

**SOPHOS**

---

simple + secure

# SafeGuard Enterprise Web Helpdesk

Produktversion: 5.60

Stand: April 2011



# Inhalt

1 SafeGuard web-basiertes Challenge/Response-Verfahren.....	3
2 Installation.....	5
3 Authentisierung.....	9
4 Auswählen des Web Help Desk Assistenten.....	11
5 Recovery-Typen - Übersicht.....	12
6 Recovery für SafeGuard Enterprise Clients (managed).....	14
7 Recovery mit virtuellen Clients.....	18
8 Recovery für Sophos SafeGuard Clients (standalone).....	23
9 SafeGuard Configuration Protection.....	26
10 Protokollierung von Web Help Desk Ereignissen .....	28
11 Technischer Support.....	29
12 Rechtliche Hinweise.....	30

# 1 SafeGuard web-basiertes Challenge/Response-Verfahren

Zur Optimierung von Workflows im Unternehmen und zur Reduzierung von Helpdesk-Kosten bietet SafeGuard Enterprise eine web-basierte Recovery-Lösung. Web Help Desk unterstützt Benutzer, die sich an ihrem Computer nicht mehr anmelden oder nicht auf mit SafeGuard Enterprise verschlüsselte Daten zugreifen können.

Darüber hinaus lässt sich die SafeGuard Configuration Protection Richtlinie vorübergehend deaktivieren.

## Nutzen und Vorteile des Challenge/Response-Verfahrens

Das Challenge/Response-Verfahren ist ein sicheres und effizientes Notfallsystem.

- Während des gesamten Vorgangs werden keine vertraulichen Daten in unverschlüsselter Form ausgetauscht.
- Informationen, die unberechtigte Dritte durch Mitverfolgen dieses Vorgangs erhalten könnten, lassen sich weder zu einem späteren Zeitpunkt noch auf anderen Geräten verwenden.
- Für den Endpoint-Computer, auf den zugegriffen werden soll, muss während des Vorgangs keine Online-Netzwerkverbindung bestehen. Der Response Code Wizard für den Helpdesk läuft auch auf einem Standalone-PC. Eine komplexe Infrastruktur ist nicht notwendig.
- Der Benutzer kann schnell wieder mit dem Computer arbeiten. Es gehen keine verschlüsselten Daten verloren, nur weil der Benutzer das Kennwort vergessen hat.

## Challenge/Response Workflow

Während des Challenge/Response-Verfahrens wird ein Challenge-Code (eine ASCII-Zeichenkette) auf dem Endpoint-Computer erzeugt und der Benutzer übermittelt diesen Code an einen Helpdesk-Beauftragten. Der Helpdesk-Beauftragte erzeugt auf der Grundlage des Challenge-Codes einen Response-Code, der den Benutzer zum Ausführen einer bestimmten Aktion auf dem Computer berechtigt.

## Typische Notfälle, in denen Hilfe beim Helpdesk angefordert wird

- Ein Benutzer hat sein Kennwort für die Anmeldung vergessen. Der Computer ist gesperrt.
- Ein Benutzer hat seinen Token/seine Smartcard vergessen oder verloren.
- Der Local Cache der Power-on Authentication ist teilweise beschädigt.
- Ein Benutzer ist krank oder im Urlaub und ein Kollege muss auf die Daten auf dem Computer zugreifen.
- Ein Benutzer möchte auf ein Volume zugreifen, das mit einem Schlüssel verschlüsselt ist, der auf dem Computer nicht verfügbar ist.

SafeGuard Enterprise Web Help Desk bietet für diese typischen Notfälle unterschiedliche Recovery-Workflows, die dem Benutzer wieder den Zugang zu seinem Computer ermöglichen.

## 1.1 Web Help Desk Funktionsumfang

Web Helpdesk bietet das SafeGuard Enterprise Challenge/Response-Verfahren über eine web-basierte Oberfläche. Die Zugangskontrolle für diese Web-Anwendung kann über SSL gesteuert werden. Der Helpdesk kann somit Aufgaben flexibel innerhalb des Unternehmens delegieren. Dies wird erreicht, ohne dass Helpdesk-Mitarbeitern Zugang zu vertraulichen Konfigurationseinstellungen oder zur zentralen Verwaltung von SafeGuard Enterprise gewährt werden muss.

Web Help Desk steht über das Internet/Intranet zur Verfügung, ohne dass dazu die SafeGuard Enterprise Software auf dem Endpoint-Computer installiert sein muss. Die Webseiten werden separat auf einem Internet Information Services (IIS) basierten SafeGuard Enterprise Server bereitgestellt.

Web Help Desk kann zusätzlich zum SafeGuard Management Center eingesetzt werden.

### **Hinweis:**

Wir empfehlen, Web Help Desk nur innerhalb des Intranets Ihres Unternehmens zur Verfügung zu stellen. Aus Sicherheitsgründen sollte Web Help Desk nicht über das Internet zur Verfügung gestellt werden.

### **Web Help Desk bietet Recovery für:**

- SafeGuard Enterprise Clients
- Virtuelle Clients
- SafeGuard Standalone Clients

Bei SafeGuard Enterprise Clients bestimmt das Programm automatisch, ob es sich um einen SafeGuard Enterprise Client mit nativer volume-basierender Verschlüsselung handelt oder um einen SafeGuard Enterprise Client mit BitLocker-Verschlüsselung und passt den Recovery-Ablauf entsprechend an.

## 2 Installation

Web Help Desk muss auf einem IIS-basierenden Web Server mit SafeGuard Enterprise Server installiert werden. Während der Installation von Web Help Desk wird geprüft, ob SafeGuard Enterprise Server bereits auf dem Server zur Verfügung steht. Ist dies nicht der Fall, so wird SafeGuard Enterprise Server in einem separaten Anwendungspool mit der Bezeichnung **SGNWHD-Pool** installiert. Nach der Installation von Web Help Desk müssen Sie den Web Server konfigurieren.

Auf dem Computer des Web Help Desk Beauftragten muss nur ein Browser installiert sein.

### 2.1 Voraussetzungen

#### Voraussetzungen für Server

Eine detaillierte Beschreibung der Systemvoraussetzungen für den Server finden Sie in den Release Notes.

- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Microsoft Internet Information Services (IIS) muss installiert sein.
- .NET Framework 3.0 Service Pack 1 mit ASP.NET 2.0 muss installiert sein.

#### Voraussetzungen für Clients

Auf dem Computer des Web Help Desk Beauftragten muss ein Browser installiert sein. Web Help Desk unterstützt folgende Browser:

- Microsoft Internet Explorer 7 und 8
- Mozilla Firefox 2 und 3

### 2.2 Installieren von Web Help Desk

Das Installationspaket SGNWebHelpDesk.msi finden Sie in Ihrer Produktlieferung.

1. Starten Sie SGNWebHelpDesk.msi.
2. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung.
4. Wählen Sie einen Installationspfad.
5. Klicken Sie auf **Beenden**, um die Installation abzuschließen.

Während der Einrichtung von Web Help Desk wird geprüft, ob SafeGuard Enterprise Server bereits auf dem IIS Server zur Verfügung steht. Ist dies nicht der Fall, wird SafeGuard Enterprise Server automatisch auf dem IIS Server installiert. Web Help Desk wird dann auf dem IIS Server in einem separaten Anwendungspool mit der Bezeichnung **SGNWHD-Pool** installiert.

## 2.2.1 Sichern des Web Servers mit SSL

Um die Sicherheit zu erhöhen, konfigurieren Sie den IIS Webserver wie folgt:

1. Zugang zu Web Help Desk ausschließlich über das Intranet  
Stellen Sie sicher, dass Web Help Desk ausschließlich über das Intranet Ihres Unternehmens zur Verfügung gestellt wird. Aus Sicherheitsgründen sollte Web Help Desk nicht über das Internet zur Verfügung gestellt werden.
2. Herstellung einer SSL-Verbindung  
Die Verfügbarkeit von Web Help Desk lässt sich über die mit IIS gelieferte IIS-Standardkonfiguration auf spezifische Benutzer eingrenzen. Stellen Sie sicher, dass SSL Security Certificate auf dem IIS Server installiert ist. Die gesamte Web Help Desk Kommunikation erfolgt dann über SSL.  
Folgende allgemeine Schritte sollten durchgeführt werden, um den Web Server mit SSL einzurichten:
  - a) Certificate Authority muss auf dem Server installiert sein, um die bei der SSL-Verschlüsselung verwendeten Zertifikate auszustellen.
  - b) Ein Zertifikat muss ausgestellt werden und der IIS Server so konfiguriert werden, dass er SSL verwendet und auf das Zertifikat zeigt.
  - c) Der Servername, den Sie bei der Konfiguration des SafeGuard Enterprise Servers angeben, muss identisch sein mit dem Servernamen, den Sie vorab im SSL-Zertifikat angegeben haben. Sonst können Client und Server nicht miteinander kommunizieren. Für jeden SafeGuard Enterprise Server wird ein separates SSL-Zertifikat benötigt.
  - d) Die Arbeitsprozesse für den Anwendungspool **SGNWHD-Pool** dürfen nicht auf mehr als 1 (Standardeinstellung) erhöht werden. Andernfalls schlägt die Authorisierung bei Web Help Desk fehl.

Weitere Informationen erhalten Sie von unserem technischen Support oder hier:

- <http://msdn2.microsoft.com/en-us/library/ms998300.aspx>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;316898>
- [https://blogs.msdn.com/sql\\_protocols/archive/2005/11/10/491563.aspx](https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx)

## 2.2.2 Registrieren und Konfigurieren des SafeGuard Enterprise Servers

Wenn SafeGuard Enterprise Server nicht bereits vor der Installation von Web Help Desk installiert und registriert wurde, muss SafeGuard Enterprise Server im SafeGuard Management Center registriert werden.

1. Starten Sie das SafeGuard Management Center.
2. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
3. Wählen Sie die Registerkarte **Server registrieren** und klicken Sie auf **Hinzufügen**.

4. Klicken Sie unter **Serverregistrierung** auf die Schaltfläche [...], um das Maschinenzertifikat des Servers auszuwählen. Es wird bei der Installation des SafeGuard Enterprise Servers erzeugt. Sie finden es standardmäßig im Verzeichnis **MachCert** des SafeGuard Enterprise Server Installationsverzeichnisses (Dateiname <Computername>.cer) Wenn der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert ist, muss diese .cer-Datei als Kopie oder Netzwerkfreigabe zugreifbar sein.

Wählen Sie nicht das MSO-Zertifikat.

Der FQDN, z. B. **server.mycompany.edu**, sowie Zertifikatsinformationen werden angezeigt.

Wenn SSL als Transportverschlüsselung zwischen Client und Server verwendet werden soll, muss der Servername, den Sie hier eingeben mit dem Servernamen übereinstimmen, den Sie im SSL-Zertifikat vergeben haben. Andernfalls können Client und Server nicht miteinander kommunizieren.

5. Klicken Sie auf **OK**.

Die Serverinformationen werden in der Registerkarte **Server registrieren** angezeigt.

6. Klicken Sie auf die Registerkarte **Server-Konfigurationspaket erstellen**. Hier werden alle verfügbaren Server angezeigt. Wählen Sie dort den gewünschten Server aus. Geben Sie einen Ausgabepfad für das Konfigurationspaket an. Klicken Sie auf **Konfigurationspaket erstellen**.

Ein Server-Konfigurationspaket (MSI) mit der Bezeichnung <Server>.msi wird im angegebenen Ausgabeort erstellt.

7. Klicken Sie auf **OK**, um die Erfolgsmeldung zu bestätigen.
8. Klicken Sie in der Registerkarte **Server registrieren** auf **Schließen**.

SafeGuard Enterprise Server ist registriert und konfiguriert. Installieren Sie nun das Server-Konfigurationspaket (MSI) auf dem Computer, auf dem der SafeGuard Enterprise Server läuft. Sie können die Serverkonfiguration in der Registerkarte **Server registrieren** jederzeit ändern.

**Hinweis:**

Wenn Sie ein neues Server-Konfigurationspaket (MSI) auf dem SafeGuard Enterprise Server installieren möchten, deinstallieren Sie zunächst das veraltete Server-Konfigurationspaket.

## 2.3 Aktualisierung von Web Help Desk

Wenn Sie eine ältere Version von Web Help Desk auf die aktuelle Version bringen möchten, wird empfohlen, Web Help Desk zuvor zu deinstallieren und die aktuelle Version von Web Help Desk neu zu installieren. Das Server-Konfigurationspaket muss nur dann neu erzeugt werden, wenn die Servereinstellungen geändert wurden.

## 2.4 Unterstützte Sprachen

Web Help Desk unterstützt mehrere Sprachen. Sie können die Sprache, in der die Anwendung angezeigt wird, dynamisch in der Anmeldemaske von Web Help Desk ändern. Klicken Sie

hierzu auf die gewünschte Sprache. Die Anwendung wird daraufhin sofort in der gewünschten Sprache angezeigt.

## 3 Authentisierung

Um den web-basierten Recovery-Assistenten benutzen zu können, müssen sich Sicherheitsbeauftragte an Web Help Desk und am SafeGuard Enterprise Server anmelden. Sicherheitsbeauftragte melden sich mit ihrem Sicherheitsbeauftragtennamen und Ihrem Kennwort entsprechend ihren Windows-Anmeldeinformationen an Web Help Desk an.

Nur Benutzer, die im SafeGuard Management Center zu Web Help Desk Sicherheitsbeauftragten gemacht wurden, können auf Web Help Desk zugreifen.

### 3.1 Vorbereitung im SafeGuard Management Center

Für die Anmeldung an Web Helpdesk müssen folgende Voraussetzungen erfüllt sein und folgende vorbereitende Schritte im SafeGuard Management Center ausgeführt werden. Weitere Informationen finden Sie in der Administrator-Hilfe.

1. Die Web Help Desk Benutzer müssen aus einem Active Directory in die SafeGuard Enterprise Datenbank importiert werden.
2. Den Benutzern müssen Benutzerzertifikate zugewiesen werden und die Zertifikate (.p12 Datei) müssen in der Datenbank zur Verfügung stehen.
3. Künftige Web Help Desk Benutzer müssen nun zu Sicherheitsbeauftragten gemacht werden.

Die neuen Sicherheitsbeauftragten können sich daraufhin mit ihrem definierten Sicherheitsbeauftragten-Namen, einer Kombination aus Ihrem Windows-Benutzernamen und dem Namen der ihnen zugewiesenen Domäne, an Web Help Desk anmelden. Das hierfür notwendige Kennwort entspricht dem Windows-Kennwort, mit dem die Zertifikate der Benutzer geschützt sind

4. Den Sicherheitsbeauftragten muss die Rolle des Helpdesk-Beauftragten zugewiesen werden, damit sie sich bei Web Help Desk authentisieren können.

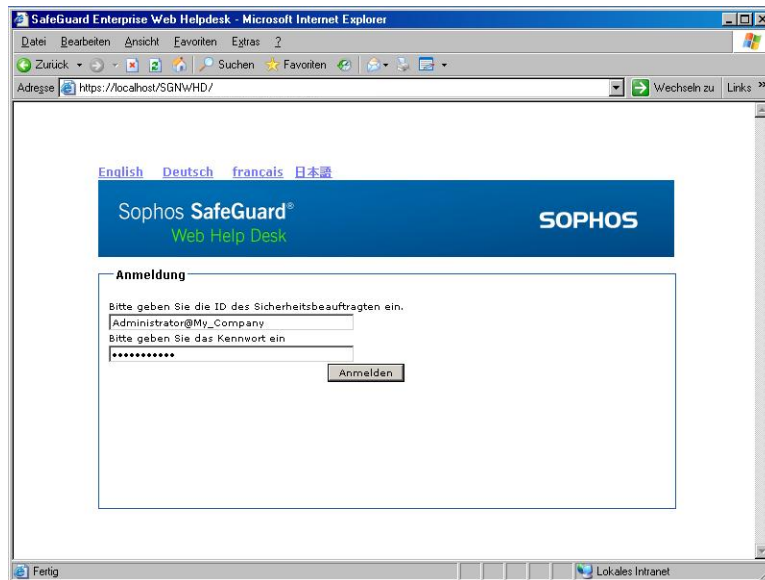
Die Voraussetzungen für eine erfolgreiche Anmeldung an Web Help Desk sind erfüllt.

**Hinweis:** Da sich Web Help Desk Sicherheitsbeauftragte am SafeGuard Enterprise Server authentisieren müssen, wird die Authentisierung mit Token in Web Help Desk nicht unterstützt.

### 3.2 Anmeldung an Web Help Desk

1. Starten Sie Ihren Browser.

- Um die Anwendung in Ihrem Browser aufzurufen, geben Sie folgende URL ein:  
**https://<Host ID oder IP Adresse>/SGNWHD**



- Geben Sie auf der **Willkommen** Seite Ihren Sicherheitsbeauftragten-Namen genau so, wie er im SafeGuard Management Center definiert ist, ein: **<Benutzername>@<DOMÄNE>** zum Beispiel **WHDOfficer@MYDOMAIN**  
Achten Sie bei der Eingabe auf Groß- und Kleinschreibung. Stellen Sie sicher, dass der Benutzername korrekt geschrieben ist.
- Geben Sie Ihr Kennwort ein. Das für die Anmeldung notwendige Kennwort ist Ihr Windows-Kennwort.
- Klicken Sie auf **Anmelden**.

Sie werden an Web Help Desk angemeldet.

## 4 Auswählen des Web Help Desk Assistenten

1. Führen Sie auf der Seite **Home** einen der folgenden Schritte aus:
  - Um Recovery-Aktionen auf Endpoint-Computern zu autorisieren, wählen Sie **Recovery**, *siehe Recovery-Typen - Übersicht* (Seite 12).
  - Um das Deaktivieren der SafeGuard Configuration Protection Richtlinie auf Endpoint-Computern zu autorisieren, wählen Sie **Deaktivieren erlauben**, *siehe SafeGuard Configuration Protection* (Seite 26).

## 5 Recovery-Typen - Übersicht

Folgende Recovery-Typen stehen zur Verfügung:

### ■ SafeGuard Enterprise Clients (managed)

Endpoint-Computer, die zentral durch das SafeGuard Management Center verwaltet werden. Sie werden im Bereich Benutzer & Computer des SafeGuard Management Centers angezeigt.

### ■ Virtuelle Clients

Eine Recovery-Aktion für verschlüsselte Volumes kann auch in Fällen durchgeführt werden, in denen Challenge/Response-Verfahren normalerweise nicht unterstützt würden, z. B. wenn die POA beschädigt ist.

Für den einfachen Zugriff auf verschlüsselte Volumes in dieser Situation können spezifische Dateien, die als virtuelle Clients bezeichnet werden, erstellt und vor dem Challenge/Response-Verfahren an den Benutzer übermittelt werden. Mit Hilfe dieser virtuellen Clients sowie dem Recovery-Tool **RecoveryKeys.exe**, das in der Produktlieferung zur Verfügung steht, kann dann ein Challenge/Response-Verfahren auf dem Endpoint-Computer eingeleitet werden. Der Benutzer muss dann nur noch den Helpdesk-Beauftragten über die benötigten Schlüssel informieren und den Response-Code eingeben, um wieder Zugriff auf die verschlüsselten Volumes zu erhalten.

### ■ Sophos SafeGuard Standalone Clients

Endpoint-Computer, die lokal verwaltet werden. Diese Computer haben nie eine Verbindung zum SafeGuard Enterprise Server. Für jeden lokal verwalteten Sophos SafeGuard Computer wird während der Konfiguration eine Recovery-Datei (.xml-Datei) erzeugt. Diese Datei enthält den definierten Computerschlüssel, der mit dem Unternehmenszertifikat verschlüsselt ist. Wenn diese Datei für den Zugriff durch den Helpdesk-Beauftragten zur Verfügung steht, z. B. auf einem USB Stick oder über eine Netzwerkfreigabe, wird das Challenge/Response-Verfahren für einen lokal verwalteten, durch Sophos SafeGuard geschützten Computer unterstützt.

Abmelden Administrator@my\_company

Sophos SafeGuard®  
Web Help Desk

SOPHOS

**Recovery-Typ**

SafeGuard Enterprise Client

Domäne

Computer

Virtueller Client

Virtueller Client

Standalone Client

XML Recovery-Datei

### Recovery-Typ auswählen

Wählen Sie nach der Auswahl von **Recovery** auf der **Home** Seite den gewünschten Recovery-Typ.

## 6 Recovery für SafeGuard Enterprise Clients (managed)

SafeGuard Enterprise bietet ein Recovery-Verfahren für in der Datenbank registrierte SafeGuard Enterprise Clients in verschiedenen Notfallszenarien, z. B. Kennwort-Recovery oder Zugriff auf Daten durch Starten von einem externen Medium.

Das Challenge/Response-Verfahren wird sowohl für native SafeGuard Enterprise Clients als auch für BitLocker verschlüsselte SafeGuard Enterprise Clients unterstützt. Während des Challenge/Response-Verfahrens wird automatisch erkannt, um welchen Enterprise Client-Typ es sich handelt und der Recovery-Ablauf entsprechend angepasst.

### 6.1 Recovery-Aktionen für SafeGuard Enterprise Clients

Der Recovery-Ablauf richtet sich danach, für welchen Typ von SafeGuard Enterprise Client das Recovery-Verfahren angefordert wird.

#### Hinweis:

Für mit BitLocker verschlüsselte Computer steht als Recovery-Aktion nur die Wiederherstellung des Schlüssels, der für die Verschlüsselung eines spezifischen Volumens verwendet wurde, zur Verfügung. Eine Recovery-Aktion für Kennwörter ist nicht verfügbar.

#### 6.1.1 Wiederherstellen des Kennworts auf POA-Ebene

Einer der am häufigsten auftretenden Recovery-Szenarien besteht darin, dass Benutzer ihr Kennwort vergessen haben. SafeGuard Enterprise wird standardmäßig mit aktivierter Power-on Authentication (POA) installiert. Das POA-Kennwort, mit dem auf den Computer zugegriffen wird, ist identisch mit dem Windows-Kennwort.

Wenn der Benutzer das Kennwort auf der POA-Ebene vergessen hat, generiert der Helpdesk-Beauftragte eine Response mit der Option **SGN Client mit Benutzeranmeldung booten**, jedoch ohne Anzeige des Benutzerkennworts. In diesem Fall startet der Computer jedoch nach Eingabe des Response-Codes bis zur Betriebssystemebene. Der Benutzer muss somit unter der Voraussetzung, dass Zugriff auf die Domäne besteht, das Kennwort auf Windows-Ebene ändern. Danach kann der Benutzer sich sowohl an Windows als auch an der Power-on Authentication mit dem neuen Kennwort anmelden.

#### Best Practice für das Wiederherstellen des Kennworts auf POA-Ebene

##### Hinweis:

Wir empfehlen, folgende Methoden anzuwenden, wenn der Benutzer sein Kennwort vergessen hat, um zu vermeiden, dass das Kennwort zentral zurückgesetzt werden muss:

**Benutzen Sie Local Self Help.** Mit Local Self Help kann sich der Benutzer selbst das aktuelle Benutzerkennwort anzeigen lassen und es weiterhin zur Anmeldung verwenden. Dadurch wird ein Zurücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden. Weitere Informationen finden Sie in der Administrator-Hilfe.

**Bei Anwendung von Challenge/Response für SafeGuard Enterprise Clients (Managed):** Wir empfehlen, das Kennwort vor dem Challenge/Response-Verfahren nicht zentral im Active Directory zurückzusetzen. Dadurch wird gewährleistet, dass das Kennwort zwischen Windows

und SafeGuard Enterprise synchron bleibt. Stellen Sie sicher, dass der Windows-Helpdesk entsprechend informiert ist.

Erzeugen Sie als SafeGuard Enterprise Helpdesk-Beauftragter eine Response für das **Booten des SGN Clients mit Benutzeranmeldung** mit der Option **Benutzerkennwort anzeigen**. Dies bietet den Vorteil, dass das Kennwort nicht im Active Directory geändert werden muss. Der Benutzer kann mit dem vorhandenen Kennwort weiterarbeiten und dieses später nach Wunsch lokal ändern.

### 6.1.2 Anzeigen des Benutzerkennworts

SafeGuard Enterprise bietet Benutzern die Möglichkeit, sich ihr Kennwort während des Challenge/Response-Verfahrens anzeigen zu lassen. Dies bietet den Vorteil, dass das Kennwort nicht im Active Directory geändert werden muss. Diese Option ist verfügbar, wenn die Anforderung **SGN Client mit Benutzeranmeldung** gestellt wird.

### 6.1.3 Zugriff auf Daten durch Starten von externen Medien

Mit Hilfe des Challenge/Response-Verfahrens lässt sich ein Computer auch von einem externen Medium wie WinPE starten. Hierzu muss der Benutzer im POA-Anmeldedialog die Option **Weiterbooten von: Diskette/externem Medium** wählen und eine Challenge starten. Nach Erhalt der Response kann der Benutzer die Anmeldeinformationen wie gewohnt in der POA eingeben und den Start-Vorgang von einem externen Medium fortsetzen.

Für den Zugriff auf ein verschlüsseltes Volume müssen folgende Voraussetzungen erfüllt sein:

- Das zu verwendende Gerät muss den SafeGuard Enterprise Filtertreiber enthalten. Für Informationen dazu, wie Sie eine solche Treiber-CD erhalten, siehe:  
<http://www.sophos.de/support/knowledgebase/article/108805.html>.
- Der Benutzer muss den Computer vom externen Medium starten und muss dazu berechtigt sein. Diese Berechtigung wird erteilt, indem man im SafeGuard Management Center eine Richtlinie erstellt und diese dem Client zuweist (Richtlinientyp **Authentisierung > Zugriff Benutzer kann nur von Festplatte booten** auf **Nein** eingestellt). Standardmäßig ist die Berechtigung zum Starten von externen Medien nicht zugewiesen.
- Der Endpoint-Computer muss den Start-Vorgang von einem anderen Medium als einer Festplatte generell unterstützen.
- Es kann nur auf Volumes, die mit dem definierten Computerschlüssel verschlüsselt sind, zugegriffen werden. Dieser Verschlüsselungstyp kann in einer Geräteschutzrichtlinie im SafeGuard Management Center definiert und dem Computer zugewiesen werden.

#### Hinweis:

Wenn Sie externe Medien, z. B. WinPE, für den Zugriff auf ein verschlüsseltes Laufwerk verwenden, ermöglicht dies den Zugriff auf das Volume nur teilweise.

### 6.1.4 Wiederherstellen des SafeGuard Enterprise Policy-Cache

Diese Aktion wird benutzt, wenn der SafeGuard Policy-Cache beschädigt ist. In diesem Fall wird der Benutzer automatisch bei der Anmeldung an der Power-on Authentication dazu aufgefordert, ein Challenge/Response-Verfahren zu starten.

## 6.2 Erzeugen einer Response für SafeGuard Enterprise Clients

Um für einen SafeGuard Enterprise Client eine Response in einem Challenge/Response-Verfahren zu generieren, werden der Name des betreffenden Endpoint-Computers und die Domäne benötigt.

**Hinweis:** Der Name muss immer der Distinguished Name des Computers sein.

1. Wählen Sie auf der **Recovery-Typ** Seite die Option **SafeGuard Enterprise Client**.
2. Wählen Sie die relevante Domäne aus der Liste.
3. Geben Sie den Computernamen ein. Hierfür gibt es mehrere Möglichkeiten:
  - Wählen Sie den Namen, indem Sie auf [...] und im Popup-Fenster auf **Suchen** klicken. Eine Liste mit Computern wird angezeigt. Wählen Sie den gewünschten Computer aus und klicken Sie auf **OK**. Der Computernamen wird im Fenster **Recovery-Typ** unter **Domäne** angezeigt.
  - Geben Sie den Kurznamen des Computers ein. Wenn Sie auf **Weiter** klicken, wird der Name in der Datenbank gesucht. Der gefundene Computernamen wird als Distinguished Name angezeigt.
  - Geben Sie den Computernamen direkt als Distinguished Name ein, zum Beispiel:  
**CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=edu**
4. Klicken Sie auf **Weiter**.

Das Programm bestimmt nun automatisch, ob es sich um einen nativen SafeGuard Enterprise Computer oder um einen mit BitLocker verschlüsselten Computer handelt, und passt den Recovery Workflow entsprechend an. Im Falle eines nativen SafeGuard Enterprise Computers wird im nächsten Schritt die Auswahl der Benutzerinformationen verlangt. Im Fall eines mit BitLocker verschlüsselten Computer, muss im nächsten Schritt das erforderliche Volume, das entschlüsselt werden soll, ausgewählt werden.

### 6.2.1 Erzeugen einer Response für native SafeGuard Enterprise Clients

Im Falle eines nativen SafeGuard Enterprise Clients muss zunächst in der Datenbank nach dem relevanten Computer gesucht werden.

1. Wählen Sie unter **Domäne** die Domäne des Benutzers. Wählen Sie für einen lokalen Benutzer **Lokaler Benutzer auf <Computernamen>**.
2. Suchen Sie nach dem Benutzernamen. Gehen Sie wie folgt vor:
  - Klicken Sie auf **Nach angezeigtem Namen suchen**. Wählen Sie den gewünschten Namen aus der Liste und klicken Sie auf **OK**.

- Klicken Sie auf **Nach Anmeldenamen suchen**. Wählen Sie den gewünschten Namen aus der Liste und klicken Sie auf **OK**.
  - Geben Sie den Benutzernamen direkt ein. Stellen Sie sicher, dass der Name korrekt geschrieben ist.
3. Klicken Sie auf **Weiter**. Ein Fenster für die Eingabe des Challenge-Codes wird angezeigt.
  4. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft. Wenn der Code nicht korrekt eingegeben wurde, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.
  5. Wenn der Challenge-Code korrekt eingegeben wurde, werden die vom SafeGuard Enterprise Client angeforderte Aktion sowie die verfügbaren Recovery-Aktionen auf dem Client angezeigt. Die verfügbaren Response-Aktionen richten sich nach den Aktionen, die auf dem Endpoint-Computer beim Aufrufen der Challenge angefordert wurden. Wenn zum Beispiel **Crypto Token erforderlich** angefordert wurde, stehen für die Response die Aktionen **SGN Client mit Benutzeranmeldung booten** und **SGN Client ohne Benutzeranmeldung booten** zur Verfügung.
  6. Wählen Sie die Aktion, die der Benutzer ausführen soll.
  7. Wenn Sie **SGN Client mit Benutzeranmeldung booten** als Response-Aktion ausgewählt haben, können Sie zusätzlich auch die Option **Benutzerkennwort anzeigen** wählen, um das Kennwort auf dem Zielcomputer anzeigen zu lassen.
  8. Klicken Sie auf **Weiter**. Es wird ein Response-Code erzeugt.
  9. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der Benutzer kann nun den Response-Code eingeben und die autorisierte Aktion durchführen.

## 6.2.2 Response für SafeGuard Enterprise Clients mit BitLocker-Verschlüsselung erzeugen

Für mit BitLocker verschlüsselte SafeGuard Enterprise Clients lässt sich ein Volume, auf das nicht mehr zugegriffen werden kann, wiederherstellen. Die Datenbank wird auf den relevanten Computer überprüft. Danach muss das Volume ausgewählt werden, für das die Recovery-Aktion am BitLocker verschlüsselten Benutzercomputer durchgeführt werden soll.

1. Wählen Sie das Volume, auf das zugegriffen werden soll, und klicken Sie auf **Weiter**. Web Help Desk zeigt nun den 48-stelligen Recovery-Schlüssel an.
2. Teilen Sie dem Benutzer diesen Schlüssel mit.

Der Benutzer kann nun den Schlüssel eingeben, um den Zugriff auf das mit BitLocker verschlüsselte Volume auf dem Benutzercomputer wiederherzustellen.

## 7 Recovery mit virtuellen Clients

Unter Verwendung virtueller Clients für Recovery-Vorgänge in SafeGuard Enterprise lässt sich der Zugriff auf verschlüsselte Volumes auch in komplexen Notfallsituationen wiederherstellen.

Dieser Recovery-Typ kann in den folgenden typischen Situationen angewendet werden:

- Die Power-on Authentication ist beschädigt.
- Ein Volume ist nicht mit dem definierten Computerschlüssel sondern mit einem anderen Schlüssel verschlüsselt. Der notwendige Schlüssel steht in der Benutzerumgebung nicht zur Verfügung. Der Schlüssel muss daher in der Datenbank identifiziert und auf sichere Art und Weise an den Computer übertragen werden.

### Hinweis:

Recovery mit virtuellen Clients sollte nur in komplexen Notfallsituationen angewendet werden. Nur wenn beide der oben genannten Sachverhalte eingetreten sind, ist ein Recovery-Vorgang mit virtuellen Clients angebracht. Wenn jedoch zum Beispiel nur ein Schlüssel für die Wiederherstellung eines Volumes fehlt, ist es am besten, den fehlenden Schlüssel dem Schlüsselbund des entsprechenden Benutzers zuzuweisen, um den Zugriff auf das Volume zu ermöglichen.

In diesen Situationen bietet SafeGuard Enterprise folgende Lösung:

Für den einfachen Zugriff auf verschlüsselte Volumes in dieser Situation können spezifische Dateien, die als virtuelle Clients bezeichnet werden, im SafeGuard Management Center erstellt und vor dem Challenge/Response-Verfahren an den Benutzer übermittelt werden. Mit Hilfe dieser virtuellen Clients, dem Recovery-Tool **RecoveryKeys.exe** sowie einem für SafeGuard Enterprise angepassten WinPE kann dann ein Challenge/Response-Verfahren auf dem Endpoint-Computer eingeleitet werden. Der Helpdesk-Beauftragte wählt dann die erforderlichen Schlüssel aus und generiert einen Response-Code. Der Zugriff auf das verschlüsselte Volume wird ermöglicht, wenn der Benutzer den Response-Code eingibt, da alle erforderlichen Schlüssel in der Response übertragen werden.

### Hinweis:

In Web Help Desk wird Recovery mit virtuellen Clients SafeGuard nicht für Sophos SafeGuard Clients (standalone) unterstützt.

### 7.1 Recovery Workflow mit virtuellen Clients

#### Hinweis:

Weitere Informationen finden Sie in der Administrator-Hilfe.

1. Der Helpdesk-Beauftragte muss den virtuellen Client im Bereich **Schlüssel & Zertifikate** des SafeGuard Management Centers anlegen und in eine Datei exportieren. Diese Datei mit der Bezeichnung **recoverytokentok** muss an die Benutzer verteilt werden und vor dem Challenge/Response-Verfahren zur Verfügung stehen.

2. Der Benutzer kann dann eine SafeGuard Enterprise Recovery-CD oder eine andere CD mit einem von SafeGuard Enterprise modifizierten WinPE vom BIOS aus ohne POA-Anmeldung starten und ein Challenge/Response-Verfahren starten.  
Zur Identifizierung in der SafeGuard Enterprise Datenbank wird die Recovery-Datei des virtuellen Client benutzt. Diese wird in der Challenge anstelle des Computernamens, der in diesem Fall nicht zur Verfügung steht, angegeben.
3. Das Key Recovery Tool zeigt dem Benutzer nun an, welche Volumes verschlüsselt sind und welche Schlüssel für die einzelnen Volumes verwendet wurden. Der Benutzer teilt diese Informationen dem Helpdesk-Beauftragten mit.
4. Der Helpdesk-Beauftragte identifiziert den virtuellen Client in der Datenbank und wählt den für den Zugriff auf die verschlüsselten Volumes erforderlichen Schlüssel aus: entweder einen einzelnen Schlüssel oder mehrere in eine Schlüsseldatei exportierte Schlüssel. Nach der Auswahl generiert der Helpdesk-Beauftragte die Response.
5. Der Benutzer gibt den Response-Code ein. Im Response-Code werden die erforderlichen Schlüssel übertragen. Durch Eingabe des Response-Codes und einen anschließenden Neustart des Computers kann der Benutzer auf die verschlüsselten Volumes zugreifen.

## 7.2 Recovery-Aktionen mit virtuellen Clients

Um auf Volumes zuzugreifen, die mit Schlüsseln verschlüsselt wurden, die dem Benutzer nicht zur Verfügung stehen, muss der bzw. die korrekte Verschlüsselungsschlüssel aus der Datenbank in die Benutzerumgebung übertragen werden.

Das Challenge/Response-Verfahren deckt daher zwei Recovery-Aktionen mit virtuellen Clients ab:

- Übertragung eines einzelnen Schlüssels
- Übertragung mehrerer Schlüssel in einer verschlüsselten Schlüsseldatei

### 7.2.1 Übertragen eines einzelnen Schlüssels

Die Challenge kann für die Bereitstellung eines einzelnen Schlüssels zum Zugriff auf ein verschlüsseltes Volume erzeugt werden. Der Helpdesk-Beauftragte muss den erforderlichen Schlüssel in der Datenbank auswählen und einen Response-Code erzeugen. Durch Eingabe des Response-Codes wird der Schlüssel verschlüsselt und an den Endpoint-Computer übertragen. Ist der Response-Code korrekt, wird der Schlüssel in den lokalen Schlüsselspeicher importiert. Danach kann auf alle Volumes, die mit diesem Schlüssel verschlüsselt sind, zugegriffen werden.

### 7.2.2 Mehrere Schlüssel in einer verschlüsselten Schlüsseldatei übertragen

Die Challenge kann für die Bereitstellung eines einzelnen Schlüssels zum Zugriff auf ein verschlüsseltes Volume erzeugt werden. Die Schlüssel werden in einer Datei gespeichert, die mit einem Kennwort verschlüsselt ist. Voraussetzung hierfür ist, dass der Helpdesk-Beauftragte einen oder mehrere der erforderlichen Schlüssel in eine Datei exportiert. Diese Datei wird mit einem Zufallskennwort verschlüsselt, das in der Datenbank gespeichert wird. Das Kennwort ist für jede angelegte Schlüsseldatei einzigartig.

Die verschlüsselte Schlüsseldatei muss in die Benutzerumgebung übertragen werden und dem Benutzer zur Verfügung stehen. Um diese Schlüsseldatei zu entschlüsseln, muss der Benutzer dann ein Challenge/Response-Verfahren mit dem Key Recovery Tool **RecoverKeys.exe** starten. Das Kennwort wird in diesem Verfahren an den Zielcomputer übertragen. Der Helpdesk-Beauftragte generiert eine Response und wählt das entsprechende Kennwort zum Entschlüsseln der Schlüsseldatei aus. Das Kennwort wird innerhalb des Response-Codes an den Zielcomputer übertragen. Die Schlüsseldatei kann dann mit dem Kennwort entschlüsselt werden.

Die Schlüssel in der Schlüsseldatei werden in den Schlüsselspeicher auf dem Endpoint-Computer übertragen und es besteht wieder Zugriff auf alle Volumes, die mit den verfügbaren Schlüsseln verschlüsselt sind.

**Hinweis:**

Bei der Anwendung von Web Help Desk werden die Schlüsseldatei und das entsprechende Kennwort nach ihrer erfolgreichen Verwendung in einem Challenge/Response-Verfahren aus der Datenbank gelöscht. Somit müssen Sie nach jedem erfolgreich durchgeführten Challenge/Response-Verfahren eine neue Schlüsseldatei und ein neues Kennwort erstellen.

## 7.3 Response mit virtuellen Clients

Um eine Response mit virtuellen Clients zu erzeugen, müssen folgende Voraussetzungen erfüllt sein.

### 7.3.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Der virtuelle Client muss im SafeGuard Management Center im Bereich **Schlüssel & Zertifikate** angelegt werden. Weitere Informationen finden Sie in der Administrator-Hilfe.
- Der Helpdesk-Beauftragte muss in der Lage sein, den virtuellen Client in der Datenbank zu finden. Virtuelle Clients werden anhand ihrer Namen identifiziert.
- Die Recovery-Datei des virtuellen Client **recoverytoken.tok** muss dem Benutzer zur Verfügung stehen. Diese Datei muss im gleichen Verzeichnis wie das Schlüssel-Recovery Tool gespeichert sein. Wir empfehlen, diese Datei auf einem USB-Stick zu speichern.
- Wird ein Recovery-Verfahren für mehrere Schlüssel angefordert, so muss der Helpdesk-Beauftragte zunächst eine Schlüsseldatei mit den notwendigen Recovery-Schlüsseln im SafeGuard Management Center im Bereich **Schlüssel & Zertifikate** anlegen. Die Schlüsseldatei muss dem Benutzer vor dem Recovery-Verfahren zur Verfügung stehen. Das für die Verschlüsselung dieser Schlüsseldatei verwendete Kennwort muss in der Datenbank zur Verfügung stehen. Weitere Informationen finden Sie in der Administrator-Hilfe.
- Der Benutzer muss das Schlüssel-Recovery Tool gestartet und das Challenge/Response-Verfahren eingeleitet haben.
- Eine Response kann nur für zugewiesene Schlüssel erzeugt werden. Ist ein Schlüssel inaktiv, d. h. der Schlüssel ist nicht mindestens einem Benutzer zugewiesen, ist eine Response mit einem virtuellen Client nicht möglich. In diesem Fall kann der inaktive Schlüssel zunächst

einem beliebigen Benutzer zugewiesen werden. Danach kann eine Response für den Schlüssel generiert werden.

### 7.3.2 Erzeugen einer Response mit virtuellen Clients

1. Als Helpdesk-Beauftragter wählen Sie im Fenster **Recovery-Typ** die Option **Virtueller Client**.
2. Geben Sie den Namen des virtuellen Client ein, den Sie vom Benutzer erhalten haben. Hierzu gibt es verschiedene Möglichkeiten:
  - Geben Sie den eindeutigen Namen direkt ein.
  - Wählen Sie den Namen, indem Sie auf [...] und im Popup-Fenster auf **Suchen** klicken. Eine Liste mit virtuellen Clients wird angezeigt. Wählen Sie den gewünschten virtuellen Client aus und klicken Sie auf **OK**. Der Name des virtuellen Client wird nun im Fenster **Recovery-Typ** unter **Virtueller Client** angezeigt.
3. Klicken Sie auf **Weiter**. Das Fenster, in dem Sie die Recovery-Aktion auswählen können, wird angezeigt.
4. Wählen Sie die vom Benutzer durchzuführende Recovery-Aktion und klicken Sie dann auf **Weiter**.
  - Wenn Sie nur einen einzelnen Recovery-Schlüssel transferieren müssen, wählen Sie **Schlüssel angefordert**. Wählen Sie den entsprechenden Schlüssel aus der Liste aus. Klicken Sie auf [...]. Sie können sich die Schlüssel entweder nach Schlüssel-ID oder symbolischem Namen anzeigen lassen. Klicken Sie auf **Suchen**, wählen Sie den Schlüssel und klicken Sie auf **OK**.
  - Wenn der Benutzer eine Schlüsseldatei mit mehreren Recovery-Schlüsseln benötigt, wählen Sie **Kennwort für Schlüsseldatei angefordert**, um das Kennwort für die verschlüsselte Schlüsseldatei an den Benutzer zu übertragen. Wählen Sie die erforderliche Schlüsseldatei aus. Klicken Sie auf [...] und dann auf **Suchen**. Wählen Sie die Schlüsseldatei aus und klicken Sie auf **OK**.

Sie können **Kennwort für Schlüsseldatei angefordert** nur dann auswählen, wenn zuvor eine Schlüsseldatei im SafeGuard Management Center angelegt wurde und das Kennwort, mit dem die Datei verschlüsselt ist, in der Datenbank gespeichert wurde. Bei der Anwendung von Web Help Desk werden Schlüsseldateien und die entsprechenden Kennwörter nach ihrer erfolgreichen Verwendung in einem Challenge/Response-Verfahren aus der Datenbank gelöscht. Somit müssen Sie nach jedem erfolgreich durchgeführten Challenge/Response-Verfahren eine neue Schlüsseldatei und ein neues Kennwort erstellen.

5. Klicken Sie auf **Weiter**. Das Fenster für die Eingabe des Challenge-Codes wird angezeigt.
6. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft. Wenn der Code nicht korrekt eingegeben wurde, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültig** angezeigt.

7. Wenn der Challenge-Code korrekt eingegeben wurde, wird der Response-Code erzeugt. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.
  - Wird ein einzelner Schlüssel angefordert, wird der erzeugte Schlüssel im Response-Code übertragen.
  - Wird ein Kennwort für die verschlüsselte Schlüsseldatei angefordert, so wird dieses im Response-Code übertragen. Die Schlüsseldatei wird dann gelöscht.
8. Der Benutzer muss den Response-Code auf dem Endpoint-Computer eingeben.
9. Der Benutzer muss den Computer neu starten und sich wieder anmelden, um auf die entsprechenden Volumes zugreifen zu können.

Auf die Volumes kann wieder zugegriffen werden.

## 8 Recovery für Sophos SafeGuard Clients (standalone)

SafeGuard Enterprise bietet auch ein Challenge/Response-Verfahren für Sophos SafeGuard Standalone Clients (standalone). Sophos SafeGuard Clients (standalone) haben niemals eine Verbindung zum SafeGuard Enterprise Server. Sie werden im Standalone-Modus betrieben und lokal verwaltet. Da sie nicht in der SafeGuard Enterprise Datenbank registriert sind, stehen keine Informationen für Ihre Identifikation, die für ein Challenge/Response-Verfahren benötigt werden, zur Verfügung.

Das Challenge/Response-Verfahren für Sophos SafeGuard Clients (standalone) basiert daher auf der Recovery-Schlüsseldatei, die während der Konfiguration des Standalone Clients erstellt wird. Die Recovery-Datei (.xml-Datei) wird für jeden Sophos SafeGuard Client (standalone) generiert und enthält den definierten Computerschlüssel, der mit dem Unternehmenszertifikat verschlüsselt ist. Diese Datei muss an einem Speicherort abgelegt sein, auf den der Helpdesk-Beauftragte während des Challenge/Response-Verfahrens zugreifen kann. Wenn der Helpdesk-Beauftragte auf die entsprechende Recovery-Datei zugreifen kann, z. B. über einen USB-Stick oder ein freigegebenes Netzwerkverzeichnis, kann eine Response generiert werden.

### 8.1 Recovery-Aktionen für Sophos SafeGuard Clients (standalone)

Ein Challenge/Response-Verfahren für einen Sophos SafeGuard Client (standalone) muss in den folgenden Situationen gestartet werden:

- Der Benutzer hat das Kennwort zu oft falsch eingegeben.
- Der Benutzer hat das Kennwort vergessen.
- Ein beschädigter Cache muss repariert werden.

Für einen Sophos SafeGuard Client (standalone) steht kein Benutzerschlüssel in der Datenbank zur Verfügung. Somit ist in einem Challenge/Response-Verfahren nur die Recovery-Aktion **SGN Client ohne Benutzeranmeldung booten** möglich.

Dem Benutzer wird über das Challenge/Response-Verfahren die Anmeldung an der Power-on Authentication ermöglicht. Der Benutzer kann sich außerdem an Windows anmelden, auch wenn das Kennwort zurückgesetzt werden muss.

#### 8.1.1 Der Benutzer hat das Kennwort zu oft falsch eingegeben

Da in diesem Fall das Kennwort nicht zurückgesetzt werden muss, ermöglicht das Challenge/Response-Verfahren dem Benutzer die Anmeldung an der Power-on Authentication. Der Benutzer kann dann das korrekte Kennwort auf Windows-Ebene eingeben und den Computer wieder benutzen.

#### 8.1.2 Der Benutzer hat das Kennwort vergessen.

**Hinweis:**

Wir empfehlen, Local Self Help einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Mit Local Self Help können Sie sich das aktuelle Benutzerkennwort anzeigen lassen und es

weiterhin zur Anmeldung verwenden. Dadurch wird ein Zurücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden. Weitere Informationen finden Sie in der Administrator-Hilfe.

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

1. Das Challenge/Response-Verfahren ermöglicht das Starten des Computers durch die Power-on Authentication.
2. Da dem Benutzer das Kennwort nicht bekannt ist, kann er es im Windows-Anmeldedialog nicht eingeben. Das Kennwort muss daher auf Windows-Ebene zurückgesetzt werden. Hierzu sind weitere Recovery-Vorgänge außerhalb von SafeGuard Enterprise erforderlich, die über Windows-Standard-Verfahren durchgeführt werden müssen. Wir empfehlen die folgenden Methoden für das Zurücksetzen des Kennworts auf Windows-Ebene:

- Über ein Service-Benutzerkonto oder ein Administratorkonto mit den erforderlichen Windows-Rechten auf dem Endpoint-Computer
- Über eine Windows-Kennwortrücksetzdiskette

Als Helpdesk-Beauftragter können Sie den Benutzer darüber informieren, welche Methode benutzt werden soll, und ihm die zusätzlichen Windows-Anmeldeinformationen oder die erforderliche Diskette zur Verfügung stellen.

3. Der Benutzer gibt das vom Helpdesk zur Verfügung gestellte neue Kennwort auf Windows-Ebene ein. Unmittelbar danach ändert der Benutzer das Kennwort in ein nur ihm bekanntes Kennwort.
4. SafeGuard Enterprise stellt fest, dass das neu gewählte Kennwort nicht mehr dem aktuellen SafeGuard Enterprise Kennwort entspricht, das in der POA verwendet wird. Der Benutzer wird aufgefordert, das alte Kennwort einzugeben. Da er das Passwort vergessen hat, muss er auf **Abbrechen** klicken.
5. Wenn das alte Kennwort nicht angegeben werden kann, ist in SafeGuard Enterprise für die Definition eines neuen Kennworts ein neues Zertifikat erforderlich.
6. Basierend auf dem neu gewählten Windows-Kennwort wird ein neues Benutzerzertifikat erzeugt. Dies ermöglicht es dem Benutzer, sich wieder an seinem Computer und an der Power-on Authentication mit dem neuen Kennwort anzumelden.

#### **Schlüssel für SafeGuard Data Exchange**

Wenn der Benutzer das Windows-Kennwort vergessen hat und es zurückgesetzt wurde, können die bereits für SafeGuard Data Exchange erstellten Schlüssel nicht mehr ohne Passphrase verwendet werden. Damit bereits vorhandene Benutzerschlüssel für SafeGuard Data Exchange weiterhin verwendet werden können, müssen dem Benutzer die SafeGuard Data Exchange Passphrasen zur Reaktivierung dieser Schlüssel bekannt sein.

## **8.2 Challenge/Response für Sophos SafeGuard Clients (standalone)**

Um in einer Challenge/Response-Sitzung eine Response für einen SafeGuard Standalone Client zu erzeugen, wird der Name der Recovery-Datei (.xml-Datei) benötigt.

1. Wählen Sie in Web Help Desk auf der **Home** Seite die Option **Recovery**.
2. Wählen Sie unter **Recovery-Typ** die Option **Standalone Client**.

3. Klicken Sie auf **Browse**, um die erforderliche Schlüssel-Recovery-Datei (.xml) auszuwählen.
4. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein.
5. Wählen Sie die vom Benutzer durchzuführende Aktion aus und klicken Sie auf **Weiter**.
6. Es wird ein Response-Code erzeugt. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der Benutzer kann den Response-Code eingeben, die angeforderte Aktion ausführen und dann wieder mit dem Computer arbeiten.

## 9 SafeGuard Configuration Protection

In Verbindung mit SafeGuard PortAuditor (siehe SafeGuard PortAuditor User Guide) bietet SafeGuard Configuration Protection eine umfassende Lösung. Mit dieser Lösung erhalten Unternehmen einen Überblick darüber, welche Ports und Geräte innerhalb des Unternehmens benutzt werden (Sichtbarkeit). Darüber hinaus können sie eine Richtlinie definieren, die die Benutzung kontrolliert und die Daten beim Übertragen schützt.

SafeGuard Configuration Protection kontrolliert jeden Endpoint und jedes Gerät über jedes Netzwerk an allen Schnittstellen. Das Modul überwacht den Datenverkehr in Echtzeit und wendet darauf abgestimmte, detailliert einstellbare Sicherheitsrichtlinien für alle Arten von Schnittstellen und externen Speichergeräten an.

Die aktuelle Richtlinie vom Typ Konfigurationsschutz kann mit Sophos SafeGuard Web Help Desk vorübergehend deaktiviert werden.

### 9.1 Deaktivieren der Konfigurationsschutz-Richtlinie

- Der Benutzer muss dazu berechtigt sein, die Konfigurationsschutz-Richtlinie vorübergehend zu deaktivieren (Richtlinie vom Typ Konfigurationsschutz, Option **Anzeigeoptionen**, **Benutzer darf Configuration Protection vorübergehend deaktivieren** auf **Ja** eingestellt).
- Dem Helpdesk muss folgende Berechtigung zugewiesen sein: **Deaktivierungs-Tool verwenden**.

So wird die Richtlinie vorübergehend deaktiviert:

1. Der Benutzer klickt auf dem Endpoint-Computer auf das System Tray Icon und wählt **Configuration Protection deaktivieren**.
2. Unter **Configuration Protection deaktivieren** wählt der Benutzer den gewünschten Zeitraum, für den der Konfigurationsschutz vorübergehend deaktiviert werden soll. Der Challenge-Code wird automatisch erzeugt. Er ist für 30 Minuten gültig. Der Benutzer teilt dem Helpdesk die Benutzerinformationen, den Challenge-Code sowie die gewünschte Zeitspanne mit.
3. Wählen Sie in Web Help Desk auf der **Home** Seite die Option **Deaktivieren erlauben**.
4. Wählen Sie auf der Seite **Benutzer** die vom Benutzer mitgeteilten Benutzerinformationen aus oder geben Sie sie ein und klicken Sie auf **Weiter**. Die Benutzerinformationen werden bestätigt.
5. Geben Sie auf der **Challenge** Seite den vom Benutzer erhaltenen Challenge-Code ein. Geben Sie den vom Benutzer angegebenen Zeitraum, für den die Richtlinie deaktiviert werden soll, ein. Der Zeitraum muss dem vom Benutzer auf dem Endpoint-Computer eingegebenen Zeitraum entsprechen. Klicken Sie auf **Weiter**.

Der Challenge-Code wird bestätigt und der Response-Code wird erzeugt.

6. Auf der **Response** Seite werden der Response-Code, die erlaubte Aktion und der Zeitraum, für den die Richtlinie deaktiviert werden soll, angezeigt. Teilen Sie dem Benutzer diese Informationen mit. Sie können die Buchstabierhilfe verwenden. Um auf die **Benutzer** Seite zurückzugehen, klicken Sie auf **Neustart**. Um auf die Assistenten-Auswahl-Seite zurückzugehen, klicken Sie oben rechts auf **Home**.

7. Der Benutzer gibt auf dem Endpoint-Computer unter **Configuration Protection** **deaktivieren** den vom Helpdesk erhaltenen Response-Code ein oder kopiert ihn aus der E-Mail oder SMS und fügt ihn ein. Der Benutzer muss sicherstellen, dass der angegebene Zeitraum dem vom Helpdesk erhaltenen Zeitraum entspricht. Der Benutzer klickt auf **OK**.

Die Richtlinie für den Konfigurationsschutz ist für den angegebenen Zeitraum deaktiviert. Für die erneute Aktivierung von Configuration Protection gibt es zwei Möglichkeiten:

- Während des festgelegten Zeitraums klickt der Benutzer auf dem Endpoint-Computer auf das System Tray Icon und wählt **Configuration Protection wieder aktivieren**.
- Nach Ablauf des festgelegten Zeitraums wird die aktuelle Konfigurationsschutz-Richtlinie wieder automatisch aktiviert.

## 10 Protokollierung von Web Help Desk Ereignissen

Ereignisse für SafeGuard Web Help Desk können in der Windows-Ereignisanzeige oder in der SafeGuard Enterprise Datenbank protokolliert werden. Es können Ereignissen zu allen Web Help Desk Aktivitäten protokolliert werden, z. B. welcher Benutzer eine Challenge angefordert hat, oder welche Recovery-Aktionen angefordert wurden.

Die Ereignisprotokollierung für Web Help Desk wird im SafeGuard Management Center durch eine Richtlinie aktiviert. Die Richtlinie muss in einem Konfigurationspaket veröffentlicht und auf dem Web Help Desk Service wirksam gemacht werden.

Ereignisse, die in der zentralen SafeGuard Enterprise Datenbank protokolliert werden, können in der SafeGuard Management Center Ereignisanzeige eingesehen werden.

### 10.1 Aktivieren der Protokollierung von Web Help Desk Ereignissen

Die Protokollierung für Web Help Desk wird im SafeGuard Management Center konfiguriert.

Sie müssen über die erforderlichen Rechte zum Erstellen von Richtlinien und Einsehen von Ereignissen verfügen.

1. Erstellen Sie im **Richtlinien** Navigationsbereich des SafeGuard Management Center eine Richtlinie vom Typ **Protokollierung**. Legen Sie fest, welche Ereignisse protokolliert werden. Speichern Sie Ihre Änderungen.
2. Erstellen Sie eine neue **Richtlinien-Gruppe**. Fügen Sie die Richtlinie vom Typ **Protokollierung** zu dieser Gruppe hinzu. Speichern Sie Ihre Änderungen.
3. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**. Wählen Sie **Konfigurationspaket (managed) erstellen** und klicken Sie auf **Konfigurationspaket hinzufügen**. Wählen Sie die zuvor erstellte Richtliniengruppe für das Konfigurationspaket aus. Legen Sie einen Speicherort fest und klicken Sie auf **Konfigurationspaket erstellen**.
4. Weisen Sie im SafeGuard Management Center die Richtliniengruppe der Domäne zu, in der sich der Web Help Desk Server befindet. Aktivieren Sie nun die Richtlinie. Weitere Informationen finden Sie in der Administrator-Hilfe im Kapitel *Richtlinien zuweisen*.
5. Installieren Sie auf dem Web Help Desk Service das zuvor erstellte Konfigurationspaket. Starten Sie den Service neu.

Die Protokollierung von Web Help Desk Ereignissen ist aktiviert.

6. Melden Sie sich an Web Help Desk an und führen Sie ein Challenge/Response-Verfahren durch.
7. Klicken Sie im SafeGuard Management Center auf **Berichte**. Klicken Sie im Aktionsbereich der Ereignisanzeige auf das Lupensymbol, um die für Web Help Desk protokollierten Ereignisse einzusehen.

## 11 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

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

## 12 Rechtliche Hinweise

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

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

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

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