

(!“\$\$%&/()*+;,:_ -) enthalten - soweit die Zusammensetzung nicht durch die allgemeinen Passwortregeln eingeschränkt wurde.

Die Zahlen des Zahlenblocks dürfen nicht verwendet werden.

Doppelklicken Sie auf „Passwort“, erscheint der Dialog, in dem das Passwort definiert wird.



Geben Sie in die obere Zeile das gewünschte Passwort ein und tragen Sie es erneut in das Feld **Bestätigung** ein. Die Wiederholung ist notwendig, da Tippfehler vermieden werden sollen. Die Gleichheit der eingegebenen Zeichen wird geprüft und eine Fehlermeldung ausgegeben, falls die Passwörter nicht übereinstimmen oder trivial (z. B. „12345“ oder „AAABBB“) sind. Aus Sicherheitsgründen wird der Eintrag nur mit '*'-Symbolen angezeigt. Zur Korrektur von Einträgen verwenden Sie bitte die Rücksteltaste.

Das Umgehen der nochmaligen Passwordeingabe durch das „Kopieren und Einfügen“-Verfahren ist nicht möglich.

16 Windows-Anmeldung konfigurieren

Sophos SafeGuard Disk Encryption verlangt mit seiner Pre-Boot Authentisierung als erste Systemkomponente eine Authentisierung. Erst nachdem das System mit gültigen Sophos SafeGuard Disk Encryption Zugangsdaten aufgesperrt wurde, erscheint der reguläre Windows-Anmeldedialog.

Sophos SafeGuard Disk Encryption stellt mit dem Sicherem Automatischen Logon eine Funktionalität bereit, die den Benutzer von Mehrfachauthentisierungen entlasten und ihn nur noch ein einziges Mal auffordern (nämlich an der Pre-Boot Authentisierung), Benutzerdaten einzutragen.

Um die Windows-Anmeldung noch benutzerfreundlicher zu machen und das Erscheinungsbild des Windows-Anmeldedialog anzupassen, gibt es zusätzliche Optionen in der administrativen Vorlage.

16.1 Sicherer automatischer Logon (SAL)

Die automatische Anmeldung ist eine Komfort-Einrichtung für die Anmeldeprozedur. Ein Benutzer gibt nur einmal seine Windows-Daten ein, bei weiteren Anmeldungen erfolgt die Windows-Anmeldung automatisch und der Benutzer authentisiert sich nur noch mit Sophos SafeGuard Disk Encryption Benutzerdaten an der Pre-Boot Authentisierung. Sophos SafeGuard Disk Encryption nennt dieses Anmeldeverfahren **Sicherem Automatischen Logon** oder kurz **SAL**.

Die automatische Anmeldung an das Betriebssystem kann nachträglich mit dem Sophos SafeGuard Disk Encryption Kommando `chgsal.exe` ausgeschaltet werden.

Hinweis: SAL wird standardmäßig installiert. Die Benutzer werden bei der ersten Anmeldung aufgefordert, SAL zu aktivieren.

Alle folgenden Anmeldungen an andere Applikationen müssen manuell erfolgen.

Ist die Windows-Option „Immer diesen Benutzer anmelden“ aktiviert, kann kein SAL durchgeführt werden.

Technisch gesehen funktioniert der SAL folgendermaßen: Ein Benutzer meldet sich in der Pre-Boot Authentisierung mit seinen Sophos SafeGuard Disk Encryption Zugangsdaten an und gibt dann im Windows Anmeldedialog seine Windows-Daten ein. Der SAL stellt zwischen dem angemeldeten Sophos SafeGuard Disk Encryption Benutzer und dem Windows-Benutzer eine Beziehung her, die in der verschlüsselten Datei `sgsal.dat` abgespeichert wird. `sgsal.dat` ist zu finden unter `<Systemlaufwerk>\SYSTEM32`. Bei einer erneuten Anmeldung in der Pre-Boot Authentisierung reicht der SAL ohne Benutzerinteraktion die Windows-Daten an den Windows-Anmeldedialog weiter.

Gehen Sie nach der Installation wie folgt vor:

1. Authentifizieren Sie sich in der Pre-Boot Authentisierung mit den Sophos SafeGuard Disk Encryption Benutzerdaten.
2. Nach der ersten Anmeldung nach der Installation von SAL erscheint der gewohnte Windows Logon-Dialog.
3. Geben Sie die korrekten Windows-Anmeldeinformationen ein und klicken Sie auf OK.
4. Der SAL-Dialog wird angezeigt.



Ja: Aktiviert die Beziehung zwischen Sophos SafeGuard Disk Encryption Benutzer und Windows-Benutzer.

Nein: Verwendet die SAL-Funktionalität nicht.

Der Status des Auswahlkästchens „Diesen Dialog für den angemeldeten Sophos SafeGuard Disk Encryption Benutzer nicht mehr anzeigen.“ entscheidet, ob der Dialog bei jeder Anmeldung erneut erscheint oder nicht.

5. Drücken Sie OK und aktivieren Sie das Kontrollkästchen. Der Sophos SafeGuard Disk Encryption Benutzer wird nun automatisch mit dem Windows-Benutzer verknüpft.

Beim nächsten Neustart des PC wird nach der Eingabe der Sophos SafeGuard Disk Encryption Benutzerdaten in der Pre-Boot Authentisierung die Anmeldung an Windows automatisch durchgeführt.

Windows-Kennwort ändern

Windows-Kennwörter müssen aus Sicherheitsgründen immer wieder geändert werden. Wie ein neues Kennwort in den sicheren automatischen Logon integriert wird, ist jedoch abhängig davon, wie es geändert wird.

■ Administrator erzwingt Kennwortänderung

Erzungen wird eine Kennwortänderung im Benutzerprofil über die Option „Benutzer muss Kennwort ändern bei der nächsten Anmeldung“. Ist die Option aktiviert, wird der Benutzer durch eine System-Mitteilung dazu aufgefordert. Der SAL ist zu diesem Zeitpunkt deaktiviert.

Diese Meldung muss mit OK bestätigt und im folgenden Dialog ein neues Kennwort

eingegeben werden. Sobald der Benutzer das neue Kennwort bestätigt hat, wird die SAL-Datei mit den neuen Daten synchronisiert. Bei der nächsten Anmeldung werden die Windows-Benutzerdaten wieder automatisch durchgereicht.

■ **Benutzer ändert Kennwort lokal**

- Drückt der Benutzer auf seinem Desktop STRG+ALT+ENTF, kann er sein Kennwort im Dialog **Windows Sicherheit** über „Kennwort ändern“ modifizieren. Erfolgt die Änderung auf diese Weise, findet eine **automatische Übernahme des Windows-Kennworts** in der Datei `Sgsal.dat` statt. Der Benutzer muss nach einem Neustart die Windows-Daten nicht erneut eintragen.
- Wird das Kennwort über die Benutzerverwaltung von Windows geändert, findet **KEINE automatische Übernahme des Windows-Kennworts** statt. Der Benutzer erhält stattdessen bei der nächsten Anmeldung einen Warnhinweis, dass das Kennwort nicht gültig ist und wird aufgefordert, das neue Kennwort in den Windows Anmeldedialog einzutragen. Das Kennwort wird dann für zukünftige Anmeldungen gespeichert.

16.1.1 SAL temporär ausschalten

Mit `CHGSAL.EXE` aus dem Sophos SafeGuard Disk Encryption Verzeichnis können SAL und Smartcard-SAL nachträglich von einem Benutzer mit Windows-Administratorrechten deaktiviert und auch wieder eingeschaltet werden.

So aktivieren/deaktivieren Sie den SAL:

1. Wechseln Sie zur Eingabeaufforderung oder rufen Sie den Befehl **Ausführen** im Windows-Startmenü auf.
2. Wechseln Sie in das Verzeichnis, in dem Sophos SafeGuard Disk Encryption installiert ist. Geben Sie folgendes Kommando mit dem entsprechenden Parameter ein:

```
CHGSAL.EXE /SAL:ON | /SAL:OFF | [ /? ]
```

<code>/SAL:ON</code>	Aktiviere „Sicherer automatischer Logon“
<code>/SAL:OFF</code>	Deaktiviere „Sicherer automatischer Logon“
<code>/?</code>	Zeige diese Hilfe

`CHGSAL` funktioniert nur, wenn Sophos SafeGuard Disk Encryption mit SAL installiert wurde.

16.1.2 SAL-Daten löschen

Wenn Sie `sgsal.dat` (<Systemlaufwerk>\system32) löschen, werden alle gespeicherten Benutzer-Daten entfernt. Nach einem Neustart des Rechners können Sie einem Sophos SafeGuard Disk Encryption Benutzer neue Daten zuweisen.

Wurde ein Sophos SafeGuard Disk Encryption Benutzer, der bereits eine Verbindung erstellt hat, auf einem System gelöscht, bleibt diese Beziehung beim erneuten Anlegen desselben Benutzers bestehen.

16.1.3 Einschränkung

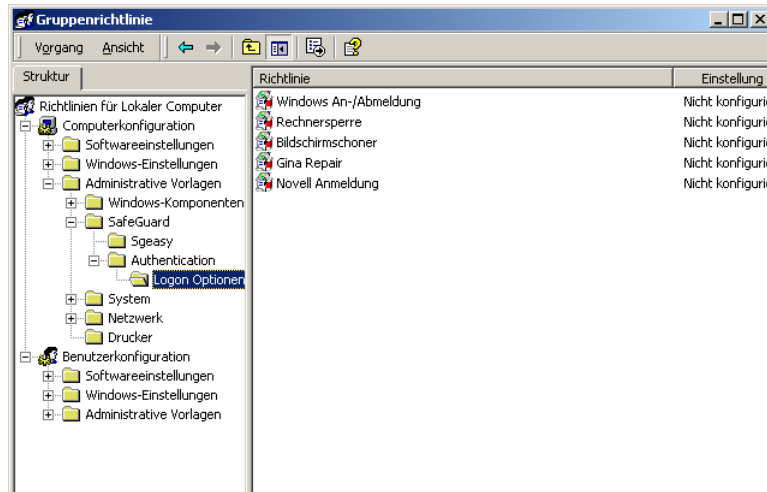
SAL ist temporär ausgeschaltet, wenn sich ein Benutzer per Challenge/Response über die Option „Einmalige Anmeldung“ anmeldet. Die „Einmalige Anmeldung“ erlaubt einem Benutzer, sich in der Pre-Boot Authentisierung von Sophos SafeGuard Disk Encryption anzumelden, ohne das Sophos SafeGuard Disk Encryption Passwort zu kennen (siehe [Fernwartung \(Challenge/Response\)](#) auf Seite 121).

Wenn nun einem Benutzer die „Einmalige Anmeldung“ in der Pre-Boot Authentisierung gestattet wurde, wird er/sie nicht automatisch an Windows angemeldet, auch wenn der SAL aktiviert ist. In diesem Fall stoppt das Betriebssystem am gewohnten Windows-Anmeldedialog und verlangt gültige Windows-Daten. Alle Aktionen werden nun unter dem Namen des angemeldeten Windows-Benutzers aufgezeichnet.

Nach jeder weiteren regulären Anmeldung mit Sophos SafeGuard Disk Encryption Zugangsdaten in der Pre-Boot Authentisierung, wird der SAL und die automatische Windows-Anmeldung wie gewohnt ausgeführt.

16.2 Zusätzliche Optionen für die Windows-Anmeldung

Über die mitgelieferte administrative Vorlage Sguard.adm lassen sich bestimmte Einstellungen für die Anmeldung an das Betriebssystem zwingend vorschreiben, die man normalerweise über Windows-Einstellungen nicht beeinflussen kann.



16.3 Windows An-/Abmeldung

Die Windows An-/Abmeldung gibt Benutzern u.a. die Oberfläche vor, die bei der Anmeldung bzw. beim Sperren der Arbeitsstation auf ihrem Bildschirm erscheint.

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration

\Administrative Vorlagen

\SafeGuard

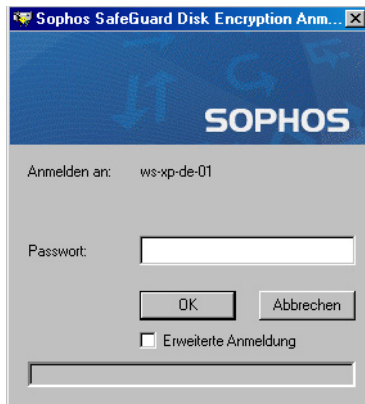
\Authentication

\Logon Optionen

\Windows An-/Abmeldung

■ Sophos Anmeldedialog benutzen

Wenn Sie das Kontrollkästchen markieren, wird bei der Anmeldung der Sophos Anmeldedialog angezeigt. Nach Entfernen der Markierung können Sie sich über den Windows Anmeldedialog im System anmelden.



■ **Sophos Startdialog benutzen**

Wenn Sie dieses Kontrollkästchen aktivieren, wird beim Booten der Sophos Dialog **Anmeldung beginnen** angezeigt. Hier werden Sie aufgefordert, **Strg+Alt+Entf** zum Öffnen des Anmeldedialogs zu drücken. Bei Entfernen der Markierung wird der entsprechende Windows Dialog angezeigt.



■ **Sophos Lockdialog benutzen**

Wenn Sie das Kontrollkästchen markieren, wird beim Sperren der Arbeitsstation mit **Strg+Alt+Entf** der SafeGuard Lockdialog anstelle des Windows-Dialogs angezeigt. Wurde eine ungültige Benutzeranmeldung registriert, so wird dies im Sophos Lockdialog angezeigt.

■ **Vorprüfung der Benutzerdaten bei DFÜ-Anmeldung ausschalten**

Wenn Sie dieses Kontrollkästchen aktivieren, wird beim Aufbau von DFÜ-Verbindungen keine Vorprüfung von Benutzerkonten durchgeführt.

■ **Deaktivieren der DFÜ-Auswahlbox im Sophos-Anmeldedialog**

Wenn Sie das Kontrollkästchen markieren, wird die Option „Anmelden über das DFÜ-Netzwerk“ im Sophos-Anmeldedialog deaktiviert.

■ **Bitmap ersetzen mit**

In diesem Eingabefeld kann ein Bitmap angegeben werden, das im Sophos Anmeldedialog angezeigt wird, z. B. das Firmenlogo auf einen entsprechenden Hintergrund. Das Bitmap muss das .BMP Format haben und sich im SYSTEM32- Verzeichnis des Windows-Installationsverzeichnis befinden. Die Größe des Bitmaps ist mit 413x140 Pixel festgelegt.

16.3.1 Hintergrund-Bitmap in der Windows-Anmeldung austauschen

Es besteht die Möglichkeit, das Bitmap anzupassen, das nach Eingabe der Sophos SafeGuard Disk Encryption Zugangsdaten erscheint. Dies ermöglicht es Kunden, den Hintergrund von Sophos SafeGuard Disk Encryption den Anforderungen ihres Unternehmens anzupassen.

Das angezeigte Standard-Bitmap hat den Namen **SgeLogo.bmp** und liegt im gewählten Sophos SafeGuard Disk Encryption Verzeichnis.

Um das Titel-Bitmap **auszutauschen**, muss nur das Standard-Bitmap mit einem angepassten Bitmap gleichen Namens und Größe ersetzt werden.

Das Hintergrund-Bitmap kann über eine Richtlinie in der administrativen SafeGuard Vorlage ausgeblendet werden.

Die Richtlinie finden Sie unter

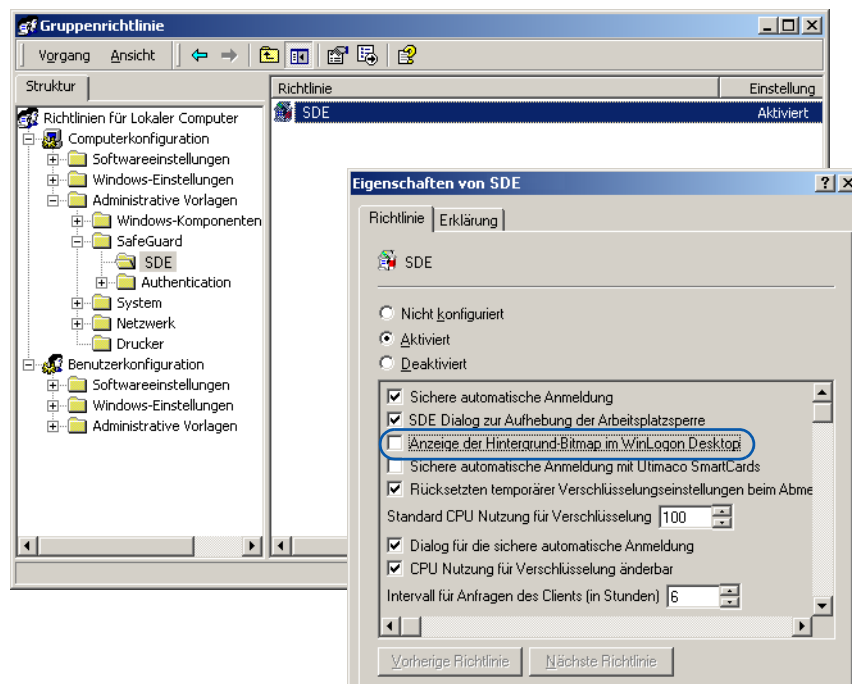
Computerkonfiguration

\Administrative Vorlagen

\SafeGuard

\SDE

Deaktivieren Sie in der Eigenschaftenseite von „SDE“ die Option **Anzeige der Hintergrund-Bitmap im WinLogon Desktop**. Daraufhin erscheint kein Sophos SafeGuard Disk Encryption Bitmap mehr.



16.3.2 Rechnersperre

Bei der Richtlinie „Rechnersperre“ wird festgelegt, nach wie vielen fehlgeschlagenen Anmeldeversuchen der Rechner gesperrt wird und wie sich die Wartezeit zwischen diesen Anmeldeversuchen erhöht.

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration

\Administrative Vorlagen

\SafeGuard

\Authentication

\Logon Optionen

\Rechnersperre

Der Mechanismus funktioniert nur bei Benutzern, die kein Mitglied der lokalen Gruppe der Administratoren sind.

■ Anmelde-Fehlversuche

In diesem Feld bestimmen Sie die Anzahl der Anmelde-Fehlversuche eines Benutzers, der sich mit einem ungültigen Benutzernamen bzw. Kennwort anmeldet. Geben Sie beispielsweise „3“ ein, wird der Rechner gesperrt, wenn der Benutzer bei der Anmeldung dreimal hintereinander seinen Benutzernamen oder sein Kennwort falsch eingibt.

Minimaler/Maximaler Wert: 0 - 999

■ Verzögerung in Sekunden

Tragen Sie hier den Basiswert ein, der multipliziert mit dem „Multiplikator“ die Wartezeit nach dem ersten fehlgeschlagenen Anmeldeversuch ergibt. Bei einem weiteren Fehlversuch wird die Wartezeit des vorherigen Fehlversuches als Basiswert genommen. Die Standardeinstellung ist „10“.

Minimaler/Maximaler Wert: 0 - 999

■ Multiplikator

Der Multiplikator wird mit der Zeitbasis Verzögerung in Sekunden multipliziert. Die Standardeinstellung ist „3“.

Minimaler/Maximaler Wert: 0 - 99

■ Deaktiviere STRG+ALT+Entf, wenn Computer gesperrt ist

Der Rechner bleibt nach Drücken der Tastenkombination STRG+ALT+Entf gesperrt.

BEISPIEL:

Verzögerung von 10 Sekunden und Multiplikator von 5:

1. Fehlversuch: 50 Sekunden Wartezeit ($10 * 5$)
2. Fehlversuch: 250 Sekunden Wartezeit ($50 * 5$)
3. Fehlversuch: 1250 Sekunden Wartezeit ($250 * 5$)

Hinweis:

Die Sperre kann aufgehoben werden

- durch Neustart des Rechners
- durch Anmeldung eines lokalen Administrators
- durch Datenreplikation vom Domänen-Controller

Beachten Sie in diesem Zusammenhang auch die Benutzersperre von Windows.

16.3.3 Bildschirmschoner

Ist auf einer Arbeitsstation festgelegt, dass ein Bildschirmschoner nach einer bestimmten Zeit starten soll, können Sie bestimmen, wie das System nach einem definierten Zeitraum auf dessen Aktivierung reagieren soll.

Die Einstellungen sind nur wirksam, wenn der Windows-Bildschirmschoner auch aktiviert ist!

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration

\Administrative Vorlagen
\SafeGuard
\Authentication
\Logon Optionen
\Bildschirmschoner

■ **Aktionen**

Folgende Aktionen stehen zur Verfügung, die nach Einsetzen des Bildschirmschoners und der definierten Aktionsverzögerung ausgeführt werden können.

A) Benutzer abmelden

Der aktuelle Benutzer wird abgemeldet. Es können sich nun (auch) andere auf der Arbeitsstation oder im Netzwerk registrierte Benutzer anmelden.

B) Computer herunterfahren

Der PC wird automatisch heruntergefahren und muss für eine weitere Arbeitssitzung neu gestartet werden.

C) Computer neu starten

Es erfolgt ein automatischer Neustart.

D) Computer in Ruhezustand versetzen

Der Computer wird in den Ruhezustand versetzt.

E) Verbindung trennen

Hat auf einer lokalen Arbeitsstation keine Auswirkung.

F) Standby

Der Computer wird in den Standby-Modus versetzt.

Überblick über mögliche Aktionen und ihre Auswirkungen auf den lokalen Rechner:

Einstellung	Aktion lokal
<Keine>	keine
Benutzer abmelden	abmelden
Computer herunterfahren	herunterfahren
Computer neu starten	neu starten
Computer in Ruhezustand versetzen	in Ruhezustand versetzen
Verbindung trennen	keine
Standby	Standby

■ **Aktionsverzögerung (Standard: 15 Minuten)**

Mit Aktionsverzögerung stellen Sie den Zeitraum (in Minuten) ein, nach dem das System eine der beschriebenen Aktionen ausführen soll. Als Standardwert ist 15 vorgegeben. Sie können die Zahl entweder direkt per Tastatureingabe oder mit den Richtungspfeilen ändern. Minimaler/Maximaler Wert: 0 - 900

■ **Bildschirmschoner sperren**

Ein gestarteter Bildschirmschoner wird in der Regel mit einer Mausbewegung oder Tastatureingabe aufgehoben und der Benutzer kann ohne Eingabe seiner Zugangsdaten weiterarbeiten. Ist das Kontrollkästchen „Bildschirmschoner sperren“ aktiviert, wird die Arbeitsstation gesperrt. Der Zugriff auf die Arbeitsstation ist erst wieder nach korrekter Eingabe der Zugangsdaten möglich.

BEISPIEL:

Auf den Arbeitsstationen ist definiert, dass der Bildschirmschoner zehn Minuten nach der letzten Benutzeraktion (Tastatureingabe, Mausbewegung) einsetzen soll. Haben Sie als auszuführende Aktion 'Computer herunterfahren' gewählt und als Aktionsverzögerung den Wert 13 eingegeben, wird der PC 23 Minuten nach der letzten Aktion am Arbeitsplatz automatisch heruntergefahren.

16.3.4 Authentisierungsmodul (GINA) reparieren

Sophos besitzt eine eigene Anmeldekomponente, die SafeGuard GINA (`SGGINA.dll`). Nach der Installation wird diese als Erste in der GINA-Kette platziert und kontrolliert damit den Anmeldemechanismus.

Die Installation anderer Produkte kann die Reihenfolge der aufgerufenen Anmeldekomponenten ändern.

Sie finden die Richtlinie in der administrativen Vorlage unter:

Computerkonfiguration

\Administrative Vorlagen

\SafeGuard

\Authentication

\Logon Optionen

\GINA Repair

■ Automatische Korrektur der Aufrufsequenz (Standard: Aktiviert)

Stellt sicher, dass die SafeGuard GINA automatisch an der ersten Stelle der GINA-Kette platziert wird.

■ Verhalten bei unbekanntem GINA

Benutzer fragen

Beim erstmaligen Initialisieren wird in einem Dialog gefragt, ob die unbekannte oder die original Microsoft GINA verwendet werden soll. Wird in diesem Dialog das Kontrollkästchen bei „Diese Meldung nicht mehr anzeigen“ aktiviert, wird die Benutzerreaktion in der Registrierung gespeichert und beim nächsten Neustart dieser Wert verwendet.

Original Microsoft GINA verwenden

Die Original Microsoft GINA wird an die erste Stelle der GINA-Kette platziert.

Unbekannte GINA verwenden

Platziert die unbekannte GINA an die erste Stelle der GINA-Kette.

17 Arbeitsplatzsperre von Sophos SafeGuard Disk Encryption

Sophos SafeGuard Disk Encryption ersetzt die reguläre Windows-Arbeitsplatzsperre mit einem eigenen Dialog.



Wenn sich der PC im Pausenmodus befindet, kann nur der Benutzer, der ihn gesperrt hatte, durch Eingabe seines Sophos SafeGuard Disk Encryption Passworts die Arbeitsoberfläche wieder aktivieren.

Bildschirm und Arbeitsoberfläche werden gesperrt

- nach Drücken von **Strg+Alt+Entf** und **Computer sperren**
- nach Ablauf einer eingestellten Zeit ohne Bedienung (Wartezeit)

Für die Arbeitsplatzsperre erscheint dasselbe Hintergrundbild wie während der Anmeldung, dieses kann jedoch geändert werden ([siehe Windows An-/Abmeldung auf Seite 92](#)).

17.1 Voraussetzungen

Die Arbeitsplatzsperre funktioniert nur, wenn

- die Pre-Boot Authentisierung aktiviert ist
- der Benutzer über den SAL automatisch an das Betriebssystem angemeldet wurde.
- der Windows-Bildschirmschoner mit Kennwortschutz eingeschaltet ist

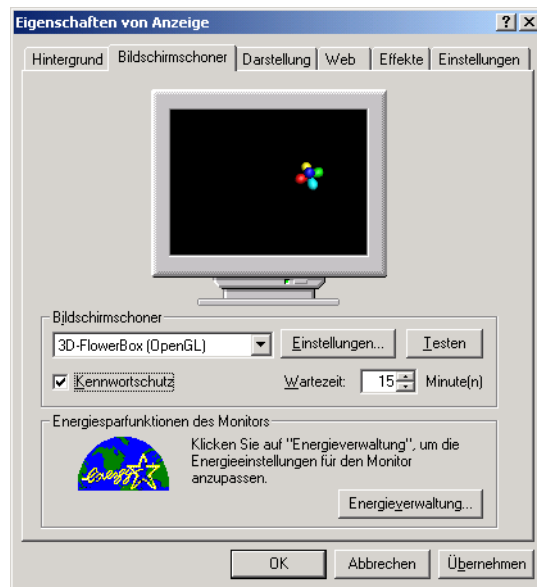
Nach der Aktivierung der Windows-Bildschirmschonereinstellungen müssen Sie den PC neu starten.

Nachträglich ausgeschaltet wird die Sophos SafeGuard Disk Encryption Arbeitsplatzsperre, wenn sich ein Benutzer nach erfolgreicher Anmeldung von Windows abmeldet und wieder anmeldet.

17.2 Windows-Bildschirmschoner mit Kennwortschutz aktivieren

Die Sophos SafeGuard Disk Encryption Arbeitsplatzsperre wird in den Windows-Einstellungen über Programme\Systemsteuerung\Anzeige\Bildschirmschoner gesteuert.

Der PC muss nach Konfigurieren des Windows-Bildschirmschoners neu gestartet werden!



Wählen Sie zunächst einen Bildschirmschoner aus. Passen Sie danach die Optionen „Kennwortschutz“ und „Wartezeit“ an.

■ Kennwortschutz

Erzwingt die Abfrage des Sophos SafeGuard Disk Encryption Passworts, muss aktiviert werden.

■ Wartezeit

Gibt die Zeit (in Minuten) an, die ohne Bedienung des Arbeitsplatzes vergehen muss, bis die Arbeitsplatzsperre aktiviert wird.

Wenn Sie hier zum Beispiel 15 einstellen, würde der Bildschirm nach 15 Minuten ohne Tastatureingabe oder Mausbedienung gesperrt.

Der Benutzer muss sich zur Fortsetzung seiner Arbeit erneut mit dem Sophos SafeGuard Disk Encryption Passwort anmelden.

Wir empfehlen, die Arbeitsplatzsperre einzuschalten, um den Arbeitsplatz vor unbefugten Benutzern zu schützen.

17.3 Sophos SafeGuard Disk Encryption Arbeitsplatzsperre nicht anzeigen

Es besteht die Möglichkeit, die Sophos SafeGuard Disk Encryption Arbeitsplatzsperre auszuschalten und stattdessen den regulären Windows-Dialog anzuzeigen.

Hinweis: Der reguläre Windows-Dialog wird nicht mit dem Sophos SafeGuard Disk Encryption Passwort, sondern mit dem Windows-Kennwort aufgesperrt.

Der Sophos SafeGuard Disk Encryption Passwortschutz für die Arbeitsplatzsperre ist damit nicht mehr gegeben!

Über die mitgelieferte administrative Vorlage lässt sich unter der Richtlinie „SDE Dialog zur Aufhebung der Arbeitsplatzsperre“ (Haken vor der Richtlinie entfernen) die Sophos SafeGuard Disk Encryption Arbeitsplatzsperre deaktivieren.

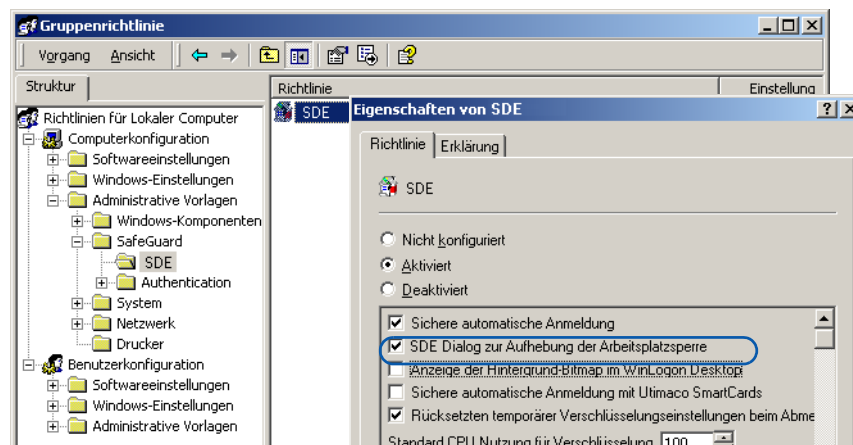
Sie finden die Richtlinie unter

Computerkonfiguration

\Administrative Vorlage

\SafeGuard

\SDE



18 Sicheres Wake On LAN

Der Wake On LAN-Modus (im folgenden WOL) von Sophos SafeGuard Disk Encryption ist der sicherste Weg, um die Vorteile von Wake On LAN mit dem Schutz des PCs durch Festplattenverschlüsselung zu kombinieren. Sophos SafeGuard Disk Encryption WOL erlaubt zu diesem Zweck, die Pre-Boot Authentisierung für eine definierte Anzahl von Neustarts auszuschalten und danach wieder zu aktivieren, um z. B. neue Software zu verteilen. Währenddessen ist es jedoch nicht möglich, die inaktive Pre-Boot Authentisierung zu nutzen und sich über eine geglückte Windows-Anmeldung ins System einzuschleichen.

WOL ist ein optimaler Kompromiss zwischen Pre-Boot-Schutz und dem Ausführen zentral gesteuerter Aufgaben.

18.1 Überblick

Generell ermöglicht Wake On LAN, einen Rechner im lokalen Netzwerk von einem zweiten Rechner aus einzuschalten, um z. B. neue Softwareupdates einzuspielen oder allgemeine Wartungsarbeiten durchzuführen.

Die WOL-Technik in Sophos SafeGuard Disk Encryption ermöglicht dem Administrator, den Sophos SafeGuard Disk Encryption Clients eine Anzahl von Neustarts zu erlauben, bevor automatisch wieder die Pre-Boot Authentisierung aktiv wird. Wenn etwa die Anzahl der Automatischen Anmeldungen auf „3“ gesetzt wird, startet der PC dreimal in Folge mit ausgeschalteter Pre-Boot Authentisierung, beim vierten Neustart wird die Pre-Boot Authentisierung wieder angezeigt (vorausgesetzt, sie ist eingeschaltet).

Während der n-maligen Bootphase wird die Windows-Anmeldung unterdrückt. Der Rechner bootet selbsttätig und das automatische Softwareupdate kann über das Netzwerk durchgeführt werden.

18.2 Sperre der Windows-Anmeldung

Im Wake On LAN Modus ist der Rechner gegen lokale Windows-Benutzeranmeldungen gesichert. Es erscheint statt des gewohnten Windows-Anmeldedialogs die Wake On LAN-Meldung ("Eine Anmeldung an Windows ist nicht zulässig, da dieser Rechner über Wake-On-LAN ohne Anmeldung gestartet wurde.")



Windows-Anmeldung im Wake-On-LAN-Modus

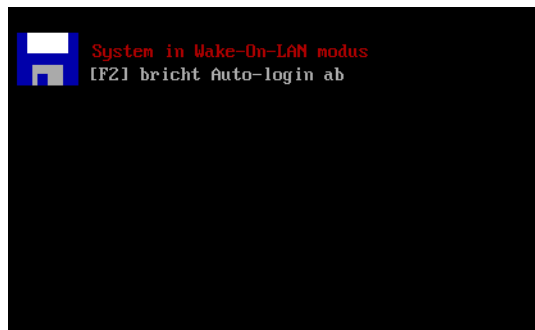
Hinweis: Die Sperre der Windows-Anmeldung im WOL-Modus funktioniert nur, wenn die Sophos SafeGuard GINA installiert ist!



18.3 Wake On LAN Sperre temporär aufheben

Wenn Benutzer trotz WOL Modus ihren PC nutzen müssen, gibt es eine Möglichkeit, die Sperre zeitweise aufzuheben:

In der Pre-Boot Phase erscheint in der linken, oberen Monitorecke für ca. 5 Sekunden ein Diskettensymbol.



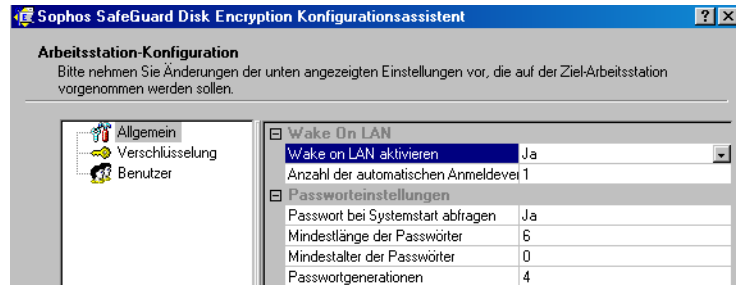
Drückt der Benutzer während dieser Zeit F2, erscheint die Pre-Boot Authentisierung und der Benutzer kann sich wie gewohnt mit gültigen Sophos SafeGuard Disk Encryption Zugangsdaten und später an Windows anmelden. Dass der Rechner sich im Wake On LAN Modus befindet, sieht der Benutzer an einer über F2 blinkenden Warnung.

Wird der PC über den abgesicherten Modus gestartet (F8 während des Bootvorgangs drücken), stellt die eingebaute SafeGuard-Sperre sicher, dass sich nur Benutzer mit Windows-Administratorrechten im abgesicherten Modus anmelden können.

18.4 Wake on LAN konfigurieren

WOL wird in der Regel in größeren IT-Umgebungen und nicht für Stand-alone PCs eingesetzt. Der Administrator erstellt eine Konfigurationsdatei mit den entsprechenden WOL Einstellungen und verteilt diese an die Clients im Unternehmen.

Konfiguriert wird Sophos SafeGuard Disk Encryption Sicheres Wake-On LAN in den Verwaltungsprogrammen über die Konfigurationsseite „Allgemein“.



Folgende Einstellungen sind möglich:

- **Wake on LAN aktiviert:**
Schaltet Wake On LAN Modus ein/aus.
- **Anzahl Automatischer Anmeldungen (Standard: 1):**
Definiert die Anzahl der Neustarts mit ausgeschalteter Pre-Boot Authentisierung, wenn Wake On LAN eingeschaltet ist.
Wir empfehlen, immer **einen Neustart mehr als notwendig zu erlauben**, um unvorhergesehene Probleme zu umgehen.

Sobald die Konfigurationsdatei an die Benutzer-PCs verteilt wurde, startet der PC nun n-Mal ohne Pre-Boot Authentisierung neu. Nach Ablauf der definierten Anzahl an Neustarts ohne Pre-Boot Authentisierung erscheint wie gewohnt die Pre-Boot Authentisierung und verlangt nach den korrekten Sophos SafeGuard Disk Encryption Benutzerdaten.

19 Ruhezustand (Hibernation)

Die Windows-Funktion „Ruhezustand“ wird von Benutzern mit mobilen Geräten gerne genutzt, um den Arbeitsvorgang temporär zu unterbrechen. Wird etwa ein Notebook bei aktiviertem Ruhezustand im laufenden Betrieb zugeklappt, schaltet sich das Gerät automatisch aus und stellt nach einem Neustart wieder exakt die Bildschirmoberfläche der letzten Sitzung her.

Zur Sicherung der Daten im Ruhezustand hat Sophos SafeGuard Disk Encryption hier eine besondere Lösung, die nicht jedes Verschlüsselungsprodukt bietet.

19.1 Überblick

Im Ruhezustand wird der Inhalt des Arbeitsspeichers (RAM) in die Systemdatei Hiberfile.sys im Hauptverzeichnis der Betriebssystempartition (in der Regel Laufwerk C) geschrieben und auf der Festplatte gespeichert. Die Größe der Hiberfile.sys entspricht in etwa der Größe des zur Verfügung stehenden Arbeitsspeichers. Anschließend wird der Computer ausgeschaltet. Wenn Sie den Computer wieder einschalten, wird der Desktop genau so wiederhergestellt, wie Sie ihn beim Herunterfahren verlassen haben (d.h. der Inhalt der Hiberfile.sys wird wieder zurück in den Arbeitsspeicher geschrieben). Nach der Deaktivierung des Ruhezustands wird die Hiberfile.sys ungültig gemacht.

19.2 Ruhezustand und Sophos SafeGuard Disk Encryption

Auf einer unverschlüsselten Betriebssystempartition ist das Umschalten des Rechners in den Ruhezustand ein Sicherheitsrisiko, weil dabei der komplette Hauptspeicherinhalt ausgelagert wird und für nicht autorisierte Dritte leicht zugänglich ist.

Auf einer verschlüsselten Betriebssystempartition erlaubt es Sophos SafeGuard Disk Encryption, den Ruhezustand zu nutzen und die erzeugte Hiberfile.sys verschlüsselt und damit sicher auf der Platte abzulegen. Somit sind alle Daten auf der Festplatte zu jeder Zeit verschlüsselt. Zugriff auf das System erhalten nur Benutzer, die sich beim Neustart des Rechners in der Pre-Boot Authentisierung (vorausgesetzt, diese ist aktiviert) mit gültigen Sophos SafeGuard Disk Encryption Zugangsdaten authentisieren können.

Hinweis: Wenn sich unterschiedliche Sophos SafeGuard Disk Encryption Benutzer eine Arbeitsstation teilen, gelangt trotz Authentisierung mit unterschiedlichen Sophos SafeGuard Disk Encryption Zugangsdaten in der Pre-Boot Authentisierung jeder von ihnen in das Profil des Sophos SafeGuard Disk Encryption Benutzers, der den Ruhezustand initiiert hat. In diesem Fall ist es möglich, beim Neustart des Rechners das Windows-Kennwort anzufordern (Energieoptionen\Erweitert\Kennwort beim Reaktivieren des Computers anfordern). Diese Einstellung zwingt die Benutzer, sich zusätzlich mit ihren Windows-Daten anzumelden (Nachteil: zweifache Authentisierung).

19.3 Voraussetzungen und Einschränkungen

Das Zusammenspiel von Sophos SafeGuard Disk Encryption und dem Ruhezustand funktioniert unter folgenden Voraussetzungen:

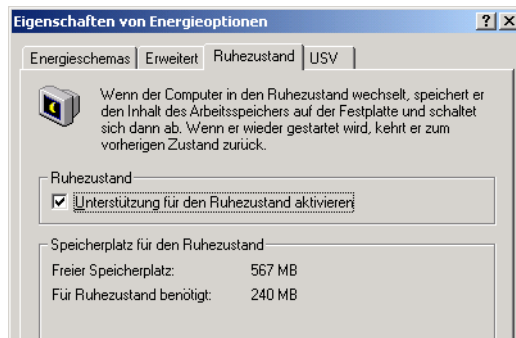
Ruhezustand mit Sophos SafeGuard Disk Encryption unterstützt ...	Ruhezustand mit Sophos SafeGuard Disk Encryption unterstützt NICHT ...
Windows 2000 und Windows XP Festplattenlaufwerke (Microsoft IDE, Serial-ATA, SCSI), die Microsoft Standardschnittstellen benutzen; bei Serial-ATA können bei manchen Geräten Probleme auftreten, wenn die Standardschnittstellen nicht benutzt werden.	Festplattentreiber von Drittherstellern

Hinweis: Bei der Verwendung von externen Geräten oder Einsteckkarten (Soundkarten etc.) bitte prüfen, ob diese die Microsoft Energieverwaltung unterstützen und der Rechner auch ohne Sophos SafeGuard Disk Encryption problemlos in den Ruhezustand versetzt/aus dem Ruhezustand zurückgeholt werden kann.

19.4 Ruhezustand einrichten

Für die bestmögliche Sicherheit bei Aktivierung des Ruhezustands empfehlen wir folgende Konfiguration:

1. Rufen Sie im Windows Startmenü nacheinander
Einstellungen\Systemsteuerung\Energieoptionen auf. In Registerkarte *Ruhezustand* aktivieren Sie das Kontrollkästchen „Unterstützung für Ruhezustand“



2. Wenn sich zwei Benutzer einen Sophos SafeGuard Disk Encryption Rechner teilen, aktivieren Sie in der Registerkarte *Erweitert* die Option „Kennwort beim Reaktivieren des Computers anfordern“.
3. Starten Sie die Sophos SafeGuard Disk Encryption Administration.
4. Aktivieren Sie die Pre-Boot Authentisierung (wenn noch nicht geschehen) unter Allgemein\Passworteinstellungen\Passwortabfrage beim Systemstart.
5. Verschlüsseln Sie mindestens die Betriebssystempartition über Verschlüsselung\Laufwerke\Festplattenlaufwerke.
Zum Schutz Ihres Systems empfehlen wir, zusätzlich zur Betriebssystempartition ihre kompletten Datenpartitionen zu verschlüsseln.

20 FIPS 140-2 (Level 1) Zertifizierung

Die FIPS-Zertifizierung beschreibt Sicherheitsanforderungen für Verschlüsselungsmodule. Beispielsweise verlangen Regierungsbehörden in den USA und in Kanada FIPS 140-2-zertifizierte Software für besonders sicherheitskritische Informationen.

Kennzeichen einer FIPS-konformen Sophos SafeGuard Disk Encryption Installation ist, dass nur bestimmte Algorithmen für die Verschlüsselung verwendet werden dürfen. Für Sophos SafeGuard Disk Encryption ist dies der folgende Algorithmus:

- AES-256

Wenn Sophos SafeGuard Disk Encryption im FIPS-Modus installiert ist, erscheint ein Icon in der Taskleiste.

Sophos SafeGuard Disk Encryption unterstützt die folgenden Funktionen, die die Anforderungen für eine FIPS 140-2 Zertifizierung erfüllen:

Known Answer Test (KAT)

Der Known Answer Test wird durchgeführt, um zu testen, ob die eingesetzten Krypto-Algorithmen korrekt arbeiten und korrekte Ergebnisse liefern. Der KAT wird für alle von FIPS zugelassenen Krypto-Algorithmen ausgeführt, auch für die Hashfunktion HMAC-256, die beim Integritätscheck verwendet wird.

Für den KAT verschlüsselt ein Verschlüsselungsmodul einen definierten Datenblock und überprüft das Verschlüsselungsergebnis, wenn die erzeugten verschlüsselten Daten die erwarteten Daten sind. Wenn das Ergebnis falsch ist, muss das Verschlüsselungsmodul jeden weiteren Verschlüsselungsprozess sperren. Verschlüsselungstreiber von Sophos SafeGuard Disk Encryption führen einen Known Answer Test (KAT) automatisch nach der Initialisierung des Treibers durch. Der KAT wird für Verschlüsselung und Dekodierung durchgeführt. Die installierten Verschlüsselungsmodule innerhalb des Sophos SafeGuard Disk Encryption Systemkerns führen die gleichen Tests durch.

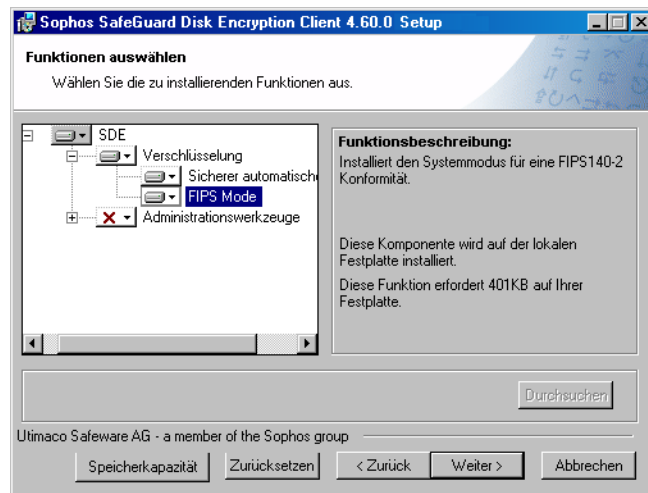
Integritätscheck

Ein Integritätscheck wird für die Verschlüsselungsmodule durchgeführt, um sicherzustellen, dass die Module nicht geändert wurden. Wenn ein Integritätscheck fehlschlägt, stoppt das System alle weiteren Prozesse. Dieser Test wird für die Verschlüsselungstreiberdateien von Sophos SafeGuard Disk Encryption und die Verschlüsselungsmodule innerhalb des Sophos SafeGuard Disk Encryption Systemkerns durchgeführt. Zusätzlich wird der Integritätscheck für die Systemdaten innerhalb des Systemkerns durchgeführt, um illegale Manipulationen zu entdecken.

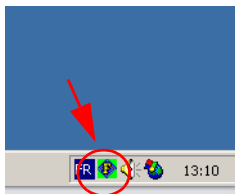
Sobald Sophos SafeGuard Disk Encryption FIPS-konform installiert wird, werden beide Testverfahren für den Systemkern und den Win32-Modus ausgeführt. Der KAT sogar auch, wenn der FIPS-Modus nicht aktiv ist.

20.1 Sophos SafeGuard Disk Encryption FIPS-konform installieren

Mit einer Installation vom Typ „Angepasst“ können Sie festlegen, ob ein Sophos SafeGuard Disk Encryption System FIPS-konform sein soll.



Nach Abschluss der Installation zeigt ein Symbol in der Systemleiste an, dass Sophos SafeGuard Disk Encryption im FIPS-Modus läuft.



20.2 Sicherer Einsatz von Sophos SafeGuard Disk Encryption in zertifizierter Konfiguration

Um Sophos SafeGuard Disk Encryption in einer zertifizierte Konfiguration einzusetzen und damit die mit dem Produkt gelieferte höchstmögliche Sicherheit zu gewährleisten, sollte das System folgendermaßen konfiguriert sein:

- Installation mit Pre-Boot Authentisierung
- Minimale Passwortlänge: 6 Zeichen
- Vollständige Verschlüsselung der Festplatte aktivieren
- Sophos SafeGuard Disk Encryption Bildschirmsperre aktivieren

21 Sophos SafeGuard Disk Encryption und Lenovo Rescue and Recovery™

Sophos SafeGuard Disk Encryption ist kompatibel mit Rescue and Recovery™. Das erlaubt Benutzern, Lenovos effiziente Backup- und Restore-Methode zu nutzen, auch wenn die Betriebssystem-Partition mit Sophos SafeGuard Disk Encryption verschlüsselt ist. Sophos SafeGuard Disk Encryption bietet hier eine einzigartige Funktionalität unter Produkten zur Festplattenverschlüsselung.

21.1 Überblick

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

Rescue and Recovery™ zielt primär auf mobile Endbenutzer, die maximale Sicherheit für ihre Notebooks anstreben, sich im Fall eines Systemproblems jedoch selbst helfen müssen.

Benutzer von Lenovo PCs und Notebooks erhalten die Möglichkeit, beschädigte Systeme wiederherzustellen, ohne die Verschlüsselung zu verlieren. Verfügbarkeit, Integrität und Vertraulichkeit von Daten ist mit der Kombination von Rescue and Recovery und Sophos SafeGuard Disk Encryption garantiert.

Für weiterführende Informationen zu Rescue and Recovery™ schlagen Sie bitte in Ihrer Lenovo Dokumentation nach.

21.2 Rescue and Recovery und Sophos SafeGuard Disk Encryption

Sophos SafeGuard Disk Encryption integriert sich reibungslos in die Rescue and Recovery-Vorgaben und unterstützt natürlich auch Lenovo-eigene Features wie den „Thinkvantage“-Button auf der Tastatur von Notebooks oder den blauen „Eingabe“-Button bei Desktop-PCs.

Angenommen, ein Benutzer verschlüsselt die komplette Festplatte mit Sophos SafeGuard Disk Encryption, so wird er unmittelbar nach der Installation aufgefordert, eine Sicherungskopie zu erstellen. In diesem Systemabbild sind u.a. die Sophos SafeGuard Disk Encryption Treiber enthalten, so dass nach dem Restore dieses Systemabbilds Windows weiterhin fehlerfrei verschlüsselt bootet (die Sicherungskopie mit Sophos SafeGuard Disk Encryption und seinen Treibern wird im folgenden kurz „SDE Backup“ genannt).

Sophos SafeGuard Disk Encryption „überlebt“ einen System-Restore, ohne dabei die Verschlüsselung zu verlieren und muss nicht neu installiert werden. Der Benutzer kann ohne

Unterbrechung nach dem Restore weiterarbeiten und wird nicht durch erneutes Anstoßen der Verschlüsselung gestört.

21.2.1 Vorteile der Kombination Rescue and Recovery und Sophos SafeGuard Disk Encryption

- Sophos SafeGuard Disk Encryption verschlüsselt die komplette Festplatte inklusive temporärer Dateien, Auslagerungsdatei, Hibernation und Memory-Dump-Datei und schützt sie durch Abfrage der Sophos SafeGuard Disk Encryption Zugangsdaten vor unerlaubtem Zugriff.
- Alle Sicherungskopien sind kryptographisch gesichert, sobald sie auf einer verschlüsselten lokalen Festplatte gespeichert sind.
- Rescue and Recovery stellt ein beschädigtes System schnell wieder her, ohne Sophos SafeGuard Disk Encryption neu installieren und die Festplatte erneut verschlüsseln zu müssen.
- Wiederherstellen eines Sophos SafeGuard Disk Encryption Backups aus der Rescue and Recovery-Umgebung ist nur möglich, wenn vorher Sophos SafeGuard Disk Encryption Zugangsdaten an der Pre-Boot Authentisierung eingetragen werden.

21.2.2 Voraussetzungen

- Lenovo-PC / Lenovo-Notebook
- aktuellstes BIOS für Ihr System
- Sophos SafeGuard Disk Encryption ab Version 4.10
- unterstützte Rescue and Recovery™-Versionen:
 - Rescue and Recovery™ 1.0 (Build 033)
 - Rescue and Recovery™ 2.0 (Build 2.00.0170)
 - Rescue and Recovery™ 3.0 (Build 3.00.0029.00)
 - Rescue and Recovery™ 4.0 (Build 4.0.0114)
 - Rescue and Recovery™ 4.2 (Build 4.20.0510)

21.3 Installation

In den folgenden Installationsbeispielen wird angenommen, dass die Rescue and Recovery-Umgebung nicht in die Service Partition installiert wird. Zu den Besonderheiten, die bei einer Verwendung der Service Partition zu berücksichtigen sind, [siehe Besonderheiten auf Seite 117](#).

Wenn Sie Rescue and Recovery™ auf einer Festplatte ohne eine Service Partition installieren, wird Rescue and Recovery mit folgenden Standardeinstellungen für die Software installiert:

- Die Umgebung von Rescue and Recovery befindet sich standardmäßig auf einer virtuellen Partition, die auf Laufwerk C (primäre Partition des Master-Festplattenlaufwerks) des Computers installiert wird.
- Die virtuelle Partition besteht aus zwei Verzeichnissen, \minint und \preboot. Diese beiden Verzeichnisse werden durch Rescue and Recovery selbst geschützt.
- 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, damit es nicht gelöscht oder verschoben wird.

Bei der Installation von Rescue and Recovery™ und Sophos SafeGuard Disk Encryption ist die Installationsreihenfolge von Bedeutung. Bitte beachten Sie unbedingt die Anweisungen in den folgenden Kapiteln.

21.3.1 Weder Sophos SafeGuard Disk Encryption noch Rescue and Recovery™ sind installiert

1. Rescue and Recovery installieren.
2. Sophos SafeGuard Disk Encryption Version 4.60 installieren.

Sophos SafeGuard Disk Encryption prüft, ob die richtige Version von Rescue and Recovery installiert ist und fügt seine Dateien und Einstellungen in die Lenovo Notfall-Umgebung ein.

Stellen Sie sicher, dass die Pre-Boot Authentisierung aktiviert ist, so dass kein Unbefugter unautorisiert beliebige Backups restaurieren kann.

Die Pre-Boot Authentisierung wird während der Installation standardmäßig aktiviert. Sie kann auch später in der Sophos SafeGuard Disk Encryption Administration über Allgemein\Passwordeinstellungen\Passwort beim Systemstart aktiviert werden.

21.3.2 Nur Sophos SafeGuard Disk Encryption ist bereits installiert

Sophos SafeGuard Disk Encryption Version 4.60 ist installiert

1. Rescue and Recovery™ installieren.
2. Vor dem Reboot aus dem Sophos SafeGuard Disk Encryption Verzeichnis nacheinander diese Tools aufrufen:
 - `MBRsync.exe`
 - `WinPERepair.exe`

21.3.3 Upgrade von Rescue and Recovery

Wann immer Rescue and Recovery™ aktualisiert wird, müssen **vor dem Reboot** die Tools `MBRsync.exe` und `WinPERepair.exe` ausgeführt werden. Beide Tools liegen im Sophos SafeGuard Disk Encryption Verzeichnis und werden einfach per Doppelklick aufgerufen.

21.4 Deinstallation

Bei der Deinstallation beider Produkte ist folgendes zu beachten:

- Deinstallieren Sie zunächst Sophos SafeGuard Disk Encryption und dann Rescue and Recovery.
- Wenn Sie Rescue and Recovery for Sophos SafeGuard Disk Encryption deinstallieren, führen Sie vor dem Neustart das Tool `MBRsync.exe` aus.
- Die Deinstallation von Sophos SafeGuard Disk Encryption darf nicht unmittelbar auf einen System-Restore folgen. Starten Sie den PC neu und deinstallieren Sie danach Sophos SafeGuard Disk Encryption.

21.5 Sicherungskopie erstellen

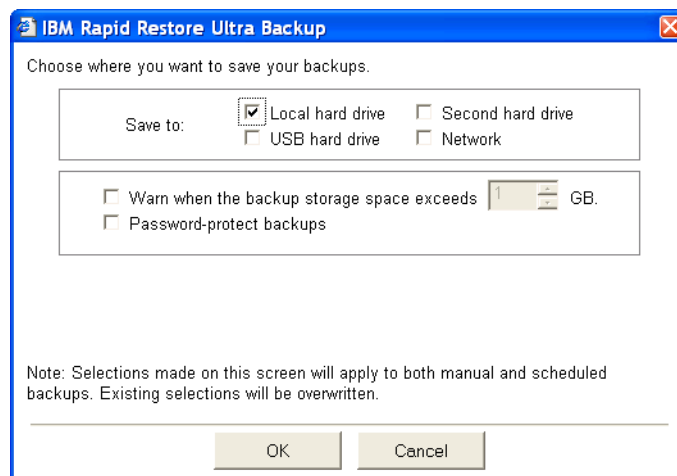
Hinweis: Die Bildschirmbeispiele in den folgenden Abschnitten zeigen Auszüge aus der Version 4.0 von Rescue and Recovery™ (Build 033). Die Funktionen auf der Benutzeroberfläche können in neueren Versionen variieren, die beschriebene Funktionalität ist jedoch identisch.

Sicherungskopien werden über die Rescue and Recovery Software in der aktiven Windows-Umgebung erstellt. Auf PCs mit Rescue and Recovery rät Sophos SafeGuard Disk Encryption dem Benutzer, nach einer erfolgreichen Installation unbedingt eine neue System-Sicherungskopie zu erstellen.

Wie Sie aus der Windows-Umgebung einen System-Backup erstellen, lesen Sie bitte in den entsprechenden Dokumenten von Lenovo nach.

Sophos SafeGuard Disk Encryption unterstützt für Sophos SafeGuard Disk Encryption Backups folgende Medien:

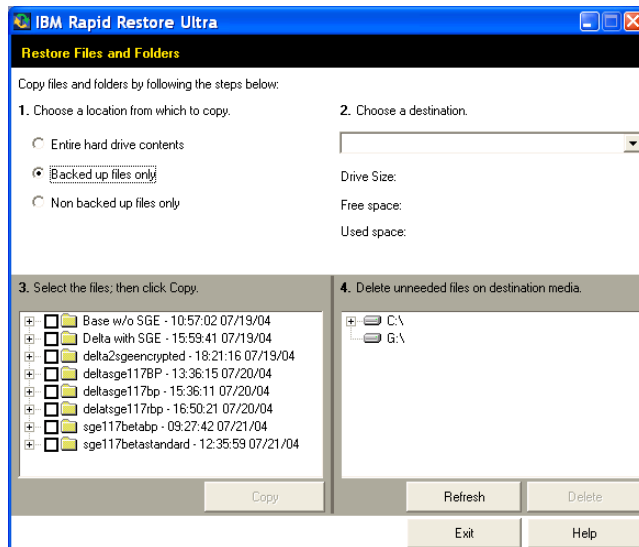
- Lokale Festplatte
- Zweites Festplattenlaufwerk
- USB-Festplattenlaufwerk
- Netzlaufwerk
- USB-Stick
- CD/DVD



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, damit es nicht gelöscht oder verschoben wird.

21.6 Dateien aus Sophos SafeGuard Disk Encryption Backup wiederherstellen

Rescue and Recovery™ stellt einzelne Dateien oder Verzeichnisse aus einem Backup, der ein installiertes Sophos SafeGuard Disk Encryption enthält, problemlos wieder her. Benutzer starten einfach Windows, dann die Rescue and Recovery Software und restaurieren die gesuchten Dateien. Es ist kein Neustart nötig, d.h. die restaurierten Daten stehen dem Benutzer sofort zur Weiterbearbeitung zur Verfügung.



21.7 Sophos SafeGuard Disk Encryption System wiederherstellen

Für den Restore eines System-Backups, der Sophos SafeGuard Disk Encryption enthält, startet der Benutzer die Rescue and Recovery-Umgebung. Diese erscheint, wenn beim Booten des PCs/ Notebooks diese Tasten gedrückt werden:

- „Thinkvantage“/„Access IBM“ (bei Lenovo Notebooks).
- die „Blaue Eingabetaste“ (bei Lenovo Desktop-PCs).
- F11 bei sonstigen Tastaturen.

Hinweis zu Rescue and Recovery™ 2.0:

Wir empfehlen generell, beim Restaurieren die komplette Festplatte wiederherzustellen.

Wenn Sie jedoch versehentlich die Option „Nur das Windows-Betriebssystem und Applikationen aus einem Backup wiederherstellen“ gewählt haben, garantiert Sophos nicht, dass die Sophos SafeGuard Disk Encryption Dateien vollständig restauriert werden. Treten in diesem Fall Probleme beim Booten auf, müssen Sie jedoch keine negativen Folgen für ihr System befürchten. Rufen Sie nach einem Neustart einfach über die Lenovo-Tasten ihres PCs oder Notebooks die Rescue and Recovery™-Umgebung auf und stellen Sie die komplette Festplatte wieder her.

21.7.1 Boot-Umgebung

Sophos SafeGuard Disk Encryption erlaubt das Booten der Rescue and Recovery-Umgebung von...

- *Lokaler Festplatte*

Virtuelle Partition auf der lokalen Festplatte oder lokale Service Partition

Sophos SafeGuard Disk Encryption erlaubt das Booten der Rescue and Recovery-Umgebung NICHT von...

- *Bootfähiger CD*

- *Bootfähiger USB-Festplatte*

Wird die Rescue and Recovery-Umgebung trotzdem von einem externen Medium gebootet, wird Sophos SafeGuard Disk Encryption während des Restore-Prozesses entfernt.

Um das System wieder abzusichern, muss Sophos SafeGuard Disk Encryption erneut installiert werden.

21.7.2 Vorgehensweise

1. Starten Sie die Rescue and Recovery-Umgebung („Thinkvantage“-Taste, „Blauen Eingabetaste“ oder F11).
2. Die Pre-Boot Authentisierung erscheint und verlangt Sophos SafeGuard Disk Encryption Zugangsdaten.
3. Die Benutzeroberfläche der Rescue and Recovery-Umgebung erscheint.
4. Schließen Sie den Willkommen-Bildschirm mit einem Klick auf Weiter.
5. Im linken Menü **Über Sicherung wiederherstellen** wählen.
6. Ein Dialog, in dem Sie die Sicherung auswählen können, wird angezeigt.
7. Wählen Sie den Backup, der ein installiertes Sophos SafeGuard Disk Encryption enthält, aus und stellen Sie ihn wieder her.

21.8 Service Partition und Factory Recovery Partition

Lenovo liefert neue PCs mit speziellen vorinstallierten Partitionen aus. Lenovo nennt diese Partitionen "Service Partion" und "Factory Recovery Partition":

- **Service Partition:** enthält die Rescue and Recovery-Bootumgebung.

- **Factory Recovery Partition:** enthält alle Informationen, um die Werkseinstellungen („Factory settings“) des Rechners wiederherzustellen.

Wenn auf Ihrem PC noch keine Service Partition vorhanden ist, Sie aber dennoch mit ihr arbeiten wollen, legen Sie sie vor der Installation von Sophos SafeGuard Disk Encryption an.

Wie Sie die Service Partition anlegen, schlagen Sie bitte in der entsprechenden Lenovo Dokumentation nach.

21.8.1 Besonderheiten

Folgende Besonderheiten sind bei Verwenden der Service Partition und der Factory Recovery Partition zu beachten:

Betriebssystem	SDE Verschlüsselungsmodus	Status der beiden speziellen Partitionen
Windows 2000	Partitionsweise	Die Partitionen sind nicht verschlüsselt.
Windows XP	Partitionsweise	Vorteil: Die Lenovo-Werkseinstellungen können von der lokalen Festplatte wiederhergestellt werden. Nachteil: Hacker können eine unverschlüsselte Rescue and Recovery-Bootumgebung manipulieren.

Wir empfehlen, entweder die Service Partition zu verschlüsseln oder stattdessen die Rescue and Recovery-Umgebung in die virtuelle Partition zu installieren. Die virtuelle Partition ist immer geschützt, sobald das Windows-Systemlaufwerk verschlüsselt ist!

21.9 Was tun, wenn...

... nach dem Neustart des PCs auf dem Bildschirm eine Sophos SafeGuard Disk Encryption Viruswarnung angezeigt wird?



Mögliche Gründe dafür sind:

1. *Sie haben einen Virus auf Ihrem System.*
Kontaktieren Sie bitte umgehend Ihren Systemadministrator.
2. *Sie haben vergessen, nach der Installation, Modifikation oder Deinstallation von Rescue and Recovery den MBR mit dem Kommando `MBRsync.exe` zu synchronisieren.*
Sophos SafeGuard Disk Encryption erkennt Modifikationen am MBR zeigt die vorhandenen Viruswarnung an. Verwenden Sie zur Sicherheit die Systemkernsicherung von einem zuvor erstellten bootfähigen Notfallmedium, siehe [Systemkern sichern und Notfallmedien erstellen](#) auf Seite 130.

...das Dateisystem beschädigt ist?

Hier genügt in der Regel ein einfaches Einspielen einer Sicherungskopie (mit Sophos SafeGuard Disk Encryption) mit Rescue and Recovery.

Alternativ kann die Festplatte über die Notfallmedien und das DOS-Tool `Sgeasy.exe` entschlüsselt werden (= Deinstallation von Sophos SafeGuard Disk Encryption). Die Festplatte ist dann wieder im Klartext vorhanden und kann mit üblichen Tools für die Datenrettung bearbeitet werden. Darf der Benutzer aufgrund fehlender Rechte Sophos SafeGuard Disk Encryption nicht deinstallieren, hilft das Sophos SafeGuard Disk Encryption Challenge/Response-Verfahren und erteilt dem Benutzer temporär das Recht dazu.

... die Festplatte physikalisch beschädigt ist?

Wenn die Festplatte physikalisch beschädigt ist und nicht einmal mit `Sgeasy.exe` entschlüsselt werden kann, kontaktieren wir auf Kundenwunsch Partner, die darauf spezialisiert sind, physikalisch beschädigte Laufwerk zu retten.

...der Sophos SafeGuard Disk Encryption Systemkern beschädigt ist?

Bei geringfügigen Fehlern wie einem überschriebenen MBR repariert `Sgeasy.exe` den MBR oder spielt einen Backup des Systemkerns ein.

...die Initialverschlüsselung abgebrochen wurde und Windows nicht mehr gebootet werden kann?

Wenden Sie sich in diesem Fall an den Sophos Support.

...die endgültige Entschlüsselung abgebrochen wurde und Windows nicht mehr gebootet werden kann?

Wenden Sie sich in diesem Fall an den Sophos Support.

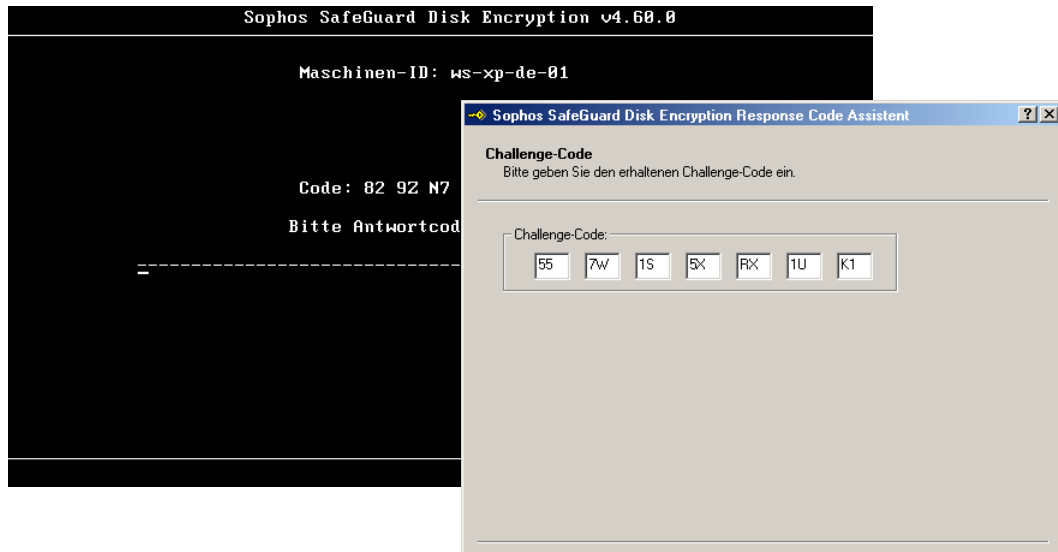
22 Kompatibilität zur Computrace Software der Absolute Software Corp.

Lenovo schützt seine Thinkpad Notebooks mit zahlreichen Sicherheitsfeatures (u.a. Sophos SafeGuard Disk Encryption und SafeGuard PrivateDisk) und garantiert seinen Benutzern damit hohe mobile Sicherheit. Neben den Produkten der SafeGuard Familie ist auch Computrace der Absolute Software Corp. auf verschiedenen Lenovo Notebooks vorinstalliert.

Computrace hilft, ein Notebook im Fall eines Diebstahls wieder aufzuspüren, sobald sich der gestohlene PC mit dem Internet verbindet. Zudem können auf Wunsch des rechtmäßigen Nutzers vertrauliche Daten vom gestohlenen Rechner gelöscht werden. Lenovo integriert Computrace als bereits in die PC-Hardware (persistent BIOS based Agent).

Durch die Kompatibilität mit Sophos SafeGuard Disk Encryption funktioniert die Computrace-Software mit verschlüsselten Festplatten.

23 Fernwartung (Challenge/Response)

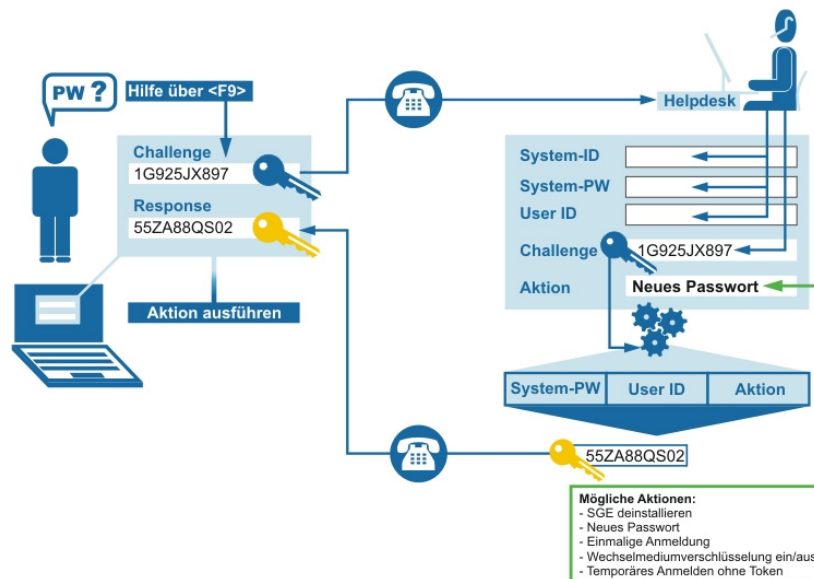


Sophos SafeGuard Disk Encryption bietet das Challenge/Response-Verfahren zum Zurücksetzen „vergessener“ Sophos SafeGuard Disk Encryption Passwörter.

Challenge/Response ist sehr sicher und effizient:

- Es werden keine vertraulichen Daten ausgetauscht.
- Das „Belauschen“ bzw. die Verwendung „abgehörter Daten“ ist nutzlos.
- Ist auch für Geräte ohne Netzwerkanbindung verwendbar.
- Der Benutzer kann in kürzester Zeit seine Arbeit wieder aufnehmen.

23.1 Funktionsweise



Benötigt ein Benutzer (entfernter Benutzer) Hilfe, muss er einen Challenge Code erzeugen. Dieser Challenge Code wird auf seinem PC als ASCII Zeichen-Kette angezeigt. Der Benutzer ruft anschließend beim Helpdesk an und gibt seine Benutzerinformationen und den Challenge Code an. Der Helpdesk startet den Sophos SafeGuard Disk Encryption Response Code Assistenten und erzeugt dann einen Response Code. Der Helpdesk teilt den Response Code per Telefon oder SMS dem Benutzer mit, und dieser kann nach der Eingabe des Response Codes sein Passwort neu setzen.

Generell können über Challenge/Response folgende Sonderrechte erteilt werden:

- Neues Sophos SafeGuard Disk Encryption Benutzerpasswort setzen (wenn das alte Passwort vergessen wurde)
- Sophos SafeGuard Disk Encryption deinstallieren
- Einmalige Anmeldung (z. B. für Wartungsarbeiten)

23.2 Challenge Code erzeugen

Der Challenge Code wird vom Benutzer erzeugt, der z. B. sein Sophos SafeGuard Disk Encryption Passwort vergessen hat. Abhängig von der Art des Systemstarts ergeben sich unterschiedliche Vorgehensweisen beim Erzeugen des Challenge Codes:

Systemstart mit Pre-Boot Authentisierung

Beim Systemstart mit Pre-Boot Authentisierung muss der Benutzer seinen Sophos SafeGuard Disk Encryption Benutzernamen an der Pre-Boot Authentisierung eingeben und anschließend in das Passwortfeld wechseln. Nach Drücken von F9 wird der Challenge Code angezeigt.



Systemstart ohne Pre-Boot Authentisierung

Beim Systemstart ohne Pre-Boot Authentisierung erscheint beim Booten des Rechners für wenige Sekunden ein Diskettensymbol in der linken oberen Ecke des Bildschirms. Der Benutzer drückt nun während dieses Zeitraums die Taste F2. Der Anmeldedialog der Pre-Boot Authentisierung erscheint, und der Benutzer gibt seinen Sophos SafeGuard Disk Encryption Benutzernamen an der Pre-Boot Authentisierung ein und wechselt ins Passwortfeld. Nach Drücken von F9 wird der Challenge Code angezeigt.

Sonderfall Deinstallation

Um Sophos SafeGuard Disk Encryption per Challenge/Response zu deinstallieren, muss der Challenge Code über den Deinstallationsdialog (Programme\Systemsteuerung\Software\Sophos SafeGuard Disk Encryption\Entfernen) erzeugt werden. Eine Deinstallation von Sophos SafeGuard Disk Encryption mit Hilfe des Challenge/Response-Verfahrens kann **nicht in der Pre-Boot Authentisierung** begonnen werden.

23.3 Response Code

Der Administrator bzw. Helpdesk-Mitarbeiter erzeugt den Response Code mit dem Response Code Assistenten.

Wer den Response Code erzeugt, muss die Daten eines Sophos SafeGuard Disk Encryption Benutzerprofils am entfernten Benutzer-PC kennen, z. B. die Daten des Benutzerprofils

„Helpdesk“. „Helpdesk“ muss am Benutzer-PC mindestens über die gleichen Rechte wie der anfragende Sophos SafeGuard Disk Encryption Benutzer verfügen.

Damit das Benutzerprofil „Helpdesk“ bestimmte Sonderrechte gewähren kann, benötigt es für die jeweilige Aktion folgende Benutzerrechte:

Geplante Helpdesk-Aktion auf einem Benutzer-PC	Nötiges Sophos SafeGuard Disk Encryption Benutzerrecht
Sophos SafeGuard Disk Encryption deinstallieren	Sophos SafeGuard Disk Encryption deinstallieren
Neues Passwort festlegen	Benutzereinstellungen ändern
Einmalige Anmeldung	Benutzereinstellungen ändern

23.3.1 Response Code erzeugen

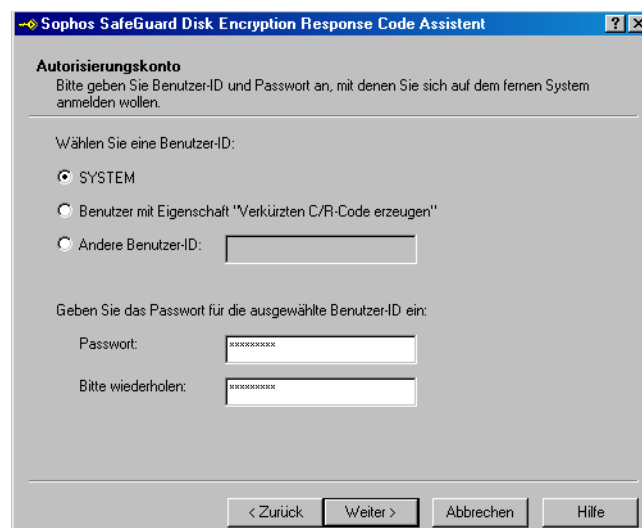
Hinweis: Auf einem PC muss der Sophos SafeGuard Disk Encryption Response Code Assistent installiert sein.

Starten Sie den Response Code Assistenten über **Programme\Sophos\SafeGuard Disk Encryption\Response Code Assistent**. Der erste Dialog zeigt Informationen über den Assistenten an.

Bestätigen Sie in der Folge korrekte Eingaben mit **Weiter**.

Autorisierungskonto

Im Dialog „Autorisierungskonto“ wählen Sie den Sophos SafeGuard Disk Encryption Benutzer, mit dem Sie sich am System des entfernten Benutzers anmelden wollen.



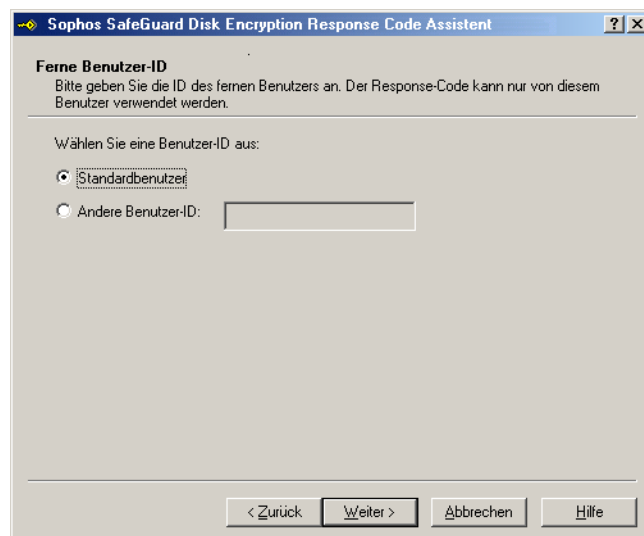
- **SYSTEM:**
Benutzername des Sophos SafeGuard Disk Encryption Benutzers SYSTEM; SYSTEM darf alle Sonderrechte gewähren.
- **Benutzer mit Eigenschaft „Vereinfachte Fernanmeldung“:**
Benutzer, dem auf dem Zielsystem diese Eigenschaft zugeordnet wurde. Er muss mindestens über die Rechte des fernen Benutzers verfügen.
- **Andere Benutzer-ID:**
Benutzernamen eines beliebigen Sophos SafeGuard Disk Encryption Benutzers, der ein Sonderrecht gewähren darf.

Der hier gewählte Benutzername beeinflusst die Länge des Response Codes, der später erzeugt wird. Je länger der Response Code, desto höher ist die Gefahr, dass beim Eintippen bzw. Übermitteln an den Benutzer Fehler auftreten.

Benutzer-ID	Länge der Response (Zeichen)
SYSTEM	30
Andere Benutzer-ID	56
Verkürzten C/R-Code erzeugen	30

Ferne Benutzer-ID

Im nächsten Dialog wählen Sie den Sophos SafeGuard Disk Encryption Benutzernamen des entfernten Benutzers. Fragen Sie den Benutzer, mit welchen Zugangsdaten er sich üblicherweise an seinem Rechner anmeldet.



■ **Standardbenutzer:**

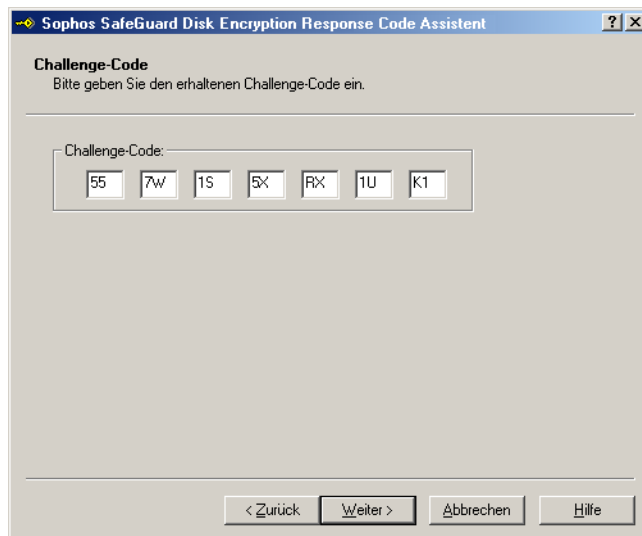
Benutzer meldet sich nur mit seinem Sophos SafeGuard Disk Encryption Passwort an, d.h. er ist auf dem Zielsystem als Standardbenutzer registriert und kennt demzufolge den Benutzernamen nicht.

■ **Andere Benutzer-ID:**

Benutzer meldet sich mit Sophos SafeGuard Disk Encryption Benutzernamen und Passwort an. Der Sophos SafeGuard Disk Encryption Benutzername ist demzufolge bekannt. Tragen Sie ihn in das Feld ein.

Challenge Code

Im nächsten Dialog geben Sie in die paarweise getrennten Felder den Code ein, den Ihnen der entfernte Benutzer (z. B. per Telefon) mitteilt. Der **Challenge Code** wird dem Benutzer auf seinem PC als ASCII-Zeichenkette (14 Zeichen) angezeigt.



Auszuführende Aktion

Im nächsten Dialog wählen Sie die **Aktion**, die dem entfernten Benutzer erlaubt werden soll:



Eine der folgende Aktionen kann ausgeführt werden:

■ **Deinstallieren**

Benutzer darf Sophos SafeGuard Disk Encryption deinstallieren. Diese Art der Deinstallation ist nur sinnvoll, wenn der Administrator nicht vor Ort ist.

■ **Neues Passwort festlegen**

Benutzer darf sein Passwort ändern, z. B. wenn er das alte Passwort vergessen hat oder sich durch mehrmalige falsche Passworteingabe die Wartezeit an der Pre-Boot Authentisierung zu sehr erhöht hat.

Das Passwort des Benutzers SYSTEM kann nicht per Challenge/Response neu vergeben werden.

■ **Einmalige Anmeldung**

Benutzer erhält er für die Dauer einer Arbeitssitzung Zugang zum betreffenden Rechner.

Dies ist sinnvoll, wenn z. B. ein Techniker Wartungsarbeiten durchführt.

Mit Bestätigen der Eingaben wird der Response Code erzeugt.

Zusammenfassung

Im letzten Dialog erhalten Sie einen kompletten Überblick über die von Ihnen in den vorangegangenen Dialogen des Response Code Assistenten getroffenen Einstellungen. Zusätzlich wird folgendes angezeigt:



Response Code

Zeigt den erzeugten Response Code in blauer Schrift an. Dieser Code muss an den entfernten Benutzer gegeben werden. Der entfernte Benutzer trägt den Response Code in die dafür vorgesehenen Felder ein. Der Response Code ist nur einmal gültig! Für jeden Request muss ein neuer erzeugt werden.

In Zwischenablage kopieren

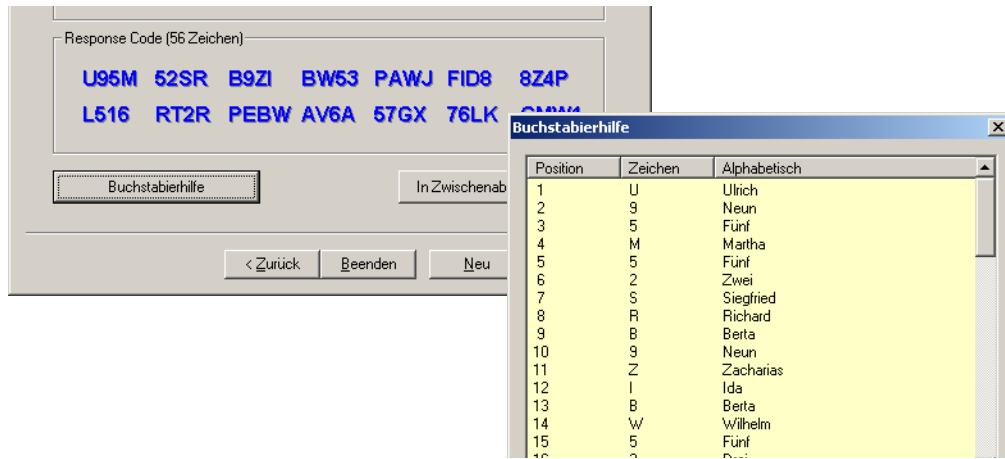
Der Response Code wird in die Zwischenablage kopiert und kann in einen beliebigen Texteditor eingefügt werden. Dieses Feature erlaubt z. B., den Response Code einfach per SMS oder E-Mail an den Benutzer zu verschicken.

Sind alle Angaben korrekt und der Benutzer konnte die erforderlichen Aktionen ausführen, wird der Response Code Assistent durch einen Klick auf **Beenden** geschlossen. Durch Klicken auf **Neu** werden alle Angaben gelöscht und Sie können eine neue/weitere Response erzeugen.

Buchstabierhilfe

Um das Übermitteln des Codes an den Benutzer zu erleichtern und Fehler zu vermeiden, gibt es im Response Code Assistenten eine Buchstabierhilfe.

Drücken Sie die Schaltfläche **Buchstabierhilfe**, erscheint ein in drei Spalten gegliedertes Fenster mit den jeweiligen Spaltenüberschriften. Unter „Position“ sehen Sie, an welcher Stelle das Zeichen innerhalb des Codes steht. Nachfragen können somit sofort ohne größeren Zeitaufwand (z. B. Abzählen der Stellen) beantwortet werden. Welches Zeichen anzugeben ist, sehen Sie unter der gleichnamigen Rubrik. „Alphabetisch“ gibt an, mit welchem Wort die Zeichen „verknüpft“ werden können, um Verwechslungen zu vermeiden. In der Regel werden Vornamen verwendet, deren erster Buchstabe dann in die Codefelder eingetragen wird. Im Fenster wird bereits der tatsächliche Response Code dargestellt. Sie müssen diesen nur von oben nach unten vorlesen.



24 Systemkern sichern und Notfallmedien erstellen

Wenn Ihr Rechner bei verschlüsselter Festplatte Sophos SafeGuard Disk Encryption Fehlermeldungen anzeigt, kann in den meisten aller Fälle der Systemkern von Sophos SafeGuard Disk Encryption nicht gefunden werden.

Der Systemkern hält die für die Authentisierung am Rechner erforderlichen Funktionen, die für den Start eines Betriebssystems notwendigen Treiber sowie alle Systemeinstellungen eines Sophos SafeGuard Disk Encryption Clients. Eine aktuelle Sicherung ist besonders in Notfallsituationen gefragt, wenn der Systemkern eines Sophos SafeGuard Disk Encryption Clients beschädigt ist und Benutzer sich nicht mehr ans System anmelden können. In solchen Fällen benutzt man einen intakten Systemkern der betreffenden Arbeitsstation, um den Urzustand wiederherzustellen und das System lauffähig zu machen.

Sophos SafeGuard Disk Encryption bietet für die Systemwiederherstellung folgende Möglichkeiten:

- Automatische Systemkernsicherung
- Assistent für Notfalldiskette
- Notfallwerkzeug `Sgeasy.exe`

Sophos SafeGuard Disk Encryption sichert den Systemkern automatisch ohne Benutzerinteraktion. Somit steht jeweils immer die aktuelle Version des Systemkerns auf der Festplatte zur Verfügung.

Da Sie im Fall eines Systemdefekts jedoch wahrscheinlich nicht auf die Festplatte zugreifen können, sollte der Systemkern immer auf einem Notfallmedium (CD, USB-Stick oder Diskette) abgelegt sein. Auf diesem Medium befinden sich der gesicherte Systemkern und Dateien, die beim Beheben von Sophos SafeGuard Disk Encryption Fehlern helfen und mit deren Hilfe Sie wieder Zugriff auf den Computer erhalten.

24.1 Systemkern automatisch sichern

Nach der Installation und nach jeder Änderung am Systemkern wird der Systemkern automatisch gesichert. Für die automatische Systemkernsicherung ist keine Benutzerinteraktion notwendig. Diese Aufgabe übernimmt eine Autobackup-Funktion. Auch nach Eingriffen in die Sophos SafeGuard Disk Encryption Konfiguration (z. B. über ausgeführte Konfigurationsdateien) erzeugt der Sophos SafeGuard Disk Encryption Client diese Sicherung. Für zusätzliche Sicherheit wird jeweils auch die letzte und die vorletzte Version des Systemkerns gespeichert.

In der Grundeinstellung wird der gesicherte Systemkern immer auf einem internen Teil der Festplatte abgelegt.

24.2 Systemkern manuell sichern

Zusätzlich zur automatischen Systemkernsicherung können Sie den Systemkern jederzeit manuell sichern und ihn an einem ausgewählten Speicherplatz speichern. Dies ist zum Beispiel bei geplanten Sicherungen nützlich.

Sie können den Systemkern mit folgende Tools manuell sichern:

- Assistent für Notfalldiskette (siehe [Systemkernsicherung/Notfallmedium erstellen](#) auf Seite 131)
- Kommandozeile (siehe [Systemkern per Kommandozeile sichern](#) auf Seite 134)

24.3 Systemkernsicherung/Notfallmedium erstellen

Mit dem Assistenten für Notfalldiskette, der nach jeder Standard-Installation auf einem Client vorhanden ist, können Sie eine Systemkernsicherung durchführen oder ein Notfallmedium erstellen.

Das Notfallmedium muss bootfähig sein und enthält den gesicherten Systemkern sowie Dateien, die beim Beheben von Sophos SafeGuard Disk Encryption Fehlern helfen und mit deren Hilfe Sie wieder Zugriff auf den Computer erhalten.

Damit auf einem Notfallmedium immer der aktuellste Systemkern vorhanden ist, sollte eine Sicherung nach jeder signifikanten Änderung wie etwa der Änderung des Verschlüsselungsstatus durchgeführt werden. Es ist über eine Option im Notfallassistenten konfigurierbar, dass Benutzer in regelmäßigen Abständen aufgefordert werden, den Systemkern zu sichern. Dieser muss dann auf die Notfallmedien kopiert werden.

Hinweis: Genaue Anweisungen zum Erstellen einer bootfähigen Notfall-CD und zum Wiederherstellen des Systems finden Sie in folgenden Artikeln in der Wissensdatenbank:

<http://www.sophos.com/support/knowledgebase/article/56544.html>

<http://www.sophos.com/support/knowledgebase/article/56456.html>

24.3.1 Notfallassistenten starten

Rufen Sie den Notfallassistent über
Programme\Sophos\SafeGuard Disk Encryption\Assistent für Notfalldiskette
auf.

Bestätigen Sie alle richtigen Angaben im Assistenten mit **Weiter**.

1. Ist der Assistent gestartet, legen Sie im zweiten Dialog fest, welche Art von Sicherung erstellt werden soll.



Folgende Optionen stehen zur Auswahl:

- **Nur Kernsicherung erstellen**
Sichert den kompletten Systemkern (Treiber für Sophos SafeGuard Disk Encryption und den Master Boot Record) in eine Datei.
- **Kernsicherung erstellen und Sophos SafeGuard Disk Encryption Notfalldateien kopieren**
Kopiert den Systemkern und die Notfalldateien.
- **Startdiskette mit Sophos SafeGuard Disk Encryption Notfalldateien und Kernsicherung erstellen**
Erstellt eine bootfähige Rettungsdiskette mit einer FreeDOS-Version, Systemkern und Notfalldateien.

2. Anschließend wählen Sie unter **Pfad-Info** aus, wo die Daten (Systemkern und Notfalldateien) gespeichert werden.

Sie können den Systemkern nur intern, auf einem lokalen Laufwerk oder auf einem Netzwerklaufwerk speichern.

Da Sie im Fall eines Systemdefekts wahrscheinlich nicht auf die Festplatte zugreifen können, empfehlen wir, den Systemkern und die Notfalldateien immer auf einer Diskette, einem Wechselmedium oder einem Netzlaufwerk abzulegen.



- Wenn Sie **Nur Kernelsicherung erstellen** ausgewählt haben, wird **Interne Kernelsicherung** automatisch aktiviert. Die Kernelsicherung wird intern auf der lokalen Festplatte gespeichert. In diesem Fall müssen Sie keinen Dateinamen angeben.

Um die Kernelsicherung an einem anderen Speicherplatz zu sichern, deaktivieren Sie **Interne Kernelsicherung** und geben Sie einen Speicherplatz für die Kernelsicherung an.

- Wenn Sie **Kernelsicherung erstellen und Sophos SafeGuard Disk Encryption Notfalldateien kopieren** oder **Startdiskette erstellen** gewählt haben, geben Sie an, wo Systemkern und Notfalldateien (wenn ausgewählt) gesichert werden sollen. Geben Sie unter *Name der Kerneldatei* einen Namen für den Systemkern. Voreinstellung ist `Backup.svf`, Name und die Extension SVF können aber geändert werden.

3. Stellen Sie im Dialog *Reminder* ein, in welchen Zeitabständen Sie an die Systemkernsicherung erinnert werden möchten.



Damit bei auftretenden Systemfehlern immer die aktuellste Systemkern Version verfügbar ist, ist es ratsam, den Systemkern regelmäßig auf einem Netzwerklaufwerk oder einem Wechselmedium zu sichern.

24.3.2 Systemkern per Kommandozeile sichern

Sie können den Systemkern auch von der Kommandozeile sichern, und zwar über

```
SGEBACK.EXE /f:<Pfad/Dateiname> | /?
```

/f : Gibt den Pfad und Dateinamen der Kernelsicherung an.

/? Zeigt diese Hilfe.

24.4 Bootfähige Notfall-CD erstellen

Im Notfall können Sie Sophos SafeGuard Disk Encryption auch von einer CD starten.



Voraussetzung: Stellen Sie sicher, dass das BIOS des Computers das Booten von einer CD unterstützt.

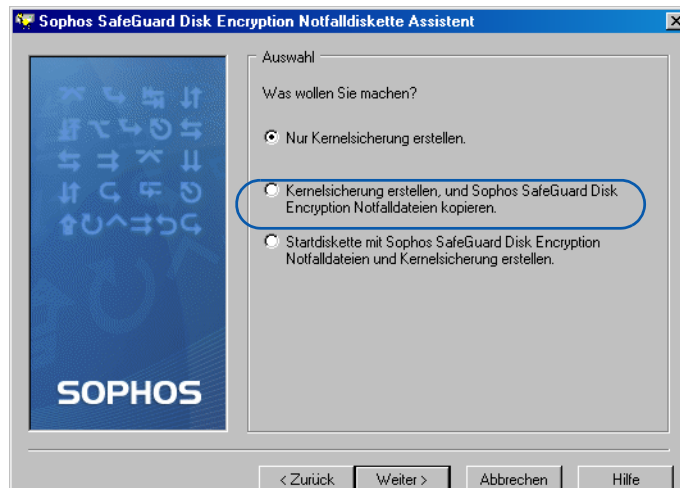
So erstellen Sie eine bootfähige CD auf dem Benutzercomputer:

1. Erstellen Sie eine aktuelle Systemkernsicherung:
 - a) Öffnen Sie auf dem Benutzercomputer den **Notfallassistenten** im Sophos SafeGuard Disk Encryption Ordner des **Start-Menüs**.
 - b) Wählen Sie im Dialog **Auswahl** die Option **Nur Kernelsicherung erstellen**.
 - c) Wählen Sie im Dialog **Pfad-Info** den Speicherort für die Systemkernsicherung.
 - d) Klicken Sie auf **Beenden**.
2. Erstellen Sie eine bootfähigen Notfall-CD. Genaue Anweisungen hierzu finden Sie im folgenden Artikel in der Wissensdatenbank:
<http://www.sophos.com/support/knowledgebase/article/56544.html>
3. Kopieren Sie die zuvor erstellte Systemkernsicherung vom jeweiligen Speicherort auf die bootfähige Notfall-CD.

Wir empfehlen, nach der Installation ein bootfähiges Wechselmedium zu erstellen und sobald der Systemkern geändert wird, nur diesen zu aktualisieren.

24.5 Bootfähigen Notfall-USB-Stick erstellen

Im Notfall können Sie Sophos SafeGuard Disk Encryption von einem bootfähigen USB-Stick starten.



Voraussetzung: Stellen Sie sicher, dass das BIOS des Computers das Booten von einem USB-Stick unterstützt.

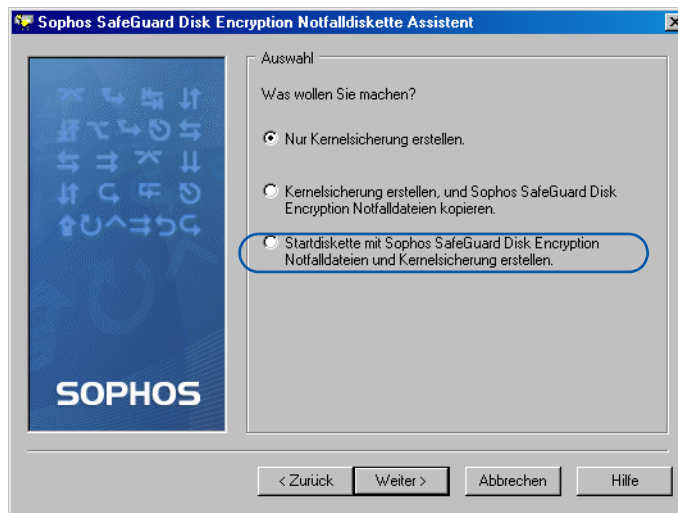
So erstellen Sie einen bootfähigen Notfall-USB-Stick auf dem Benutzercomputer:

1. Formatieren Sie einen USB-Stick, so dass er bootfähig ist.
2. Öffnen Sie auf dem Benutzercomputer den **Notfallassistenten** im Sophos SafeGuard Disk Encryption Ordner des **Start-Menüs**.
3. Wählen Sie im Dialog **Auswahl** die Option **Kernelsicherung erstellen und Sophos SafeGuard Disk Encryption Notfalldateien kopieren**.
4. Wählen Sie im Dialog **Pfad-Info** den Speicherort für die Systemkernelsicherung und die Notfalldateien.
5. Klicken Sie auf **Beenden**.
6. Kopieren Sie die Systemkernelsicherung und die Sophos SafeGuard Disk Encryption Notfalldateien auf den bootfähigen USB-Stick.

Wir empfehlen, nach der Installation ein bootfähiges Wechselmedium zu erstellen und sobald der Systemkern geändert wird, nur diesen zu aktualisieren.

24.6 Bootfähige Notfalldiskette erstellen

Als zusätzliche Option bietet der Notfallassistent an, eine bootfähige Startdiskette samt Systemkern, Notfalltools und Treiberdateien für das Tastaturlayout zu erstellen. Dies ist eine komfortable Möglichkeit, Bootdiskette und Sophos SafeGuard Disk Encryption Notfalldiskette zu kombinieren.



Voraussetzung: Stellen Sie sicher, dass das BIOS des Computers das Booten von einer Diskette unterstützt.

So erstellen Sie eine bootfähige Notfalldiskette auf dem Benutzercomputer:

1. Legen Sie eine formatierte Diskette ein und starten Sie den Notfallassistenten.
2. Wählen Sie im Dialog **Auswahl** die Option **Startdiskette mit Sophos SafeGuard Disk Encryption Notfalldateien und Kernsicherung erstellen**.

Die Systemkernsicherung und die Notfalldateien werden auf die Diskette kopiert.

3. Klicken Sie auf **Beenden**.

Wir empfehlen, nach der Installation eine bootfähige Startdiskette zu erstellen und sobald der Systemkern geändert wird, nur diesen zu aktualisieren.

24.6.1 Sophos SafeGuard Disk Encryption Notfalldateien manuell auf Diskette sichern

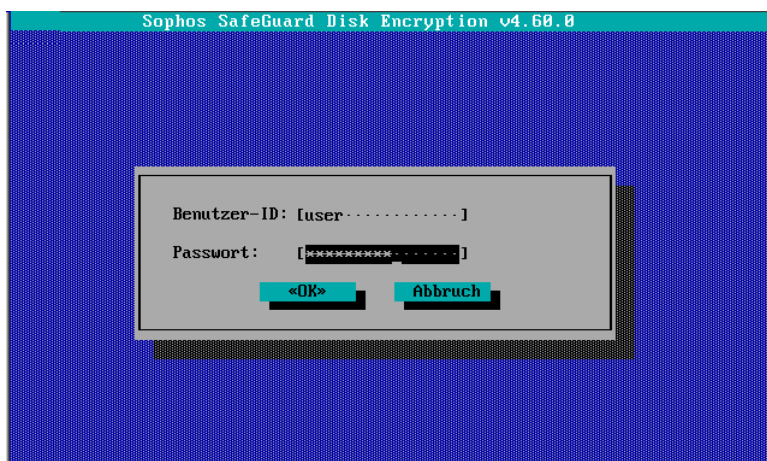
Sie können die Notfalldateien auch manuell auf eine Diskette sichern. Kopieren Sie folgende Dateien aus dem Installationsverzeichnis von Sophos SafeGuard Disk Encryption:

- SGEASY.exe
- Sgeasy.hmf
- Sgecrypt.mod
- Sgenls.mod
- Sgekrnl.mod

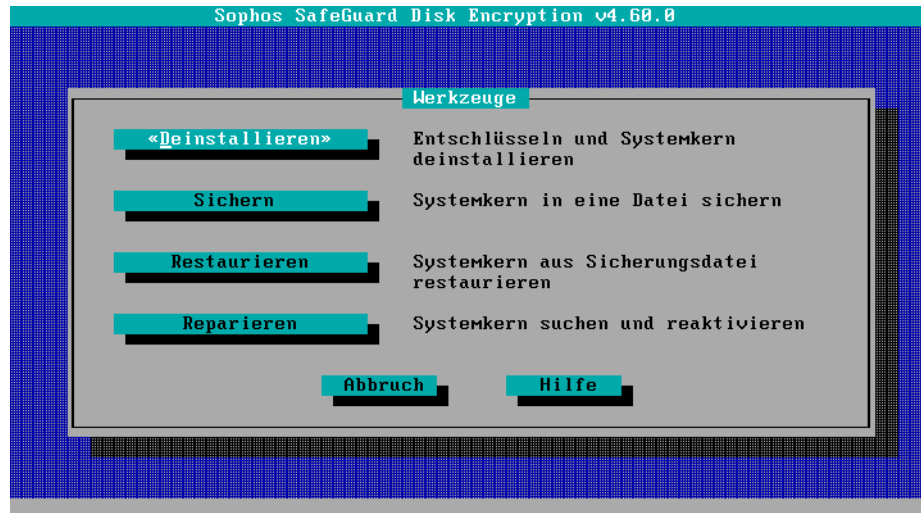
24.7 Notfallstart durchführen

Tritt ein Systemfehler bei verschlüsselter Festplatte auf, gehen Sie folgendermaßen vor:

1. Legen Sie ein Notfallmedium ein und starten Sie den PC.
2. Das Notfallprogramm `Sgeasy.exe` wird automatisch gestartet.
3. Geben Sie das Sophos SafeGuard Disk Encryption Passwort ein. Klicken Sie auf OK, um das Passwort zu bestätigen.



4. Es erscheint dann ein Menü mit den Optionen *Deinstallieren*, *Sichern*, *Restaurieren*, *Reparieren*.



Hinweis: Weitere Informationen finden Sie in folgendem Wissensdatenbankartikel:
<http://www.sophos.com/support/knowledgebase/article/56456.html>.

24.7.1 Systemkern restaurieren

Da der Systemkern automatisch intern auf der Festplatte gesichert wird, steht auf der Arbeitsstation, die zur Wiederherstellung des Systemkerns benutzt wird, immer eine gültige und aktuelle Systemkernsicherung zur Verfügung. Wenn Sie die Option Restaurieren auswählen, werden Sie gefragt, ob Sie diese interne Sicherung verwenden möchten.

- Wenn Sie Ja wählen, werden der MBR (Master Boot Record) und der Sophos SafeGuard Disk Encryption Systemkern einfach unter Anwendung der internen Systemkernsicherung auf dem PC wiederhergestellt.
- Wenn Sie Nein wählen, erhalten Sie die Möglichkeit, nach der gewünschten Systemkernsicherung zu suchen.

Diese Funktion darf *nicht* ausgeführt werden, wenn

- Sophos SafeGuard Disk Encryption vorher deinstalliert wurde
- die Systemkernsicherung nicht dem aktuellen Stand entspricht.

Alle Sophos SafeGuard Disk Encryption Benutzer eines PCs (nicht nur "SYSTEM" Benutzer) dürfen einen gesicherten Systemkern wieder einspielen.

24.7.2 Systemkern reparieren

Im Gegensatz zu „Restaurieren“ funktioniert ein Reparieren auch ohne Sicherungskopie des Systemkerns. Die Reparieren-Funktion durchsucht die komplette Festplatte nach dem Sophos

SafeGuard Disk Encryption Systemkern und versucht ihn wiederherzustellen (keine Erfolgsgarantie!).

Diese Funktion wird nur dann benötigt, wenn die Sicherungsdatei nicht dem aktuellen Stand entspricht.

Nach Wahl von „Reparieren“ versucht eine Diagnoseroutine den Systemkern zu lokalisieren und wieder zu aktivieren. Dies kann mehrere Minuten dauern. Der Verlauf wird in einer Fortschrittsanzeige dargestellt. Anschließend wird Ihnen mitgeteilt, ob das Reparieren erfolgreich gewesen ist.

Hinweis: Der Versuch, einen Systemfehler mit Reparieren zu beheben, führt nicht immer zum Erfolg. Daher sollten Sie immer eine aktuelle Sicherung des Systemkerns zur Verfügung haben.

24.7.3 Notfalldeinstallation von Sophos SafeGuard Disk Encryption

Wenn der Systemfehler weder mit „Restaurieren“ noch mit „Reparieren“ zu beheben ist, hilft nur noch das Entschlüsseln der Festplatte samt Ausschalten der Pre-Boot Authentisierung. Nach der Deinstallation wird die Arbeitsstation zweimal automatisch neu gestartet.

Zu diesem Zweck muss jedoch das Sophos SafeGuard Disk Encryption Benutzerprofil mit entsprechenden Rechten ausgestattet sein. Fehlt einem Benutzer das Recht zur Deinstallation, kann es ihm mit Hilfe des Challenge/Response-Verfahrens erteilt werden (siehe [Fernwartung \(Challenge/Response\)](#) auf Seite 121).

Zusätzlich sollten Sie nach der Notfallentschlüsselung eine Datenträgerüberprüfung in Windows durchführen. Informationen hierzu finden Sie in Ihrer Windows Dokumentation.

Fehlerhafte Entschlüsselung

Kontaktieren Sie bitte unseren Support, falls die Erstverschlüsselung oder die Entschlüsselung aus irgendeinem Grund fehlschlägt.

Erweiterte Forensic Unterstützung (Parameter /NoReboot)

Die Sophos SafeGuard Disk Encryption Notfallentschlüsselung bietet für das Notfallprogramm `Sgeasy.exe` den Kommandozeilen-Parameter `/NoReboot`. Mit diesem Kommandozeilenparameter wird der automatische Neustart nach der Notfallentschlüsselung unterdrückt. Dies ist nützlich zur forensischen Analyse der Platte.

Ablauf:

1. Booten Sie das Notfallmedium.
2. Starten Sie `Sgeasy.exe /NoReboot`.

3. Die Notfallentschlüsselung/Deinstallation wird abgeschlossen
4. Der PC wird angehalten und ein Informationstext erscheint. In diesem Zustand wird kein Programmstart oder Benutzereingabe akzeptiert.

Hinweis: Weitere Informationen zu Entschlüsselung und Deinstallation im Notfall erhalten Sie in folgendem Wissensdatenbankartikel:

<http://www.sophos.com/support/knowledgebase/article/58682.html>.

Defekte Festplatte

Bitte beachten Sie: Wenn Sie vermuten, dass Ihre verschlüsselte Festplatte physikalisch beschädigt ist, empfehlen wir, die betreffende Festplatte NICHT per Notfallmedium zu entschlüsseln.

Ein physikalischer Defekt macht sich z. B. so bemerkbar: die Festplatte gibt ratternde oder klickende Geräusche von sich, wird nicht mehr vom BIOS erkannt etc. Unternehmen Sie in diesem Fall keine weiteren Rettungsversuche auf eigene Faust, sondern wenden Sie sich an Spezialisten. Diese werden versuchen, den Inhalt der korrupten Festplatte auf eine intakte zu überspielen und dort eine Notfallentschlüsselung durchzuführen.

Durch externe Hilfe entstehen weitere Kosten, entscheiden Sie selbst, wie wertvoll die Daten auf der defekten Festplatte für Sie sind.

Hinweis: Weitere Informationen zu diesem Thema erhalten Sie in folgendem Wissensdatenbankartikel:

<http://www.sophos.com/support/knowledgebase/article/57259.html>.

24.7.4 Hinweise

■ Ablage des Systemkerns

Ist die Windows-Bootpartition nicht auf der ersten Festplatte, wird der Sophos SafeGuard Disk Encryption Systemkern während der Installation automatisch auf der C: Partition abgelegt. Diese Partition sollte demzufolge nach der Installation nicht mehr formatiert werden, da sie die wichtigsten Windows Informationen (Systemkern, Treiber, etc.) enthält. Wird dennoch eine Formatierung nach der Sophos SafeGuard Disk Encryption Installation durchgeführt, muss das System neu installiert werden.

Die Systemkernsicherung ist system-spezifisch, d.h. der Systemkern kann nur auf dem PC wiederhergestellt werden, auf dem er gesichert wurde.

Da Sie im Fall eines Systemdefekts wahrscheinlich nicht auf die Festplatte zugreifen können, sollte der Systemkern samt Notfalldateien immer auf einer Diskette, einem Wechselmedium oder dem Netzlaufwerk abgelegt sein.

■ Spracheinstellung im Notfallprogramm Sgeasy.exe

Die Sprache der Benutzeroberfläche des Notfallprogramms bestimmt die Datei Sgeasy.hmf (befindet sich auf der Notfalldiskette). Die verschiedenen Ausgaben der Sprachdatei für

Deutsch (Sgeasy07.hmf), Englisch (Sgeasy09.hmf) und Französisch (Sgeasy0C.hmf) sind im Sophos SafeGuard Disk Encryption Installationsverzeichnis zu finden. Der Benutzer muss die jeweilige Sprachdatei Sgeasy<09,07,0C>.hmf für die Notfalldiskette in Sgeasy.hmf umbenennen, um die gewünschte Sprache in Sgeasy.exe zu erhalten.

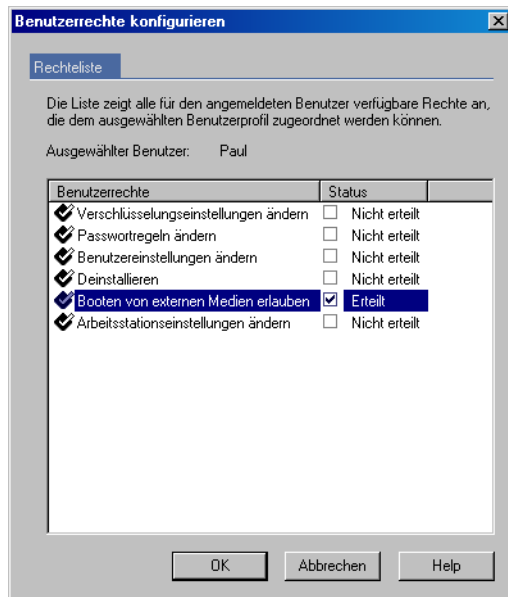
24.8 Nach Booten von externen Medien im Notfall auf verschlüsselte Daten zugreifen

In bestimmten (Notfall-)Situationen wollen Benutzer ein mit Sophos SafeGuard Disk Encryption verschlüsseltes System von einem externen Medium starten, z. B. um Daten zu retten, wenn das Betriebssystem nicht mehr startet. Benutzer können das System allerdings erst dann von einem externen Bootmedium starten (und auf die PC-Daten zugreifen), nachdem gültige Sophos SafeGuard Disk Encryption Zugangsdaten in der Pre-Boot Authentisierung eingetragen wurden.

Als Bootmedien unterstützt Sophos SafeGuard Disk Encryption Boot-CDs/USB-Sticks (für DOS und Windows PE) und Bootdisketten. Wichtig ist, dass die Bootmedien die Sophos SafeGuard Disk Encryption Treiber enthalten. Die Boot-Methode ist empfehlenswert, um im Notfall Daten zu sichern, bevor das Betriebssystem repariert bzw. Sophos SafeGuard Disk Encryption per Notfall-Deinstallation entfernt wird.

24.8.1 Voraussetzung

Das Booten von einem externen Medium ist ein administratives Sophos SafeGuard Disk Encryption Recht, das in der Grundeinstellung nur dem Sophos SafeGuard Disk Encryption Benutzer „SYSTEM“ gewährt ist. Soll das System von einem externen Medium gestartet werden, muss das in der Pre-Boot Authentisierung angemeldete Sophos SafeGuard Disk Encryption Profil über das Recht „Booten von externen Medien erlauben“ verfügen.



24.8.2 Vorgehensweise

1. Booten Sie das System von der Festplatte.
2. Die Sophos SafeGuard Disk Encryption Pre-Boot Authentisierung erscheint.
3. Geben Sie die Sophos SafeGuard Disk Encryption Zugangsdaten in der Pre-Boot Authentisierung ein.
4. a) **Boot-Diskette** einlegen, Daten mit **Eingabe** bestätigen.
b) **Boot-CD** einlegen, Daten mit **F7** bestätigen.
5. Der PC startet neu vom externen Bootmedium.
6. Nach erfolgreichem Neustart ist es möglich, auf Daten zuzugreifen oder diese zu sichern.

24.8.3 Hinweise

- Das erfolgreiche Booten über CD / USB-Stick ist abhängig vom BIOS Support des PC! Eine Beschreibung für das Erstellen einer bootfähigen Windows BartPE CD ist in der Wissensdatenbank abgelegt:
<http://www.sophos.com/support/knowledgebase/article/57525.html>.

- Wenn Sophos SafeGuard Disk Encryption mit Lenovo Rescue and Recovery installiert ist, erstellt das Feature „Create Rescue Media“ automatisch eine CD inkl. Sophos SafeGuard Disk Encryption Treibern. Die Option ist aufrufbar über Programme\Thinkvantage.



24.8.4 Was tun, wenn...

...das Booten nach der Pre-Boot Authentisierung von einem externen Medium fehlschlägt?

Folgende Gründe sind denkbar:

- Der angemeldete Sophos SafeGuard Disk Encryption Benutzer verfügt nicht über das Recht „Booten von externem Medium erlaubt“.
- Die Verschlüsselung der Festplatte wurde angestoßen, ist aber noch nicht beendet.

Für das Fehlschlagen des Bootens von Diskette ist zusätzlich folgender Grund denkbar:

- Das Diskettenlaufwerk wird im PC nicht über den Standard-Disketten-Controller angesprochen, sondern über die USB-Schnittstelle.

24.9 BartPE Unterstützung

BartPE (Bart's Preinstalled Environment) ist eine abgespeckte Variante von Microsoft Windows 32-bit Betriebssystemen, die im Notfall für die Reparatur von korrupten Windows-Installationen verwendet werden kann.

Im Produktordner von SafeGuard Sophos Disk Encryption finden Sie ein spezifisches Plug-in, mit dem sich eine BartPE Notfall-CD erstellen lässt.

Hinweis: Dieses Plug-in ist für Sophos SafeGuard Disk Encryption (SDE) gültig, auch wenn es sich in einigen Fällen auf „SGEasy“ oder „SGE“ bezieht.

Eine Beschreibung für das Erstellen einer bootfähigen Windows BartPE CD ist in der Wissensdatenbank abgelegt:

<http://www.sophos.com/support/knowledgebase/article/57525.html>.

25 Systemstatus von Sophos SafeGuard Disk Encryption anzeigen

Sophos SafeGuard Disk Encryption bietet mit Sophos Disk Encryption State Tool (`SGESTate.exe`) ein Kommandozeilentool, das den aktuellen Status einer Sophos SafeGuard Disk Encryption Installation auf einem Benutzer-PC anzeigt (Versionsangabe, Verschlüsselt/Nicht verschlüsselt etc.). Das Tool eignet sich am besten für Installationen in großen Umgebungen, da ein Administrator auf einfache Weise den Status einer Sophos SafeGuard Disk Encryption Installation abfragen kann.

Man kann Sophos Disk Encryption State Tool aber beispielsweise auch so einsetzen, dass bestimmte Tätigkeiten/Prozesse erst ausgeführt werden, wenn die Installation von Sophos SafeGuard Disk Encryption (bzw. die Verschlüsselung) abgeschlossen ist.

Sie finden `SGESTate.exe` im heruntergeladenen Sophos SafeGuard Disk Encryption Produktordner.

25.1 Reporting

`SGESTate.exe` kann auch zu Reporting-Zwecken genutzt werden:

Der Befehl `SGESTate /LD` liefert eine für LANDesk (und ggf. andere Produkte) formatierte Ausgabe, die in eine Datei umgeleitet werden kann.

25.2 Parameter

Der Befehl `SGESTate` kann mit folgenden Parametern aufgerufen werden:

```
SGESTATE [/?] [/Q | /L | /LD] [/E [/Mvalue]] [/Dvalue] [/R]
```

Der Befehl `SGESTATE /?` gibt einen Überblick über alle verfügbaren Kommandozeilenparameter.

```
c:\ Command Prompt
C:\Dokumente und Einstellungen\Administrator.WS-XP-DE-01>sgestate.exe /?

Sophos Disk Encryption State Tool U3.16
Copyright (c) 1992 - 2009 by Utinaco Safeware AG - a member of the Sophos group.
All rights reserved

Usage: SGESTATE [/Q | /L | /LD] [/E [/Mvalue]] [/Dvalue] [/R]
/Q...Quiet mode: No output, program ends with return code:
    0...Sophos Disk Encryption not installed.
    2...Sophos Disk Encryption installed.
    3...Sophos Disk Encryption installed. Encryption or decryption process active.
255...An error occurred during the check. In this case, a message
to the console will state the nature of the problem.
/L...Loud mode. Will display details to the console including:
Operating System: [WINDOWS 2000 | WINDOWS XP | WINDOWS SERVER 2003]
Installation Status      : [INSTALLED | NOT INSTALLED | UNKNOWN |
                          INSTALLED <NOT READY FOR BACKUP>]
Version number           : [N/A | number]
Installation Mode        : [N/A | STANDARD | PARTITIONED | BOOT PROTECTION |
                          UNKNOWN]
Disk Encryption          : [N/A | OFF | ON]
Initial Encryption       : [N/A | ACTIVE | INACTIVE]
Pre Boot Authentication  : [N/A | OFF | ON]
Current Authentication   : [N/A | USER | WAKE ON LAN]
Secure Auto Logon        : [N/A | OFF | ON]
Disk Encryption Status   : [N/A | [%s | <drive letter>=<state>]
Drive letter states:
SDE volume is recognized but not encrypted      : 0
SDE volume en-/decryption in process           : 1
SDE volume is fully encrypted                  : 2
SDE volume is unrecognized (new partition after SGE installation) : 3
Return code                                     : [ReturnCode]
/LD...The details are displayed in LANdesk mode
/E...Extended return code:
En-/Decryption in process                      : 1
SafeGuard Lite installed                       : 2
Disk Encryption "ON"                           : 8
Installation Mode "Boot Protection": 16 (hex 10)
Installation Mode "Partitioned"      : 32 (hex 20)
Installation Mode "Standard"         : 64 (hex 40)
only one mode is possible, (16, 32 or 64)
/Mvalue...value mask for extended return code 1..127
For example: SGESTATE /E produces return code 43 (hex 2b). This indicates:
Partitioned mode, Disk Encryption "ON", SafeGuard Lite installed, Encryption in
process
```

26 Protokollierung

Die Aufzeichnung sicherheitsrelevanter Vorfälle ist Voraussetzung für eine gründliche Systemanalyse. Anhand der protokollierten Ereignisse können Vorgänge auf einer Arbeitsstation bzw. innerhalb eines Netzwerks exakter nachvollzogen werden. Durch die Protokollierung können z. B. Schutzverletzungen unautorisierter Dritter nachgewiesen werden. Dem Administrator bietet die Protokollierung auch eine Hilfe, um irrtümlich verwehrte Benutzerrechte ausfindig zu machen und zu korrigieren.

Von Sophos SafeGuard Disk Encryption ausgelöste Ereignisse, z. B. die Anmeldung eines Benutzers über PBA oder die Änderung eines Passworts, werden in der Windows-Ereignisanzeige protokolliert.

Der Benutzer mit den entsprechenden Rechten kann die protokollierten Ereignisse direkt über die Windows eigene Ereignisanzeige einsehen.

Folgende Sophos SafeGuard Disk Encryption Ereignisse zeichnet die Protokollierung auf:

- Ablauf des Anmeldevorgangs an der Pre-Boot Authentisierung (erfolgreich/fehlgeschlagen)
- Administrationstätigkeiten (Erzeugen eines Benutzers etc.)
- Erfolgreiche/fehlgeschlagene Ausführung von Konfigurationsdateien.
- Installations-/Deinstallationsvorgänge
- Ver-/Entschlüsselungsvorgänge

26.1 Protokollierte Ereignisse ansehen

Protokollierte Ereignisse können in der Ereignisanzeige eingesehen werden.

Die Windows Ereignisanzeige ist ein Werkzeug für die Protokollierung der Überwachungsinformationen. Die Ereignisanzeige kann Protokolle für System-, Sicherheits- und Anwendungs-Ereignisse anzeigen und verwalten, sowie diese Ereignisprotokolle sichern.

Dargestellt werden

- Computer: Name des Computers, auf dem das protokollierte Ereignis auftrat.
- Datum: Systemdatum, an dem das Ereignis erzeugt wurde.
- Zeit: Systemzeit, an dem das Ereignis erzeugt wurde.
- Benutzer: Benutzer, der beim Auftreten des Ereignisses angemeldet war
- Typ: Klassifizierung des Ereignisses durch Windows, z.B Warnung, Fehler.
- Ereignis-ID: Nummer zur Identifizierung des Ereignisses. Die Event ID ist eine Nummer

zwischen 0 und 0xffffffff (z. B. 4 294 967 295).

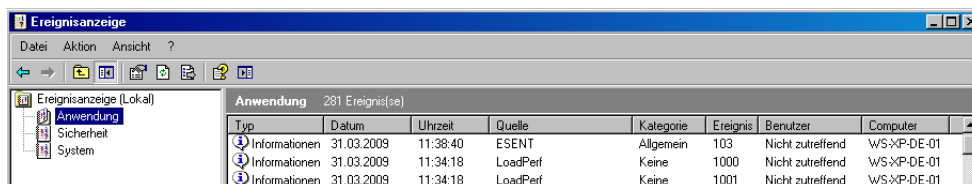
- Quelle: Die Software, die das Ereignis produziert hat.
- Kategorie: Klassifizierung des Ereignisses durch die Quelle.

Die Ereignisse werden immer in der eingestellten Systemsprache ausgegeben.

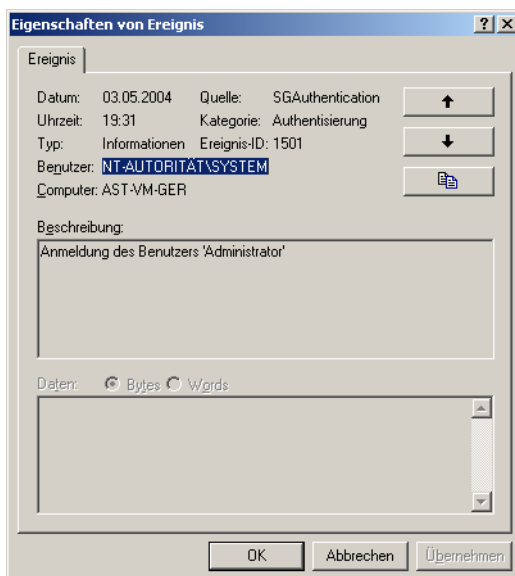
26.1.1 Ereignisanzeige

Die Ereignisse werden im *Anwendungsprotokoll* der *Windows-Ereignisanzeige* aufgezeichnet.

Zum Starten der Ereignisanzeige klicken Sie unter Windows auf Start, zeigen auf Programme, dann auf Verwaltung und klicken dann auf Ereignisanzeige. Rufen Sie dann das Anwendungsprotokoll auf, werden im sogenannten Detailbereich die protokollierten Ereignisse angezeigt.



Doppelklicken Sie auf ein bestimmtes Ereignis im Detailbereich, erscheinen die Detailinformationen zum Ereignis.



27 Fehlermeldungen

In diesem Kapitel finden Sie eine Liste aller Fehlermeldungen. Da bei jeder Fehlermeldung von Sophos SafeGuard Disk Encryption die Fehlernummer angezeigt wird, können Sie den gesuchten Kommentar leicht finden.

Alle Fehlermeldungen haben folgendes Format:

SDEnnnn: <Erklärung des Fehlers>

‘SDE’ ist die Produkt-ID von Sophos SafeGuard Disk Encryption, ‘nnnn’ eine vierstellige Fehlernummer.

Für bestimmte Sophos SafeGuard Disk Encryption Fehler erhalten Sie zusätzliche Informationen in der Wissensdatenbank:

<http://www.sophos.com/support/knowledgebase/article/58683.html>

Hier finden Sie ausführliche Informationen zu folgenden Sophos SafeGuard Disk Encryption Fehlermeldungen:

0104, 0113, 1048, 1104, 1109, 1121, 1123, 1244, 1254, 1264, 1274, 1306, 1315, 1602.

Produktspezifische Fehler

- | | |
|------|---|
| 0001 | Fataler Fehler. |
| 0002 | Wiederhole. |
| 0100 | Andere Version von [PN] oder Crypton bereits installiert. |
| 0101 | Konfigurationsdatei kann nicht gelesen werden. |
| 0102 | Ungültige Konfigurationsdatei. |
| 0103 | Konfigurationsdatei kann nicht geschrieben werden. |
| 0104 | Der momentan installierte Treiber ist nicht konsistent. |
| 0105 | Treiber bereits installiert. |
| 0106 | Dieses Programm läuft nicht unter &0. |
| 0107 | Backup Datei kann nicht geschrieben werden. |
| 0108 | Backup Datei kann nicht gelesen werden. |

- 0109 Backup Datei ungültig.
- 0110 Eine zweite Boot Partition kann nicht erzeugt werden.
- 0111 Installation auf OS/2 Boot Manager nicht möglich.
- 0112 Eine frühere Version von [PN] oder C:CRYPT ist bereits installiert.
- 0113 Letzter Installations-, Deinstallations- oder Updatevorgang nicht beendet.
- 0114 Nicht genügend zusammenhängenden freien Festplattenspeicher auf der Boot Partition.
- 0115 Zugriff auf Treiber Boot Partition nicht möglich.
- 0116 Keine Resource Dateien gefunden.
- 0117 Resource Datei kann nicht geöffnet werden.
- 0118 Ungültige oder fehlerhafte Resource Datei.
- 0119 Algorithmus Modul fehlt.
- 0120 Kernel Modul fehlt.
- 0121 PBA Modul fehlt.
- 0122 *AUTOUSER kann nicht erzeugt werden.
- 0200 Festplatten Struktur kann nicht analysiert werden.
- 0201 Festplatten Lesefehler.
- 0202 Festplatten Schreibfehler.
- 0203 Ungültige Partitionstabelle auf Festplatte 0.
- 0204 Inkompatibles ROM BIOS.
- 0205 Ungültiger Bootsektor.
- 0206 Volume kann nicht gelockt werden.
- 0300 Schreibschutzfehler.
- 0301 Unbekannte Einheit.

0302	Laufwerk &0 nicht bereit.
0303	Unbekannter Befehl.
0304	Daten Checksummenfehler.
0305	Bad request structure length.
0306	Suchfehler.
0307	Unbekannter Medientyp.
0308	Sektor nicht gefunden.
0309	Drucker hat kein Papier mehr.
0310	Schreibfehler.
0311	Lesefehler.
0312	Genereller Fehler.
0320	Nicht genügend Speicherplatz.
0321	Divisionsfehler an Programmadresse &0.
0322	Runtime stack overflow.
0500	Verschlüsselungstreiber nicht installiert.
0501	Inkorrekte Version des Verschlüsselungstreibers.
0502	Kommandozeilenargumente) ungültig.
0503	Kein Schlüssel für die Verschlüsselung definiert.
0999	Unbekannter Fehler.

System API Fehler

1001	Kein Subsystem aktiv.
1002	Unzulässige Änderung einer Systemeinstellung.

- 1003 Verschlüsselungsalgorithmus fehlt oder ist ungültig.
- 1004 Interner Fehler im Subsystem entdeckt.
- 1005 Das Subsystem meldet einen I/O Fehler.
- 1006 Zugriff auf den Kernel nicht erfolgreich.
- 1007 Ein Benutzer hat sich bereits an
[[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102] angemeldet.
- 1008 Ein ungültiger Benutzer wurde angelegt.
- 1009 Die Zuweisung definierter Rechte an den Benutzer ist nicht erlaubt.
- 1010 Angelegter Benutzer existiert bereits!
- 1011 Das vergebene Passwort wurde von diesem Benutzer bereits verwendet.
- 1012 Das vergebene Passwort gehört zur List der nicht erlaubten Passwörter.

Dateifehler

- 1031 Datei <Name der Datei> kann nicht geöffnet werden.
- 1032 Datei <Name der Datei> kann nicht geschlossen werden.
- 1033 Datei <Name der Datei> kann nicht erzeugt werden.
- 1034 Fehler während Schreibzugriff auf Datei <Name der Datei>.
- 1035 Fehler während Lesezugriff in Datei <Name der Datei>.
- 1036 Fehler beim Zugriff auf Datei <Name der Datei>.
- 1037 Datei <Name der Datei> konnte nicht gefunden werden.
- 1038 Ungültige Datei oder Pfadname.
- 1039 Nicht genügend Speicherplatz auf dem Datenträger.
- 1040 Die Festplattenpartition ist zu stark fragmentiert.

- 1041 Ungültiges Dateisystem entdeckt.
- 1042 Unbekanntes Dateisystem entdeckt.
- 1043 Datei <Name der Datei> existiert bereits.
- 1044 Korrupte Struktur im Dateisystem entdeckt.
- 1045 Ungültiger Eintrag im Dateisystem gefunden.
- 1046 Anforderung nach Partitionsinformationen fehlgeschlagen.
- 1047 Unbekanntes oder ungültiges Dateisystem entdeckt.
- 1048 Datei <Name der Datei> konnte nicht kopiert werden.
- 1049 Datei <Name der Datei> konnte nicht gelöscht werden.
- 1052 Checksumme der Datei <Name der Datei> fehlerhaft.
- 1053 Datei <Name der Datei> konnte nicht umbenannt werden.

Installationsfehler

- 1061 Ungültiges Installationslaufwerk.
- 1063 Sophos SafeGuard Disk Encryption ist bereits installiert.
- 1065 Datei Config.sys ist schreibgeschützt.
- 1066 Eintrag in INI-Datei oder Konfigurationsdatei nicht gefunden.
- 1067 Auf einem Rechner mit dynamischen Partitionen kann weder ein komplettes noch ein Laufzeit-System von [PN] installiert werden. Nur die Installation von Administrationswerkzeugen ist auf diesem Rechner erlaubt.
- 1068 Die Kerneldatei konnte nicht erzeugt werden.
- 1069 Die Datei Config.sys konnte nicht modifiziert werden.
- 1070 Die Datei <Name der Datei> konnte nicht kopiert werden.
- 1071 Kein Zielverzeichnis definiert.

- 1072 Ein falsches Systemverwalterpasswort wurde angegeben. Wollen Sie es nochmals versuchen?
- 1073 Kein Systemverwalterpasswort angegeben.
- 1076 Die Deinstallation ist fehlgeschlagen. Zusätzliche Informationen können Sie der Datei SGEASY.LOG entnehmen.
- 1077 Die Deinstallation des GINA Systems ist fehlgeschlagen.
- 1078 Neue Treiber und Systemdienste wurden installiert. Es wird empfohlen, daß Sie jetzt ein neues Backup erzeugen, da die alten Backupdaten nicht für ein Restore verwendet werden können, solange Sophos SafeGuard Disk Encryption installiert ist!
- 1079 Die Deinstallation der GINA Clients SGEGINA schlug fehl.
- 1080 Das Erzeugen eines Menüeintrages schlug fehl.
- 1081 Das Entfernen eines Menüeintrages schlug fehl.
- 1082 Eintrag in INI-Datei nicht gefunden.
- 1083 Die Installation der Cardman API schlug fehl.
- 1086 Ein komplettes [PN] System ist noch installiert auf Ihrem Computer auf einer anderen Plattform. Sie müssen dieses System zuerst deinstallieren, bevor Sie das Runtime System des aktuellen Systems deinstallieren können.
- 1087 Die Installation eines [PN] Systems ist nicht erlaubt.
- 1088 Eine benötigte PBA Ressourcendatei (.MOD) konnte nicht gefunden werden!
- 1089 Die Installation von [PN] ist fehlgeschlagen! Folgender Fehler trat auf: Bitte klicken Sie auf OK, um alle bereits installierten Komponenten von [PN] wieder zu entfernen. Danach wird das System automatisch neu gestartet.
- 1090 Falsche Betriebssystemversion vorgefunden.
- 1091 Falsche Betriebssystemversion vorgefunden. Das Betriebssystem Windows 95/98/ME ist erforderlich!
- 1092 Der Deinstallationsvorgang kann nicht gestartet werden, weil eine oder mehrere [PN] Komponenten sind momentan nicht aktiv.

- 1093 Dieser Prozess kann nicht ausgeführt werden, weil zur Zeit ein Verschlüsselungsprozess läuft. Bitte warten Sie bis alle Verschlüsselungsvorgänge beendet sind und starten Sie dann das Programm erneut.
- 1094 Die Deinstallation läuft gerade. Administration ist nicht möglich.
- 1095 Die maximal Anzahl an Festplatten ist übertroffen. Die Installation eines [PN] Systems ist nicht erlaubt.
- 1096 Einige non-DOS Partitionen wurden gefunden, die unter Verwendung des gewählten Installationstyps verschlüsselt werden würden. Wir empfehlen daher, den Installationstyp 'Partitionsweise' auszuwählen.
- 1097 Falsche Betriebssystemversion gefunden. Es wird das Betriebssystem Windows 2000 benötigt.
- 1098 Die Installation von Sophos SafeGuard Disk Encryption ist fehlgeschlagen.
- 1099 Die Deinstallation von Sophos SafeGuard Disk Encryption ist fehlgeschlagen.

Allgemeine Fehler

- 1101 Selbstüberprüfung schlug fehl.
- 1102 Das Hilfesystem konnte nicht initialisiert werden.
- 1103 Eine Klasse konnte nicht registriert werden.
- 1104 Die Informationen über die Partitionskonfiguration sind inkonsistent.
- 1105 Ungültiger oder falscher Parameter definiert.
- 1106 Keiner oder zu wenige Parameter wurden definiert.
- 1107 Unbekannter Parameter definiert.
- 1108 Nicht genügend freier Speicher verfügbar.
- 1109 Modul '<Modulname>' konnte nicht geladen werden.
- 1110 Ein Dialog konnte nicht kreiert werden.
- 1111 Ein Dialog konnte nicht initialisiert werden.

- 1112 Ein Thread konnte nicht kreiert werden.
- 1113 Ein Fenster konnte nicht kreiert werden.
- 1114 Sie benötigen Administrator-Rechte, um zu installieren oder zu deinstallieren!
- 1115 Es ist eine Speicherschutzverletzung aufgetreten!
- 1117 Die Logdatei '<Dateiname>' konnte nicht geöffnet werden.
- 1118 Das Deinstallationsprogramm und das Administrationsprogramm von [PN] können nicht gleichzeitig gestartet sein.
- 1119 Kerneldatei nicht gefunden.
- 1120 Die Installation des 'control handler' schlug fehl.
- 1121 Unbekannte Umgebungsvariable definiert.
- 1122 Eine Umgebungsvariable konnte nicht gesetzt werden.
- 1123 Puffergröße unzureichend.
- 1124 Die DLL '%5' konnte nicht geladen werden!
- 1125 Die spezifizierte Funktion '%5' konnte nicht gefunden werden!
- 1126 Die Semaphore '%5' konnte nicht geöffnet werden!
- 1127 Das Modul '%5' konnte nicht freigegeben werden!
- 1128 Ein Ausnahmefehler trat auf während der Ausführung einer [PN] Subsystem Funktion! Last error code :%1Function return code: %2Module :%3Line number :%4Address :%5Bitte kontaktieren Sie: Utimaco Safeware AG - a member of the Sophos group!
- 1129 Ein kritischer Fehler trat auf bei der Ausführung einer oder mehrerer [PN] Subsystem Funktion(en)!Fatal error code: %1\nOS error code : %2\nModule : %3Function : %4\Beschreibung: [[MSGLINK]=%1].
- 1130 Belegter Hauptspeicher konnte nicht freigegeben werden.
- 1131 Eine Funktion wird zur Zeit nicht unterstützt.
- 1132 Zugriff verweigert.
- 1133 Programmstart von '<Name der Datei>' schlug fehl.

- 1134 Funktion oder Ressource nicht verfügbar.
- 1135 Der Prozess wurde vom Benutzer abgebrochen.
- 1136 Ungültiger oder falscher Eintrittspunkt definiert.
- 1137 Das System verändert zur Zeit einige Systemeinstellungen. Gegenwärtig sind keine weiteren Änderungen erlaubt.
- 1139 Ungültiger Datentyp für das Dialogfeld
- 1141 Kernel Backup schlug fehl.
- 1143 Definierte Arbeitsstation existiert nicht.
- 1144 Der Logon Klient 'SgeGina.dll' konnte nicht gefunden werden. Das limitiert ein Reihe von Funktionen von [PN] und kann ernsthafte Probleme nach sich ziehen, die einen Neuinstallation von [PN] oder des Betriebssystems erfordern könnten.
- 1145 Der Dienst 'SgeCtl.exe' konnte nicht gefunden werden. Das limitiert ein Reihe von Funktionen von [PN] und kann ernsthafte Probleme nach sich ziehen, die einen Neuinstallation von [PN] oder des Betriebssystems erfordern könnten.
- 1146 System Kernel ist defekt.
- 1147 Eine Partition wird gerade ver- oder entschlüsselt oder ein solcher Prozess wurde initiiert.
Ein Kernelbackup kann nur durchgeführt werden, wenn alle Ver-oder Entschlüsselungsprozesse beendet sind.
- 1148 Das Interface konnte nicht gefunden werden.
Klasse :%1 (%3)
Interface :%2
Result :%4 ([[OSERRLINK]=%5])\n\nMöglicherweise ist
[[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102] auf '%6' nicht installiert!

Fehler in der Konfigurationsdatei

- 1151 Die Konfigurationsdatei <Name der Datei> konnte nicht gefunden werden.
- 1152 Keine Konfigurationsdatei definiert.
- 1153 Sektionseintrag in der Konfigurationsdatei fehlt.

- 1154 Ungültiger Eintrag in der Konfigurationsdatei gefunden.
- 1155 Konfigurationsdatei <Name der Datei> konnte nicht gefunden werden.
- 1156 Fehler in Zeile <Name der Datei> der Konfigurationsdatei gefunden.
- 1158 Die angegebene Konfigurationsdatei konnte nicht gefunden werden!
- 1159 Ein unbekannter Befehl wurde in der Konfigurationsdatei gefunden.
- 1160 Unbekannter Typ einer Konfigurationsdatei gefunden.
- 1161 Typ der Konfigurationsdatei ist ungültig.
- 1162 Der Handle für die Konfigurationsdatei ist ungültig.
- 1163 Konfigurationsdatei für die Deinstallation konnte nicht erzeugt werden.
- 1164 Konfigurationsdatei zur Deinstallation konnte nicht erzeugt werden.
- 1165 Die Konfigurationsdatei <Name der Konfigurationsdatei> konnte nicht gefunden werden.
- 1166 Der Typ der Konfigurationsdatei ist ungültig.
- 1167 SGE1157: Ausführung der Konfigurationsdatei '<Name der Konfigurationsdatei>' schlug fehl.

MESSAGE Control Fehler

- 1171 Message ID <Nummer der ID> nicht gefunden.
- 1172 Kein Control Text für eine Control ID gefunden.
- 1173 Die Windows NT Logdatei konnte nicht geschrieben werden!
- 1174 Eine ungültige Datei oder ein ungültiger Message Link wurden gefunden:
Message identifier: %1\nLink command : %2.
- 1175 Das Format der Messagedatei '<Name der Datei>' ist ungültig!
- 1176 Falsche Definition der Messagebox-Attribute

Passwortfehler

- 1181 Kein Systemverwalterpasswort definiert.
- 1182 Unbekanntes Passwort.
- 1183 Kein Passwort definiert.
- 1184 Definiertes Passwort ist zu kurz.
- 1185 Definiertes Passwort ist zu lang.
- 1186 Definierte Passwörter stimmen nicht überein.
- 1187 Das Passwort ist trivial.\nWollen Sie ein anderes Passwort eingeben?
- 1188 Das vergebene Passwort existiert für einen anderen Benutzer. Wollen Sie das Passwort dennoch verwenden?
- 1189 Das vergebene Passwort enthält nicht die geforderte Anzahl von Buchstaben, Sonderbuchstaben, Ziffern und Symbolen.
- 1190 Das Passwort hat noch nicht sein definiertes Mindestalter erreicht.

Schlüsselfehler

- 1201 Kein Festplattenschlüssel angegeben.\n\nDie Festplattenverschlüsselung kann nur gesetzt werden, wenn ein Festplattenschlüssel angegeben wurde.
- 1206 Die angegebenen Schlüssel stimmen nicht überein.
- 1207 Kein Schlüssel definiert!
- 1209 Der Modus 'Standard' verlangt einen Schlüssel für die Verschlüsselung der Festplatte!

IPC Fehler

- 1221 IPC Server konnte nicht gestartet werden.
- 1222 IPC Client konnte nicht gestartet werden.
- 1223 IPC Verbindung konnte nicht aufgebaut werden.
- 1224 IPC Meldung konnte nicht aufgenommen werden.
- 1225 IPC Meldung konnte nicht abgesetzt werden.
- 1226 IPC Funktion IPC_SGE_PROCESS_DEF_MSG\nkonnte nicht verarbeitet werden.
- 1227 IPC Server konnte nicht geschlossen werden.
- 1228 IPC Klient konnte nicht geschlossen werden.
- 1229 IPC Thread konnte nicht gestartet werden.
- 1230 Das Warten auf eine IPC Meldung schlug fehl.
- 1231 IPC Kommunikationsobjekt nicht gefunden.

Laufwerksfehler

- 1241 Unbekanntes oder ungültiges Laufwerk definiert.
- 1242 Keine weiteren Laufwerke gefunden.
- 1243 Laufwerks-I/O-Operation schlug fehl.
- 1244 Lesezugriff von einem Laufwerk schlug fehl.
- 1245 Schreibzugriff auf ein Laufwerk schlug fehl.
- 1246 Startzugriff auf ein Laufwerk schlug fehl.
- 1247 Laufwerk nicht bereit!
- 1248 Sperren eines Laufwerks schlug fehl.

- 1249 Entsperrn eines Laufwerks schlug fehl.
- 1250 Die Systemartition muss eine primäre Partition sein.\n\nDas ist z. B. notwendig, wenn die Option 'Unterstützung für Compaq Setup-Partition' aktiviert wurde.
- 1251 Freigeben eines Volumes schlug fehl.\n\nEventuell sind einige Dateien oder Fenster noch offen.
- 1252 Die erste physikalische Disk ist keine Festplatte.
- 1253 Alle Einträge in der Partitionstabelle des MBR Sectors auf der ersten Festplatte sind bereits belegt.\n\nDie Option „Unterstützung für Compaq Setup-Partition“ erfordert einen freien, unbenutzten Eintrag in der Partitionstabelle!
- 1254 System wurde im Kompatibilitätsmodus gestartet.
- 1255 Um Sophos SafeGuard Disk Encryption zu installieren, entfernen Sie bitte die steckbare Festplatte.
- 1256 Es sind keine Laufwerke dieses Typs vorhanden
- 1257 Interner Fehler beim Zugriff auf die Systempartition

SERVICE Fehler

- 1261 Informationen über ein Speicherobjekt für einen Systemdienst konnten nicht freigegeben werden.
- 1262 Fehler im Systemdienst-Dispatcher entdeckt.
- 1263 Systemdienst konnte nicht gestartet werden.
- 1264 Status des Systemdienstes konnte nicht gewechselt werden.
- 1265 Der Handler für den Systemdienst konnte nicht registriert werden.
- 1266 Die Funktion zur Dienste-Installation meldete einen Fehler!
- 1267 Der 'service information block' konnte nicht gefunden werden. Vermutlich ist nicht genügend Speicher verfügbar!\n\nErrorcode: %1.

REGISTRY Fehler

- 1271 Eintrag in der Registry konnte nicht geöffnet werden.
- 1272 Eintrag in der Registry konnte nicht gelesen werden.
- 1273 Eintrag in der Registry konnte nicht geschrieben werden.
- 1274 Eintrag in der Registry konnte nicht kreiert werden.
- 1275 Eintrag in der Registry konnte nicht gelöscht werden.
- 1276 Eintrag für einen Systemdienst in der Registry konnte nicht geöffnet werden.
- 1277 Eintrag für einen Systemdienst in der Registry konnte nicht kreiert werden.
- 1278 Eintrag für einen Systemdienst in der Registry konnte nicht gelöscht werden.
- 1279 Eintrag für einen Systemdienst in der Registry existiert bereits.
- 1280 Der 'Session Control Manager' konnte nicht geöffnet werden.
- 1281 Registryeintrag für eine Session konnte nicht gefunden werden.
- 1282 Ungültiger Registryeintrag entdeckt.

Datenbanktreiber-Fehler

- 1291 Keine weiteren Verschlüsselungstreiber gefunden.
- 1292 Datenbanktreiberdatei nicht gefunden.
- 1293 Fehler trat auf beim Lesen der Datenbanktreiberdatei.
- 1294 Datenbanktreiberdatei ist leer.
- 1295 Ungültiger oder illegaler Eintrag Eintrag in der Datenbanktreiberdatei.

CRAREA Fehler

- 1301 Zugriffsfehler auf das Installationslaufwerk.
- 1302 Anforderung nach Partitionsinformationen schlug fehl.
- 1303 Zugriff auf die Bootpartition schlug fehl.
- 1304 Ungültige Prozessoption definiert.
- 1305 Unbekanntes oder ungültiges Dateisystem definiert.
- 1306 Unterschied entdeckt zwischen dem aktuellen und dem definiertem Dateisystem.
- 1307 Unterschied entdeckt zwischen der aktuellen und der definierten Clustergröße.
- 1308 Ungültiger Start-Cluster für den Kernelbereich definiert.
- 1309 Ungültiger Start-Sektor für den Kernelbereich definiert.
- 1310 Ungültiger Partitionstyp definiert.
- 1311 Keine freien Cluster für den Kernel gefunden.
- 1312 Cluster konnten nicht als 'gebraucht' markiert werden.
- 1313 Cluster konnten nicht als 'gut' markiert werden.
- 1314 Cluster konnten nicht als 'unbenutzt' markiert werden.
- 1315 Cluster konnten nicht als 'schlecht' markiert werden.
- 1316 Cluster Informationen korrupt.
- 1317 Der als 'bad' markierte Bereich konnte nicht markiert werden.
- 1318 Ungültige Größe des Kernelbereichs definiert.
- 1319 Der MBR Sektor auf der ersten Festplatte konnte nicht ersetzt werden.

SGOCA Fehler

- 1401 Die angeforderten 'object communication area' Informationen existieren bereits.
- 1402 Die 'object communication area' existiert bereits.
- 1403 Die angeforderten 'object communication area' Informationen existieren bereits.
- 1404 Die 'object communication area' konnte nicht gefunden werden.
- 1405 Die angeforderte 'object communication area' Informationen existieren nicht.
- 1406 Zusätzliche 'object information data' gefunden.

SGUICL Fehler

- 1511 Die Komponenten Konfiguration konnte nicht geladen werden!

ADMLOGON Fehler

- 1601 Die Anmeldung war erfolglos. Versuchen Sie es bitte noch einmal !
- 1602 Das [PN] Subsystem erlaubt nicht mehr als 5 Anmeldeversuche. Sie müssen den Rechner neu starten und die Anwendung neu starten!
- 1603 Der Start der [PN] Logonkomponente schlug fehl.
- 1604
- 1605 Der Logon an [PN] war erfolgreich, aber Sie haben nicht genügend Rechte, um das Produkt zu deinstallieren.

Administration Fehler - USER

- 1801 Der Benutzer '<Benutzername>' kann nicht erzeugt werden, weil die Maximalanzahl an Benutzern erreicht ist.
- 1802 Es ist nicht möglich, den Benutzer '*AUTOUSER' zu erzeugen oder zu löschen.
- 1803 Der Benutzer '<Benutzername>' existiert bereits. Bitte legen Sie den Benutzer unter einem anderen Namen an.
- 1804 Die Maximalanzahl an Benutzern wurde überschritten!
- 1805 Es ist nicht erlaubt, den Benutzer 'SYSTEM' anzulegen oder zu löschen. Nur ein Modifizieren ist erlaubt.
- 1807 Die Applikation wartet bereits 30 Sekunden auf Abschluß des Vorganges. Der Computer kann zu sehr beschäftigt sein. Sie können warten, bis der Vorgang beendet ist, oder möchten Sie abbrechen?

SGEGINA Fehler

- 2100 Der Auto Logon schlug fehl. Wollen Sie die Verbindung zwischen dem Sophos SafeGuard Disk Encryption Benutzer und dem Betriebssystem Benutzer editieren?
- 2101 Sie müssen ihr Passwort jetzt wechseln. \nDer Auto Logon (SAL) ist für diese Anmeldung deaktiviert!

Deinstallation Fehler

- 2201 Die Deinstallationsprozedur kann nicht gestartet werden, weil ein Chiffrier- oder Dechiffriervorgang gerade läuft!
- 2202 Die Deregistrierung einer Komponente ist fehlgeschlagen!

- 2203 Die Deinstallation von [[MSGFILE]=SGE_INFO.dll][[MSGLINK=102] kann nicht fortgesetzt werden. Es wurde eine Festplatten gefunden, die vor der Installation nicht vorhanden war. Bitte entfernen Sie die nachträglich eingebaute Festplatte!

Erweiterte Installation - Fehler

- 2301 Das Installationspaket hat die falsche Version und kann nicht verwendet werden !
- 2302 Beim Installationsmodus 'Standard' oder 'Bootschutz' sind nicht mehr als 8 Partitionen pro Festplatte erlaubt!
- 2303 Eine COM Komponente konnte nicht registriert werden!
- 2304 Die Installation von [PN] benötigt den 'Windows Installer' von Microsoft. Nähere Informationen finden Sie im Handbuch oder in der README Datei.
- 2305 Falsche Betriebssystemversion vorgefunden. Das Betriebssystem Windows NT/2000 ist erforderlich!

Notfallassistent - Fehler

- 2401 Die Erzeugung der Kernelbackupdatei wurde abgebrochen!
- 2402 Nicht alle Notfalldateien konnten erfolgreich kopiert werden!

SAL Fehler

- 2501 Die SAL-Datei konnte nicht geöffnet werden
- 2502 Die SAL-Datei befindet sich in einem undefiniertem Zustand
- 2503 Undefinierter Fehler bei Dateioperationen
- 2504 SAL- Datei konnte nicht korrekt positioniert werden

- 2505 SAL-Datei Lesefehler
- 2506 SAL-Datei Schreibfehler
- 2507 Der angegebene Benutzer konnte nicht gefunden werden
- 2508 Keinen derzeit angemeldeten Benutzer gefunden
- 2509 Es konnte nicht geschrieben werden, weil ein existierender Eintrag zu klein für den neuen Eintrag ist
- 2510 Der Zielpuffer ist zu klein für den ganzen Eintrag
- 2511 Kein Speicher verfügbar

Interface Fehler

- 3001 Das COM Interface Object kann nicht verschlüsselt werden.\nInterface Name:%1\nFehler Nummer: %2Zusatzinformation:%3
- 3002 Die Ausführung einer Interface Methode ist fehlgeschlagen. Folgende detaillierte Fehler Informationen wurden gemeldet: \nFehler Nummer: %1\nhResult: %2\nBeschreibung: %3\nInterface :%4\nBitte kontaktieren Sie Ihren Systemadministrator!

28 Technischer Support

Technischen Support erhalten Sie auf <http://www.sophos.de/support>.

Halten Sie u.a. folgende Informationen bereit:

- Versionsnummer(n) der Sophos Software
- Betriebssystem(e) und Patch-Level(s)
- Den genauen Wortlaut etwaiger Fehlermeldungen

29 Copyright

Copyright © 1992 - 2009 Utimaco Safeware AG - a member of the Sophos group

Alle Rechte vorbehalten. 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.

Sophos ist eine eingetragene Marke von Sophos Plc und Sophos Group.

SafeGuard ist eine eingetragene Marke von Utimaco Safeware AG - a member of the Sophos group.

Patentrechte von Ascom Tech Ltd. eingereicht in EP, JP, US. IDEA ist ein Markenname von Ascom, Tech Ltd.

Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

