einem Kennwort gefragt oder aufgefordert, über einen USB-Stick einen BitLocker Systemstartschlüssel zu generieren, um die Verschlüsselungsschlüssel zu speichern. Es öffnet sich ein Dialog, in dem die gültigen Ziellaufwerke zum Speichern des Systemstartschlüssels angezeigt werden. Später müssen Sie den Stick immer dann einstecken, wenn Sie den Computer starten.

Hinweis: Bei Bootlaufwerken ist es wesentlich, dass der Systemstartschlüssel verfügbar ist, wenn Sie den Endpoint starten. Der Systemstartschlüssel kann daher nur auf einem Wechselmedium gespeichert werden.

Bei Daten-Volumes kann der BitLocker Systemstartschlüssel auf einem Boot-Volume gespeichert werden, das bereits verschlüsselt ist. Dies erfolgt automatisch, wenn der Sicherheitsbeauftragte **Auto-Unlock** als Anmeldemodus für Nicht-Boot-Volumes eingerichtet hat. Wählen Sie ansonsten ein Wechselmedium aus, das unter **Gültiges Ziellaufwerk** als Speicherort angezeigt wird.

BitLocker Recovery-Schlüssel

Für die BitLocker Recovery sieht SafeGuard Enterprise ein Challenge/Response-Verfahren vor, das es erlaubt, Informationen vertraulich auszutauschen und die BitLocker Recovery-Schlüssel beim Helpdesk abzurufen (siehe Challenge/Response für BitLocker-Benutzer (Seite 82) und BitLocker Recovery-Schlüssel (Seite 83)).

Damit Recovery-Vorgänge über Challenge/Response durchgeführt werden können, müssen die notwendigen Daten für den Helpdesk verfügbar sein. Die für die Recovery benötigten Daten werden in die SafeGuard Enterprise-Datenbank geladen und dort gespeichert.

Hinweis: Wenn ein mit BitLocker verschlüsseltes Volume in einem Computer durch ein neues Volume ersetzt wird, dieses den Volume-Buchstaben des alten Volume erhält und ebenfalls mit BitLocker verschlüsselt wird, speichert SafeGuard Enterprise nur den BitLocker Recovery-Schlüssel des neuen Volume. Sie müssen von dem Schlüssel des bisherigen Volume eine Sicherungskopie mit den von Microsoft zur Verfügung gestellten Sicherungsmechanismen erstellen.

Verwaltung von Volumens, die bereits mit BitLocker verschlüsselt sind

Sollte es bei der Installation von SafeGuard Enterprise auf Ihrem Computer Volumes geben, die bereits mit BitLocker verschlüsselt sind, übernimmt SafeGuard Enterprise die Verwaltung dieser Volumes.

Verschlüsselte Boot-Volumes

- Abhängig von der verwendeten SafeGuard Enterprise BitLocker Unterstützung werden Sie möglicherweise aufgefordert, Ihren Computer neu zu starten. Es ist wichtig, dass Sie den Neustart so bald als möglich durchführen.
- Wenn für das verschlüsselte Volume eine SafeGuard Enterprise-Verschlüsselungsrichtlinie gilt:
  - **BitLocker Challenge/Response** ist installiert: Die Verwaltung wird übernommen und SafeGuard Challenge/Response ist möglich.
  - **SafeGuard BitLocker** ist installiert: Die Verwaltung wird übernommen und SafeGuard Recovery ist möglich.
- Wenn für das verschlüsselte Volume keine SafeGuard Enterprise Verschlüsselungsrichtlinie gilt:
  - **BitLocker Challenge/Response** ist installiert: Es wird keine Verwaltung übernommen und SafeGuard Challenge/Response ist nicht möglich.
  - **SafeGuard BitLocker** ist installiert: SafeGuard Recovery ist möglich.

Verschlüsseltes Data-Volume

- Wenn für das verschlüsselte Volume eine SafeGuard Enterprise-Verschlüsselungsrichtlinie gilt:

  Die Verwaltung wird übernommen und SafeGuard Recovery ist möglich.
- Wenn für das verschlüsselte Volume keine SafeGuard Enterprise Verschlüsselungsrichtlinie gilt:

  SafeGuard Recovery ist möglich.

Wichtig: Wenn ein mit BitLocker verschlüsseltes Volume in einem Computer durch ein neues Volume ersetzt wird, dieses den Volume-Buchstaben des alten Volume erhält und ebenfalls mit BitLocker verschlüsselt wird, speichert SafeGuard Enterprise nur den BitLocker Recovery-Schlüssel des neuen Volume. Sie müssen von dem Schlüssel des bisherigen Volume eine Sicherungskopie mit den von Microsoft zur Verfügung gestellten Sicherungsmechanismen erstellen.

Hinweis: Es kann vorkommen, dass SafeGuard Enterprise die Verwaltung eines bereits verschlüsselten Volume nicht übernehmen kann. In einem solchen Fall können Sie Sophos SafeGuard nicht für die Wiederherstellung verwenden. Kontaktieren Sie Ihren Sicherheitsbeauftragten.

7.2.4 Erstverschlüsselung auf einem durch BitLocker geschützten Endpoint

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

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

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

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

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

Hinweis: Wenn BitLocker-Laufwerkverschlüsselung für Ihr Betriebssystemlaufwerk oder Datenlaufwerke von SafeGard Enterprise verwaltet wird, schalten Sie BitLocker für diese Volumes nicht händisch ein.

7.2.4.1 Systemstartschlüssel speichern

Wenn Ihr Sicherheitsbeauftragter **TPM + Systemstartschlüssel** or **Systemstartschlüssel** als Anmeldemodus definiert hat, müssen Sie angeben, wo der Systemstartschlüssel gespeichert werden soll. Stecken Sie einen USB-Stick ein, um den Schlüssel zu speichern. Verwenden Sie keinen verschlüsselten USB-Stick. Die gültigen Ziellaufwerke für den Systemstartschlüssel sind in dem Dialog angegeben. Später müssen Sie den Stick immer dann einstecken, wenn Sie den Computer starten.

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

7.2.4.2 Kennwort setzen

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

Hinweis: Wenn Sie in Ihrem Kennwort Sonderzeichen verwenden, beachten Sie, dass das von Ihnen verwendete Tastaturlayout unter Umständen nicht dem von BitLocker unterstützten EN-US Tastaturlayout entspricht. Sie können Ihr Tastaturlayout zum Festlegen des Kennworts vorübergehend auf EN-US setzen.

7.2.4.3 PIN setzen

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

Hinweis: Wenn Ihr Sicherheitsbeauftragter so genannte erweiterte PINs aktiviert hat, können Sie in Ihrer PIN Sonderzeichen verwenden. Beachten Sie, dass das von Ihnen verwendete Tastaturlayout unter Umständen nicht dem von BitLocker unterstützten EN-US Tastaturlayout entspricht. Sie können Ihr Tastaturlayout zum Festlegen der PIN vorübergehend auf EN-US setzen.

7.2.4.4 Dialog für TPM-only

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

7.2.5 Entschlüsselung mit BitLocker

Computer, die mit BitLocker verschlüsselt wurden, lassen sich nicht automatisch entschlüsseln. Die Entschlüsselung muss entweder über den Menüpunkt **BitLocker Drive Encryption** in der **Systemsteuerung** oder mit dem Microsoft Befehlszeilentool "Manage-bde" ausgeführt werden.

8 SafeGuard Data Exchange

Mit SafeGuard Data Exchange können Sie Daten auf beliebigen Wechselmedien, die mit Ihrem Computer verbunden sind, verschlüsseln und diese Daten einfach und sicher mit anderen Benutzern austauschen. Alle Ver- und Entschlüsselungsprozesse laufen transparent und mit minimaler Benutzerinteraktion ab.

Nur Benutzer, die über die entsprechenden Schlüssel verfügen, können den Inhalt der verschlüsselten Daten lesen. Alle nachfolgenden Verschlüsselungsprozesse laufen transparent. Für den Benutzer bedeutet transparente Verschlüsselung, dass verschlüsselt gespeicherte Daten automatisch beim Öffnen durch eine Anwendung entschlüsselt werden.

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

Hinweis: Wie sich SafeGuard Data Exchange auf Ihrem Computer verhält, wird zentral von Ihrem Sicherheitsbeauftragten festgelegt.

Ihr Sicherheitsbeauftragter legt in der zentralen Administration fest, wie mit Daten auf den Medien umgegangen werden soll. Er kann z. B. festlegen, dass ausschließlich verschlüsselte Dateien auf den Medien zugelassen sind. In diesem Fall werden alle bereits auf dem Medium bestehenden Dateien initial verschlüsselt. Außerdem werden alle neuen Dateien, die auf dem Medium gespeichert werden, verschlüsselt. Sollen bereits existierende Dateien nicht verschlüsselt werden, kann der Zugriff auf die bereits auf dem Medium vorhandenen unverschlüsselten Dateien gestattet werden. In diesem Fall verschlüsselt SafeGuard Data Exchange die bereits vorhandenen unverschlüsselten Dateien nicht. Die neu hinzugekommen Dateien werden jedoch verschlüsselt. Somit können Sie die vorhandenen unverschlüsselten Dateien lesen und auch bearbeiten. Solche Daten werden erst verschlüsselt, wenn der Name der Datei geändert wird. Der Sicherheitsbeauftragte kann auch festlegen dass Sie nicht dazu berechtigt sind, auf unverschlüsselte Dateien zuzugreifen, und die Dateien bleiben unverschlüsselt.

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

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

Wichtig: Beim Extrahieren eines ZIP-Archivs mit dem integrierten Archivprogramm von Microsoft Windows wird der Vorgang angehalten, sobald eine verschlüsselte Datei entdeckt wird, für die kein Schlüssel verfügbar ist. Der Benutzer erhält eine Nachricht, dass der Zugriff verweigert wurde, aber er wird nicht darüber informiert, dass Dateien vorhanden sind, die

nicht verarbeitet wurden und somit fehlen. Andere Archivierprogramme wie z. B. 7-Zip eignen sich sehr gut für ZIP-Archive, die verschlüsselte Dateien enthalten.

8.1 Einstellungen für Wechselmedien

Ist auf Ihrem Computer SafeGuard Data Exchange installiert, werden Wechselmedien so behandelt wie von Ihrem Sicherheitsbeauftragten vordefiniert. Ein Sicherheitsbeauftragter kann für SafeGuard Data Exchange die folgenden Einstellungen definieren, die auch in Kombination festgelegt werden können:

- **Initialverschlüsselung aller Dateien:** In diesem Fall startet die Verschlüsselung aller Daten auf einem Wechselmedium, sobald dieses mit Ihrem Computer verbunden ist. Diese Einstellung stellt sicher, dass sich auf den Wechselmedien ausschließlich verschlüsselte Daten befinden. Wenn die Verschlüsselung startet, werden Sie entweder aufgefordert, einen Schlüssel auszuwählen oder es wird ein vordefinierter Schlüssel verwendet.
- **Benutzer darf Initialverschlüsselung abbrechen:** Wenn die Initialverschlüsselung startet, wird ein Dialog angezeigt, in dem Sie die Initialverschlüsselung abbrechen können.
- **Benutzer darf auf unverschlüsselte Dateien zugreifen: Nein**: In diesem Fall akzeptiert SafeGuard Data Exchange nur verschlüsselte Daten auf Wechselmedien. Sollten sich unverschlüsselte Daten auf dem Medium befinden, wird Ihnen der Zugriff verweigert. Erst wenn Sie die Dateien verschlüsselt haben, können Sie darauf zugreifen.
- **Benutzer darf Dateien entschlüsseln:** In diesem Fall besteht die Möglichkeit, Dateien auf einem Wechselmedium explizit zu entschlüsseln. Dateien, die explizit entschlüsselt wurden, bleiben in Klartext auf dem Wechselmedium, wenn dieses z. B. an einen Dritten weitergegeben wird.
- **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen:** Wenn Sie das erste Mal ein Wechselmedium mit Ihrem Computer verbinden, werden Sie aufgefordert, eine Medien-Passphrase einzugeben.
- **Klartext-Ordner**: Der Sicherheitsbeauftragte kann einen Klartext-Ordner definieren, der auf allen Wechselmedien, die Sie verwenden, angelegt wird. Die Dateien in diesem Ordner werden von SafeGuard Data Exchange nicht verschlüsselt.
- **Benutzer darf über Verschlüsselung entscheiden:** Wenn Sie Wechselmedien mit Ihrem Computer verbinden, wird eine Meldung angezeigt, die Sie dazu auffordert zu entscheiden, ob die Dateien auf dem angesteckten Medium verschlüsselt werden sollen. Darüber hinaus können Sie, falls dies per Richtlinie aktiviert ist, auswählen, ob diese Einstellung gespeichert und immer auf das relevante Medium angewendet werden soll. Wenn Sie **Einstellung speichern und Dialog nicht mehr anzeigen** wählen, wird die Meldung für das relevante Medium nicht mehr angezeigt. In diesem Fall steht der neue Befehl **Verschlüsselung wieder aktivieren** im Kontextmenü des relevanten Mediums im Windows Explorer zur Verfügung. Wählen Sie diesen Befehl, um Ihre Entscheidung über die Verschlüsselung für das relevante Medium rückgängig zu machen. Ist dies nicht möglich, weil Sie zum Beispiel nicht über die notwendigen Rechte für das Medium verfügen, so wird eine Fehlermeldung angezeigt. Nachdem Sie Ihre Entscheidung rückgängig gemacht haben, werden Sie wieder dazu aufgefordert zu entscheiden, ob die Dateien auf dem relevanten Medium verschlüsselt werden sollen.

8.2 Eine Medien-Passphrase für alle mit dem Computer verbundenen Wechselmedien

SafeGuard Data Exchange unterstützt die Festlegung einer einzigen Medien-Passphrase, die Ihnen den Zugriff auf alle mit Ihrem Computer verbundenen Wechselmedien ermöglicht. Dies ist unabhängig von dem für die Verschlüsselung der einzelnen Dateien verwendeten Schlüssel.

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

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

Eine Medien-Passphrase ist in den folgenden Situationen nützlich:

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

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

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

Unterstützte Medien

SafeGuard Data Exchange unterstützt folgende Wechselmedien:

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

- Speicherkarten in USB-Kartenlesern

8.3 Verschlüsseln von Wechselmedien

Die Verschlüsselung von unverschlüsselten Daten auf einem Wechselmedium startet entweder automatisch, wenn Sie das Wechselmedium mit dem System verbinden, oder Sie muss von Ihnen angestoßen werden. Alle nachfolgenden Ver- und Entschlüsselungsvorgänge laufen transparent und nahezu ohne Benutzerinteraktion ab.

8.3.1 Initialverschlüsselung

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

So starten Sie den Verschlüsselungsvorgang manuell:

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

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

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

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

Abbrechen der Initialverschlüsselung

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

Initialverschlüsselung für Benutzer mit einer Medien-Passphrase

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

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

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

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

8.3.2 Manuelle Verschlüsselung

Wenn Sie berechtigt sind zu entscheiden, ob Dateien auf Wechselmedien verschlüsselt werden sollen, können Sie den Verschlüsselungsvorgang manuell starten. So können Sie auch bereits verschlüsselte Dateien mit einem anderen Schlüssel verschlüsseln.

So starten Sie den Verschlüsselungsvorgang manuell:

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

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

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

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

8.3.3 Transparente Verschlüsselung

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

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

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

8.3.3.1 Medien-Passphrase

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

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

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

8.3.3.2 Ändern/Zurücksetzen der Medien-Passphrase

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

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

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

8.3.3.3 Synchronisierung der Medien-Passphrase

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

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

8.4 Datenaustausch mit SafeGuard Data Exchange

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

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

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

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

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

- Austausch von Daten mit Benutzern ohne SafeGuard Enterprise

Für Benutzer, die SafeGuard Enterprise nicht installiert haben, steht SafeGuard Portable zur Verfügung. Auch bei der Verwendung von SafeGuard Portable müssen lokale Schlüssel mit Passphrase verwendet werden.

Zusätzlich muss SafeGuard Portable auf das Wechselmedium kopiert werden. Auch in diesem Fall müssen Sie dem Empfänger der verschlüsselten Daten die Passphrase bekannt geben. Dieser kann dann mit SafeGuard Portable und der Passphrase die Daten entschlüsseln, eventuell bearbeiten und wieder verschlüsselt auf dem Wechselmedium speichern. Da es sich bei SafeGuard Portable um eine autarke Applikation handelt, muss auf dem Computer keine zusätzliche Software installiert werden, um auf die verschlüsselten Daten zugreifen zu können.

Hinweis: Ob SafeGuard Portable auf Wechselmedien kopiert wird, bestimmt Ihr Sicherheitsbeauftragter in der für Sie geltenden Sicherheitsrichtlinie.

8.4.1 Import von Schlüsseln aus einer Datei

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

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

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

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

8.4.2 Erzeugen von lokalen Schlüsseln

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

   Der interne Name des Schlüssels wird im Feld darunter angezeigt.

4. Bestätigen Sie die Passphrase.

   Wenn Sie eine unsichere Passphrase eingeben, wird ein Hinweis angezeigt. Zur Erhöhung des Sicherheitsniveaus ist die Verwendung von komplexen Passphrasen empfehlenswert. Sie können selbst entscheiden, ob Sie die unsichere Passphrase dennoch verwenden wollen. Die Passphrase muss außerdem den Unternehmensrichtlinien entsprechen. Ist dies nicht der Fall, so wird eine Warnungsmeldung angezeigt.

5. Wenn Sie den Dialog über ein Kontextmenü geöffnet haben, enthält dieses die Option **Als neuen Standardschlüssel für Pfad verwenden**. Mit der Option **Als neuen Standardschlüssel für Pfad verwenden** können Sie diesen Schlüssel als Standardschlüssel für ein Volume oder einen Cloud Storage-Synchronisierungsordner festlegen.

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

6. Klicken Sie auf **OK**.

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

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

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

8.5 Brennen von Dateien auf CD mit dem Windows Assistenten zum Schreiben von CDs

Mit SafeGuard Data Exchange können Sie verschlüsselte Dateien über den im Windows Explorer integrierten Assistenten zum Schreiben von CDs auf CDs brennen.

Dazu muss für das CD-Laufwerk eine Verschlüsselungsregel definiert sein. SafeGuard Data Exchange erweitert dann den Assistenten um einen Dialog. Dort können Sie festlegen, wie die Dateien auf CD gebrannt werden sollen (verschlüsselt oder in Klartext).

Hinweis: Wenn für das optische Medium keine Verschlüsselungsregel festgelegt ist, werden die Dateien immer in Klartext auf das Medium geschrieben. Der Dialog von SafeGuard Data Exchange, über den der Verschlüsselungsstatus der Daten auf dem Datenträger festgelegt werden kann, wird nicht angezeigt.

Nachdem Sie einen Namen für die zu brennende CD eingegeben haben, wird die SafeGuard Data Exchange Disc Burning Erweiterung angezeigt.

Im Abschnitt **Statistik** wird angezeigt,

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

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

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

Die Situation, dass zu brennende Dateien mit verschiedenen Schlüsseln verschlüsselt sind, kann dann entstehen, wenn die Verschlüsselungsregel für das optische Laufwerk geändert wurde. Unverschlüsselte Dateien befinden sich dann im Ordner für zu brennende Dateien, wenn die Verschlüsselungsregel deaktiviert war, als diese hinzugefügt wurden.

Dateien verschlüsselt auf CD brennen

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

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

Dateien in Klartext auf CD brennen

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

SafeGuard Portable auf das optische Speichermedium kopieren

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

8.5.1 Schreiben auf CDs und DVDs

In Windows steht ein Assistent für das Schreiben auf CDs/DVDs zur Verfügung.

Die SafeGuard Disc Burning Erweiterung für den Assistenten für das Schreiben auf CDs steht nur beim Brennen von CDs/DVDs im **Mastered** Format zur Verfügung. Der Assistent wird nur angezeigt, wenn Daten in diesem Format gebrannt werden sollen.

Für das Livedateisystem ist kein Assistent notwendig. Das optische Laufwerk wird in diesem Fall wie jedes andere Wechselmedium behandelt. Dateien werden automatisch beim Kopieren auf die CD/DVD verschlüsselt, wenn eine entsprechende Verschlüsselungsregel existiert.

8.6 SafeGuard Portable

SafeGuard Portable ermöglicht Ihnen den verschlüsselten Datenaustausch auf Wechselmedien, ohne dass der Empfänger der Daten SafeGuard Data Exchange installiert haben muss. Daten, die mit SafeGuard Data Exchange verschlüsselt wurden, können mit Hilfe von SafeGuard Portable ent- bzw. verschlüsselt werden. Dies wird durch ein eigenes Programm (SGPortable.exe) erreicht, das automatisch auf das Wechselmedium kopiert wird.

Hinweis: SafeGuard Portable ver- und entschlüsselt ausschließlich mit AES 256 verschlüsselte Dateien.

Mit SafeGuard Portable in Verbindung mit der relevanten Medien-Passphrase erhalten Sie Zugriff auf alle verschlüsselten Dateien. Dabei spielt es keine Rolle, welcher lokale Schlüssel für die Verschlüsselung verwendet wurde. Mit der Passphrase eines lokalen Schlüssels hingegen erhalten Sie lediglich Zugriff auf die Dateien, die mit diesem spezifischen Schlüssel verschlüsselt wurden. Der Empfänger kann jeweils die verschlüsselten Daten entschlüsseln und sie auch wieder verschlüsseln.

Hinweis: Die Medien-Passphrase oder die Passphrase für einen lokalen Schlüssel müssen dem Empfänger zuvor mitgeteilt werden.

Der Empfänger hat die Wahl, ob er bereits vorhandene Schlüssel, die mit SafeGuard Data Exchange erzeugt wurden, für die Verschlüsselung wählt, oder ob er (z. B. bei neuen Dateien) einen neuen Schlüssel mit SafeGuard Portable erzeugt und diesen zur Verschlüsselung der Daten verwendet.

SafeGuard Portable muss dabei nicht auf dem Computer Ihres Kommunikationspartners installiert oder kopiert werden. Es verbleibt auf dem Wechselmedium.

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

8.6.1 Bearbeiten von Dateien mit SafeGuard Portable

Sie haben ein Wechselmedium erhalten, auf dem sich neben den mit SafeGuard Data Exchange verschlüsselten Dateien ein Ordner **`SGPortable`** befindet. In diesem Ordner befindet sich die Datei **`SGPortable.exe`**.

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

   Mit Hilfe von SafeGuard Portable können Sie die verschlüsselten Dateien auf dem wechselbaren Medium ent- und auch wieder verschlüsseln. SafeGuard Portable bietet Ihnen eine ähnliche Funktionalität, wie sie Sie vom Windows Explorer kennen.

   Zusätzlich zu den aus dem Windows Explorer bekannten Dateimerkmalen (Name, Größe usw.) zeigt SafeGuard Portable die Spalte **Schlüssel** an. Diese Spalte gibt an, ob die Daten verschlüsselt sind. Ist die Datei verschlüsselt, wird der Name des verwendeten Schlüssels angezeigt.

   Hinweis: Sie können nur Dateien entschlüsseln, für deren Schlüssel Sie die entsprechende Passphrase wissen.

2. Wenn Sie Dateien auf Ihrem Wechselmedium bearbeiten wollen, (Entschlüsseln/Verschlüsseln usw.) klicken Sie auf die relevante Datei und wählen Sie entweder über das Kontextmenü der rechten Maustaste oder über den Menübefehl **Datei** das entsprechende Kommando.

   Folgende Menübefehle stehen Ihnen über das Kontextmenü der rechten Maustaste zur Verfügung:

Verschlüsselungsschlüssel setzen	Öffnet den Dialog **Schlüssel eingeben**. Hier können Sie einen Schlüssel für die Verschlüsselung mit Hilfe von SafeGuard Portable generieren.
Verschlüsseln	Verschlüsselt die aktivierte Datei auf Ihrem Wechselmedium. Der zuletzt benutzte Schlüssel wird für die Verschlüsselung verwendet.
Entschlüsseln	Öffnet den Dialog **Passphrase eingeben**. Geben Sie hier die Passphrase zum Entschlüsseln der ausgewählten Datei ein.
Verschlüsselungsstatus	Öffnet einen Dialog, in dem der Verschlüsselungsstatus angezeigt wird.
Kopieren nach	Kopiert die Datei in den Ordner Ihrer Wahl und entschlüsselt diese.
Löschen	Löscht die aktivierte Datei von Ihrem Wechselmedium.

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

8.6.1.1 Setzen von Verschlüsselungsschlüsseln

So verschlüsseln Sie eine Datei auf einem Wechselmedium und legen einen Verschlüsselungschlüssel an:

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

   Der Dialog **Schlüssel eingeben** wird angezeigt.

2. Geben Sie einen **Namen** und eine **Passphrase** für den Schlüssel ein. **Bestätigen** Sie die Passphrase und klicken Sie auf **OK**.

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

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

8.6.1.2 Verschlüsseln von Dateien auf Wechselmedien

1. Markieren Sie die Datei im Explorer von SafeGuard Portable und wählen Sie über das Kontextmenü der rechten Maustaste den Menübefehl **Verschlüsseln**.

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

   Wenn Sie per Drag & Drop über den Explorer von SafeGuard Portable neue Dateien auf Ihrem Wechselmedium speichern, werden Sie gefragt, ob Sie diese Dateien verschlüsseln wollen.

   Geschieht dies, ohne dass vorher eine Verschlüsselung mit SafeGuard Portable durchgeführt wurde, dann öffnet sich der Dialog zum Setzen eines Schlüssels. Geben Sie dort den Namen des Schlüssels und eine Passphrase ein (die Eingabe der Passphrase muss wiederholt werden). Klicken Sie auf **OK**.

2. Markieren Sie danach mit der linken Maustaste die Datei, die mit dem eben gesetzten Schlüssel verschlüsselt werden soll, und wählen Sie über das Kontextmenü der rechten Maustaste oder über den Hauptmenübefehl **Datei** den Menübefehl **Verschlüsseln**.

   Die Datei wird nun verschlüsselt. Sie erhalten eine Meldung, wenn diese Aktion erfolgreich abgeschlossen ist.

   Hinweis: Alle weiteren Verschlüsselungen, die Sie mit SafeGuard Portable vornehmen, werden ab jetzt mit dem zuletzt verwendeten und von SafeGuard Portable gesetzten Schlüssel vorgenommen. Es sei denn, Sie setzen einen neuen Schlüssel.

8.6.1.3 Entschlüsseln von Dateien auf Wechselmedien

1. Markieren Sie die Datei im Explorer von SafeGuard Portable und wählen Sie **Entschlüsseln** aus dem Kontextmenü.

   Der Dialog zur Eingabe der Medien-Passphrase oder der Passphrase eines lokalen Schlüssels wird angezeigt.

2. Geben Sie dort die entsprechende Passphrase ein (die Passphrase muss Ihnen vom Absender der Daten mitgeteilt werden) und klicken Sie auf **OK**.

   Die Datei wird entschlüsselt.

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

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

Haben Sie einmal Dateien auf Ihrem Wechselmedium entschlüsselt und die Passphrase des Schlüssels eingegeben, dann müssen Sie die Eingabe beim nächsten Entschlüsseln und Verschlüsseln nicht wiederholen, wenn die Dateien mit dem gleichen Schlüssel verschlüsselt worden sind.

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

Wenn Sie die Dateien entschlüsseln, liegen diese in Klartext auf dem Wechselmedium vor. Entschlüsselte Dateien werden wieder verschlüsselt, wenn Sie SafeGuard Portable schließen.

8.6.1.4 Verschlüsseln von neuen Dateien mit SafeGuard Portable

Sie können mit SafeGuard Portable auch Ihre eigenen Dateien verschlüsselt auf das Wechselmedium kopieren.

1. Ziehen Sie dazu die gewünschten Dateien einfach in den Explorer von SafeGuard Portable.

   Sie werden gefragt, ob Sie die Datei verschlüsseln wollen.

2. Bestätigen Sie, dass Sie die Datei verschlüsseln möchten. Die Datei wird mit dem zuletzt verwendeten Schlüssel verschlüsselt und auf das Wechselmedium kopiert.

8.6.1.5 Zeigt den Verschlüsselungsstatus eines Laufwerks an.

1. Markieren Sie mit der linken Maustaste diese Datei und wählen Sie entweder über das Kontextmenü der rechten Maustaste oder über den Hauptmenübefehl **Datei** den Menübefehl **Verschlüsselungsstatus**.

   Der Verschlüsselungsstatus wird Ihnen auch im SafeGuard Portable Explorer neben dem Dateinamen in der Spalte **Schlüssel** angezeigt.

8.6.2 Weitere SafeGuard Portable Funktionen

Folgende weitere Funktionen stehen zur Verfügung:

- **Öffnen**: Dieser Menübefehl steht Ihnen nur über das Hauptmenü **Datei** von SafeGuard Portable zur Verfügung.

  Wenn Sie eine verschlüsselte Datei über diesen Menübefehl öffnen, werden Sie, wenn diese Datei verschlüsselt ist, zur Eingabe der Passphrase aufgefordert. Geben Sie die Passphrase ein und klicken Sie auf **OK**. Die Datei wird entschlüsselt und geöffnet.

- **Löschen**: Löscht die markierte Datei.
- **Kopieren nach**: Dieser Menübefehl steht Ihnen nur über das Kontextmenü der rechten Maustaste des Explorers von SafeGuard Portable zur Verfügung.

  Sie können damit Dateien, die sich auf einem Wechselmedium befinden, auf ein anderes Volume Ihres Computers kopieren.

- **Exit**: Dieser Menübefehl steht Ihnen nur über das Hauptmenü **Datei** von SafeGuard Portable zur Verfügung.

  Exit beendet SafeGuard Portable.

9 SafeGuard File Encryption

Das SafeGuard Enterprise-Modul „File Encryption“ ermöglicht die dateibasierende Verschlüsselung auf lokalen Laufwerken und im Netzwerk. Das Modul ist insbesondere für Arbeitsgruppen nützlich, die Daten sicher auf Netzwerkfreigaben ablegen möchten.

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

- 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 den Schlüssel für eine verschlüsselte Datei nicht haben, wird der Zugriff verweigert.
- Wenn Sie auf einem Computer, auf dem File Encryption nicht installiert ist, auf eine verschlüsselte Datei zugreifen, wird der verschlüsselte Inhalt angezeigt.
- Sie können den Verschlüsselungsstatus Ihrer Dateien mit den SafeGuard Enterprise Explorer-Erweiterungen für die dateibasierende Verschlüsselung überprüfen (siehe Explorer-Erweiterungen für die dateibasierende Verschlüsselung (Seite 62)).

9.1 Gemäß Richtlinie verschlüsseln

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

Wir empfehlen, diese Initialverschlüsselung durchzuführen, sobald auf Ihrem Endpoint eine File Encryption Richtlinie eingeht, obwohl Ihr Sicherheitsbeauftragter diesen Verschlüsselungsvorgang auch automatisch starten kann. Damit stellen Sie sicher, dass Ihre Daten so bald wie möglich nach Eingang einer File Encryption Richtlinie gemäß der Richtlinie verschlüsselt sind.

Einige Anwendungen legen nach dem Ändern des Inhalts einer Datei eine neue Datei an und löschen die alte. Nur bei diesen Anwendungen wird die Datei nach der Änderung verschlüsselt. Alle anderen Anwendungen lassen die Datei unverschlüsselt, wenn sie vor der Änderung unverschlüsselt war.

So starten Sie den Verschlüsselungsvorgang manuell:

1. Wählen Sie **Dateiverschlüsselung > Gemäß Richtlinie verschlüsseln** aus dem Kontextmenü des *Arbeitsplatz*-Knotens im Windows Explorer.
2. Der **SafeGuard Assistent für Dateiverschlüsselung** wird angezeigt.

   Alle Dateien in Ordnern und Unterordnern, für die Verschlüsselungsregeln gelten, werden mit dem in der entsprechenden Regel festgelegten Schüssel verschlüsselt.

9.2 SafeGuard Assistent für Dateiverschlüsselung

Der SafeGuard Assistent für Dateiverschlüsselung wird gestartet, wenn Sie den Befehl **Gemäß Richtlinie verschlüsseln** im Kontextmenü des Arbeitsplatz-Knotens oder den Befehl

Verschlüsselung beginnen im Kontextmenü von Ordnern oder Dateien im Windows Explorer auswählen.

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

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

Ein Status-Bild zeigt den Gesamtstatus des Vorgangs:

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

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

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

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

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

9.3 Persistente Verschlüsselung

Der Inhalt von mit File Encryption verschlüsselten Dateien wird jeweils direkt entschlüsselt, wenn Sie den notwendigen Schlüssel haben. Wenn der Inhalt in einer neuen Datei an einem Ablageort gespeichert wird, für den keine Verschlüsselungsregel gilt, bleibt die resultierende neue Datei unverschlüsselt.

Mit persistenter Verschlüsselung bleiben Kopien von verschlüsselten Dateien auch dann verschlüsselt, wenn sie an einem Speicherort abgelegt werden, für den keine Verschlüsselungsregel gilt.

Hinweis: Sicherheitsbeauftragte können dieses Verhalten deaktivieren. Wird es deaktiviert, so werden Dateien nicht verschlüsselt, wenn Sie an einen Speicherort kopiert oder verschoben werden, für den keine Verschlüsselungsregel gilt.

10 SafeGuard Cloud Storage

Das SafeGuard Enterprise Modul Cloud Storage bietet dateibasierende Verschlüsselung von in der Cloud gespeicherten Daten.

Das Modul beeinflusst nicht die Art und Weise, wie Sie mit in der Cloud gespeicherten Daten arbeiten. Cloud Storage stellt vielmehr sicher, dass die lokalen Kopien Ihrer Cloud-Daten transparent verschlüsselt werden und auch verschlüsselt bleiben, wenn sie in der Cloud gespeichert werden.

Hinweis: Fügen Sie keine Dateien zu Ihrem Dropbox Ordner hinzu, indem Sie sie auf das Dropbox Symbol am Windows Schreibtisch ziehen. Diese Dateien würden im Klartext in Ihren Dropbox Ordner kopiert. Um Dateien zu verschlüsseln, kopieren Sie sie direkt in Ihren Dropbox Ordner.

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

10.1 Cloud Storage - Automatische Erkennung

SafeGuard Cloud Storage ermittelt Ihren Cloud Storage Provider automatisch. Die Verschlüsselungsrichtlinie wird automatisch auf den zu synchronisierenden Ordner eingestellt.

10.2 Cloud Storage - Initialverschlüsselung

SafeGuard Cloud Storage führt keine Initialverschlüsselung Ihrer Daten durch. Dateien, die vor der Installation oder Aktivierung von SafeGuard Cloud Storage per Richtlinie gespeichert wurden, bleiben unverschlüsselt.

Wenn Sie solche Daten verschlüsseln möchten, müssen Sie sie zunächst aus der Cloud entfernen und sie dann wieder hinzufügen.

10.3 Festlegen von Standardschlüsseln

Mit SafeGuard Cloud Storage können Sie Standardschlüssel für die Verschlüsselung von Daten in Ihrem Cloud Storage festlegen. Mit Standardschlüsseln können Sie verschiedene Unterordner mit unterschiedlichen Schlüsseln verschlüsseln, indem Sie für jeden Ordner einen eigenen Standardschlüssel festlegen. Um Standardschlüssel festzulegen, verwenden Sie den Befehl **Dateiverschlüsselung > Standardschlüssel festlegen...** in den SafeGuard Explorer-Erweiterungen (siehe Festlegen eines Standardschlüssels (Seite 63)).

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

Hinweis: Wenn Sie verschlüsselte Dateien auf Android- und iOS-Geräten mit Sophos Mobile Encryption lesen möchten, müssen Sie für die Verschlüsselung lokale Schlüssel verwenden.

Weitere Informationen zu Sophos Mobile Encryption finden Sie in der *Sophos Disk Encryption Hilfe*.

Gehen wir zum Beispiel davon aus, Sie möchten mit Hilfe von Dropbox gesicherte Daten unterschiedlichen Partnern zur Verfügung stellen. Jeder Partner soll Zugriff auf einen Unterordner Ihrer Dropbox erhalten. Hierzu müssen Sie nur für jeden der Unterordner einen separaten Standardschlüssel festlegen. SafeGuard Enterprise fügt dann automatisch eine Kopie von SafeGuard Portable hinzu. SafeGuard Portable ermöglicht Partnern ohne SafeGuard Cloud Storage Zugriff auf die verschlüsselten Daten in den Unterordnern. Sie teilen Ihren Partnern dann die jeweiligen Passphrasen für die Schlüssel mit. Mit SafeGuard Portable und den Passphrasen können Ihre Partner die Daten in den für sie erstellten Ordnern entschlüsseln. Sie haben jedoch keinen Zugriff auf die Daten in anderen Unterordnern, da diese mit einem anderen Schlüssel verschlüsselt sind.

10.4 SafeGuard Portable für Cloud Storage

Unter Umständen möchten Sie von zu Hause auf Ihre Cloud Storage zugreifen oder verschlüsselte Daten über einen freigegebenen Ordner in Ihrer Cloud Storage austauschen. SafeGuard Portable ermöglicht den Zugriff auf verschlüsselte Daten, die in der Cloud gespeichert sind, ohne SafeGuard Cloud Storage Installation.

Daten, die mit SafeGuard Cloud Storage verschlüsselt wurden, können mit Hilfe von SafeGuard Portable ent- bzw. verschlüsselt werden. Dies wird durch ein eigenes Programm (SGPortable.exe) erreicht, das automatisch in Ihren Synchronisierungsordner kopiert wird.

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

Hinweis: Die Passphrase für einen lokalen Schlüssel muss dem Empfänger zuvor mitgeteilt werden.

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

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

Eine detaillierte Beschreibung von SafeGuard Portable finden Sie unter Bearbeiten von Dateien mit SafeGuard Portable (Seite 49).

Hinweis: Wenn Sie auf eine Datei doppelklicken oder den Öffnen-Befehl verwenden, wird die Datei nicht an Ort und Stelle entschlüsselt, da entschlüsselte Dateien im Cloud Storage Synchronisierungsordner automatisch in die Cloud synchronisiert würden. In diesem Fall wird ein Dialog angezeigt, der Sie dazu auffordert, einen sicheren Speicherplatz für die Datei auszuwählen. Entschlüsselte Dateien werden nicht automatisch gelöscht, wenn SafeGuard Portable geschlossen wird. Änderungen, die in mit SafeGuard Portable für Cloud Storage entschlüsselten Dateien vorgenommen werden, werden nicht in die verschlüsselten Original-Dateien übernommen.

Hinweis: Speichern Sie Cloud Storage Synchronisierungsordner nicht auf Wechselmedien oder auf dem Netzwerk. Andernfalls erzeugt SafeGuard Portable in diesen Ordnern entschlüsselte Dateien. SafeGuard Portable sollte in diesen Fällen nicht verwendet werden. Erwägen Sie stattdessen, die Synchronisierungsordner auf lokale Festplattenlaufwerke zu verschieben.

11 SafeGuard Enterprise und selbst-verschlüsselnde Opal-Festplatten

Selbst-verschlüsselnde Festplatten bieten hardware-basierende Verschlüsselung der Daten, die auf die Festplatte geschrieben werden. Die Trusted Computing Group (TCG) hat den anbieter-unabhängigen Opal-Standard für selbst-verschlüsselnde Festplatten veröffentlicht. Festplatten, die dem Opal-Standard entsprechen, werden von unterschiedlichen Herstellern angeboten. SafeGuard Enterprise unterstützt den Opal-Standard und bietet die Verwaltung von Endpoints mit selbst-verschlüsselnden Festplatten, die dem Opal-Standard entsprechen. Nähere Informationen finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/113366.aspx.

11.1 Verschlüsselung von Opal-Festplatten

Festplatten, die dem Opal-Standard entsprechen, sind selbst-verschlüsselnd. Daten werden automatisch verschlüsselt, wenn sie auf die Festplatte geschrieben werden.

Opal-Festplatten werden mit einem AES 128/256 Schlüssel als Opal-Kennwort gesperrt. Dieses Kennwort wird von SafeGuard Enterprise über eine Verschlüsselungsrichtlinie verwaltet. Ihr Sicherheitsbeauftragter definiert diese Verschlüsselungsrichtlinie im SafeGuard Management Center und überträgt sie an Ihren Computer.

11.2 System Tray Icon und Explorer-Erweiterungen auf Endpoints mit Opal-Festplatten

Wenn SafeGuard Enterprise auf Ihrem Computer installiert ist, wird das SafeGuard Enterprise Produktsymbol im Infobereich (System Tray) der Taskleiste des Endpoint-Computers angezeigt. Als Benutzer haben Sie die Möglichkeit, auf alle wichtigen Funktionen, die SafeGuard Enterprise auf Ihrem Computer zur Verfügung stellt, zentral zuzugreifen. Beachten Sie, dass die Funktionen, die auf Ihrem Computer verfügbar sind, von den Einstellungen im SafeGuard Management Center abhängig sind. Ihr Sicherheitsbeauftragter legt diese Einstellungen zentral im SafeGuard Management Center fest und verteilt sie an die Endpoint-Computer.

Wenn Sie der Sicherheitsbeauftragte per Richtlinie dazu berechtigt hat, Opal-Festplatten zu entsperren, steht der SafeGuard Enterprise **Entschlüsseln** Befehl im Windows Explorer Kontextmenü zur Verfügung.

12 System Tray Icon und Balloon-Ausgabe

Als Benutzer haben Sie die Möglichkeit, auf alle wichtigen Funktionen, die SafeGuard Enterprise auf Ihrem Computer zur Verfügung stellt, zentral zuzugreifen. Zu diesem Zweck wird ein Symbol in der Windows Task-Leiste platziert, das SafeGuard Enterprise System Tray Icon.

Hinweis: Wie sich das System Tray Icon auf Ihrem Computer verhält, wird von Ihrem Sicherheitsbeauftragten festgelegt. Er bestimmt in einer Richtlinie, ob es auf Ihrem Computer angezeigt wird oder nicht. Darüber hinaus kann es vom Sicherheitsbeauftragten auch auf „stumm“ gesetzt werden. Dann werden die Balloon-Ausgaben auf Ihrem Computer nicht angezeigt.

Über das System Tray Icon können Sie sich Informationen anzeigen lassen oder bestimmte Aktionen ausführen. Ein Klick mit der rechten Maustaste auf das Symbol öffnet ein Menü mit folgenden Einträgen:

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

    Hinweis: Wenn Ihr Endpoint von einem Standalone-Endpoint zu einem zentral verwalteten Endpoint migriert wurde, kann eine zweite Anmeldung an SafeGuard Enterprise notwendig sein um Ihre benutzerdefinierten lokalen Schlüssel anzuzeigen.
  - **Benutzerzertifikat**: Zeigt Informationen zu Ihrem Zertifikat an.
  - **Unternehmenszertifikat**: Zeigt Informationen zum verwendeten Unternehmenszertifikat an.
- **Neuen Schlüssel erzeugen**: Öffnet einen Dialog zum Erzeugen eines neuen Schlüssels für die Verwendung zum Datenaustausch über Wechselmedien oder SafeGuard Cloud Storage (siehe SafeGuard Data Exchange (Seite 40) und SafeGuard Cloud Storage (Seite 55)).
- **Local Self Help**:

  Wenn für Ihren Computer die Funktion Local Self Help per Richtlinie aktiviert ist, wird im Kontextmenü des System Tray Icon der Befehl Local Self Help angezeigt. Mit diesem Befehl starten Sie den Local Self Help Assistenten. Local Self Help ist eine Recovery-Methode, für die keine Unterstützung durch den Helpdesk erforderlich ist. Weitere Informationen finden Sie unter Recovery mit Local Self Help (Seite 66).
- **Medien-Passphrase ändern**: Öffnet einen Dialog zum Ändern der Medien-Passphrase (siehe SafeGuard Data Exchange (Seite 40)).
- **Daten abgleichen**: Stößt den Datenabgleich mit dem SafeGuard Enterprise Server an. Balloon-Ausgaben zeigen den Fortschritt und das Ergebnis des Datenabgleichs an.

  Hinweis: Ein Doppelklick auf das System Tray Icon stößt den Datenabgleich ebenfalls an.
- **Status**: Zeigt in einem Dialog Informationen über den derzeitigen Status des durch SafeGuard Enterprise geschützten Computer:

Feld	Information
Zuletzt erhaltene Richtlinie	Zeigt, wann (Datum und Uhrzeit) der Computer zuletzt eine neue Richtlinie empfangen hat.
Letzter Schlüsselempfang	Zeigt, wann (Datum und Uhrzeit) der Computer zuletzt einen neuen Schlüssel empfangen hat.
Letzter Zertifikatsempfang	Zeigt, wann (Datum und Uhrzeit) der Computer zuletzt ein neues Zertifikat empfangen hat.
Letzter Server-Kontakt	Zeigt Datum und Uhrzeit des letzten Kontakts zum Server.
SGN-Benutzerstatus	Zeigt den Status des Benutzers, der am Computer angemeldet ist (Windows-Anmeldung): ▪ **Ausstehend**: Die Replikation des Benutzers in der SafeGuard POA steht noch aus, d. h., der initiale Benutzerabgleich ist noch nicht abgeschlossen. Diese Information ist vor allem nach Ihrer ersten Anmeldung an SafeGuard Enterprise wichtig, da Sie sich erst an der SafeGuard Power-on Authentication anmelden können, wenn der initiale Benutzerabgleich abgeschlossen ist. ▪ **SGN-Benutzer**: Der in Windows angemeldete Benutzer gilt als SafeGuard Enterprise-Benutzer. Ein SGN-Benutzer kann sich bei der SafeGuard Power-on Authentication anmelden, wird der UMA (User Machine Assignment - Benutzer-Computer Zuordnung) hinzugefügt und erhält ein Benutzerzertifikat und einen Schlüsselring für den Zugriff auf verschlüsselte Daten. ▪ **SGN-Benutzer (Besitzer)**: Sofern die Standardeinstellungen nicht geändert wurden, kann der Besitzer es anderen Benutzern ermöglichen, sich an dem Endpoint anzumelden und SGN-Benutzer zu werden. ▪ **SGN-Gast**: SGN-Gastbenutzer werden nicht der UMA hinzugefügt, erhalten keine Berechtigungen zum Anmelden bei der SafeGuard POA, bekommen kein Zertifikat und keinen Schlüsselring zugewiesen und werden nicht in der Datenbank gespeichert. ▪ **SGN-Gast (Service Account)**: Der an Windows angemeldete Benutzer ist ein SafeGuard Enterprise Gastbenutzer, der sich mit einem Service Account für administrative Aufgaben angemeldet hat.

Feld	Information
	▪ **SGN Windows-Benutzer** Ein SafeGuard Enterprise Windows-Benutzer wird nicht zur SafeGuard POA hinzugefügt, verfügt jedoch über einen Schlüsselring, mit dem er auf verschlüsselte Dateien zugreifen kann wie ein SafeGuard Enterprise-Benutzer. Die Benutzer werden der UMA hinzugefügt, d. h. sie dürfen sich auf diesem Endpoint bei Windows anmelden. ▪ **Unbekannt**: Gibt an, dass der Benutzerstatus nicht ermittelt werden konnte.
Policy Cache Status **Zu versendende Datenpakete**	Gibt an, ob Datenpakete vorhanden sind, die an den SafeGuard Enterprise Server geschickt werden sollen.
Local Self Help (LSH) Status **Freigeschaltet** **Aktiv**	Gibt an, ob Local Self Help per Richtlinie freigeschaltet ist, und vom Benutzer auf dem Computer aktiviert wurde.
Bereit zum Zertifikatwechsel	Dieser Text wird angezeigt, wenn der Sicherheitsbeauftragte ein neues Zertifikat für die Anmeldung mit Token an Ihren Computer zugewiesen hat. Sie können jetzt das Zertifikat für die Anmeldung mit Token ändern (siehe Ändern des Zertifikats für die Anmeldung mit Token (Seite 19)).

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

12.1 Erzeugen von lokalen Schlüsseln

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

   Der interne Name des Schlüssels wird im Feld darunter angezeigt.

4. Bestätigen Sie die Passphrase.

   Wenn Sie eine unsichere Passphrase eingeben, wird ein Hinweis angezeigt. Zur Erhöhung des Sicherheitsniveaus ist die Verwendung von komplexen Passphrasen empfehlenswert. Sie können selbst entscheiden, ob Sie die unsichere Passphrase dennoch verwenden wollen. Die Passphrase muss außerdem den Unternehmensrichtlinien entsprechen. Ist dies nicht der Fall, so wird eine Warnungsmeldung angezeigt.

5. Wenn Sie den Dialog über ein Kontextmenü geöffnet haben, enthält dieses die Option **Als neuen Standardschlüssel für Pfad verwenden**. Mit der Option **Als neuen Standardschlüssel für Pfad verwenden** können Sie diesen Schlüssel als Standardschlüssel für ein Volume oder einen Cloud Storage-Synchronisierungsordner festlegen.

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

6. Klicken Sie auf **OK**.

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

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

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

12.2 Overlay-Symbole

Overlay-Symbole sind kleine Symbole, die über Elementen im Windows Explorer angezeigt werden. Die Data Exchange Overlay-Symbole werden nur bei Dateien und Volumes angezeigt. Sie sollen eine schnelle Information über den Verschlüsselungsstatus einer Datei geben oder darauf hinweisen, dass auf ein Volume eine Verschlüsselungsregel angewendet wurde.

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

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

13 Zugriff auf Funktionen über Explorer-Erweiterungen

Die Funktionen zur Verschlüsselung sind über Einträge des Windows Explorer Kontextmenüs aufrufbar.

Hinweis: Die angezeigten Funktionen richten sich nach den in Richtlinien festgelegten Einstellungen. Außerdem spielt es eine Rolle, ob die relevante Funktion für den ausgewählten Explorer-Knoten verfügbar ist. Der Umfang der Funktionen hängt davon ab, ob datei- oder volume-basierende Verschlüsselung für das relevante Volume, den Ordner oder die Datei verwendet wurde.

13.1 Explorer-Erweiterungen für dateibasierende Verschlüsselung

Die Funktionen zur dateibasierenden Verschlüsselung (Data Exchange, File Encryption, Cloud Storage) sind über entsprechende Einträge in den Windows Explorer Kontextmenüs aufrufbar. Sie finden sie in den Kontextmenüs von:

- dem 'Arbeitsplatz'-Knoten
- Wechselmedien
- Ordnern
- Dateien

Welche Funktionen in den Menüs angezeigt werden, hängt von den installierten Komponenten ab.

Dem Kontextmenü wird der Eintrag **Dateiverschlüsselung** hinzugefügt. Über dieses Menü sind die einzelnen Funktionen aufrufbar.

Gilt für das ausgewählte Volume, das Wechselmedium, den Ordner oder die Datei eine dateibasierende Verschlüsselungsrichtlinie, werden dem Kontextmenü Einträge für die dateibasierende Verschlüsselung hinzugefügt.

Folgende Funktionen stehen zur Verfügung:

- **Gemäß Richtlinie verschlüsseln** Dieser Befehl wird nur dann angezeigt, wenn File Encryption installiert ist und der 'Arbeitsplatz'-Knoten ausgewählt wird. Wenn Sie diese Option wählen, werden alle Dateien in Ordnern und Unterordnern, für die Verschlüsselungsegeln gelten, gemäß der für Ihren Computer gültigen Richtlinie verschlüsselt.
- **Verschlüsselung beginnen**: Wenn Sie diese Option in einem Kontextmenü auswählen, können alle Dateien mit einem neuen Schlüssel verschlüsselt bzw. umgeschlüsselt werden. Wenn eine File Encryption Richtlinie gilt, wird ein Dateiverschlüsselungs-Assistent gestartet.
- **Status der Verschlüsselung anzeigen**: Zeigt für ein Volume, ein Wechselmedium oder eine Datei an, ob die Datei verschlüsselt ist, welcher Schlüssel verwendet wurde, ob der Schlüssel in Ihrem Schlüsselring vorhanden ist und ob Sie Zugriff auf diese Datei haben.
- **Entschlüsseln**: Entschlüsselt die markierten Dateien.

Hinweis: Dateien, für die eine File Encryption Verschlüsselungsrichtlinie gilt, können nicht entschlüsselt werden.

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

13.1.1 Festlegen eines Standardschlüssels

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

Definieren Sie den Standardschlüssel über das Kontextmenü

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

So legen Sie einen Standardschlüssel fest:

Wenn Sie im Kontextmenü auf **Dateiverschlüsselung > Standardschlüssel festlegen** klicken, wird ein Dialog zur Auswahl eines Schlüssels angezeigt.

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

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

Ein Standardschlüssel, der zur Verschlüsselung verwendet werden soll, kann per Richtlinie definiert sein. Ist der Standardschlüssel nicht per Richtlinie definiert und sind Sie dazu berechtigt, Standardschlüssel festzulegen, so werden Sie dazu aufgefordert, einen initialen Standardschlüssel angegeben.

13.1.2 Import von Schlüsseln aus einer Datei

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

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

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

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

13.2 Explorer-Erweiterungen für volume-basierende Verschlüsselung

Dem Windows Explorer Kontextmenü eines Volumes wird der Eintrag **Verschlüsselung** hinzugefügt.

Ist das Volume verschlüsselt, wird neben dem Eintrag ein Schlüsselsymbol angezeigt. Wird ein grüner Schlüssel angezeigt, besitzen Sie den notwendigen Schlüssel und können auf das Volume zugreifen.

Hinweis: Der Eintrag **Dateiverschlüsselung > Verschlüsselungsstatus** zeigt den Verschlüsselungsstatus der Dateien auf dem Volume aus der Sicht der dateibasierenden Verschlüsselung. Dateien auf einem verschlüsselten Volume können zusätzlich auch noch dateibasierend verschlüsselt sein. Ist dies für Dateien der Fall, wird dies in einem Dialog angezeigt.

Schlüssel hinzufügen/entfernen

Wenn es die Einstellungen in den für Sie geltenden Richtlinien erlauben, können Sie dem verschlüsselten Volume Schlüssel hinzufügen und Schlüssel entfernen. Damit geben Sie jedem Besitzer dieses Schlüssels die Möglichkeit, auf die verschlüsselten Daten auf diesem Volume zuzugreifen.

Schlüssel können dem Volume im **Eigenschaften** Dialog des Volumes zugewiesen werden. Dieser enthält eine Registerkarte **Verschlüsselung**(Rechtsklick auf **Volume > Eigenschaften > Verschlüsselung**).

Wählen Sie einen Schlüssel aus der unteren Liste aus und klicken Sie auf **Schlüssel hinzufügen**. Der Schlüssel wird aus der Schlüsselauswahlliste nach oben verschoben. Er ist nun in der Liste der Schlüssel, mit denen ein Zugriff auf das verschlüsselte Volume möglich ist.

Mit **Schlüssel entfernen** können Sie den Schlüssel aus der Liste der Schlüssel, die für den Medienzugriff verwendet werden können, wieder entfernen.

14 Recovery-Optionen

SafeGuard Enterprise bietet verschiedene Recovery-Optionen (z. B. wenn Sie Ihr Kennwort vergessen haben), die auf unterschiedliche Szenarien zugeschnitten sind:

- **Recovery für die Anmeldung mit Local Self Help** (nur für SafeGuard POA verfügbar)

  Wenn Sie Ihr Kennwort vergessen haben, können Sie sich über Local Self Help ohne die Unterstützung eines Helpdesk wieder an Ihrem Computer anmelden. Sie erhalten somit auch in Situationen, in denen Sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu Ihrem Computer. Um sich anzumelden, müssen Sie lediglich eine bestimmte Anzahl an vordefinierten Fragen in der SafeGuard Power-on Authentication beantworten.

  Weitere Informationen finden Sie unter Recovery mit Local Self Help (Seite 66).

- **Recovery über Challenge/Response oder mit BitLocker Recovery-Schlüssel**

  Das Challenge/Response-Verfahren ist ein sicheres und effizientes Recovery-System, das Sie unterstützt, wenn Sie sich nicht mehr an ihrem Computer anmelden oder nicht mehr auf verschlüsselte Daten zugreifen können. Während eines Challenge/Response-Verfahrens übermitteln Sie einen auf Ihrem Computer erzeugten Challenge-Code an den Helpdesk-Beauftragten. Dieser erzeugt auf der Grundlage des Challenge-Codes einen Response-Code, der Sie zum Ausführen einer bestimmten Aktion auf dem Computer berechtigt.

  An Endpoints, die Challenge/Response nicht unterstützen, werden Recovery-Schlüssel bereitgestellt. Das ist die normale Vorgangsweise von Microsoft. Während dem Recovery nennen Sie dem Helpdesk-Mitarbeiter den Computernamen und dieser teilt Ihnen den Recovery-Schlüssel mit, den Sie zum Starten Ihres Computers benötigen.

  Weitere Informationen finden Sie unter Recovery über Challenge/Response oder mit Recovery-Schlüssel (Seite 76).

Alle Recovery-Optionen werden durch den Sicherheitsbeauftragten für die Anwendung auf Ihrem Computer per Richtlinie aktiviert.

15 Recovery mit Local Self Help

Hinweis: Local Self Help ist nur für Windows 7 Endpoints mit SafeGuard Power-on Authentication (POA) verfügbar.

Wenn Sie Ihr Kennwort vergessen haben, können Sie sich über Local Self Help ohne die Unterstützung eines Helpdesk wieder an Ihrem Computer anmelden.

Über Local Self Help erhalten Sie auch in Situationen, in denen Sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu Ihrem Computer. Sie können sich an Ihren Computer durch die Beantwortung einer festgelegten Anzahl an zuvor definierten Fragen in der SafeGuard Power-on Authentication anmelden.

Die zu beantwortenden Fragen können vom Sicherheitsbeauftragten zentral vordefiniert und an die Endpoints verteilt werden. Sie können jedoch auch selbst Fragen definieren, wenn Sie per Richtlinie dazu berechtigt sind. Der Local Self Help Assistent unterstützt Sie bei der ersten Beantwortung und Bearbeitung der Fragen. Um den Local Self Help Assistenten zu öffnen, klicken Sie auf das SafeGuard Enterprise System Tray Icon in der Windows-Taskleiste.

Voraussetzungen

Damit Sie Local Self Help für Recovery-Vorgänge benutzen können, müssen folgende Voraussetzungen erfüllt sein:

- Der zuständige Sicherheitsbeauftragte hat Local Self Help in der relevanten Richtlinie freigeschaltet und die Einstellungen für die Funktion (z. B. Berechtigung zur Definition eigener Fragen) definiert.
- Sie haben Local Self Help auf Ihrem Computer aktiviert.

15.1 Aktivieren von Local Self Help

Nach dem Wirksamwerden der Richtlinie, die Sie zur Benutzung von Local Self Help berechtigt, müssen Sie die Funktion durch Beantwortung der erhaltenen Fragen oder durch Erstellung und Beantwortung eigener Fragen aktivieren.

Local Self Help ist erst dann auf Ihrem Computer aktiv, wenn Sie eine vordefinierte Anzahl an Fragen beantwortet und gespeichert haben. Der Sicherheitsbeauftragte legt fest, wie viele Fragen Sie beantworten müssen. Der Local Self Help Assistent führt Sie durch den Vorgang und zeigt, wie viele Antworten erforderlich sind. Hierzu gibt es je nach den Einstellungen in der für Sie wirksamen Richtlinie folgende möglichen Szenarien:

- **Sie haben vordefinierte Fragen erhalten und sind *nicht* dazu berechtigt, eigene Fragen zu definieren.**

  Beantworten und speichern Sie die erhaltenen vordefinierten Fragen. Der Local Self Help Assistent zeigt, wie viele Antworten erforderlich sind.

- **Sie haben vordefinierte Fragen erhalten und sind dazu berechtigt, eigene Fragen zu erstellen.**

  Beantworten und speichern Sie die erforderliche Anzahl an Fragen - vordefinierte, eigene oder eine Kombination aus beiden Fragenarten.

- **Sie haben keine vordefinierten Fragen erhalten und sind dazu berechtigt, eigene Fragen zu definieren.**

  Definieren, beantworten und speichern Sie die erforderliche Anzahl an Fragen.

Hinweis: Um sich mit Local Self Help an der SafeGuard Power-on Authentication anzumelden, müssen Sie die Fragen, die per Zufallsprinzip aus den mit Antworten hinterlegten Fragen ausgewählt werden, korrekt beantworten. Der Sicherheitsbeauftragte legt fest, wie viele Fragen Sie in der SafeGuard POA beantworten müssen.

Voraussetzung: Nach Erhalt der Richtlinie informiert Sie eine Balloon-Ausgabe darüber, dass unbeantwortete Local Self Help Fragen vorliegen. Starten Sie nun Ihren Computer neu. Dadurch wird der Befehl **Local Self Help** zum Kontextmenü des System Tray Icons in der Windows-Taskleiste hinzugefügt.

So aktivieren Sie Local Self Help:

1. Klicken Sie mit der rechten Maustaste auf das SafeGuard Enterprise System Tray Icon in der Windows-Taskleiste.
2. Wählen Sie **Local Self Help**.

   Der **Willkommen** Dialog des Local Self Help Assistenten wird angezeigt.

   Aus Sicherheitsgründen werden Sie zur Eingabe Ihres Kennworts aufgefordert.

3. Geben Sie Ihr Kennwort ein und klicken Sie auf **Weiter**.

   Der Dialog **Statusübersicht** wird angezeigt.

   Dieser Dialog gibt Ihnen eine kurze Anleitung zur Aktivierung von Local Self Help. Darüber hinaus zeigt er die aktuellen Statusinformationen. Unter anderem wird hier angegeben, wie viele benutzerdefinierte und vordefinierte Fragen vorhanden und wie viele beantwortet sind.

4. Klicken Sie auf **Weiter**.

   Wenn Sie mit dem Wirksamwerden der Richtlinie vordefinierte Fragen erhalten haben, wird der Dialog **Vordefinierte Fragen** angezeigt.

   - Wenn Sie mehrere Fragenthemen erhalten haben, können Sie in der Dropdown-Liste des Felds **Thema** zwischen den einzelnen Fragenthemen wählen.
   - Um alle Themen in einer fortlaufenden Liste anzuzeigen, wählen Sie in der Dropdown-Liste die Option **Alle Themen** (Standardeinstellung).
   - Um die einzelnen Fragen zu beantworten, klicken Sie auf die jeweilige Frage und geben Sie in der Spalte **Antworten** Ihre Antwort ein.
   - Nach der Eingabe wird die Antwort verborgen. Um den Text anzuzeigen, aktivieren Sie das Kontrollkästchen **Antworten zeigen**.

   Hinweis: Beachten Sie, dass Sie die Antworten bei der späteren Beantwortung der Fragen in der SafeGuard Power-on Authentication im Rahmen eines Recovery-Vorgangs exakt so eingeben müssen, wie Sie sie im Local Self Help Assistenten eingegeben haben. So unterscheidet Local Self Help auch zwischen Groß- und Kleinschreibung.

   Hinweis: Nicht alle Zeichen, die in Windows eingegeben werden können, können von der SafeGuard POA verarbeitet werden. Hebräische oder arabische Zeichen können z. B. nicht verwendet werden. Für die Eingabe von Antworten auf Japanisch müssen Romaji-Zeichen (römische/lateinische Zeichen) verwendet werden. Andernfalls ergibt sich bei der Eingabe der Antworten in der SafeGuard Power-on Authentication keine Übereinstimmung.

5. Wenn Sie die Beantwortung der vordefinierten Fragen abgeschlossen haben, klicken Sie auf **Weiter**.
6. Wenn Sie dazu berechtigt sind, eigene Fragen zu definieren, wird der Dialog **Benutzerdefinierte Fragen und Antworten** angezeigt.
   a) Um eine neue Frage hinzuzufügen, klicken Sie auf **Neue Frage**.

      Der Fragenliste wird eine neue Zeile hinzugefügt.

   b) Geben Sie in der Spalte **Fragen** die Frage und in der Spalte **Antworten** die Antwort ein.

      Nach der Eingabe wird die Antwort verborgen.

   c) Um den Text anzuzeigen, aktivieren Sie das Kontrollkästchen **Antworten zeigen**.

   Hinweis: Beachten Sie, dass Sie die Antworten bei der späteren Beantwortung der Fragen in der SafeGuard Power-on Authentication im Rahmen eines Recovery-Vorgangs exakt so eingeben müssen, wie Sie sie im Local Self Help Assistenten eingegeben haben. So unterscheidet Local Self Help auch zwischen Groß- und Kleinschreibung.

   Hinweis:

   Nicht alle Zeichen, die in Windows eingegeben werden können, können von der SafeGuard POA verarbeitet werden. Hebräische oder arabische Zeichen können z. B. nicht verwendet werden. Für die Eingabe von Antworten auf Japanisch müssen Romaji-Zeichen (römische/lateinische Zeichen) verwendet werden. Andernfalls ergibt sich bei der Eingabe der Antworten in der SafeGuard Power-on Authentication keine Übereinstimmung.

7. Wenn Sie die Definition und Beantwortung der Fragen abgeschlossen haben, klicken Sie auf **Weiter**.

   Im letzten Dialog des Local Self Help Assistenten werden die neuen Statusinformationen nach Beantwortung der Fragen angezeigt. Eine Meldung informiert Sie darüber, ob die Voraussetzungen für die Aktivierung von Local Self Help erfüllt sind.

8. Klicken Sie auf **Beenden**.

   Die Fragen und Antworten werden gespeichert. Eine Meldung wird angezeigt, die Sie über die erfolgreiche Aktivierung informiert.

9. Klicken Sie auf **OK**.

Local Self Help ist auf Ihrem Computer aktiv. Sie können Local Self Help für Recovery-Vorgänge, die die Anmeldung betreffen, in der SafeGuard Power-on Authentication benutzen.

15.2 Aktivieren von Local Self Help - Erinnerung

Es ist wichtig, dass Sie Local Self Help aktivieren. Aus diesem Grund erinnert SafeGuard Enterprise Sie daran, sich bei Local Self Help anzumelden.

SafeGuard Enterprise erinnert Sie daran, Ihre Local Self Help-Fragen in drei Phasen einzurichten:

- **Schritt 1**

  Ein Ballon-Tooltip erscheint einen Kalendertag lang jede Stunde und weist darauf hin, dass Local Self Help eingerichtet werden muss. Am darauffolgenden Kalendertag beginnt Phase 2.

- **Schritt 2**

  Neben dem Verhalten der Phase 1 wird der Local Self Help-Assistent immer dann gestartet, wenn Sie sich anmelden oder den Computer entsperren. Sie können die Ausführung des Assistenten auf einen späteren Zeitpunkt verschieben. Nach 3 Kalendertagen beginnt Phase 3.

- **Schritt 3**

  Neben dem Verhalten der Phase 2, aber ohne Tooltip-Benachrichtigung, startet alle 60 Minuten der Local Self Help-Assistent.

Der Benutzer wird sofort mit einem Balloon-Tooltip benachrichtigt und Phase 1 wird begonnen, wenn Local Self Help aufgrund einer der folgenden Änderungen reaktiviert werden muss:

- der Local Self Help-Parameter
- des Windows-Kennworts
- des Zertifikats

15.3 Bearbeiten von Fragen

Nach der Aktivierung von Local Self Help auf Ihrem Computer lassen sich die Fragen nachträglich jederzeit bearbeiten:

- Bei vordefinierten Fragen können Sie die bei der initialen Beantwortung eingegebenen Antworten ändern. Vordefinierte Fragen können jedoch nicht gelöscht werden.
- Bei benutzerdefinierten Fragen können Sie die bei der initialen Beantwortung eingegebenen Antworten ändern, neue Fragen hinzufügen oder Fragen löschen.

1. Klicken Sie mit der rechten Maustaste auf das SafeGuard Enterprise System Tray Icon in der Windows-Taskleiste.
2. Wählen Sie **Local Self Help**.

   Der **Willkommen** Dialog des Local Self Help Assistenten wird angezeigt.

   Aus Sicherheitsgründen werden Sie zur Eingabe Ihres Kennworts aufgefordert.

3. Geben Sie Ihr Kennwort ein und klicken Sie auf **Weiter**.

   Der Dialog **Statusübersicht** wird angezeigt.

   Dieser Dialog gibt Ihnen eine kurze Anleitung zur Aktivierung von Local Self Help. Darüber hinaus zeigt er die aktuellen Statusinformationen. Unter anderem wird hier angegeben, wie viele benutzerdefinierte und vordefinierte Fragen vorhanden und wie viele beantwortet sind.

4. Klicken Sie auf **Weiter**. Wenn Sie vordefinierte Fragen erhalten und beantwortet haben, wird der Dialog **Vordefinierte Fragen** mit den beantworteten Fragen angezeigt.

   a) Wenn Sie mehrere Fragenthemen erhalten haben, können Sie in der Dropdown-Liste des Felds **Thema** zwischen den einzelnen Fragenthemen wählen.

   b) Um alle Themen in einer fortlaufenden Liste anzuzeigen, wählen Sie in der Dropdown-Liste die Option **Alle Themen** (Standardeinstellung).

Standardmäßig werden die bereits eingegebenen Antworten nicht als Text angezeigt.

c) Um die Antworten anzeigen zu lassen, wählen Sie das Kontrollkästchen **Antworten zeigen**.

d) Um die Antworten zu ändern, klicken Sie auf die jeweilige Frage und geben Sie in der Spalte **Antworten** eine neue Antwort ein.

5. Klicken Sie auf **Weiter**. Wenn Sie dazu berechtigt sind, eigene Fragen zu definieren, wird der Dialog **Benutzerdefinierte Fragen und Antworten** angezeigt. Standardmäßig werden die bereits eingegebenen Antworten nicht als Text angezeigt.

   a) Um die Antworten anzeigen zu lassen, wählen Sie das Kontrollkästchen **Antworten zeigen**.

   b) Um bereits vorhandene Antworten zu ändern, klicken Sie auf die jeweilige Frage und geben Sie in der Spalte **Antworten** eine neue Antwort ein.

   c) Um eine neue Frage hinzuzufügen, klicken Sie auf **Neue Frage**.

      Der Fragenliste wird eine neue Zeile hinzugefügt. Geben Sie in der Spalte **Fragen** die Frage und in der Spalte **Antworten** die Antwort ein.

   d) Um Fragen zu löschen, klicken Sie auf die jeweilige Frage und dann auf die Schaltfläche **Frage löschen**.

      Eine Meldung wird angezeigt, die Sie zur Bestätigung des Löschvorgangs auffordert. Klicken Sie auf **Ja**.

6. Klicken Sie auf **Weiter**.

   Im letzten Dialog des Local Self Help Assistenten werden die neuen Statusinformationen nach dem Bearbeiten der Fragen angezeigt. Eine Meldung informiert Sie darüber, ob die Voraussetzungen dafür, dass Local Self Help aktiv bleibt, erfüllt sind.

7. Klicken Sie auf **Beenden**.

   Die Fragen und Antworten werden gespeichert. Eine Meldung wird angezeigt, die Sie darüber informiert, dass der Vorgang erfolgreich durchgeführt wurde und Local Self Help aktiv bleibt.

8. Klicken Sie auf **OK**.

   Die Änderungen in den Fragenlisten werden wirksam.

Wenn Sie Local Self Help das nächste Mal in der SafeGuard Power-on Authentication starten, werden entsprechend per Zufallsprinzip die geänderten/neuen Fragen angezeigt. Die geänderten/neuen Antworten gelten.

Hinweis: Sollte durch die vorgenommenen Änderungen die erforderliche Mindestanzahl an beantworteten Fragen unterschritten werden, so werden Sie im letzten Local Self Help Assistent Dialog durch eine Warnungsmeldung darauf hingewiesen, dass Local Self Help nach Beenden des Assistenten deaktiviert wird. Wenn Sie Local Self Help nicht deaktivieren möchten, können Sie in die Dialoge **Benutzerdefinierte Fragen** und **Vordefinierte Fragen** wechseln, indem Sie auf **Zurück** klicken. Sie können nun Fragen hinzufügen oder neue Fragen beantworten. Wenn Sie auf **Beenden** klicken und die erforderliche Mindestanzahl an beantworteten Fragen wurde unterschritten, so werden Sie durch eine weitere Warnungsmeldung darauf hingewiesen dass Local Self Help nicht mehr auf Ihrem Computer aktiv ist. Sie können Local Self Help in diesem Fall jedoch jederzeit wieder aktivieren.

15.4 Änderungen von Fragenparametern

Der Sicherheitsbeauftragte kann für Local Self Help Fragen folgende Parameter definieren:

- Die Anzahl der Fragen, die Sie im Local Self Help Assistenten beantworten müssen, um Local Self Help auf Ihrem Computer zu aktivieren. Die angegebene Anzahl an Fragen muss mit den entsprechenden Antworten verfügbar sein, damit Local Self Help aktiv ist.

- Die Anzahl der Fragen, die Sie in der SafeGuard POA beantworten müssen, um sich mit Local Self Help anzumelden. Die in der SafeGuard POA angezeigten Fragen werden per Zufallsprinzip aus den Fragen, die Sie im Local Self Help Assistenten beantwortet haben, ausgewählt.

Wenn sich diese Parameter aufgrund einer neuen Richtlinie, die an Ihren Computer übertragen wurde, ändern, ergeben sich folgende mögliche Szenarien:

Bedingung	LSH-Aktion	Benutzer-Aktion erforderlich
Die Anzahl der Fragen, die Sie im Local Self Help Assistenten beantworten müssen, ändert sich. Die Anzahl an verfügbaren Fragen reicht jedoch aus, damit Local Self Help auf Ihrem Endpoint-Computer aktiv bleibt.	Local Self Help bleibt auf Ihrem Computer aktiv.	Keine
Die Anzahl der Fragen, die Sie im Local Self Help Assistenten beantworten müssen, ändert sich und es sind nicht genügend Fragen verfügbar, damit Local Self Help auf Ihrem Computer aktiv bleibt.	Es wird eine Meldung angezeigt, die Sie darüber informiert, dass sich die Local Self Help Einstellungen geändert haben. Die auf Ihrem Computer verfügbaren Fragen sind nicht mehr gültig. Local Self Help ist nicht mehr auf Ihrem Computer aktiv.	Um Local Self Help zu reaktivieren, starten Sie den Local Self Help Assistenten und folgen Sie den Anweisungen.
Die Anzahl der Fragen, die Sie in der SafeGuard POA beantworten müssen, um sich mit Local Self Help anzumelden, ändert sich.	Es wird eine Meldung angezeigt, die Sie darüber informiert, dass sich die Local Self Help Einstellungen geändert haben. Die auf Ihrem Computer verfügbaren Fragen bleiben gültig. Das Zahlenverhältnis zwischen verfügbaren Fragen und gültigen Antworten hat sich geändert.	Starten Sie den Local Self Help Assistenten und folgen Sie den Anweisungen.

15.5 Änderungen von Local Self Help Bedingungen oder Parametern während der Definition/Bearbeitung von Fragen

Local Self Help Parameter oder andere Bedingungen, die für die Benutzung der Funktion wichtig sind, können sich während der Definition oder Bearbeitung von Fragen im Local Self Help Assistenten ändern.

Zum Beispiel:

- Ein neues Benutzerkennwort oder ein neues Zertifikat wird spezifiziert.
- Eine neue Richtlinie mit neuen Local Self Help Einstellungen und/oder einem neuen Fragensatz für Local Self Help wird über den regulären Aktualisierungsmechanismus an Ihren Computer übertragen.

Treten solche Änderungen während des Bearbeitungsvorgangs auf, sind die von Ihnen definierten Fragen und Antworten unter Umständen nicht mehr gültig und es stehen nicht genug beantwortete Fragen zur Verfügung. In diesem Fall wird bzw. bleibt Local Self Help auf Ihrem Computer nicht aktiv.

Jedes Mal, wenn Sie die Definition oder Bearbeitung von Fragen im Local Self Help Assistenten beenden, überprüft der Assistent daher, ob eine der folgenden Bedingungen zutrifft und reagiert entsprechend:

Bedingung	Aktion des LSH-Assistenten	Ergebnis
Local Self Help wurde durch eine neue Richtlinie allgemein deaktiviert.	Der Local Self Help Assistent zeigt eine Meldung an, die Sie darüber informiert, dass Local Self Help allgemein deaktiviert wurde. Danach wird der Local Self Help Assistent geschlossen.	Local Self Help kann nicht mehr benutzt werden.
Local Self Help Parameter (z. B. die Mindestlänge für Antworten, das Recht, eigene Fragen zu definieren, die Anzahl der zu beantwortenden Fragen usw.) wurden durch eine neue Richtlinie geändert. Local Self Help wurde jedoch nicht allgemein deaktiviert. Die von Ihnen definierten Fragen und Antworten sind weiterhin gültig und ausreichend, damit Local Self Help auf Ihrem Computer aktiv bleibt.	Der Local Self Help Assistent zeigt eine Meldung an, die Sie darüber informiert, dass sich die Local Self Help Parameter geändert haben. Ihre Änderungen werden gespeichert. Danach wird der Local Self Help Assistent geschlossen.	Local Self Help ist auf Ihrem Computer aktiv und kann für Recovery-Vorgänge, die die Anmeldung betreffen, benutzt werden. Das Zahlenverhältnis zwischen verfügbaren Fragen und gültigen Antworten hat sich jedoch unter Umständen durch die Parameteränderungen geändert. Um das ursprüngliche Zahlenverhältnis wiederherzustellen, fügen Sie Fragen und/oder Antworten hinzu oder löschen Sie

Bedingung	Aktion des LSH-Assistenten	Ergebnis
		Fragen und/oder Antworten.
▪ Das Benutzerkennwort wurde geändert **und/oder** ▪ Local Self Help Parameter (z. B. die Mindestlänge für Antworten, das Recht, eigene Fragen zu definieren, die Anzahl der zu beantwortenden Fragen usw.) wurden durch eine neue Richtlinie geändert. Local Self Help wurde jedoch nicht allgemein deaktiviert. Die von Ihnen definierten Fragen und Antworten sind jedoch dadurch nicht mehr gültig. Die vorhandenen Fragen und Antworten sind nicht mehr ausreichend dafür, dass Local Self Help auf Ihrem Computer aktiv ist.	Der Local Self Help Assistent zeigt eine Meldung an, die Sie darüber informiert, dass sich Benutzerkennwort oder Local Self Help Parameter geändert haben. Local Self Help ist auf Ihrem Computer nicht aktiv. Sie werden dazu aufgefordert, den Assistenten erneut zu starten, um die notwendigen Schritte durchzuführen. Danach wird der Assistent geschlossen.	Um Local Self Help zu aktivieren, führen Sie den Local Self Help Assistenten erneut aus und definieren Sie die Fragen und Antworten erneut. Danach können Sie Local Self Help für Recovery-Vorgänge, die die Anmeldung betreffen, benutzen.
Das Benutzerzertifikat hat sich geändert.	Der Local Self Help Assistent zeigt eine Meldung an, die Sie darüber informiert, dass sich das Benutzerzertifikat geändert hat. Local Self Help ist auf Ihrem Computer nicht aktiv. Sie werden dazu aufgefordert, den Assistenten erneut zu starten, um die notwendigen Schritte durchzuführen. Danach wird der Assistent geschlossen.	Um Local Self Help zu aktivieren, führen Sie den Local Self Help Assistenten erneut aus und definieren Sie die Fragen und Antworten erneut. Danach können Sie Local Self Help für Recovery-Vorgänge, die die Anmeldung betreffen, benutzen.

15.6 Anmeldung an der SafeGuard POA mit Local Self Help

1. Klicken Sie im SafeGuard POA-Anmeldedialog auf **Recovery**.
   - Wenn für Sie nur Local Self Help aktiviert ist, wird Local Self Help gestartet.
   - Wenn für Sie sowohl Local Self Help als auch Challenge/Response zur Verfügung stehen, wird ein Dialog mit diesen beiden Auswahlmöglichkeiten angezeigt. Klicken Sie auf die Schaltfläche **Local Self Help**.

   Hinweis:

   Wenn Sie sich normalerweise mit einem Token oder einer Smartcard an der SafeGuard Power-on Authentication anmelden, entfernen Sie zunächst den Token/die Smartcard von Ihrem Computer. Daraufhin wird der SafeGuard POA-Dialog für die Anmeldung mit Benutzername und Kennwort angezeigt. Geben Sie Ihren Benutzernamen ein und klicken Sie auf **Recovery**.

   Der **Willkommen** Dialog von Local Self Help wird angezeigt.

   Dieser Dialog gibt Ihnen eine kurze Anleitung zu den folgenden Handlungsschritten.

2. Klicken Sie auf **Weiter**, um mit der Beantwortung der Fragen zu beginnen.

   Die erste Frage wird angezeigt.

3. Geben Sie die Antwort ein.

   Der eingegebene Text wird standardmäßig aus Sicherheitsgründen nicht im Eingabefeld angezeigt. Um sich die Antwort anzeigen zu lassen, deaktivieren Sie das Kontrollkästchen **Antwort verbergen**.

4. Klicken Sie nach Beantwortung der Frage auf **Weiter**.

   Die Schaltfläche **Weiter** wird erst aktiv, wenn Sie eine Antwort auf die Frage eingegeben haben. Erst dann können Sie mit der nächsten Frage fortfahren.

5. Beantworten Sie nun alle weiteren Fragen. Wenn Sie die letzte Frage beantwortet haben, klicken Sie auf **OK**.

   Im folgenden Dialog können Sie sich Ihr derzeit gültiges Kennwort anzeigen lassen.

6. Um das Kennwort anzeigen zu lassen, drücken Sie **Enter** oder die Leertaste oder klicken Sie auf das blaue Feld.

   Hinweis:

   Klicken Sie NICHT auf **OK**. Nach dem Klicken auf **OK** wird der Bootvorgang OHNE Kennwortanzeige fortgesetzt.

   Das Kennwort wird für höchstens 5 Sekunden angezeigt. Danach wird der Bootvorgang automatisch fortgesetzt.

   Hinweis: Achten Sie unbedingt darauf, dass kein Unbefugter zufällig oder absichtlich Ihren Bildschirm einsehen kann. Sie können das Kennwort durch Drücken der **Leer**- bzw. **Enter**-Taste oder durch einen Mausklick auf das blaue Anzeigefeld sofort verbergen.

7. Sie können das Kennwort lesen und es wieder zur Anmeldung an der SafeGuard Power-on Authentication und an Windows verwenden.
8. Wenn Sie das Kennwort gelesen haben, klicken Sie auf **OK**. Der Bootvorgang wird andernfalls nach dem Anzeigen des Kennworts nach 5 Sekunden automatisch fortgesetzt.

Sie werden an der SafeGuard Power-on Authentication und an Windows angemeldet.

15.7 Fehlgeschlagene Anmeldeversuche

Wenn Sie eine oder mehrere Fragen falsch beantwortet haben, erfolgt keine Anmeldung. In diesem Fall wird eine Meldung angezeigt, die Sie darüber informiert, dass die Anmeldung fehlgeschlagen ist. Aus Sicherheitsgründen zeigt Local Self Help nicht an, welche der Fragen Sie falsch beantwortet haben.

Das Fehlschlagen eines Recovery-Vorgangs über Local Self Help entspricht einem fehlgeschlagenen Anmeldeversuch, der als Ereignis protokolliert wird. Für die Anmeldung tritt in diesem Fall eine Verzögerung in Kraft. Die Anmeldeverzögerung verlängert sich mit jedem fehlgeschlagenen Anmeldeversuch.

Wenn Sie nach dem fehlgeschlagenen Anmeldeversuch den Computer neu starten und erneut die Anmeldung mit Local Self Help wählen, werden aus der Fragenliste wieder Fragen per Zufallsprinzip ausgewählt.

15.8 Erneutes Aktivieren von Fragen und Antworten nach einer Kennwortänderung auf mehreren Maschinen

Wenn Sie mehrere Computer mit aktivierter Local Self Help Funktion benutzen und Ihr Windows-Kennwort auf einem Computer ändern, sind die Local Self Help Fragen und Antworten nach Inkrafttreten der Kennwortänderung auf dem zweiten (und jedem weiteren) Computer nicht mehr aktiv. Die Fragen und Antworten stehen jedoch noch im Local Self Help Assistenten zur Verfügung. Um dieselben Fragen wieder auf dem zweiten Computer zu verwenden, bestätigen Sie diese über den Local Self Help Assistenten.

1. Nachdem Sie Ihr Kennwort auf einem Computer geändert haben, melden Sie sich am zweiten Computer an.

   Ein Tooltip informiert Sie darüber, dass unbeantwortete Local Self Help Fragen vorhanden sind.

2. Klicken Sie mit der rechten Maustaste auf das SafeGuard Enterprise System Tray Icon in der Windows-Taskleiste und wählen Sie **Local Self Help**.

   Der **Willkommen** Dialog des Local Self Help Assistenten wird angezeigt.

3. Geben Sie Ihr Kennwort ein und klicken Sie auf **Weiter**.
4. Bestätigen Sie alle weiteren Dialoge des Local Self Help Assistenten mit **Weiter** und klicken Sie im letzten Dialog auf **Beenden**.

Die zuvor auf dem Computer gespeicherten Fragen und Antworten sind wieder aktiv und werden bei der Anmeldung an der SafeGuard POA mit Local Self Help benutzt.

16 Recovery über Challenge/Response oder mit Recovery-Schlüssel

Wenn Sie als SafeGuard Enterprise Benutzer, z. B. Ihr Kennwort vergessen haben, sind Sie mit Hilfe eines zentralen Helpdesk rasch wieder produktiv.

Hinweis: Wenn Sie Windows 7 und die SafeGuard POA nutzen, empfehlen wir, vergessene Kennwörter mit Local Self Help wiederherzustellen. Sie können das aktuelle Kennwort in Local Self Help anzeigen und weiter verwenden, so dass Sie das Kennwort nicht zurücksetzen oder sich an den Helpdesk wenden müssen.

16.1 Challenge/Response für SafeGuard POA-Benutzer

Für Recovery-Vorgänge bietet **SafeGuard Enterprise** ein **Challenge/Response-Verfahren** zum Austauschen von Informationen auf vertraulichem Weg an.

Beim Challenge/Response-Verfahren erzeugen Sie auf Ihrem Computer einen Challenge Code (eine ASCII-Zeichenkette) und geben diesen einem Helpdesk-Mitarbeiter bekannt. Dieser erzeugt darauf basierend einen Response Code, der Sie zum einmaligen Ausführen einer bestimmten Aktion auf Ihrem Computer berechtigt.

Recovery mit Challenge/Response steht in der SafeGuard Power-on Authentication für die folgenden Anmeldemethoden zur Verfügung:

- Anmeldung mit Benutzername und Kennwort
- Anmeldung mit Fingerabdruck
- Anmeldung mit nicht-kryptograpischem Token

16.1.1 Typische Szenarien, für die Sie Hilfe anfordern können

- Sie haben Ihr Kennwort vergessen.
- Sie haben das Kennwort zu oft falsch in der SafeGuard POA eingegeben. Der Computer wurde gesperrt.
- Sie haben Ihren Token/Ihre Smartcard vergessen oder verloren.
- Der lokale Cache der SafeGuard Power-on Authentication ist teilweise beschädigt.
- Ein anderer Benutzer muss den durch SafeGuard Enterprise geschützten Computer starten.

16.1.2 Aktionen, für die eine Response angefordert werden kann, und die entsprechenden Anlassfälle

- **Starten des SafeGuard Enterprise Client ohne Benutzeranmeldung:**

  Ein Start des Computers ohne Benutzeranmeldung hilft Ihnen weiter, wenn Sie das Kennwort zu oft falsch eingegeben haben, Sie das Kennwort aber eigentlich wissen (z. B. wegen Tippfehlern, Feststelltaste war aktiviert, etc.). Durch das

Challenge/Response-Verfahren werden Sie an Ihren Computer angemeldet, ohne dass das Kennwort neu gesetzt wird.

Haben Sie das Kennwort zu oft falsch eingegeben, wird vom Helpdesk automatisch ein Response Code für den Start ohne Benutzeranmeldung erzeugt. Die Anforderung für diesen spezifischen Anlassfall ist in der Challenge enthalten. Sie können sich danach wieder mit Ihrem Benutzernamen und Kennwort anmelden.

- **Starten des SafeGuard Enterprise Client mit Benutzeranmeldung:**

  Wenn Sie Ihr Kennwort vergessen haben, versuchen Sie nicht erst, ein Kennwort einzugeben. Fordern Sie sofort eine Challenge an. Der Helpdesk kann dann eine Response sowohl für die Anmeldung ohne als auch mit Benutzernamen erzeugen. Bitten Sie den Helpdesk bei der Anmeldung mit Benutzernamen um die Anzeige des alten Kennworts während des Challenge/Response-Verfahrens. Dadurch kann das Zurücksetzen des Kennworts vermieden werden. Andernfalls müssen Sie im Rahmen des Challenge/Response-Verfahrens bei der Anmeldung mit Benutzernamen auch Ihr Kennwort für die Windows-Anmeldung neu setzen.

  Hinweis: Für Benutzer, die offline arbeiten, also keine Verbindung zum Domain-Controller haben, sind einige Besonderheiten zu beachten (siehe Challenge/Response für Offline-Benutzer (Seite 80)).

- **Zurückspielen des SafeGuard Enterprise Policy-Cache:**

  Diese Aktion wird notwendig, wenn der SafeGuard Policy Cache beschädigt ist. Im Local Cache werden alle Schlüssel, Richtlinien, Benutzerzertifikate und Audit-Dateien gespeichert. Standardmäßig ist Recovery für die Anmeldung bei einem beschädigten Local Cache deaktiviert, d. h. der Local Cache wird automatisch aus seiner Sicherungskopie wiederhergestellt. In diesem Fall ist für das Reparieren des Local Cache kein Challenge/Response-Verfahren erforderlich. Soll der Local Cache jedoch explizit mit einem Challenge/Response-Verfahren repariert werden, so lässt sich Recovery für die Anmeldung über eine Richtlinie aktivieren. In diesem Fall werden Sie automatisch zur Durchführung eines Challenge/Response-Verfahrens aufgefordert, wenn der Local Cache beschädigt ist.

16.1.3 Ablauf eines Challenge/Response-Verfahrens

1. Die SafeGuard Power-on Authentication startet.

   Hinweis: Für ein Challenge/Response-Verfahren stehen Ihnen ab dem Erzeugen der Challenge bis zur korrekten Eingabe der vom Helpdesk erzeugten Response 30 Minuten zur Verfügung. Danach verliert der Response Code seine Gültigkeit und kann nicht mehr verwendet werden.

2. Challenge anfordern:

   Öffnen Sie den **Challenge** Dialog in der SafeGuard Power-on Authentication. Es wird ein Challenge-Code aus Ziffern und Buchstaben erzeugt und angezeigt.

3. Kontaktieren Sie den Helpdesk.

   Teilen Sie dem Helpdesk Ihre Benutzerdaten (Benutzername, Computer-ID usw.), wie sie im **Challenge** Dialog angezeigt werden, sowie den Challenge-Code mit.

4. Der Helpdesk erzeugt einen Response-Code im SafeGuard Management Center.
5. Der Helpdesk teilt die Response per Telefon oder SMS mit.

6. Geben Sie den Response-Code in der SafeGuard Power-on Authentication ein.

   Sie können nun die Aktion, zu der Sie berechtigt sind, durchführen. Zum Beispiel können Sie Ihr Kennwort zurücksetzen.

Sie können nun weiterarbeiten.

16.1.4 Anfordern einer Challenge

1. Klicken Sie im SafeGuard POA-Anmeldedialog auf die Schaltfläche **Recovery**.

   Die Schaltfläche **Recovery** wird erst aktiviert, wenn Sie einen Benutzernamen oder im PIN Eingabedialog zumindest ein Zeichen eingeben.

   Hinweis: Wenn Sie Ihr Kennwort/Ihre PIN zu oft falsch eingeben oder der Policy Cache beschädigt ist, werden Sie von SafeGuard Enterprise automatisch darüber informiert. Ihnen wird die Möglichkeit angeboten, das Problem mit Challenge/Response zu beheben.

   Ihre Benutzerdaten und ein zufällig erzeugter Challenge-Code werden angezeigt. Zur besseren Übersicht ist der Code in Blocks von je 5 Zeichen unterteilt.

2. Rufen Sie den SafeGuard Enterprise Helpdesk an. Teilen Sie dem Helpdesk-Beauftragten Ihre Benutzerdaten mit und geben Sie den Challenge-Code durch.

   Sie können dazu eine Buchstabierhilfe über die Schaltfläche **Buchstabieren** einblenden.

   Der Helpdesk-Beauftragte kann das relevante Szenario anhand des Challenge-Codes identifizieren.

3. Klicken Sie auf **Weiter**.

16.1.5 Eingeben der Response

1. Geben Sie den Response-Code, den Sie vom Helpdesk-Beauftragten erhalten, im Dialog **Response** ein. Klicken Sie auf **OK**.

   Als Hilfestellung bei Eingabefehlern wird der Zeichenblock, in dem sich ein Fehler befindet, rot markiert.

2. Sie werden an der SafeGuard Power-on Authentication angemeldet.

Wenn die Änderung der Windows-Anmeldedaten erforderlich ist, werden Sie von SafeGuard Enterprise dazu aufgefordert.

16.1.6 Best Practice

16.1.6.1 Sie haben das Kennwort zu oft falsch eingegeben

Sie haben das Kennwort in der SafeGuard Power-on Authentication zu oft falsch eingegeben (Tippfehler, Feststelltaste war aktiviert usw.), wissen aber das korrekte Kennwort. Sie sind mit der Domäne verbunden.

1. Ihr Computer ist gesperrt. Sie werden aufgefordert, ein Challenge/Response-Verfahren einzuleiten, um Ihren Computer wieder zu entsperren.

2. Der Helpdesk-Beauftragte generiert dann eine Response für das Starten des Computers ohne Benutzeranmeldung.

   Booten ohne Benutzeranmeldung bedeutet, dass Sie Ihr Kennwort vor der Anmeldung an Windows nicht ändern müssen.

3. Der Windows-Anmeldedialog wird angezeigt. Geben Sie in diesem Dialog Ihr Windows-Kennwort ein, um sich anzumelden.

   Sie werden am System angemeldet.

4. Der Zähler, wie oft das Kennwort ohne Konsequenzen falsch eingegeben werden darf, wird zurückgesetzt.

   Hinweis: Sie können auch eine Response mit Benutzeranmeldung anfordern. In diesem Fall werden Sie vor der Anmeldung an Windows zum Ändern der Windows-Benutzerdaten aufgefordert.

16.1.6.2 Sie haben Ihr Kennwort vergessen

Wir empfehlen, die folgenden Methoden einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Durch Anwenden dieser Methoden vermeiden Sie ein zentrales Rücksetzen des Kennworts:

- Benutzen Sie Local Self Help. Mit Recovery mit Local Self Help können Sie selbst ohne die Unterstützung des Helpdesk ihr vergessenes Kennwort anzeigen lassen und es weiterverwenden, ohne es zurücksetzen zu müssen.

- Beim Einsatz von Challenge/Response: Bitten Sie den Helpdesk um eine Anmeldung mit Benutzernamen und um die Anzeige des alten Kennworts während des Challenge/Response-Verfahrens. Dadurch kann das zentrale Zurücksetzen des Kennworts vermieden werden. Sie können mit dem alten Kennwort weiterarbeiten und es bei Bedarf danach lokal ändern.

Wenn Sie nicht eine dieser beiden Methoden verwenden, gehen Sie wie folgt vor:

1. Wenn Sie Ihr Kennwort vergessen haben, erhalten Sie eine Response für das Booten Ihres Computers mit Benutzeranmeldung. Sie müssen dann im Rahmen der Anmeldung an Windows Ihr Kennwort ändern (Voraussetzung: die Domäne ist erreichbar).
2. Wenn Sie Ihr Kennwort geändert haben, verwenden Sie das neue Kennwort zur Anmeldung in der SafeGuard Power-on Authentication.

16.1.6.3 Sie haben Ihren Token vergessen oder verloren

In diesem Fall ist das Challenge/Response-Verfahren mit Benutzeranmeldung erforderlich.

1. Sie werden während des Challenge/Response-Verfahrens zum Wechseln des Kennworts aufgefordert.

   Hinweis: Der Dialog zum Wechseln des Kennworts wird nur angezeigt, wenn eine Verbindung zum Domänen-Controller besteht.

2. Wenn eine Anmeldung mit Token und PIN obligatorisch ist, haben Sie die Möglichkeit zu entscheiden, ob Sie das Kennwort wechseln wollen, oder ob Sie den Wechsel des Kennworts durch Klicken auf **Abbrechen** übergehen wollen.

   - **Sie haben Ihren Token vergessen**

     Das Abbrechen des Dialogs durch Klicken auf **Abbrechen** macht nur Sinn, wenn Sie Ihren Token vergessen haben und z. B. am nächsten Tag wieder zur Verfügung haben. Wenn Sie auf **Abbrechen**klicken, werden Sie angemeldet und können auf Ihrem Computer weiterarbeiten.

     Ohne Token können Sie sich nur über Challenge/Response in der SafeGuard Power-on Authentication anmelden. Wenn Sie Ihren Token wieder zur Verfügung haben, können Sie sich damit auch wieder in der SafeGuard POA anmelden.

   - **Sie haben Ihren Token verloren**

     Wenn Sie Ihren Token verloren haben, geben Sie im Dialog zum Wechsel des Kennworts ein neues Kennwort an. Sie werden mit diesem Kennwort an Windows angemeldet. Wenn es die Richtlinien auf Ihrem Computer erlauben (Token-Anmeldung in der SafeGuard POA ist nicht verpflichtend), können Sie sich mit diesem Kennwort auch in der SafeGuard Power-on Authentication anmelden.

     Ein Missbrauch des Token durch einen Finder kann ausgeschlossen werden. Unberechtigte Benutzer können den Token nicht zur Anmeldung benutzen, auch wenn ihnen die PIN des Token bekannt sein sollte, da ja auch Ihr Kennwort geändert wurde.

16.1.6.4 Sie haben Ihre PIN vergessen

1. Wenn Sie die PIN Ihres Token vergessen haben, fordern Sie eine Response an und geben Sie ein neues Kennwort ein. Sie werden mit diesem Kennwort an Windows angemeldet. Sie können sich mit diesem Kennwort auch an der SafeGuard Power-on Authentication anmelden, vorausgesetzt dass Sie zur Anmeldung mit einem Kennwort berechtigt sind.
2. Der Token muss danach von einem Sicherheitsbeauftragten mit einer neuen PIN versehen werden und Ihre neuen Anmeldeinformationen müssen darauf gespeichert werden. Sie können den Token dann für die Anmeldung verwenden.

16.1.6.5 Sie können nicht mehr auf Ihren Computer zugreifen

Wenn Sie nicht mehr auf Ihren Computer zugreifen können, ist u. U. die SafeGuard Power-on Authentication beschädigt. Auch in dieser kritischen Situation bietet SafeGuard Enterprise ein Challenge/Response-Verfahren, über das Sie wieder Zugriff auf Ihre verschlüsselten Laufwerke erhalten. Das Challenge/Response-Verfahren wird in diesem Fall über eine WinPE-Umgebung ausgeführt. Sollte diese kritische Situation eintreten, wenden Sie sich an Ihren SafeGuard Enterprise Helpdesk. Der Helpdesk-Beauftragte stellt Ihnen die notwendigen Dateien zur Verfügung und führt Sie durch die notwendigen Handlungsschritte, um den Zugriff auf Ihren Computer wiederherzustellen.

16.1.7 Challenge/Response für Offline-Benutzer

Beim Challenge/Response-Verfahren für Offline-Benutzer sind einige Besonderheiten zu beachten. Für Offline-Benutzer, also Benutzer die keine Verbindung zum Domänen-Controller haben (z. B. Vertriebsmitarbeiter im Außendienst, die mit ihren Notebooks arbeiten), kann im Rahmen des Challenge/Response-Verfahrens kein automatischer Kennwortwechsel ausgelöst werden.

16.1.7.1 Challenge/Response für Offline-Benutzer mit Anmeldemodus Benutzername/Kennwort

Beispiel:

Sie arbeiten Offline, haben also keine Verbindung zum Domänen-Controller und haben Ihr Kennwort vergessen. Das Challenge/Response-Verfahren verhilft Ihnen einfach und schnell wieder zum Zugriff auf Ihren Computer.

SafeGuard Enterprise würde Sie im Rahmen des Challenge/Response-Verfahrens auch automatisch an Windows anmelden. Da Sie aber auch nach diesem Challenge/Response-Verfahren Ihr Kennwort noch nicht wissen, müssten Sie dieses Verfahren bei jedem Start-Vorgang wiederholen. Sie wären außerdem nicht in der Lage, eine mögliche Sperre des Computers (z. B. Computersperre bei Aktivierung des Bildschirmschoners) wieder aufzuheben. Sie müssten dann mit der Gefahr des Datenverlustes den Computer neu starten (und ein erneutes Challenge/Response-Verfahren durchführen).

Hinweis: Aus diesem Grund bietet SafeGuard Enterprise die Möglichkeit, sich das Kennwort im Rahmen eines Challenge/Response-Verfahrens anzeigen zu lassen. Als Offline-Benutzer sollten Sie sich Ihr Kennwort bei einem Challenge/Response-Verfahren immer anzeigen lassen. Bitte weisen Sie Ihren Helpdesk-Beauftragten darauf hin, dass Sie das Kennwort angezeigt haben möchten. Der Helpdesk- Beauftragte muss die Anzeige des Kennworts explizit aktivieren, bevor er Ihren Response-Code erzeugt.

Gehen Sie wie folgt vor:

1. Starten Sie das Challenge/Response-Verfahren durch Klicken auf die Schaltfläche **Recovery** im SafeGuard POA-Anmeldedialog.
2. Rufen Sie bei Ihrem Helpdesk an und geben Sie den Challenge- Code durch.
3. Weisen Sie den Helpdesk-Beauftragten darauf hin, dass Sie Ihren Computer mit Benutzeranmeldung booten und Ihr Kennwort angezeigt haben möchten.
4. Klicken Sie im **Challenge/Response** Dialog auf **Weiter** und geben Sie die Response ein.
5. Klicken Sie auf **OK**.

   Sie werden gefragt, ob Sie das Kennwort auf dem Bildschirm angezeigt bekommen möchten.

6. Beantworten Sie die Frage mit **Ja** und klicken Sie auf **OK**.
7. Im folgenden Dialog werden Sie darüber informiert, dass das Kennwort angezeigt wird, wenn Sie **Enter** oder die **Leertaste** auf der Tastatur drücken, oder in den Text klicken.

   Hinweis: Klicken Sie **NICHT** auf **OK**. Nach dem Klicken auf **OK** wird der Bootvorgang OHNE Kennwortanzeige fortgesetzt.

   Das Kennwort wird für 5 Sekunden angezeigt. Danach wird der Bootvorgang automatisch fortgesetzt.

8. Drücken Sie **Enter** oder die **Leertaste** auf der Tastatur, oder klicken Sie in den Text.

   Das Kennwort wird angezeigt.

   Hinweis: Achten Sie unbedingt darauf, dass kein Unbefugter zufällig oder absichtlich Ihren Bildschirm einsehen kann. Sie können das Kennwort durch Drücken der **Leer-** bzw. der **Enter**-Taste oder durch einen Mausklick auf das blaue Anzeigefeld sofort verbergen. Das Kennwort wird für höchstens 5 Sekunden angezeigt.

9. Sie können das Kennwort lesen und sich damit wieder in der SafeGuard Power-on Authentication und an Windows anmelden.

   Sie können wie gewohnt weiterarbeiten.

16.1.7.2 Challenge/Response für Offline-Benutzer mit Anmeldemodus „Nur Token“

Wenn Sie in diesem Fall Ihre PIN/Ihren Token vergessen oder verloren haben, ist die Vorgehensweise abhängig davon, ob Sie ihre Windows-Anmeldeinformationen kennen oder nicht.

- Windows-Anmeldeinformationen bekannt

  a) Wenn Sie Ihre Windows-Anmeldeinformationen kennen, starten Sie wie bereits beschrieben ein Challenge/Response-Verfahren. Sie werden automatisch an Windows angemeldet.

  Der Anmeldemodus **Nur Token** wird für die Dauer der Arbeitssitzung, die an das Challenge/Response-Verfahren anschließt, zurückgesetzt. So ist eine Anmeldung an Windows auch mit Benutzername und Kennwort möglich.

  Sollte also die Computersperre aktiviert werden, können Sie den Computer durch die Eingabe Ihres Windows-Kennworts wieder entsperren. Die Anmeldung an der SafeGuard Power-on Authentication ist jedoch nur über Challenge/Response möglich.

- Windows-Anmeldeinformationen nicht bekannt

  a) Sollten Sie Ihre Windows-Anmeldeinformationen nicht kennen, können Sie auch im Fall einer vergessenen PIN ein Challenge/Response-Verfahren starten, während Ihnen Ihr Kennwort angezeigt wird.

  b) Weisen Sie den Helpdesk-Beauftragten darauf hin, dass Sie das Kennwort angezeigt haben möchten.

  Da der Anmeldemodus **Nur Token** außer Kraft gesetzt wird, können Sie dann auch eine eventuelle Sperre des Computers mit dem Kennwort aufheben. Die Anmeldung an der SafeGuard Power-on Authentication ist jedoch ausschließlich über Challenge/Response möglich.

16.2 Challenge/Response für BitLocker-Benutzer

Allgemeine Hinweise zur Benutzung der Maus und/oder der Tastatur

- Sie können Steuerelemente mit der Maus und/oder der Tastatur auswählen. Um mit Hilfe der Tastatur von einem Steuerelement zum nächsten zu springen, drücken Sie die **Tab** Taste. Um zum vorigen Steuerelement zurückzukehren, drücken Sie die Tastenkombination **Umschalttaste+Tab Taste**.
- Um eine Auswahl zu bestätigen, drücken Sie die **Enter** Taste.

Challenge/Response-Verfahren

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

1. Starten Sie den PC neu. Nach dem Neustart wird eine Meldung mit gelbem Text auf schwarzem Grund angezeigt. Drücken Sie innerhalb der nächsten drei Sekunden eine beliebige Taste.
2. Der Challenge/Response-Bildschirm wird angezeigt.
3. Im zweiten Schritt erhalten Sie die Informationen, die Sie benötigen, um sich an den Helpdesk zu wenden.
4. Teilen Sie dem Helpdesk die folgenden Informationen mit:

Computer, zum Beispiel Sophos\<Computername>

Challenge-Code, z. B. ABC12-3DEF4-56GHO-892UT-Z654K-LM321. Fahren Sie mit der Maus über die einzelnen Zeichen, um eine Buchstabierhilfe einzublenden. Oder drücken Sie mehrmals **F1**, um diese Hilfe einzublenden. Der Code wird nach 30 Minuten ungültig. Dann wird der PC automatisch heruntergefahren.

5. Geben Sie dann den vom Helpdesk erhaltenen **Response-Code** (sechs Blöcke mit jeweils zwei Text-Feldern, pro Feld sind 5 Zeichen erforderlich) ein.
   - Wenn ein Textfeld komplett mit Zeichen ausgefüllt ist, geht der Fokus automatisch auf das nächste Textfeld über.
   - Wenn Sie in einem Block ein falsches Zeichen angeben, wird der entsprechende Block rot markiert. Korrigieren Sie die Einträge mit der **Entf**oder der **Backspace**Taste.
6. Klicken Sie nach erfolgreicher Eingabe des Response-Code auf **Weiter** oder drücken Sie **Enter**, um die Challenge/Response-Aktion abzuschließen.

BitLocker-Anmeldeinformationen zurücksetzen

Sobald Sie sich erneut am System angemeldet haben, geben Sie die neuen BitLocker-Anmeldeinformationen ein, damit Sie das Challenge/Response-Verfahren beim nächsten Anmelden nicht erneut durchlaufen müssen. Abhängig vom Betriebssystem und der BIOS/UEFI-Version zeigt das System einen Dialog zum Zurücksetzen der Anmeldeinformationen an.

Wenn dieser Dialog nicht automatisch angezeigt wird, klicken Sie mit der rechten Maustaste auf das SafeGuard Enterprise-Symbol in der Taskleiste. Es öffnet sich ein Kontextmenü. Wählen Sie **BitLocker Anmeldeinformationen zurücksetzen** aus und folgen Sie den Anweisungen auf dem Bildschirm.

Hinweis:

Wenn Sie das System herunterfahren oder neu starten möchten, klicken Sie mit der Maus auf die Shutdown-Schaltfläche oder drücken Sie die **Tab** Taste wenn die Shutdown-Schaltfläche hervorgehoben ist.

16.3 BitLocker Recovery-Schlüssel

Als BitLocker Benutzer eines Systems, das SafeGuard Challenge/Response nicht unterstützt, können Sie einen BitLocker Recovery-Schlüssel von Ihrem Helpdesk anfordern.

Allgemeine Hinweise zur Benutzung der Maus und/oder der Tastatur

- Sie können Steuerelemente mit der Maus und/oder der Tastatur auswählen. Um mit Hilfe der Tastatur von einem Steuerelement zum nächsten zu springen, drücken Sie die **Tab** Taste. Um zum vorigen Steuerelement zurückzukehren, drücken Sie die Tastenkombination **Umschalttaste+Tab Taste**.
- Um eine Auswahl zu bestätigen, drücken Sie die **Enter** Taste.

Anforderung des Recovery-Schlüssels

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

1. Starten Sie den Endpoint neu. Drücken Sie nach dem Neustart die **Esc**-Taste auf dem BitLocker-Anmeldebildschirm.
2. Der Bildschirm für die Eingabe eines BitLocker Recovery-Schlüssels wird angezeigt.
3. Im zweiten Schritt erhalten Sie die Informationen, die Sie benötigen, um sich an den Helpdesk zu wenden.

   Zum Beispiel: <Computername> C: 25.09.2014

4. Teilen Sie dem Helpdesk den **Computernamen** mit.
5. Geben Sie dann den vom Helpdesk erhaltenen **BitLocker Recovery-Schlüssel** (acht Blöcke mit jeweils 6 Zeichen pro Feld) ein.
6. Wenn Sie den Response-Code erfolgreich eingeben haben, klicken Sie auf **Fortsetzen**oder drücken Sie die **Enter** Taste, um die Challenge/Response-Aktion abzuschließen.

BitLocker-Anmeldeinformationen zurücksetzen

Sobald Sie sich erneut am System angemeldet haben, geben Sie die neuen BitLocker-Anmeldeinformationen ein, damit Sie das Challenge/Response-Verfahren beim nächsten Anmelden nicht erneut durchlaufen müssen. Abhängig vom Betriebssystem und der BIOS/UEFI-Version zeigt das System einen Dialog zum Zurücksetzen der Anmeldeinformationen an.

Wenn dieser Dialog nicht automatisch angezeigt wird, klicken Sie mit der rechten Maustaste auf das SafeGuard Enterprise-Symbol in der Taskleiste. Es öffnet sich ein Kontextmenü. Wählen Sie **BitLocker Anmeldeinformationen zurücksetzen** aus und folgen Sie den Anweisungen auf dem Bildschirm.

Hinweis:

Wenn Sie das System herunterfahren oder neu starten möchten, klicken Sie mit der Maus auf die Shutdown-Schaltfläche oder drücken Sie die **Tab** Taste wenn die Shutdown-Schaltfläche hervorgehoben ist.

17 SafeGuard Enterprise und Lenovo Rescue and Recovery

Hinweis: Lenovo Rescue and Recovery ist nur für Windows 7 Endpoints verfügbar.

Es besteht die Möglichkeit, vollständige Betriebssystem-Sicherungskopien auf einer verschlüsselten Partition wiederherzustellen, ohne dass dazu die Festplatte zunächst entschlüsselt werden muss. Dies bewirkt eine erhebliche Zeitersparnis bei der Durchführung von Recovery-Vorgängen in Notfallsituationen. SafeGuard Enterprise wurde offiziell von Lenovo für diese Funktionalität zertifiziert.

Lenovo Rescue and Recovery bietet als zentrale Funktion die Wiederherstellung von Daten per Tastendruck. Auch wenn das primäre Betriebssystem beschädigt ist und nicht mehr startet, rettet Rescue and Recovery Daten über eine Notfall-Umgebung. Die Recovery-Tools sind über den Microsoft Windows Desktop oder die in Lenovo-Systeme integrierte, blaue „ThinkVantage“-Taste aufrufbar.

Lenovo Rescue and Recovery zielt primär auf mobile Endbenutzer, die maximale Sicherheit für ihre Notebooks anstreben, sich im Fall eines Systemproblems jedoch selbst helfen müssen. So können Benutzer zum Beispiel auf Geschäftsreisen mit Lenovo Rescue and Recovery Recovery-Vorgänge durchführen.

Informationen zu den von SafeGuard Enterprise unterstützten Lenovo Rescue and Recovery (RnR)-Versionen finden Sie unter
http://www.sophos.com/de-de/support/knowledgebase/108383.aspx

17.1 Überblick

SafeGuard Enterprise integriert sich reibungslos in die Rescue and Recovery-Funktionalität und unterstützt natürlich auch Lenovo-eigene Features wie die „Thinkvantage“-Taste auf der Tastatur von Notebooks oder die blaue „Eingabe“-Taste bei Desktop-PCs.

In der Anwendung von SafeGuard Enterprise in Verbindung mit Lenovo Rescue and Recovery können Sie diese effiziente Backup- und Recovery-Methode mit Betriebssystempartitionen, die mit SafeGuard Enterprise verschlüsselt sind, benutzen. Sicherungskopien von verschlüsselten SafeGuard Enterprise Systemen lassen sich auf jedem von RnR benutzten Laufwerk speichern. Somit kann ein System im Notfall durch Laden der Sicherungskopie von einer virtuellen Partition oder einer Service-Partition, oder von einem Wechselmedium (z. B. CD/DVD oder USB-Festplatte) wiederhergestellt werden.

SafeGuard Enterprise „überlebt“ eine Systemwiederherstellung, ohne dass dabei die Verschlüsselung verloren geht, und muss nicht neu installiert werden. Sie werden nicht durch erneutes Anstoßen der Verschlüsselung gestört.

In einer SafeGuard Enterprise Umgebung basiert Rescue and Recovery auf WinPE Recovery. WinPE kann wie folgt gestartet werden:

- von einer virtuellen Partition oder einer Service-Partition aus,
- von einem Wechselmedium aus, z. B. CD/DVD oder USB-Festplatte.

17.2 Voraussetzungen

- Aktuelles BIOS für den PC/das Notebook
- Informationen zur Kompatibilität von Lenovo Rescue and Recovery Versionen mit SafeGuard Enterprise Versionen finden Sie unter folgendem Link: http://www.sophos.com/de-de/support/knowledgebase/108383.aspx
- Lenovo Rescue and Recovery kann benutzt werden, um mit SafeGuard Enterprise verschlüsselte Volumes wiederherzustellen. Das `SGNClient.msi` Paket muss installiert sein.
- Für Rescue and Recovery müssen Volumes mit dem definierten Computerschlüssel verschlüsselt sein. Für Volumes, die mit einem anderen Schlüssel verschlüsselt sind, wird Rescue and Recovery nicht unterstützt.

17.3 Installation

Wenn Sie Rescue and Recovery auf einer Festplatte ohne eine Service-Partition installieren, sind folgende Aspekte zu beachten:

Die Umgebung von Rescue and Recovery wird auf einer virtuellen Partition auf Laufwerk C (primäre Partition des Master-Festplattenlaufwerks) des Computers installiert.

Beachten Sie in den folgenden Abschnitten die Reihenfolge, in der Rescue and Recovery und SafeGuard Enterprise installiert werden. Wir empfehlen, zunächst Lenovo Rescue and Recovery und dann SafeGuard Enterprise zu installieren.

17.3.1 Installieren von Rescue and Recovery und SafeGuard Enterprise

Wir empfehlen diese Installationsreihenfolge.

1. Installieren Sie die aktuellste Version von Rescue and Recovery.
2. Installieren Sie die aktuellste Version des Moduls SafeGuard Enterprise Device Encryption (SGNClient.msi).

   SafeGuard Enterprise prüft, ob Rescue and Recovery installiert ist, und fügt seine Dateien und Einstellungen in die Lenovo Notfallumgebung ein.

3. Stellen Sie sicher, dass die SafeGuard Power-on Authentication aktiviert ist, so dass kein Unbefugter unautorisiert beliebige Backups wiederherstellen kann.

   Die SafeGuard Power-on Authentication wird während der Installation von SafeGuard Enterprise aktiviert.

17.3.2 Rescue and Recovery ist bereits installiert

RnR WinPE befindet sich auf der ersten Festplatte auf einer Service-Partition oder einer virtuellen Partition.

In diesem Fall werden alle notwendigen Treiber und Dateien in die entsprechenden Speicherorte von RnR WinPE kopiert und alle notwendigen Registry-Einträge werden in die Registry-Dateien von WinPE eingefügt.

Installieren Sie die aktuellste Version des Moduls SafeGuard Enterprise Device Encryption (SGNClient.msi).

SafeGuard Enterprise prüft, ob Rescue and Recovery installiert ist, und fügt seine Dateien und Einstellungen in die Lenovo Notfall-Umgebung (WinPE) ein.

17.4 Upgrade

Eine Aktualisierung bedeutet, dass SafeGuard Enterprise und Rescue and Recovery installiert sind und Sie eine der beiden Versionen auf eine neuere Version aktualisieren möchten.

SafeGuard Enterprise Aktualisierung

Durch eine Aktualisierung von SafeGuard Enterprise wird das gesamte System aktualisiert. Sie müssen somit keine weiteren Konfigurationseinstellungen vornehmen.

17.5 Deinstallation

Bei der Deinstallation beider Produkte ist folgendes zu beachten:

- Wir empfehlen, zunächst SafeGuard Enterprise und danach Rescue and Recovery zu deinstallieren. Wenn SafeGuard Enterprise deinstalliert wird und Rescue and Recovery weiterhin installiert ist, werden alle SafeGuard Enterprise spezifischen Änderungen, z. B. hinzugefügte Laufwerke, Dateien und Registry-Einträge, aus RnR WinPE entfernt.
- Die Deinstallation von SafeGuard Enterprise darf nicht unmittelbar auf eine Systemwiederherstellung folgen. Starten Sie nach einer Systemwiederherstellung den Computer neu und deinstallieren Sie danach SafeGuard Enterprise.
- Wenn Rescue and Recovery deinstalliert wird und SafeGuard Enterprise weiterhin installiert ist, werden die RnR-Änderungen des MBR-Boot-Sektors entfernt und der ursprüngliche MBR-Boot-Sektor wird wiederhergestellt.

17.6 Boot-Umgebung und Recovery-Optionen

SafeGuard Enterprise erlaubt das Booten der Rescue and Recovery-Umgebung nach der erfolgreichen Anmeldung an der SafeGuard Power-on Authentication (POA)...

... von lokaler Festplatte

- Virtuelle Partition auf der lokalen Festplatte oder lokale Service-Partition
- Die Volumes müssen in SafeGuard Enterprise mit dem definierten Computerschlüssel verschlüsselt worden sein. Alle notwendigen Treiber müssen zu RnR WinPE hinzugefügt worden sein. Der definierte Computerschlüssel ist dann in der RnR WinPE Umgebung verfügbar und es besteht wieder Zugriff auf die Volumes.

Hinweis: SafeGuard Enterprise erlaubt das Booten der Rescue and Recovery-Umgebung beim direkten Starten von BIOS aus nicht.

... von boot-fähiger CD/DVD oder von anderen boot-fähigen Wechselmedien

- In diesem Fall wird keine Authentisierung an der SafeGuard Power-on Authentication durchgeführt und es stehen keine Schlüssel zur Verfügung. Somit besteht kein Zugriff auf verschlüsselte Volumes. Wird die Rescue and Recovery-Umgebung direkt vom BIOS aus gestartet, so wird das Betriebssystem wiederhergestellt. SafeGuard Enterprise wird während des Wiederherstellungsprozesses entfernt. Um das System wieder abzusichern, muss SafeGuard Enterprise erneut installiert werden.

17.7 Erstellen einer Sicherungskopie

Sicherungskopien werden über die Rescue and Recovery Software in der aktiven Windows-Umgebung erstellt. Auf Computern, auf denen bereits Rescue and Recovery installiert ist und SafeGuard Enterprise danach installiert wird, wird eine Meldung angezeigt, die den Benutzer zum Erstellen einer Sicherungskopie auffordert.

Bevor Sie eine System-Sicherungskopie erstellen, lesen Sie bitte in den entsprechenden Dokumenten von Lenovo nach.

SafeGuard Enterprise unterstützt für Sicherungskopien folgende Medien:

- Lokale Festplatte
- Zweites Festplattenlaufwerk
- USB-Festplattenlaufwerk
- Netzlaufwerk
- Systemstartschlüssel
- CD/DVD

Die Sicherungen bzw. Sicherungskopien werden in der Standardeinstellung unter `C:\RRUbackups` gespeichert. Dieses Verzeichnis wird, wenn es sich auf der lokalen Partition des primären Festplattenlaufwerks befindet, durch Rescue and Recovery geschützt. In diesem Fall kann es nicht gelöscht oder verschoben werden.

17.8 Wiederherstellen von Dateien aus Sicherungskopien

Rescue and Recovery stellt einzelne Dateien oder Verzeichnisse aus einem Backup, der ein installiertes SafeGuard Enterprise enthält, problemlos wieder her. Starten Sie einfach Windows, dann die Rescue and Recovery Software und stellen Sie die gesuchten Dateien wieder her. Es ist kein Neustart nötig, d. h. die wiederhergestellten Daten stehen Ihnen sofort zur Weiterbearbeitung zur Verfügung.

17.9 Wiederherstellen des SafeGuard Enterprise Systems

Um einen System-Backup, der SafeGuard Enterprise enthält, wiederherzustellen, starten Sie die Rescue and Recovery-Umgebung. Diese erscheint, wenn Sie beim Starten des PCs/Notebooks die folgenden Tasten drücken:

- „Thinkvantage" (bei Lenovo Notebooks)
- Die „Blaue Eingabetaste“ (bei Lenovo Desktop-PCs)
- **F11** bei anderen Tastaturen

1. Sie benutzen einen Lenovo-Computer:
   a) Starten Sie die Rescue and Recovery Umgebung von einer lokalen Festplatte, indem Sie die blaue „Thinkvantage“-Taste auf der Tastatur des Lenovo-Notebooks oder die blaue „Eingabe“-Taste auf der Tastatur des PCs drücken.

      Die SafeGuard Power-on Authentication wird angezeigt.

   b) Geben Sie Ihre SafeGuard Enterprise Anmeldeinformationen ein.

2. Sie benutzen keinen Lenovo-Computer:
   a) Melden Sie sich an der SafeGuard POA mit Ihren SafeGuard Enterprise Anmeldeinformationen an.
   b) Drücken Sie während des Startvorgangs des Computers **F11**, um die Rescue and Recovery Umgebung zu starten.

   Die Benutzeroberfläche für Rescue and Recovery wird angezeigt. Das Willkommen-Fenster wird angezeigt.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie im Menü auf der linken Seite die Option **Über Sicherung wiederherstellen**.

   Das System zeigt einen Dialog an, in dem Sie die Sicherungskopie auswählen können.
5. Wählen Sie die Sicherungskopie aus und stellen Sie sie wieder her.

17.10 Service und Factory Recovery Partitionen

Lenovo liefert neue Computer mit speziellen vorinstallierten Partitionen aus:

- **Lenovo Service Partition:** Enthält die Rescue and Recovery Boot-Umgebung.
- **Factory Recovery Partition:** Enthält alle Informationen zu den Werkseinstellungen des Computers sowie zu den Factory Recovery Funktionen.

Diese Partitionen sind in Windows unter separaten Laufwerksbuchstaben sichtbar.

Hinweis: Wenn diese Partitionen auf dem Computer zur Verfügung stehen, werden sie nicht verschlüsselt, auch wenn eine Verschlüsselungsrichtlinie zur Verschlüsselung aller Volumes definiert wurde.

Wenn auf dem Computer keine Partitionen dieser Art zur Verfügung stehen und sie aber dennoch mit diesen Partitionen arbeiten wollen, sollten Sie die Partition vor der Installation von SafeGuard Enterprise anlegen. Weitere Informationen finden Sie in Ihrer Lenovo-Dokumentation.

17.11 Deaktivierte SafeGuard POA und Lenovo Rescue and Recovery

Sollte auf Ihrem Computer die SafeGuard Power-on Authentication deaktiviert sein, so sollte zum Schutz vor dem Zugriff auf verschlüsselte Dateien aus der Rescue and Recovery Umgebung heraus die Rescue and Recovery Authentisierung eingeschaltet sein.

Detaillierte Informationen zur Aktivierung der Rescue and Recovery Authentisierung finden Sie in der Lenovo Rescue and Recovery Dokumentation.

18 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.

19 Rechtliche Hinweise