

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Benutzerhilfe

Produktversion: 5.60

Stand: April 2011



Inhalt

1	Über Sophos SafeGuard.....	3
2	Schlüssel-Backup für Recovery.....	5
3	Power-on Authentication.....	6
4	Power-on Authentication unter Windows Vista und Windows 7.....	18
5	Anmelden an Windows Vista und Windows 7.....	21
6	Anmeldung mit Lenovo Fingerabdruck-Leser.....	23
7	Recovery-Optionen.....	30
8	Recovery mit Local Self Help.....	31
9	Recovery mit Challenge/Response.....	41
10	System Tray Icon und Balloon-Ausgabe.....	45
11	Zugriff auf Funktionen über Explorer-Erweiterungen.....	48
12	Datenverschlüsselung.....	50
13	SafeGuard Data Exchange.....	54
14	Sophos SafeGuard und selbst-verschlüsselnde Opal-Festplatten.....	67
15	Sophos SafeGuard und Lenovo Rescue and Recovery.....	68
16	Technischer Support.....	73
17	Rechtliche Hinweise.....	74

1 Über Sophos SafeGuard

Sophos SafeGuard schützt die Informationen auf einem Endpoint-Computer durch ein richtlinienbasiertes Verschlüsselungskonzept. Die zentralen Sicherheitsfunktionen sind die Verschlüsselung von Daten sowie der Schutz vor nicht autorisiertem Zugriff auf den Computer. Sophos SafeGuard ist für den Endbenutzer einfach zu bedienen. Die Sophos SafeGuard eigene Authentisierung, die Power-on Authentication (POA), sorgt für den umfassenden Zugriffsschutz und bietet komfortable Unterstützung bei der Wiederherstellung von Anmeldeinformationen.

Die Verwaltung erfolgt über den SafeGuard Policy Editor. Mit dem SafeGuard Policy Editor werden Richtlinien angelegt und verwaltet. Darüber hinaus bietet der SafeGuard Policy Editor Recovery-Funktionen. Ein durch Sophos SafeGuard geschützter Computer erhält Sicherheitsrichtlinien über ein Konfigurationspaket, das im SafeGuard Policy Editor erstellt wird. Das Konfigurationspaket lässt sich über unternehmenseigene Verteilungs-Tools verteilen. Es kann jedoch auch manuell auf dem Computer installiert werden.

Hinweis: Sophos SafeGuard steht in unterschiedlichen Produkt-Bundles zur Verfügung: SGE (SafeGuard Easy) und ESDP (Endpoint Security and Data Protection). Ab Version 5.50 ist SGE der neue Produktname für SafeGuard Enterprise Standalone. Für die einzelnen Bundles sind unterschiedliche Module und Funktionen verfügbar. Module und Funktionen, die für ESDP nicht zur Verfügung stehen, sind in dieser Benutzerhilfe durch entsprechende Hinweise gekennzeichnet.

Folgende Module stehen für durch Sophos SafeGuard geschützte Computer zur Verfügung:

■ SafeGuard Device Encryption

Power-on Authentication

Die Benutzeranmeldung an das Gerät findet unmittelbar nach dem Einschalten statt. Nach erfolgreicher Power-on Authentication erfolgt die Anmeldung am Betriebssystem automatisch. Sie können die Power-on Authentication auch deaktivieren. Die Benutzer-Authentisierung erfolgt dann durch das Betriebssystem.

Volume-basierende Verschlüsselung

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

■ SafeGuard Data Exchange

Hinweis:

SafeGuard Data Exchange und SafeGuard Portable stehen mit ESDP nicht zur Verfügung.

SafeGuard Data Exchange bietet einfachen Datenaustausch mit Wechselmedien auf allen Plattformen ohne Neuverschlüsselung.

Dateibasierende Verschlüsselung

Es werden alle mobilen beschreibbaren Medien inklusive externe Festplatten und USB-Sticks transparent 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.

1.1 Sophos SafeGuard Features

Sophos SafeGuard bietet folgende Features:

■ Recovery-Optionen in der Power-on Authentication

Für Recovery-Vorgänge (z. B., wenn Sie Ihr Kennwort vergessen haben), bietet Sophos SafeGuard folgende Optionen:

Wenn Sie Ihr Kennwort vergessen haben, erhalten Sie mit Hilfe der Funktion **Local Self Help** schnell und einfach wieder Zugang zu Ihrem Computer, ohne dass Sie dafür die Unterstützung des Helpdesk benötigen. Um sich wieder an Ihrem Computer anzumelden, beantworten Sie einfach eine Reihe von vordefinierten Fragen in der Power-on Authentication. Mit Local Self Help erhalten Sie auch in Situationen wieder Zugang zu Ihrem Computer, in denen Sie weder Telefon- noch Netzwerkverbindungen nutzen können (z. B. in einem Flugzeug). Für weitere Informationen, [siehe Recovery mit Local Self Help](#) (Seite 31).

Challenge/Response ist ein sicheres und effizientes Recovery-System mit Unterstützung durch den Helpdesk, das Ihnen hilft, wenn Sie sich nicht mehr an Ihrem Computer anmelden können oder nicht mehr auf verschlüsselte Daten zugreifen können. Für weitere Informationen, [siehe Recovery mit Challenge/Response](#) (Seite 41).

■ Sophos SafeGuard System Tray icon

Über das Sophos SafeGuard System Tray Icon können Sie auf alle wichtigen Sophos SafeGuard Funktionen zugreifen. Das System Tray Icon befindet sich in der Windows-Taskleiste. Für weitere Informationen, [siehe System Tray Icon und Balloon-Ausgabe](#) (Seite 45).

■ Sophos SafeGuard Explorer-Erweiterungen

Über die entsprechenden Einträge in Windows Explorer Kontextmenüs können Sie auf alle Funktionen zugreifen, die sich auf die Verschlüsselung beziehen, [siehe Zugriff auf Funktionen über Explorer-Erweiterungen](#) (Seite 48).

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.

2 Schlüssel-Backup für Recovery

Für Recovery-Vorgänge bietet Sophos SafeGuard ein Challenge/Response-Verfahren [siehe Recovery mit Challenge/Response](#) (Seite 41)) für den vertraulichen Austausch von Informationen.

Damit Recovery-Vorgänge über Challenge/Response durchgeführt werden können, müssen die notwendigen Daten für den Helpdesk verfügbar sein. Die für den Recovery-Vorgang erforderlichen Daten werden in spezifischen Schlüssel-Recovery-Dateien (.XML-Dateien) gespeichert.

Wenn die Sophos SafeGuard Konfiguration auf Ihren Computer angewendet wird, wird die Schlüssel-Recovery-Datei automatisch an einem vom Sicherheitsbeauftragten angegebenen Speicherort erstellt. Wenn der Sicherheitsbeauftragte keinen Speicherort angegeben hat, werden Sie dazu aufgefordert, die Datei manuell zu speichern.

Ihr Sicherheitsbeauftragter kann beim Erstellen des Konfigurationspakets einen Speicherort für die Sicherungsdateien angeben. Der Speicherort ist in der Regel ein freigegebenes Netzwerklaufwerk. Die Sicherungsdatei wird automatisch dort erstellt.

Ist der vorgegebene Speicherort nicht erreichbar, wenn Sophos SafeGuard versucht, die Datei anzulegen, so erscheint eine Balloon-Ausgabe und eine entsprechende Meldung wird in das System-Ereignisprotokoll aufgenommen. Sophos SafeGuard versucht in diesem Fall, die Datei zu einem späteren Zeitpunkt zu speichern. Wenn der Sicherheitsbeauftragte keinen Speicherort angegeben hat, werden Sie aufgefordert, die Datei manuell zu speichern.

Wenn der Sicherheitsbeauftragte ein freigegebenes Netzwerklaufwerk für die Schlüssel-Recovery-Dateien angelegt hat und wenn Sie als lokaler Benutzer an Windows angemeldet sind, (zum Beispiel, wenn der Computer kein Domänen-Mitglied ist), werden Sie aufgefordert, die Zugangsdaten für das freigegebene Netzwerklaufwerk einzugeben. Ihr Sicherheitsbeauftragter kann Ihnen den erforderlichen Benutzernamen und das Kennwort nennen.

Hinweis: Speichern Sie die Datei, wenn Sie dazu aufgefordert werden, und stellen Sie sicher, dass Ihr Helpdesk Zugriff darauf hat. Die Dateien sind verschlüsselt und können auf einem beliebigen externen Medium gespeichert und so dem Helpdesk zugänglich gemacht werden. Auch das Versenden der Dateien via Mail ist möglich. Wenn Sie die Dateien nicht speichern, wird diese Aufforderung nach jedem Neustart angezeigt.

Über das Sophos SafeGuard System Tray Icon können Sie jederzeit ein neues Schlüssel-Backup erzeugen. Das Erzeugen eines neuen Schlüssel-Backups kann z. B. notwendig werden, wenn bereits erzeugte Schlüsseldateien beschädigt oder für den Helpdesk nicht mehr verfügbar sind.

3 Power-on Authentication

Die 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 POA

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

Angepasst werden können:

■ Anmeldebild

Das Standard-Anmeldebild der 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 Power-on Authentication werden in der Standardsprache angezeigt, die bei der Installation von Sophos SafeGuard in den Regions- und Sprachoptionen von Windows am Client gesetzt ist. Nach der Installation können Sie den POA-Dialogtext ändern, indem Sie die Standardsprache in den Windows Regions- und Sprachoptionen ändern. Die Sprache des Dialogtexts kann auch vom Sicherheitsbeauftragten in einer Richtlinie festgelegt werden.

3.1 Erste Anmeldung nach der Installation von Sophos SafeGuard

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

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

Hinweis: Die erfolgreiche Registrierung und der Erhalt aller notwendigen Daten, wird auf Ihrem Computer als Balloon-Ausgabe angezeigt.

Danach wird beim nächsten Neustart die Power-on Authentication aktiviert. Ab diesem Zeitpunkt müssen Sie nur noch Ihre Windows-Anmeldedaten in der POA eingeben. Sie werden dann (wenn die automatische Anmeldung an Windows aktiviert ist) ohne weitere Kennworteingabe auch an Windows angemeldet.

Sie können sich an der Power-on Authentication mit Ihrem Windows-Benutzernamen und Ihrem Kennwort anmelden.

Hinweis: Die Einstellungen für die Endpoint-Computer, auf denen Sophos SafeGuard installiert ist, werden vom Sicherheitsbeauftragten im SafeGuard Policy Editor definiert und in Richtliniendateien an die Benutzer verteilt.

3.2 Anmeldung an der Power-on Authentication

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

Hinweis:

Durch Klicken auf der **Optionen** >> Schaltfläche im Anmeldedialog und Abwählen der Option **Durchgehende Anmeldung an Windows** kann die automatische Anmeldung an Windows aufgehoben werden. Dies ist z. B. notwendig, um weiteren Benutzern die Anmeldung an der Power-on Authentication auf diesem Computer zu ermöglichen (*siehe Weiteren Benutzern die Anmeldung an der POA ermöglichen* (Seite 8)). 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.

Achten Sie bei der Anmeldung an der POA auf Groß- und Kleinschreibung.

Anmeldeverzögerung bei nicht erfolgreicher Anmeldung

Wenn die Anmeldung an der 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

Je nach geltender Richtlinie kann der Computer nach einer festgelegten Anzahl an fehlgeschlagenen Anmeldeversuchen gesperrt werden. Um die Computersperre aufzuheben, starten Sie ein Challenge/Response Verfahren *siehe Recovery mit Challenge/Response* (Seite 41).

3.2.1 Beispiel für die erste Anmeldung eines Benutzers an der POA

Voraussetzung dafür, dass die erste Anmeldung wie hier beschrieben abläuft, ist, dass die Power-on Authentication für Ihren Computer installiert und aktiviert.

Je nach Systemkonfiguration werden Sie dazu aufgefordert, **Ctrl+Alt+Del** zu drücken. Der Anmeldevorgang wird daraufhin fortgesetzt.

1. Schalten Sie Ihren Computer ein.

Der **POA Autologon** Dialog wird angezeigt.

2. Anschließend erscheint der Windows-Anmeldedialog. Melden Sie sich an Windows an.

Sie sind nun der „Besitzer“. Pro Computer gibt es einen Besitzer. In der Standardeinstellung ist der erste Benutzer, der sich anmeldet, der Besitzer.

3. Sind Benutzerrichtlinien, Zertifikat und Schlüssel auf dem Endpoint-Computer komplett vorhanden, wird ein Eintrag für Sie im Sophos SafeGuard Systemkern erzeugt.
4. Nach dem Neustart des Computers können Sie sich an der Power-on Authentication anmelden.

Hinweis: Der erste Benutzer, der sich in Windows anmeldet, wird in der Standardeinstellung automatisch als „Besitzer“ dieses Computers eingetragen. Nur der Besitzer eines Computers ist in der Lage, weiteren Benutzern die Anmeldung in der Power-on Authentication zu ermöglichen.

Damit sich weitere Benutzer in der POA anmelden können, muss ihnen das vom Besitzer des Computers ermöglicht werden (*siehe Weiteren Benutzern die Anmeldung an der POA ermöglichen* (Seite 8)).

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.

3.3 Weiteren Benutzern die Anmeldung an der POA ermöglichen

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

1. Schalten Sie den Computer ein.

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

2. Damit sich der zweite Benutzer an der 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 POA-Anmeldedialog auf **Optionen** und deaktivieren Sie das **Durchgehende Anmeldung an Windows** Kontrollkästchen.

Der Windows-Anmeldedialog wird angezeigt und der zweite Benutzer wird zur Anmeldung aufgefordert.

4. Der zweite Benutzer gibt seine Windows-Anmeldedaten ein.
5. Im Sophos SafeGuard Systemkern wird ein Eintrag für den zweiten Benutzer erzeugt.

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

3.4 Temporäres Kennwort in der POA

Sophos SafeGuard bietet Ihnen die Möglichkeit, das Kennwort in der 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 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 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 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 POA gültig!

5. Klicken Sie auf **OK**.

Sie werden an Windows angemeldet.

Zur Anmeldung in der 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 POA bis zu Windows - möglich.

Ändern des temporären Kennworts

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

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

Der Dialog mit der Aufforderung zum Wechseln des Kennworts kann ohne tatsächliche Änderung des Kennworts abgebrochen werden. Er wird in diesem Fall bei jeder Anmeldung angezeigt, bis das Kennwort tatsächlich geändert wird.

Hinweis: Das 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 POA bei der Anmeldung an Windows der Dialog zum Wechseln des Kennworts angezeigt. Er kann jedoch abgebrochen werden und das "alte Kennwort" kann zur Anmeldung verwendet werden. Die Änderung kann dann zu einem späteren Zeitpunkt vorgenommen werden.

3.5 Anmeldung an der Power-on Authentication mit Smartcard oder Token

Hinweis:

Die Anmeldung mit Token steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

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.

Hinweis: Smartcards und Token werden aus Sicht von Sophos SafeGuard 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.

3.5.1 Erste 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 (*siehe Speichern von Windows-Anmeldeinformationen auf dem Token* (Seite 11)), bevor Sie den Computer neu starten. Denn die für Sie gültigen Sicherheitsrichtlinien könnten eine verpflichtende Anmeldung an die Power-on Authentication mit Token vorschreiben. Befinden sich jedoch Ihre Anmeldeinformationen nicht auf dem Token, können Sie sich in der Power-on Authentication nicht anmelden.

3.5.2 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 die Power-on Authentication mit Token vorschreiben. Befinden sich keine Benutzerinformationen auf dem Token, können Sie sich in der 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 POA mit Benutzernamen und Kennwort angemeldet - können Sie Ihren Token auch später ausstellen.

Klicken Sie hierzu im 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.

3.5.3 Anmeldung an der Power-on Authentication 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 Benutzer-ID und Kennwort nicht angezeigt, können Sie sich in der Power-on Authentication ausschließlich mit Token anmelden.

3. Geben Sie Ihre Token-PIN ein.

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

3.5.4 Ändern der PIN

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

Wenn in der 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 diese Option bei der 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.

3.5.5 Recovery für die Anmeldung mit Token

Wenn Sie Ihre PIN vergessen haben, erhalten Sie mit einer der beiden folgenden Recovery-Methoden wieder Zugang zu Ihrem Computer:

- Recovery mit Local Self Help, [siehe Recovery mit Local Self Help](#) (Seite 31).
- Recovery mit Challenge/Response, [siehe Recovery mit Challenge/Response](#) (Seite 41).

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**.

3.5.6 Entsperren von Token

Wenn Sie die PIN zu oft falsch eingeben, wird Ihr Token gesperrt. Ihr Sicherheitsbeauftragter kann Sophos SafeGuard 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, bereits verwendete PINs können verboten sein usw.).

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. Mit Challenge/Response erhalten Sie zwar Zugriff auf Ihren Computer, eine Änderung der PIN bzw. Ihrer Benutzerinformationen ist aber nicht möglich.

3.5.7 Remotedesktop-Verbindung

Unter Windows XP ist es nicht möglich, eine Remotedesktop-Verbindung zu einem Computer aufzubauen, wenn die lokale Anmeldung an den Computer mit Token durchgeführt wurde.

Eine Remote-Übernahme kann in diesem Fall also nicht durchgeführt werden.

3.6 Recovery für die Anmeldung

Für Recovery-Vorgänge, wenn Sie z. B. ihr Kennwort vergessen haben, bietet Sophos SafeGuard 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. Für weitere Informationen, [siehe Recovery-Optionen](#) (Seite 30).

3.7 Virtuelle Tastatur

Sie haben die Möglichkeit, sich in der 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 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 und das Layout kann mit den gleichen Einstellungen wie das normale Tastaturlayout geändert werden (*siehe Ändern des Tastaturlayouts* (Seite 14)).

3.8 Tastaturlayout

Beinahe jedes Land hat ein eigenes Tastaturlayout. In der POA macht sich das Tastaturlayout bei der Eingabe von Benutzernamen, Kennwort und Response Code bemerkbar.

Sophos SafeGuard übernimmt standardmäßig das Tastaturlayout, das in den Regions- und Sprachoptionen von Windows für den Windows-Standardbenutzer zum Zeitpunkt der Installation von Sophos SafeGuard eingestellt ist. Ist unter Windows „Deutsch“ als Tastaturlayout gesetzt, wird in der POA das deutsche Tastaturlayout verwendet.

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

3.8.1 Ändern des Tastaturlayouts

Das normale wie das virtuelle Tastaturlayout der 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. Aktivieren 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 POA merkt sich das bei der letzten erfolgreichen Anmeldung verwendete Tastaturlayout und aktiviert dieses beim nächsten Anmelden automatisch. Hierzu sind zwei Neustarts des Endpoint-Computers notwendig. 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 Power-on Authentication eingelesen werden und dann auch über diese eingestellt werden kann.

Sie können das gewünschte Tastaturlayout der Power-on Authentication 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**.

3.9 Unterstützte Hotkeys und Funktionstasten in der Power-on Authentication

Bestimmte Hardware-Einstellungen und -Funktionalitäten können Probleme beim Booten des Computers verursachen, die dazu führen, dass der Rechner im Startvorgang hängen bleibt. Die 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 Sophos SafeGuard Installation die aktuelle Version der POA-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung: <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

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 POA-Konfigurationsdatei definiert ist oder gefunden wird.

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

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

Für weitere Informationen, siehe <http://www.sophos.de/support/knowledgebase/article/65700.html>.

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

3.9.1 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 - F3	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.

Shift - F3	Shift - F3	Shift - F7	Legacy	USB 1.x	USB 2.0	Anmerkung
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 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 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 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 Sophos SafeGuard Client über eine **.mst** Datei vordefiniert wurden.

Nach dem Ändern der Hardware-Einstellungen über die Hotkeys im Rahmen der 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 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 POA verwendet wurde. Unveränderte Werte werden schwarz angezeigt. Um den Dialog zu schließen, drücken Sie nochmal **F5** oder **Return**.

3.9.2 Funktionstasten im Anmeldedialog

Hinweis: Die Funktionstasten sind keine Hotkeys!

F2 = Abbrechen des Autologon

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

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

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

Abbrechen und POA auf den Shutdown vorbereiten

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

Hinweis: Bei aktivierter Anmeldung mit Fingerabdruck können Sie im POA-Dialog für die Anmeldung mit Fingerabdruck durch Drücken von **Strg+Alt+Entf** in den POA-Dialog für die Anmeldung mit Benutzername und Kennwort wechseln. Für weitere Informationen zur Anmeldung mit Fingerabdruck, [siehe Anmeldung mit Lenovo Fingerabdruck-Leser](#) (Seite 23).

3.10 Kennwortsynchronisierung

Sophos SafeGuard erkennt automatisch, wenn ein Windows-Kennwort geändert wurde und daher nicht mehr mit dem in der Sophos SafeGuard 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 Sophos SafeGuard einen solchen Fall erkennt, wird der Benutzer informiert und dazu aufgefordert, das alte Kennwort einzugeben. Danach wird das von Sophos SafeGuard gespeicherte Kennwort durch das neue Windows-Kennwort aktualisiert.

Die Kennwort-Synchronisierung wird in zwei Situationen durchgeführt:

- Während der Anmeldung
- Während eines Windows Sperren/Entsperren-Vorgangs

4 Power-on Authentication unter Windows Vista und Windows 7

Die Power-on Authentication unter Windows Vista und Windows 7 ist in Ihrem Erscheinungsbild und Verhalten identisch zu der unter Windows XP. Unterschiede ergeben sich nur bei der Anmeldung an das Betriebssystem selbst.

Hinweis: Dieser Abschnitt beschreibt nur die Unterschiede, die sich für Windows Vista und Windows 7 ergeben. Wird nicht ausdrücklich auf Unterschiede hingewiesen, sind die zuvor beschriebenen Verfahren/Abläufe auch für Windows Vista und Windows 7 gültig ([siehe Power-on Authentication](#) (Seite 6)).

4.1 Erste Anmeldung nach der Installation von Sophos SafeGuard unter Windows Vista und Windows 7

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

Hinweis: Unter Windows Vista und Windows 7 müssen Sie zunächst die Tastenkombination **STRG+ALT+ENTF** (CTRL+ALT+DEL) drücken, um Autologon und Windows-Logon zu starten. Diese Einstellung kann der Administrator in der MMC-Konsole im Gruppenrichtlinien-Objekteditor unter **Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen** deaktivieren. (Für die interaktive Anmeldung ist **Strg+Alt+Entf** nicht erforderlich.)

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 Sophos SafeGuard Benutzer registriert. Diese Registrierung ist die Bedingung dafür, dass ihre Zugangsdaten beim nächsten Systemstart auch in der POA bekannt sind.

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

Danach wird beim nächsten Neustart die Power-on Authentication aktiviert. Ab diesem Zeitpunkt müssen Sie nur noch Ihre Windows-Anmeldedaten in der POA eingeben. Sie werden dann (wenn die automatische Anmeldung an Windows aktiviert ist) ohne weitere Kennworteingabe auch an Windows angemeldet.

Die Anmeldung in der Power-on Authentication ist möglich mit Benutzername und Kennwort.

Hinweis: Die Einstellungen für die Endpoint-Computer, auf denen Sophos SafeGuard installiert ist, werden vom Sicherheitsbeauftragten im SafeGuard Policy Editor festgelegt und in Richtliniendateien an die Endpoint-Computer verteilt.

4.1.1 Ablauf der ersten Anmeldung

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

1. Nach dem Starten des Computers wird der Sophos SafeGuard Autologon Dialog angezeigt.
Ein Autouser wird angemeldet.

2. Der Windows Vista/Windows 7 Anmeldebildschirm wird angezeigt.

Unter Windows Vista und Windows 7 bietet SafeGuard Enterprise die SafeGuard Enterprise Authentisierungsmethode sowie die Windows Vista/Windows 7 Authentisierungsmethode.

3. Windows Vista/Windows 7 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 Sophos SafeGuard Symbol angezeigt, wählen Sie dieses aus. Ist dies nicht der Fall, wählen Sie das Symbol für **Anderer Benutzer**.

4. Geben Sie wie gewohnt Ihre Windows-Benutzerdaten ein.

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

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

4.2 Anmeldung an der Power-on Authentication unter Windows Vista und Windows 7

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

Hinweis: Durch Drücken der **Optionen** >> Schaltfläche im Anmeldedialog und Deaktivieren der Option **Durchgehende Anmeldung an Windows** kann die automatische Anmeldung an Windows aufgehoben werden. Dies ist z. B. notwendig, um weiteren Benutzern die Anmeldung an der Power-on Authentication auf diesem Computer zu ermöglichen (*siehe Weiteren Benutzern die Anmeldung an der POA ermöglichen* (Seite 8)). 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 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

Je nach geltender Richtlinie kann der Computer nach einer festgelegten Anzahl an fehlgeschlagenen Anmeldeversuchen gesperrt werden. Um die Computersperre aufzuheben, starten Sie ein Challenge/Response Verfahren [siehe Recovery mit Challenge/Response](#) (Seite 41).

5 Anmelden an Windows Vista und Windows 7

Unter Windows Vista und Windows 7 stellt Sophos SafeGuard eine weitere Authentisierungsmethode parallel zu bereits vorhandenen zur Verfügung.

Wenn Sie im Anmeldedialog der Power-on Authentication die Option **Durchgehende Anmeldung an Windows** deaktivieren, wird der Windows Vista/Windows 7 Anmeldebildschirm angezeigt. In diesem Dialog können Sie auch eine andere Authentisierungsmethode auswählen.

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

5.1 Anmeldung mit Sophos SafeGuard

In der Regel werden Sie nach der Kennworteingabe in der Power-on Authentication automatisch an Windows angemeldet. Wenn Sie die **durchgehende Anmeldung an Windows** im POA-Anmeldedialog deaktivieren und zur Anmeldung an Windows die Sophos SafeGuard Methode verwenden, ist Sophos SafeGuard nach der Anmeldung an Windows Vista/Windows 7 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 Vista und Windows 7 Authentisierungsmethode

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

Wenn Sie die Windows Vista/Windows 7 Authentisierungsmethode verwenden, erfolgt die Anmeldung an Sophos SafeGuard erst nach der Anmeldung an das Betriebssystem.

Nach der Anmeldung an Windows Vista/Windows 7 wird, falls notwendig, automatisch die Sophos SafeGuard Authentisierungsapplikation gestartet, um die vollständige Sophos SafeGuard 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 Sophos SafeGuard zur Verfügung und Sie können z. B. auf verschlüsselte Daten zugreifen, wenn Sie den entsprechenden Schlüssel besitzen.

5.3 Kennwortsynchronisierung unter Windows Vista und Windows 7

Sophos SafeGuard erkennt automatisch, wenn ein Windows-Kennwort geändert wurde und daher nicht mehr mit dem 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 Sophos SafeGuard einen solchen Fall erkennt, wird der Benutzer informiert und dazu aufgefordert, das alte Kennwort einzugeben. Danach wird das von Sophos SafeGuard gespeicherte Kennwort durch das neue Windows-Kennwort aktualisiert.

Die Kennwort-Synchronisierung wird in zwei Situationen durchgeführt:

- Während der Anmeldung
- Während eines Windows Sperren/Entsperren-Vorgangs

6 Anmeldung mit Lenovo Fingerabdruck-Leser

Hinweis:

Diese Funktion steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

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.

Sophos SafeGuard unterstützt die Anmeldung mit Fingerabdruck in der 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 jedoch auch über externe USB-Tastaturen möglich.

Hinweis:

- Es wird jeweils nur ein angeschlossener Fingerabdruck-Leser an einem Computer akzeptiert.
- 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.
- Sophos SafeGuard
- Die empfohlene herstellerspezifische Software-Version muss vor Sophos SafeGuard installiert werden:
 - ThinkVantage Fingerprint for AuthenTecoder
 - ThinkVantage Fingerprint for UPEK.

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

Systemvoraussetzungen

- Windows XP, 32 Bit
- Windows Vista, 32 Bit, 64 Bit
- Windows 7, 32 Bit, 64 Bit

Unterstützte Hardware

Informationen zur unterstützten Hardware für die Fingerabdruck-Anmeldung finden Sie unter <http://www.sophos.de/support/knowledgebase/article/108789.html>.

Unterstützte Software

Informationen zur unterstützten Software für die Fingerabdruck-Anmeldung finden Sie unter <http://www.sophos.de/support/knowledgebase/article/111626.html>.

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 Sophos SafeGuard installiert sind.

1. Melden Sie sich an Ihrem Computer in der 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 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 PC/Ihr Notebook neu.

- 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 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.

- Starten Sie Ihren Computer neu.

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

- Führen Sie einen der registrierten Finger über den Leser.

Wird der Fingerabdruck erkannt, so liest die 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 25)).

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 Power-on Authentication 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 an Windows aktiviert oder deaktiviert ist und ob es Ihnen möglich ist, diese Einstellungen im POA-Anmeldedialog für die Anmeldung mit Benutzername und Kennwort (*siehe Anmeldung mit Benutzername/Kennwort* (Seite 27)) zu ändern, wird in den für Sie geltenden Richtlinien vom Sicherheitsbeauftragten festgelegt.

6.3.1 Symbole im Anmeldevorgang

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

	<p>Fordert Sie auf, den Finger über den Fingerabdruck-Leser zu führen.</p>
	<p>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.</p>
	<p>Gibt an, dass der Fingerabdruck-Leser gerade arbeitet und ausgelastet ist.</p>
	<p>Gibt an, dass der Fingerabdruck erfolgreich gelesen und eine Übereinstimmung gefunden wurde.</p>
	<p>Gibt an, dass der Fingerabdruck erfolgreich gelesen, jedoch keine Übereinstimmung gefunden wurde.</p>
	<p>Gibt an, dass der Fingerabdruck nicht eingelesen werden konnte. Führen Sie den Finger erneut über den Fingerabdruck-Leser.</p>
	<p>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.</p>

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

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 Power-on Authentication anmelden, falls

z. B. die Anmeldung mit Fingerabdruck aufgrund eines defekten Fingerabdruck-Lesers nicht möglich ist.

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

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

Hinweis: Wenn Sie im 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 korrupten 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 POA-Dialog für die Anmeldung mit Fingerabdruck zurückzukehren, drücken Sie nach Wunsch erneut die **Esc** Taste.

Wenn Sie mit der Esc-Taste in den 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 POA-Dialog für die Anmeldung mit Fingerabdruck wechseln müssen.

6.4 Ändern des Kennworts

1. Bei aktivierter Anmeldung mit Fingerabdruck in der 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 POA-Dialog für die Anmeldung mit Fingerabdruck. Dadurch wird der POA-Dialog für die Anmeldung mit Benutzername und Kennwort angezeigt.
3. Klicken Sie auf die Schaltfläche **Optionen** und deaktivieren Sie die Option **Durchgehende Anmeldung an Windows**.

Hinweis: Ob die durchgehende Anmeldung an Windows aktiviert oder deaktiviert ist und ob es Ihnen möglich ist, diese Einstellungen im 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 Sophos SafeGuard folgende Recovery-Methoden:

- Recovery mit Local Self Help, [siehe Recovery mit Local Self Help](#) (Seite 31).
- Recovery mit Challenge/Response, [siehe Recovery mit Challenge/Response](#) (Seite 41).

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 Ihnen beim Starten des Computers ein Kennwortwechsel angeboten wird, 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 Recovery-Optionen

Sophos SafeGuard 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

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 Power-on Authentication beantworten.

Für weitere Informationen, [siehe Recovery mit Local Self Help](#) (Seite 31).

■ Recovery mit Challenge/Response

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.

Für weitere Informationen, [siehe Recovery mit Challenge/Response](#) (Seite 41).

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

8 Recovery mit Local Self Help

Für den Fall, dass Sie Ihr Kennwort vergessen haben und keine Möglichkeit haben, mit dem Helpdesk in Kontakt zu treten, bietet Sophos SafeGuard die Funktion Local Self Help.

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 Power-on Authentication anmelden.

Die zu beantwortenden Fragen können vom Sicherheitsbeauftragten zentral vordefiniert und an die Endpoint-Computer 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 Sophos SafeGuard System Tray Icon in der Windows-Taskleiste.

Recovery mit Local Self Help steht in der Power-on Authentication für die folgenden Anmeldeverfahren zur Verfügung:

- Anmeldung mit Benutzername und Kennwort
- Anmeldung mit Fingerabdruck
- Anmeldung mit nicht kryptographischem Token, unter der Voraussetzung, dass die Anmeldung mit Benutzer-ID und Kennwort auch als möglicher Anmeldemodus per Richtlinie aktiviert ist.

Hinweis:

Die Anmeldung mit Fingerabdruck und Token steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

Voraussetzungen

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

- Der zuständige Sicherheitsbeauftragte hat Local Self Help per Richtlinie freigeschaltet und die Einstellungen für die Funktion (z. B. Berechtigung zur Definition eigener Fragen) definiert.
- Sie haben Local Self Help auf Ihrem Computer über den Local Self Help Assistenten aktiviert (*siehe Aktivieren von Local Self Help* (Seite 31)).

8.1 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 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 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 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:

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 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 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:

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 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 Power-on Authentication benutzen.

Hinweis:

Wenn auf Ihrem Computer Local Self Help aktiv ist und Sie über ein Challenge/Response-Verfahren Ihr Kennwort zurücksetzen, sind die hinterlegten Antworten nach der Anmeldung über Challenge/Response nicht mehr gültig. Local Self Help ist dann nicht mehr auf Ihrem Computer aktiv. Um Local Self Help wieder zu aktivieren, beantworten Sie die Fragen erneut.

8.2 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 Sophos SafeGuard 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**.
 - a) Wenn Sie vordefinierte Fragen erhalten und beantwortet haben, wird der Dialog **Vordefinierte Fragen** mit den beantworteten Fragen angezeigt.
 - b) Wenn Sie mehrere Fragenthemen erhalten haben, können Sie in der Dropdown-Liste des Felds **Thema** zwischen den einzelnen Fragenthemen wählen.
 - c) 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.
 - d) Um die Antworten anzeigen zu lassen, wählen Sie das Kontrollkästchen **Antworten zeigen**.
 - e) Um die Antworten zu ändern, klicken Sie auf die jeweilige Frage und geben Sie in der Spalte **Antworten** eine neue Antwort ein.
5. Wenn Sie Ihre Änderungen abgeschlossen haben, 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.
6. Um die Antworten anzeigen zu lassen, aktivieren Sie das Kontrollkästchen **Antworten zeigen**.
 - a) Um bereits vorhandene Antworten zu ändern, klicken Sie auf die jeweilige Frage und geben Sie in der Spalte **Antworten** eine neue Antwort ein.
 - b) 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.
 - c) 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**.
7. Wenn Sie Ihre Änderungen abgeschlossen haben, 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.
8. 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.
9. Klicken Sie auf **OK**.
Die Änderungen in den Fragenlisten werden wirksam.

Wenn Sie Local Self Help das nächste Mal in der 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 Dialog **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, (*siehe Aktivieren von Local Self Help* (Seite 31)).

8.3 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 POA beantworten müssen, um sich mit Local Self Help anzumelden. Die in der 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. Die Anzahl an verfügbaren Fragen reicht nicht aus, damit Local Self Help auf Ihrem Endpoint-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	Um Local Self Help zu reaktivieren, starten Sie den Local Self Help Assistenten und folgen Sie den Anweisungen.

Bedingung	LSH-Aktion	Benutzer-Aktion erforderlich
	dann nicht mehr auf Ihrem Computer aktiv.	
Die Anzahl der Fragen, die Sie in der 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.

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

Local Self Help Parameter können sich während der Definition oder Bearbeitung von Fragen im Local Self Help Assistenten ändern. So kann z. B. eine neue Richtlinie mit neuen Local Self Help Einstellungen und/oder einem neuen Fragensatz für Local Self Help über unternehmensspezifische Verteilungsmechanismen an Ihren Computer übertragen werden.

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.	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

Bedingung	Aktion des LSH-Assistenten	Ergebnis
<p>Die von Ihnen definierten Fragen und Antworten sind weiterhin gültig und ausreichend, damit Local Self Help auf Ihrem Computer aktiv bleibt.</p>		<p>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 Fragen und/oder Antworten.</p>
<p>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.</p>	<p>Der Local Self Help Assistent zeigt eine Meldung an, die Sie darüber informiert, dass sich 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.</p>	<p>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.</p>

8.5 Anmeldung an der POA mit Local Self Help

1. Klicken Sie im 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 Power-on Authentication anmelden, entfernen Sie zunächst den Token/die Smartcard von Ihrem Computer. Daraufhin wird der POA-Dialog für die Anmeldung mit Benutzername und Kennwort angezeigt. Geben Sie Ihre Benutzer-ID ein und klicken Sie auf **Recovery**.

Hinweis:

Die Anmeldung mit Token steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

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 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 Power-on Authentication und an Windows angemeldet.

8.6 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.

9 Recovery mit Challenge/Response

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

Hinweis:

Wir empfehlen, Local Self Help einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Mit Local Self Help können Sie sich das aktuelle Benutzerkennwort anzeigen lassen und es weiterhin zur Anmeldung verwenden. Dadurch wird ein Zurücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden.

Beim Challenge/Response-Verfahren erzeugen Sie auf Ihrem Computer einen Challenge Code (eine Zeichenkette aus Ziffern und Buchstaben) und geben Sie 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 Local Self Help steht in der Power-on Authentication für die folgenden Anmeldeverfahren zur Verfügung:

- Anmeldung mit Benutzername und Kennwort
- Anmeldung mit Fingerabdruck

Hinweis:

Die Anmeldung mit Fingerabdruck steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

9.1 Voraussetzungen

Voraussetzung für Recovery für die Anmeldung über das Challenge/Response-Verfahren ist, dass der Helpdesk auf die Schlüssel-Recovery-Datei zugreifen kann. Diese Dateien müssen dem Helpdesk über ein Netzwerklaufwerk, via E-Mail, oder ein anderes Medium zugänglich gemacht werden.

Für den Fall, dass Sie Ihr Kennwort vergessen haben, muss auf dem Computer ein weiteres Benutzerkonto, das das Zurücksetzen des Kennworts ermöglicht, vorhanden sein. Sie können auch eine Kennwortrücksetzdiskette verwenden.

Über das Challenge/Response-Verfahren können Sie sich an der Power-on Authentication anmelden. Sie können sich auch an Windows anmelden, auch wenn das Windows-Kennwort zurückgesetzt werden muss.

9.2 Sie haben das Kennwort zu oft falsch eingegeben

Wenn Sie Ihr Kennwort zu oft falsch eingegeben haben und Ihr Computer auf POA-Ebene gesperrt ist, ermöglicht das Challenge/Response-Verfahren das Booten des Computers durch die Power-on Authentication. Danach wird der Windows-Anmeldedialog angezeigt. Geben Sie in diesem Dialog Ihr Windows-Kennwort ein, um sich anzumelden.

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

9.3 Sie haben Ihr Kennwort vergessen

Wenn das Kennwort über ein Challenge/Response-Verfahren wiederhergestellt wird, muss das Kennwort zurückgesetzt werden.

Hinweis:

Mit Local Self Help können Sie sich das aktuelle Benutzerkennwort anzeigen lassen und es weiterhin zur Anmeldung verwenden. Dadurch wird ein Rücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden. Für weitere Informationen, [siehe Recovery mit Local Self Help](#) (Seite 31).

1. Starten Sie ein Challenge/Response-Verfahren und folgen Sie den Anweisungen des Helpdesk. Ihr Computer bootet durch die Power-on Authentication bis auf Windows-Ebene.
2. Da Ihnen das Kennwort nicht bekannt ist, können Sie es im Windows-Dialog nicht eingeben. Sie müssen das Kennwort auf Windows-Ebene wiederherstellen. Hierzu sind weitere Recovery-Vorgänge außerhalb von Sophos SafeGuard erforderlich, die über Windows-Standard-Verfahren durchgeführt werden müssen.

Das Kennwort lässt sich auf Windows-Ebene über zwei verschiedene Methoden zurücksetzen:

- Über ein Service-Benutzerkonto oder ein Administratorkonto mit den erforderlichen Windows-Rechten, das auf Ihrem Computer zur Verfügung stehen muss.
- Über eine Windows-Kennwortrücksetzdiskette

Der Helpdesk-Beauftragte wird Sie darüber informieren, welche Methode benutzt werden soll, und die zusätzlichen Windows-Anmeldeinformationen oder die erforderliche Diskette zur Verfügung stellen.

3. Geben Sie das neue Kennwort, das Sie vom Helpdesk erhalten haben, auf Windows-Ebene ein und ändern Sie es unmittelbar danach in ein nur Ihnen bekanntes Kennwort.

Sophos SafeGuard stellt fest, dass das neu gewählte Kennwort nicht mehr mit dem aktuellen Sophos SafeGuard Kennwort übereinstimmt. Sie werden aufgefordert, das alte Kennwort einzugeben.

4. Für den Fall, dass Sie den Windows-Kennwortwechsel selber durchgeführt haben und das alte Kennwort noch wissen, können Sie den Kennwortwechsel auch für Sophos SafeGuard nachziehen, indem Sie hier das alte Kennwort eingeben. Ist dies nicht der Fall, klicken Sie auf **Abbrechen**.

Wenn das alte Kennwort nicht angegeben werden kann, ist in Sophos SafeGuard für die Definition eines neuen Kennworts ein neues Zertifikat erforderlich. Diese Aktion müssen Sie bestätigen. Basierend auf dem neu gewählten Windows-Kennwort wird ein neues Benutzerzertifikat erzeugt. Mit dem neuen Zertifikat können Sie sich wieder an Ihrem Computer und an der Power-on Authentication mit dem neuen Kennwort anmelden.

5. Melden Sie sich an der POA mit dem neuen Kennwort an.

Hinweis:

Schlüssel für SafeGuard Data Exchange: Wenn Sie das Windows-Kennwort vergessen haben und es zurückgesetzt wurde, können Sie die bereits für SafeGuard Data Exchange erstellten

Schlüssel nicht mehr ohne Passphrase verwenden. Damit bereits für SafeGuard Data Exchange generierte Benutzerschlüssel weiterhin verwendet werden können, müssen Ihnen die SafeGuard Data Exchange Passphrasen zur Reaktivierung dieser Schlüssel bekannt sein.

SafeGuard Data Exchange ist mit ESDP (Endpoint Security and Data Protection) nicht verfügbar.

9.4 Sie können nicht mehr auf Ihren Computer zugreifen

Wenn Sie nicht mehr auf Ihren Computer zugreifen können, ist u. U. die Power-on Authentication beschädigt. Auch in dieser kritischen Situation bietet Sophos SafeGuard 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 Sophos SafeGuard 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.

9.5 Ablauf eines Challenge/Response-Verfahrens

Das Challenge/Response-Verfahren muss gestartet werden:

- Wenn Sie das Kennwort zu oft falsch eingegeben haben.
- Wenn Sie das Kennwort nicht mehr wissen.
- Für das Reparieren eines beschädigten Caches.

Hinweis:

Standardmäßig ist Recovery für die Anmeldung bei einem beschädigten Local Cache deaktiviert. Er 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.

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.

1. Klicken Sie im POA-Anmeldedialog auf **Recovery**.

- Wenn für Sie nur Challenge/Response für Recovery für die Anmeldung aktiviert ist, wird das Challenge/Response-Verfahren gestartet.
- Wenn für Sie sowohl Challenge/Response als auch die Funktion Local Self Help zur Verfügung stehen, wird ein Dialog mit diesen beiden Auswahlmöglichkeiten angezeigt. Klicken Sie auf die Schaltfläche **Challenge/Response**, um das Challenge/Response-Verfahren zu starten.

Es wird ein Dialog angezeigt, der den Namen der für das Challenge/Response-Verfahren notwendigen Datei enthält.

2. Rufen Sie Ihren Helpdesk an. Teilen Sie dem Helpdesk-Beauftragten den Namen der Datei mit.

3. Klicken Sie auf **Weiter**.

Ihre Benutzerdaten und ein zufällig erzeugter Challenge-Code werden angezeigt. Zur besseren Übersicht ist der Code in Blocks von je 5 Zeichen unterteilt. Geben Sie dem Helpdesk-Beauftragten den Challenge-Code durch. Sie können dazu eine Buchstabierhilfe über die Schaltfläche **Buchstabieren** einblenden.

4. Klicken Sie auf **Weiter**.

Der Dialog **Challenge/Response - Schritt 3 von 3** wird angezeigt.

Der Helpdesk teilt Ihnen per Telefon oder SMS die Response mit.

5. Geben Sie den Response-Code in die Eingabefelder im Dialog **Challenge/Response - Schritt 3 von 3** ein.

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

6. Klicken Sie auf **OK**.

Die Anmeldung an der Power-on Authentication wird durchgeführt.

10 System Tray Icon und Balloon-Ausgabe

Über das System Tray Icon stehen folgende Funktionen zur Verfügung:

■ Anzeigen

■ Schlüsselring

Zeigt alle für Sie verfügbaren Schlüssel an.

Hinweis:

Der Sophos SafeGuard Computer benutzt einen definierten Computerschlüssel für die volume- und dateibasierende Verschlüsselung von Laufwerken. Diese Schlüssel wird *nicht* im Dialog angezeigt. Es werden nur Schlüssel, die lokal auf dem Computer erzeugt werden, angezeigt. Wenn Sie keine Schlüssel erzeugt haben, wird in diesem Dialog auch kein Schlüssel angezeigt.

Beachten Sie, dass die dateibasierende Verschlüsselung nicht mit ESDP (Endpoint Security and Data Protection) zur Verfügung steht.

■ Zertifikat

Zeigt Informationen zu Ihrem Zertifikat an.

■ Neuen Schlüssel erzeugen

Öffnet einen Dialog zum Erzeugen eines neuen Schlüssels für die Verwendung zum Datenaustausch über Wechselmedien.

Hinweis:

Diese Funktion steht mit ESDP nicht zur Verfügung.

■ Schlüssel-Backup

Über diese Funktion kann jederzeit eine Sicherungskopie der Schlüsseldatei erzeugt werden. Die Schlüsseldatei ist für das Recovery für die Anmeldung über Challenge/Response notwendig.

■ Local Self Help

Wenn für Sie 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. Für weitere Informationen, [siehe Recovery mit Local Self Help](#) (Seite 31).

- **Status:** Zeigt in einem Dialog Informationen über den derzeitigen Status des durch Sophos SafeGuard geschützten Computer:

Feld	Information
Zuletzt erhaltene Richtlinie	Zeigt, wann (Datum und Uhrzeit), der Computer zuletzt Richtlinien empfangen hat.

Feld	Information
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.
SGN-Benutzerstatus	<p>Zeigt den Status des Benutzers, der am Computer angemeldet ist (Windows-Anmeldung):</p> <ul style="list-style-type: none"> <p>■ Ausstehend</p> <p>Der Benutzer wird der Sophos SafeGuard Installation als Sophos SafeGuard-Benutzer zugewiesen. Bitte warten Sie, bis die Benutzerdaten verarbeitet worden sind. Danach wird der Benutzerstatus automatisch auf SGN-Benutzer, d. h. Sophos SafeGuard Benutzer, gesetzt.</p> <p>■ SGN-Benutzer</p> <p>Der Benutzer wurde der Sophos SafeGuard Installation als Sophos SafeGuard Benutzer zugewiesen.</p> <p>■ SGN-Gast</p> <p>Der an Windows angemeldete Benutzer ist ein Sophos SafeGuard Gastbenutzer. Der Benutzer kann sich an Windows anmelden, ohne dem durch Sophos SafeGuard geschützten Computer als Sophos SafeGuard Benutzer zugewiesen zu werden.</p> <p>■ SGN-Gast (Service Account)</p> <p>Der an Windows angemeldete Benutzer ist ein Sophos SafeGuard Gastbenutzer, der sich mit einem Service Account für administrative Aufgaben angemeldet hat.</p> <p>■ Unbekannt</p> <p>Gibt an, dass der Benutzerstatus nicht ermittelt werden konnte.</p>
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.

■ **Hilfe**

Öffnet die Sophos SafeGuard Online-Hilfe.

■ **Über Sophos SafeGuard**

Zeigt Informationen über Ihre Sophos SafeGuard Version.

Der Tooltip für das System Tray Icon gibt an, dass es sich bei dem Computer um einen Sophos SafeGuard Client (Standalone) handelt.

Hinweis:

Eine Balloon-Ausgabe informiert Sie über die erfolgreiche initiale Synchronisierung.

Starten Sie Ihren Computer nach erfolgreichem Abschluss der initialen Synchronisierung neu. Erst nach dem Neustart stehen Ihnen alle Sophos SafeGuard Funktionen zur Verfügung.

11 Zugriff auf Funktionen über Explorer-Erweiterungen

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

11.1 Explorer-Erweiterungen für dateibasierende Verschlüsselung

Hinweis:

Die dateibasierende Verschlüsselung steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

Die Funktionen zur dateibasierenden Verschlüsselung (*siehe Dateibasierende Verschlüsselung* (Seite 51)) sind über Einträge des Windows Explorer Kontextmenüs aufrufbar. Sie finden sie in den Kontextmenüs von:

- Volumes
- Wechselmedien
- Verzeichnissen
- Dateien

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

Gilt für das ausgewählte Volume keine dateibasierende Verschlüsselungsrichtlinie, kann im Kontextmenü nur der Verschlüsselungsstatus abgefragt und der Dialog zum Erzeugen neuer Schlüssel aufgerufen werden.

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

Hinweis: Die angezeigten Funktionen richten sich nach den in Richtlinien festgelegten Einstellungen. Außerdem spielt es eine Rolle, ob die relevante Funktion für das ausgewählte Volume verfügbar ist. Der Umfang der Funktionen ist unterschiedlich abhängig davon, ob es sich um ein dateibasierend oder volume-basierend verschlüsseltes Volume handelt.

Folgende Funktionen stehen zur Verfügung:

- **Verschlüsselung beginnen:** Wenn Sie diese Option im Kontextmenü eines Laufwerks auswählen, können alle Dateien mit einem neuen Schlüssel verschlüsselt bzw. umgeschlüsselt werden.
- **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 das ausgewählte Volume oder die ausgewählte Datei.
- **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.
- **Schlüsselverwaltung: Neuen Schlüssel erzeugen:** Öffnet den Dialog zum Erzeugen von benutzerdefinierten lokalen Schlüsseln.

11.2 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.

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.

Für weitere Informationen, [siehe Volume-basierende Verschlüsselung](#) (Seite 50).

12 Datenverschlüsselung

Sophos SafeGuard verschlüsselt Daten auf Ihrem Computer entweder volume-basierend oder dateibasierend.

Hinweis:

Hinweis: Die dateibasierende Verschlüsselung steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

Welche Volumes (Laufwerke) auf Ihrem Computer verschlüsselt werden, legt Ihr Sicherheitsbeauftragter in Sicherheitsrichtlinien fest.

12.1 Transparente Verschlüsselung

Die Dateien auf verschlüsselten Laufwerken 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.

12.2 Initialverschlüsselung

Wenn die erste Verschlüsselungsrichtlinie auf Ihrem Computer wirksam wird, wird die Initialverschlüsselung gemäß der erhaltenen Richtlinie durchgeführt. Je nach den Einstellungen der Verschlüsselungsrichtlinie startet die initiale Verschlüsselung entweder automatisch oder Sie müssen Sie selbst anstoßen.

12.3 Volume-basierende Verschlüsselung

Auf einem durch Sophos SafeGuard geschützten Computer, wird ein automatisch erzeugter Computerschlüssel zur volume-basierenden Verschlüsselung der Daten verwendet.

Gilt für Ihren Computer eine Richtlinie, die eine solche Verschlüsselung festlegt, werden die Daten automatisch verschlüsselt. Dem Volume können keine weiteren Schlüssel hinzugefügt werden.

Während die Verschlüsselung des Volumes ausgeführt wird, 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. Aktivieren 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 unverschlüsselte Volume Ihres Computers.

Hinweis:

Für Windows 7 Professional, Enterprise und Ultimate wird auf den Endpoint-Computern eine Systempartition angelegt, der kein Laufwerksbuchstabe zugeordnet ist. Diese Systempartition kann von Sophos SafeGuard nicht verschlüsselt werden.

Hinweis:

Wird eine neue Richtlinie, die die Entschlüsselung erlaubt, auf Ihren Computer angewendet, so gilt Folgendes: Nach einer vollständigen volume-basierenden Verschlüsselung müssen Sie Ihren Computer mindestens einmal neu starten, bevor die Entschlüsselung gestartet werden kann.

12.4 Dateibasierende Verschlüsselung

Hinweis:

Die dateibasierende Verschlüsselung steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

Gilt für ein Laufwerk auf Ihrem Computer eine Richtlinie, die die Verschlüsselung eines Laufwerks vorsieht, wird im Windows Explorer ein gelber Schlüssel bei diesem Laufwerk angezeigt.

Das gelbe Schlüsselsymbol alleine bedeutet nicht zwingend, dass alle Dateien auf diesem Laufwerk bereits verschlüsselt sind. Damit alle Dateien verschlüsselt sind, muss eine initiale Verschlüsselung durchgeführt werden.

Für die dateibasierende Verschlüsselung werden von Ihnen selbst erzeugte lokale Schlüssel verwendet. Die Verschlüsselung eines Volumens startet entweder automatisch automatisch oder Sie müssen den Vorgang starten.

1. Wird die Verschlüsselung nicht automatisch gestartet, können Sie die Verschlüsselung über das Windows Explorer Kontextmenü über **Dateiverschlüsselung > Verschlüsselung beginnen** starten.
2. Wenn die Verschlüsselung startet, werden Sie aufgefordert, einen lokalen Schlüssel auszuwählen.
3. Wenn der Dialog für die Schlüsselauswahl keinen Schlüssel enthält, schließen Sie den Dialog und erzeugen Sie zunächst einen oder mehrere Schlüssel (**System Tray Icon > Neuen Schlüssel erzeugen**).
4. Melden Sie sich wieder an Ihrem Computer an.

Die Verschlüsselung startet erneut, die Schlüssel werden jetzt im Dialog zur Initialverschlüsselung angezeigt und können ausgewählt werden.

5. Wählen Sie einen Schlüssel und klicken Sie auf **OK**.

Alle Daten, die sich auf dem relevanten Volume befinden, werden verschlüsselt.

12.4.1 Festlegen eines Standardschlüssels

Welcher Schlüssel zur Verschlüsselung im laufenden Betrieb verwendet wird, bestimmen Sie durch das Festlegen eines Standardschlüssels.

1. Der Standardschlüssel wird über das Kontextmenü einer Datei auf dem Volume oder über das Kontextmenü des Volumes selbst festgelegt.
2. 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 Verschlüsselungsvorgänge auf dem Volume verwendet.

3. Wenn Sie einen anderen Schlüssel verwenden möchten, müssen Sie einen neuen Standardschlüssel festlegen.

12.4.2 Verschlüsselungsstatus

Bei dateibasierend verschlüsselten Volumes werden die einzelnen Dateien mit Schlüsseln in verschiedenen Farben gekennzeichnet. Die Farben der Schlüssel repräsentieren den Verschlüsselungsstatus.

- **Grüner Schlüssel:** Die Datei ist verschlüsselt und Sie können darauf zugreifen.
- **Grauer Schlüssel:** Für die Datei besteht eine Verschlüsselungsrichtlinie. Sie ist aber noch nicht verschlüsselt.
- **Roter Schlüssel:** Die Datei ist mit einem Schlüssel verschlüsselt, der sich nicht in Ihrem Schlüsselring befindet. Sie können nicht darauf zugreifen.

Sie können sich den Verschlüsselungsstatus einer Datei auch über deren Kontextmenü anzeigen lassen. **Dateiverschlüsselung > Status der Verschlüsselung anzeigen** öffnet ein Fenster, in dem der Status angezeigt wird.

Wenn Sie im Kontextmenü des Volumes selbst auf **Dateiverschlüsselung > Status der Verschlüsselung** klicken, wird ein Dialog angezeigt, der alle Dateien und ihren Verschlüsselungsstatus anzeigt.

12.5 Zugriffsrestriktionen

Sophos SafeGuard 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 Sophos SafeGuard nicht eindeutig als unverschlüsselt oder verschlüsselt 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.

13 SafeGuard Data Exchange

Hinweis:

SafeGuard Data Exchange und SafeGuard Portable werden mit ESDP (Endpoint Security and Data Protection) nicht unterstützt.

Mit SafeGuard Data Exchange können Sie Daten auf beliebigen wechselbaren Speichermedien, 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 von Ihrem Sicherheitsbeauftragten in einer Richtlinie 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 hinzugekommenen 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 Sophos SafeGuard 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 Sophos SafeGuard *nicht* installiert:** Sophos SafeGuard 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.

13.1 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.
- **Sie dürfen die Initialverschlüsselung abbrechen:** Wenn die Initialverschlüsselung startet, wird ein Dialog angezeigt, in dem Sie die Initialverschlüsselung abbrechen können.
- **Sie dürfen nicht auf unverschlüsselte Dateien zugreifen:** 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.
- **Sie dürfen Dateien entschlüsseln:** In diesem Fall besteht die Möglichkeit, Dateien auf einem Wechselmedium explizit zu entschlüsseln. Dateien, die explizit entschlüsselt wurden, bleiben im Klartext auf dem Wechselmedium, wenn dieses z. B. an einen Dritten weitergegeben wird.
- **Sie dürfen eine Medien-Passphrase für Wechselmedien definieren:** Wenn Sie das erste Mal ein Wechselmedium mit Ihrem Computer verbinden, werden Sie aufgefordert, eine Medien-Passphrase einzugeben.
- **Klartext-Ordner auf Wechselmedien:** 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.
- **Sie dürfen entscheiden, ob Dateien verschlüsselt werden:** 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.

13.2 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 gebunden.

Eine Medien-Passphrase ist in den folgenden Situationen nützlich:

- Sie möchten verschlüsselte Daten auf Wechselmedien auf Computern benutzen, auf denen Sophos SafeGuard 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 wurden.

Sie können auch den Zugriff auf alle Dateien einschränken, indem Sie den externen Benutzern nur die Passphrase eines spezifischen Schlüssels 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.

Unterstützte Medien

SafeGuard Data Exchange unterstützt folgende wechselbare Speichermedien:

- USB-Sticks
- Externe Festplatten, die über USB oder FireWire angeschlossen sind.
- CD-RW-Laufwerke (UDF)
- DVD-RW-Laufwerke (UDF)
- FireWire
- Speicherkarten in USB-Kartenlesern (inkl. ZIP; JAZ)

13.3 Verschlüsseln von Wechselmedien

13.3.1 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 aus.

Wenn der Dialog für die Schlüsselauswahl keinen Schlüssel enthält, schließen Sie den Dialog und erzeugen Sie zunächst einen oder mehrere Schlüssel (**System Tray Icon > Neuen Schlüssel erzeugen**).

3. 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.

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

Timeout der Initialverschlüsselung

Wenn die Initialverschlüsselung per Konfiguration automatisch startet, sind Sie möglicherweise dazu berechtigt, die Initialverschlüsselung abubrechen. 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 erst gestartet, wenn Sie die Medien-Passphrase eingegeben haben. Danach startet die Initialverschlüsselung automatisch.

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, startet auch die Initialverschlüsselung nicht!

13.3.2 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.

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.

Ändern/Zurücksetzen der Medien-Passphrase

Sie können Ihre Medien-Passphrase jederzeit mit dem Befehl **Medien-Passphrase ändern** im Menü des System Tray Icons ändern. In diesem Fall 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** aktivieren 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. Wählen Sie dann den Befehl **Medien-Passphrase ändern** aus dem Menü des System Tray Icons. Sie werden darüber informiert, dass keine Medien-Passphrase vorhanden ist, und dazu aufgefordert, eine neue einzugeben.

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).

Festlegen eines Standardschlüssels

Welcher Schlüssel zur Verschlüsselung im laufenden Betrieb verwendet wird, bestimmen Sie durch das Festlegen eines Standardschlüssels.

Der Standardschlüssel wird über das Kontextmenü einer Datei auf dem Wechselmedium oder über das Kontextmenü des Wechselmediums selbst festgelegt. Sie können einen Schlüssel auch unmittelbar beim Anlegen eines neuen lokalen Schlüssels im Dialog **Schlüssel erzeugen** als Standardschlüssel auswählen.

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 verwendet. Wollen Sie einen anderen Schlüssel verwenden, müssen Sie einen neuen Standardschlüssel festlegen.

Ein Standardschlüssel, der zur Verschlüsselung verwendet werden soll, kann per Richtlinie definiert sein. Ist der Standardschlüssel nicht per Richtlinie definiert, werden Sie dazu aufgefordert, einen initialen Standardschlüssel anzugeben.

13.4 Datenaustausch mit SafeGuard Data Exchange

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

- Austausch von Daten mit Sophos SafeGuard 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 Sophos SafeGuard 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 Sophos SafeGuard

Für Benutzer, die Sophos SafeGuard 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.

13.4.1 Import von Schlüsseln aus einer Datei

Wenn Sie ein Wechselmedium mit verschlüsselten Daten erhalten haben 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.

Wählen Sie dazu die entsprechende Datei auf dem Wechselmedium und klicken Sie auf **Dateiverschlüsselung > Schlüsselverwaltung > Schlüssel importieren**.

Geben Sie im nun angezeigten Dialog die Passphrase ein. Der Schlüssel wird importiert und Sie können auf die Datei zugreifen.

13.4.2 Erzeugen von lokalen Schlüsseln

So erzeugen Sie einen benutzerdefinierten lokalen Schlüssel:

1. Klicken Sie mit der rechten Maustaste auf das Sophos SafeGuard System Tray Icon in der Windows-Taskleiste.
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. Mit der Option **Als neuen Standardschlüssel für Laufwerk <...> verwenden** können Sie diesen Schlüssel als Standardschlüssel für das angezeigte Laufwerk 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**.

Wenn Sie diesen Schlüssel als Standardschlüssel festlegen, werden alle Daten, die ab diesem Zeitpunkt auf das Wechselmedium kopiert werden, mit diesem Schlüssel verschlüsselt.

Von lokalen Schlüsseln werden keine Sicherungskopien erstellt und sie können nicht für Recovery-Vorgänge verwendet werden.

Damit der Empfänger alle Daten auf dem Wechselmedium entschlüsseln kann, müssen Sie gegebenenfalls die Daten auf dem Wechselmedium 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.

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

Hinweis:

Mit Windows XP können Sie Dateien mit dem Windows Assistenten zum Schreiben von CDs nur auf CDs brennen. Windows XP unterstützt nicht das Schreiben von Daten auf DVDs mit dem 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.

13.5.1 Brennen von Daten auf CDs/DVDs mit Windows Vista und Windows 7

Unter Windows Vista und Windows 7 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.

13.6 SafeGuard Portable

Hinweis:

SafeGuard Portable steht mit ESDP (Endpoint Security and Data Protection) nicht zur Verfügung.

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

13.6.1 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 bieten 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.) können Sie die Datei mit der linken Maustaste markieren und entweder über das Kontextmenü der rechten Maustaste oder über den Menüpunkt **Datei** das entsprechende Kommando auswählen.

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.

13.6.1.1 Setzen von Verschlüsselungsschlüsseln

So verschlüsseln Sie eine Datei auf einem Wechselmedium und legen einen Verschlüsselungsschlüssel 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.

13.6.1.2 Verschlüsseln von Dateien auf Wechselmedien

1. Markieren Sie die Datei im Explorer von SafeGuard Portable und aktivieren 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 an (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 aktivieren 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.

13.6.1.3 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 lokalen 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. Entschlüsselte Dateien werden wieder verschlüsselt, wenn Sie SafeGuard Portable schließen.

13.6.1.4 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 über Drag & Drop 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.

13.6.1.5 Verschlüsselungsstatus

So bestimmen Sie den Verschlüsselungsstatus einer Datei:

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.

13.6.2 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.

Öffnen Sie eine verschlüsselte Datei über diesen Menübefehl, 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 Ihrem Wechselmedium befinden, auf ein anderes Laufwerk Ihres Computers kopieren.

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

Exit beendet SafeGuard Portable.

14 Sophos SafeGuard 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. Sophos SafeGuard unterstützt den Opal-Standard.

14.1 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 256 Schlüssel als Opal-Kennwort gesperrt. Dieses Kennwort wird von Sophos SafeGuard über eine Verschlüsselungsrichtlinie verwaltet. Ihr Sicherheitsbeauftragter definiert diese Verschlüsselungsrichtlinie im SafeGuard Policy Editor und verteilt sie an Ihren Computer.

14.2 System Tray Icon und Explorer-Erweiterungen auf Endpoint-Computern mit Opal-Festplatten

Wenn Sophos SafeGuard auf Ihrem Computer installiert ist, wird das Sophos SafeGuard Produktsymbol im Infobereich (System Tray) der Taskleiste des Endpoint-Computers angezeigt. Als Benutzer haben Sie die Möglichkeit, auf alle wichtigen Funktionen, die Sophos SafeGuard auf Ihrem Computer zur Verfügung stellt, zentral zuzugreifen. Beachten Sie, dass die Funktionen, die auf Ihrem Computer verfügbar sind, von den vom Sicherheitsbeauftragten definierten Einstellungen abhängig sind.

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

15 Sophos SafeGuard und Lenovo Rescue and Recovery

Für Informationen zu den von Sophos SafeGuard unterstützten Lenovo Rescue and Recovery (RnR) Versionen, siehe <http://www.sophos.de/support/knowledgebase/article/108383.html>.

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. Sophos SafeGuard 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 Sie z. B. auf einer Geschäftsreise Lenovo Rescue and Recovery benutzen, um wieder mit dem Computer arbeiten zu können.

15.1 Überblick

Sophos SafeGuard 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 Sophos SafeGuard in Verbindung mit Lenovo Rescue and Recovery können Sie diese effiziente Backup- und Recovery-Methode mit Betriebssystempartitionen, die mit Sophos SafeGuard verschlüsselt sind, benutzen. Sicherungskopien von verschlüsselten Sophos SafeGuard 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.

Sophos SafeGuard „überlebt“ eine Systemwiederherstellung, ohne dass dabei die Verschlüsselung verloren geht, und muss nicht neu installiert werden. Nach der Systemwiederherstellung können Sie somit ohne Unterbrechung weiterarbeiten. Sie werden nicht durch erneutes Anstoßen der Verschlüsselung gestört.

In einer Sophos SafeGuard 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.

15.2 Voraussetzungen

- Aktuellstes BIOS für den PC/das Notebook

- Informationen zur Kompatibilität von Rescue and Recovery Versionen mit Sophos SafeGuard Versionen finden Sie hier:
<http://www.sophos.de/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery kann benutzt werden, um mit Sophos SafeGuard 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.

15.3 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 Sophos SafeGuard installiert werden. Wir empfehlen, zunächst Lenovo Rescue and Recovery und dann Sophos SafeGuard zu installieren.

15.3.1 Installieren von Rescue and Recovery und Sophos SafeGuard

Wir empfehlen diese Installationsreihenfolge.

1. Installieren Sie die aktuellste Version von Rescue and Recovery.
2. Installieren Sie die aktuellste Version des Moduls Sophos SafeGuard Device Encryption (**SGNClient.msi**).
Sophos SafeGuard prüft, ob Rescue and Recovery installiert ist, und fügt seine Dateien und Einstellungen in die Lenovo Notfallumgebung ein.
3. Stellen Sie sicher, dass die Power-on Authentication aktiviert ist, so dass kein Unbefugter unautorisiert beliebige Backups restaurieren kann.

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

15.3.2 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 Sophos SafeGuard Device Encryption (**SGNClient.msi**).

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

15.4 Upgrade

Ein Upgrade bedeutet, dass Sophos SafeGuard und Rescue and Recovery installiert sind und Sie eine der beiden Versionen auf eine neuere Version aktualisieren möchten.

Sophos SafeGuard Upgrade

Durch einen Upgrade von Sophos SafeGuard wird das gesamte System aktualisiert. Sie müssen somit keine weiteren Konfigurationseinstellungen vornehmen.

15.5 Deinstallation

Bei der Deinstallation beider Produkte ist folgendes zu beachten:

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

15.6 Boot-Umgebung und Recovery-Optionen

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

... von lokaler Festplatte

- Virtuelle Partition auf der lokalen Festplatte oder lokale Service-Partition
- Die Volumes müssen in Sophos SafeGuard 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: Sophos SafeGuard 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 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. Sophos SafeGuard wird während des Wiederherstellungsprozesses entfernt. Um das System wieder abzusichern, muss Sophos SafeGuard erneut installiert werden.

15.7 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 Sophos SafeGuard 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.

Sophos SafeGuard unterstützt für Sicherungskopien folgende Medien:

- Lokale Festplatte
- Zweites Festplattenlaufwerk
- USB-Festplattenlaufwerk
- Netzlaufwerk
- USB-Stick
- 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.

15.8 Wiederherstellen von Dateien aus Sicherungskopien

Rescue and Recovery stellt einzelne Dateien oder Verzeichnisse aus einem Backup, der ein installiertes Sophos SafeGuard 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.

15.9 Wiederherstellen des Sophos SafeGuard Systems

Um einen System-Backup, der Sophos SafeGuard 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 Power-on Authentication wird angezeigt.

- b) Geben Sie Ihre Sophos SafeGuard Anmeldeinformationen ein.
2. Sie benutzen keinen Lenovo-Computer:
 - a) Melden Sie sich an der Power-on Authentication mit Ihren Sophos SafeGuard 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.

15.10 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 Sophos SafeGuard anlegen. Weitere Informationen finden Sie in Ihrer Lenovo-Dokumentation.

15.11 Deaktivierte POA und Lenovo Rescue and Recovery

Sollte auf Ihrem Computer die 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.

16 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das SophosTalk-Forum unter <http://community.sophos.com/> auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter <http://www.sophos.de/support/>.
- Laden Sie Dokumentation zu den Produkten unter <http://www.sophos.de/support/docs/> herunter.
- Senden Sie eine E-Mail an den technischen Support support@sophos.de und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Sophos Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

17 Rechtliche Hinweise

Copyright © 1996 - 2011 Sophos Group. Alle Rechte vorbehalten. SafeGuard ist ein eingetragenes Warenzeichen von Sophos Group.

Sophos ist ein eingetragenes Warenzeichen von Sophos Limited, Sophos Group bzw. Utimaco Safeware AG. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Copyright-Informationen von Drittanbietern finden Sie in der Datei Disclaimer and Copyright for 3rd Party Software.rtf in Ihrem Produktverzeichnis.