

SOPHOS

SafeGuard® Enterprise 5.50 Web Helpdesk

Stand: April 2010



Inhaltsverzeichnis

1	SafeGuard Enterprise web-basiertes Challenge/Response-Verfahren.....	2
2	Installation	5
3	Authentisierung.....	11
4	Recovery-Typen	14
5	Recovery für SafeGuard Enterprise Clients.....	15
6	Recovery mit virtuellen Clients.....	21
7	Recovery für SafeGuard Standalone Clients.....	27
8	Technischer Support.....	31
9	Copyright	32

1 SafeGuard Enterprise 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. Mit einem benutzerfreundlichen Challenge/Response-Verfahren unterstützt Web Helpdesk SafeGuard Enterprise Benutzer, die sich an ihrem Computer nicht mehr anmelden oder nicht auf verschlüsselte Daten zugreifen können.

1.1 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 Benutzercomputer, 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.

1.2 Challenge/Response Workflow

Während des Challenge/Response-Verfahrens wird ein Challenge-Code (eine ASCII-Zeichenkette) auf dem Benutzercomputer 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.

1.3 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 Helpdesk bietet für diese typischen Notfälle unterschiedliche Recovery- Workflows, die dem Benutzer wieder den Zugang zu seinem Computer ermöglichen.

1.4 Web Helpdesk 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 Helpdesk steht über das Internet/Intranet zur Verfügung. Es muss keine SafeGuard Enterprise Software auf dem Computer des Benutzers installiert sein. Die Webseiten werden separat auf einem Internet Information Services (IIS) basierten SafeGuard Enterprise Server bereitgestellt.

Web Helpdesk kann zusätzlich zum SafeGuard Management Center eingesetzt werden.

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

1.4.1 Web Helpdesk 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 volumen-basierender Verschlüsselung handelt oder um einen SafeGuard Enterprise Client mit BitLocker-Verschlüsselung und passt den Recovery-Ablauf entsprechend an.

1.5 Optionale Erweiterung: Web Self Help

SafeGuardWeb Self Help Web Self Help ist eine Erweiterung, die es Benutzern ermöglicht, Ihre eigenen Kennwörter selbständig zurückzusetzen, wenn Sie ihr SafeGuard Enterprise Kennwort vergessen haben. Dieser „Selbsthilfe“-Mechanismus reduziert die Anzahl an Helpdesk-Anforderungen zum Zurücksetzen eines Kennworts. Helpdesk-Mitarbeitern werden somit Routine-Aufgaben abgenommen und sie können sich auf komplexere Support-Anforderungen konzentrieren. Der Vorgang ist web-basiert und somit für alle Benutzer auf einfache Art und Weise zugänglich. Zusätzliche Software auf dem Benutzercomputer ist nicht erforderlich.

2 Installation

Web Helpdesk muss auf einem IIS-basierenden Web Server mit SafeGuard Enterprise Server installiert werden. Während der Installation von Web Helpdesk wird geprüft, ob SafeGuard Enterprise Server bereits auf dem Server zur Verfügung steht. Ist dies nicht der Fall, wird SafeGuard Enterprise Server automatisch in einem separation Application Pool „SGNWHDPool“ installiert. Nach der Installation von Web Helpdesk müssen Sie den Web Server konfigurieren.

Auf dem Computer des Web Helpdesk-Beauftragten muss nur ein Browser installiert sein.

2.1 Voraussetzungen

2.1.1 Voraussetzungen für Server

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

- Sie benötigen Windows Administratorrechte.
- Microsoft Internet Information Services (IIS) muss installiert sein.
- .NET Framework 3.0 Service Pack 1 mit ASP.NET 2.0 muss installiert sein.

2.1.2 Voraussetzungen für Clients

Auf dem Computer des Web Helpdesk-Beauftragten muss ein Browser installiert sein. Web Helpdesk unterstützt folgende Browser:

- Microsoft Internet Explorer 7.0
- Mozilla Firefox 2 und Firefox 3

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

2.2 Web Helpdesk installieren

Das Installationspaket SGNWebHelpDesk.msi finden Sie auf Ihrer Produkt-CD.

1. Starten Sie SGNWebHelpDesk.msi von der Produkt-CD.
2. Klicken Sie im Willkommen-Fenster auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung.
4. Wählen Sie einen Installationspfad aus.
5. Bestätigen Sie die erfolgreiche Installation.

Während der Einrichtung von Web Helpdesk 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 in einem separation Application Pool „SGNWHD-Pool“ installiert. Web Helpdesk wird auf dem IIS Server installiert.

2.2.1 Web Server sichern mit SSL

Zur Sicherheitsoptimierung sollte der IIS Server wie folgt konfiguriert werden:

1. Zugang zu Web Helpdesk ausschließlich über das Intranet

Stellen Sie sicher, dass Web Helpdesk ausschließlich über das Intranet Ihres Unternehmens zur Verfügung gestellt wird. Aus Sicherheitsgründen sollte Web Helpdesk nicht über das Internet zur Verfügung gestellt werden.

2. Herstellung einer SSL-Verbindung

Die Verfügbarkeit von Web Helpdesk 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 Helpdesk 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 Konfigurierung 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.

Weiterführende Informationen zur SSL-Einrichtung finden Sie unter den folgenden Links, oder wenden Sie sich an den Kundendienst.

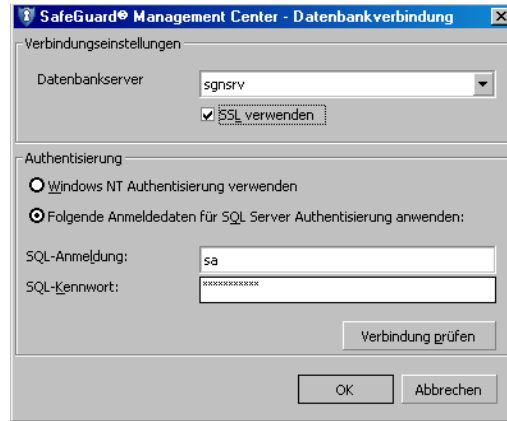
- <http://msdn2.microsoft.com/en-us/library/ms998300.aspx>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;316898>
- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

2.2.2 SafeGuard Enterprise Server konfigurieren und registrieren

Wenn SafeGuard Enterprise Server nicht bereits vor der Installation von Web Helpdesk installiert und registriert wurde, muss SafeGuard Enterprise Server nach dem Abschluss der Installation von Web Helpdesk im SafeGuard Management Center registriert werden.

1. Starten Sie das Management Center und wählen Sie in der Menüleiste **Extras > Konfigurationspakete**.
2. Wählen Sie **Server registrieren** und klicken Sie auf **Hinzufügen**.
3. Wählen Sie das Maschinenzertifikat des Servers. Es wird bei der Installation des SafeGuard Enterprise Servers erzeugt. Sie finden es standardmäßig im Verzeichnis `MachCert` des SafeGuard Enterprise Server Installationsverzeichnis. Es trägt den Dateinamen `<Computername>.cer`. Ist der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert, so muss diese `.cer`-Datei als Kopie oder Netzwerkfreigabe zugreifbar sein.
4. Der Server und die Servereigenschaften werden in der Registerkarte **Server registrieren** angezeigt.
5. Aktivieren Sie **Skripts ausführen**, wenn Sie den Skript-API nutzen möchten.

6. Klicken Sie auf **Datenbankverbindung** und dann auf [...], um die Verbindung zur Datenbank zu konfigurieren.



- Wählen Sie den gewünschten Datenbankserver aus, mit der der Web Helpdesk Server verbunden werden soll.
- Aktivieren Sie **SSL verwenden**, um die Verbindung zwischen Datenbank und dem ausgewählten Web Server mit SSL zu sichern.
- In Authentisierung legen Sie die Anmeldeinformationen für die ausgewählte Datenbank fest: **Windows Authentisierung** oder **SQL Authentisierung**.

Verwenden Sie **SQL Authentisierung** für Computer, die nicht Teil einer Domäne sind. Verwenden Sie ansonsten die Windows Authentisierung, die jedoch zusätzliche Konfiguration erfordert.

Wenn Sie **SQL Authentisierung** verwenden, empfehlen wir dringend, die Verbindung zur Datenbank mit SSL zu sichern, um den Transport der SQL-Anmeldeinformationen zu verschlüsseln.

- Prüfen Sie die Verbindung zum Datenbankserver. Selbst wenn die Prüfung nicht erfolgreich ist, kann ein neues Serverpaket erstellt werden.

Sie können die Eigenschaften und Einstellungen für jeden registrierten Server und seine Datenbankverbindung jederzeit aktualisieren. Sie müssen danach nur dafür sorgen, ein neues Serverpaket zu erstellen und es an den entsprechenden Server zu verteilen. Sobald das neue Serverpaket auf dem Server installiert ist, kann auf die neue Datenbankverbindung zugegriffen werden.

7. Wechseln Sie auf die Registerkarte Server-Paket erstellen.
8. Wählen Sie dort den gewünschten Server aus.
9. Legen Sie den Ausgabepfad fest.
10. Klicken Sie auf Server-MSI erstellen. Es wird unter dem Ausgabepfad eine .msi-Datei mit dem Namen `<Server>.msi` (im Beispiel `server.utimaco.edu.msi`) erzeugt.
11. Führen Sie diese neue .msi-Datei am SafeGuard Enterprise Server aus.

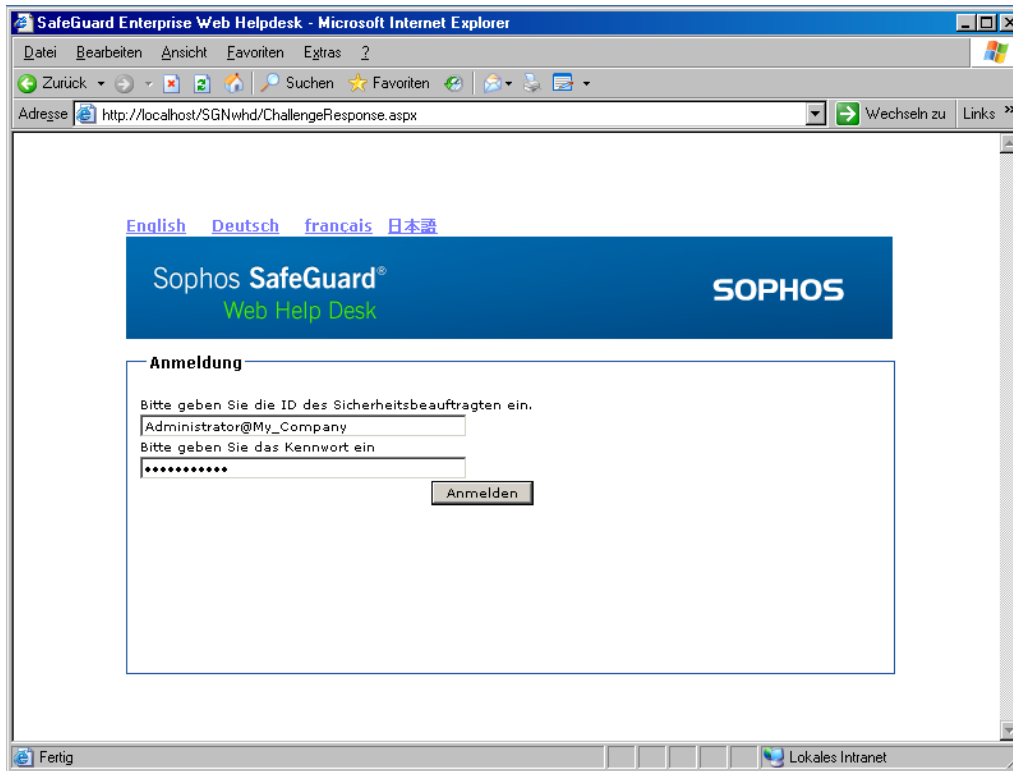
Der Computer ist als SafeGuard Enterprise Server registriert.

2.3 Web Helpdesk aktualisieren

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

2.4 Unterstützte Sprachen

Web Helpdesk unterstützt verschiedene Sprachen. Sie können die Sprache, in der die Anwendung angezeigt wird, dynamisch in der Anmeldemaske von Web Helpdesk 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 Helpdesk und am SafeGuard Enterprise Server anmelden. Sicherheitsbeauftragte melden sich mit ihrer Sicherheitsbeauftragten-ID und Ihrem Kennwort entsprechend ihren Windows-Anmeldeinformationen an Web Helpdesk an.

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

3.1 Vorbereitung im SafeGuard Management Center

Für den Zugang zu Web Helpdesk müssen folgende Voraussetzungen erfüllt sein und folgende vorbereitende Schritte im SafeGuard Management Center ausgeführt werden. Detaillierte Informationen hierzu finden Sie im SafeGuard Enterprise Administrationshandbuch.

1. Die Web Helpdesk 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 Helpdesk Benutzer müssen nun zu Sicherheitsbeauftragten gemacht werden. Jeder Benutzer, der aus einem Active Directory importiert wird, kann zu einem Sicherheitsbeauftragten gemacht werden.

Die neuen Sicherheitsbeauftragten können sich daraufhin mit ihrer definierten Sicherheitsbeauftragten-ID, einer Kombination aus Ihrem Windows-Benutzernamen und dem Namen der ihnen zugewiesenen Domäne, an Web Helpdesk 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 Helpdesk authentisieren können.

Die Voraussetzungen für eine erfolgreiche Anmeldung an Web Helpdesk sind erfüllt

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

3.2 An Web Helpdesk anmelden

Verfahren Sie wie folgt:

1. Starten Sie Ihren Browser.
2. Um die Anwendung in Ihrem Browser aufzurufen, geben Sie die URL ein:
`https://<Host-ID oder IP-Adresse>/SGNWHHD`



3. Geben Sie im Willkommen-Fenster Ihre Sicherheitsbeauftragten-ID genau so, wie sie im SafeGuard Management Center definiert ist, ein: <user name>@<DOMAIN> zum Beispiel WHDOfficer@MYDOMAIN

Bitte beachten Sie, dass bei der Eingabe zwischen Groß- und Kleinschreibung unterschieden wird. Stellen Sie daher sicher, dass der Name korrekt geschrieben ist.

Eine Liste mit Benutzernamen wird nicht zur Verfügung gestellt, um die Informationen vor nicht autorisierten Benutzern zu schützen.

4. Geben Sie Ihr Kennwort ein. Das für die Anmeldung notwendige Kennwort ist Ihr Windows-Kennwort.
5. Klicken Sie auf **Anmelden**

Der Web Helpdesk Recovery-Assistent wird gestartet.

4 Recovery-Typen

Folgende Recovery-Typen stehen zur Verfügung:

■ SafeGuard Enterprise Clients

Benutzercomputer, 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` von der Produkt-CD kann dann ein Challenge/Response-Verfahren auf dem Benutzercomputer 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.

■ SafeGuard Standalone Clients

Benutzercomputer, die lokal verwaltet werden. Diese Benutzercomputer haben niemals eine Verbindung zum SafeGuard Enterprise Server. Für jeden SafeGuard Standalone Client wird während der Konfiguration eine Recovery-Datei (.xml-Datei) erzeugt. Diese Datei enthält den definierten Computerschlüssel, der mit dem Unternehmenszertifikat verschlüsselt ist. Wenn diese Recovery-Schlüsseldatei (z. B. auf einem USB-Stick oder über eine freigegebenes Netzwerkverzeichnis) zur Verfügung steht, so dass der Helpdesk-Beauftragte darauf zugreifen kann, wird ein Challenge/Response-Verfahren für den SafeGuard Standalone Client unterstützt.

4.1 Recovery-Typ auswählen

Nach der erfolgreichen Anmeldung an Web Helpdesk können Sie den gewünschten Recovery-Typ auswählen.

5 Recovery für SafeGuard Enterprise Clients

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 Booten 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.

5.1 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. Ein Recovery-Aktion für Kennwörter ist nicht verfügbar.

5.1.1 Kennwort auf POA-Ebene wiederherstellen

Einer der am häufigsten auftretenden Notfälle 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-Bbeauftragte eine Response mit der Option **SGN Client mit Benutzeranmeldung booten**, jedoch ohne Anzeige des Benutzerkennworts. In diesem Fall startet der Computer nach Eingabe des Response-Codes bis zur Betriebssystemebene. Der Benutzer muss somit das Kennwort auf Windows-Ebene ändern, unter der Voraussetzung, dass Zugriff auf die Domäne besteht. 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, in erster Linie 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 Recovery über Local Self Help kann sich der Benutzer das aktuelle Kennwort anzeigen lassen und dieses weiterhin benutzen, ohne es zurücksetzen zu müssen. Bei der Benutzung von Local Self Help ist außerdem keine Unterstützung durch den Helpdesk erforderlich. Weitere Informationen finden Sie in der Administrator-Hilfe.

Wenn Sie Challenge/Response benutzen: 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 ist deswegen vorteilhaft, weil das Kennwort in diesem Fall nicht im Active Directory zurückgesetzt werden muss. Der Benutzer kann mit dem alten Kennwort weiterarbeiten und dieses später nach Wunsch lokal ändern.

5.1.2 Benutzerkennwort anzeigen

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.

5.1.3 Kennwort auf Windows-Ebene wiederherstellen

Benutzern kann der Zugriff auf ihren Computer auch auf Windows-Ebene verwehrt werden, z. B. nach einer Desktop-Sperre oder nach Abmelden und erneutem Anmelden am Betriebssystem. Der Helpdesk-Beauftragte generiert in diesem Fall eine Response mit der Anforderung **SGN Client ohne Benutzeranmeldung booten**.

Das Kennwort muss auch im Active Directory geändert werden.

1. Das Kennwort muss durch den Domänen-Support auf Windows-Ebene geändert werden.
2. Der Benutzer meldet sich an Windows mit dem neuen Kennwort an.
3. Beim nächsten Neustart wird ihm die Anmeldung an der POA verwehrt.

4. Er muss jetzt ein Challenge/Response-Verfahren starten und dem Helpdesk-Beauftragten das neue Kennwort mitteilen.
5. Der Helpdesk-Beauftragte muss folgende Aktionen im SafeGuard Management Center durchführen:
 - a) Benutzerzertifikat im Bereich **Benutzer & Computer** unter **Zertifikat** löschen.
 - b) Computer, an dem sich der Benutzer derzeit anzumelden versucht, im Bereich **Benutzer & Computer** unter **Benutzer** löschen.
6. Der Helpdesk-Beauftragte generiert dann eine Response für das Starten des Computers ohne Benutzeranmeldung.
7. Der Benutzer gibt die Response ein und meldet sich mit dem neuen Kennwort an Windows an.
8. Der Benutzer muss den Computer neu starten, um die Kennwortänderung auch auf POA-Ebene durchzuführen.

5.1.4 Zugriff auf Daten durch Booten von externem Medium

Mit Hilfe des Challenge/Response-Verfahrens lässt sich ein Computer auch von einem externen Medium wie WinPE booten. 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 Boot-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. Wie Sie eine solche Treiber-CD erhalten, erfahren Sie in der Wissensdatenbank unter:
<http://www.sophos.com/support/knowledgebase/article/108805.html>, suchen Sie nach SGN & Enterprise & Recovery.
- Der Benutzer muss von einem externen Medium booten und muss die hierzu erforderliche Berechtigung haben. Diese Berechtigung erteilt der Sicherheitsbeauftragte im SafeGuard Management Center, indem er eine Richtlinie erstellt und diese dem Client zuweist. (Richtlinie Authentisierung > Zugriff: Benutzer darf nur von Festplatte booten auf „Nein“ setzen). Standardmäßig ist die Berechtigung zum Booten von externen Medien nicht zugewiesen.
- Der Benutzercomputer muss den Boot-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 Client zugewiesen werden.

Hinweis: Bitte beachten Sie, dass bei Anwendung von externen Medien wie WinPE für den Zugriff auf ein verschlüsseltes Laufwerk der Zugriff auf das Volume nur teilweise gewährt wird.

5.1.5 SafeGuard Enterprise Policy-Cache wiederherstellen

Dieser Vorgang ist notwendig, wenn der SafeGuard Enterprise 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.

5.2 Response für SafeGuard Enterprise Clients erzeugen

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

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

1. Wählen Sie im Fenster **Recovery-Typ** die Option **SafeGuard Enterprise Client**.
2. Wählen Sie die Domäne aus der Liste aus.
3. Wählen Sie den Computernamen. Hierzu gibt es mehrere Möglichkeiten:
 - Wählen Sie einen 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 nun 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=Utlimaco,DC=edu
4. Klicken Sie auf **Weiter**.

Das Programm bestimmt nun automatisch, ob es sich um einen nativen SafeGuard Enterprise Client oder um einen BitLocker verschlüsselten SafeGuard Enterprise Client handelt, und passt den Recovery-Ablauf entsprechend an.

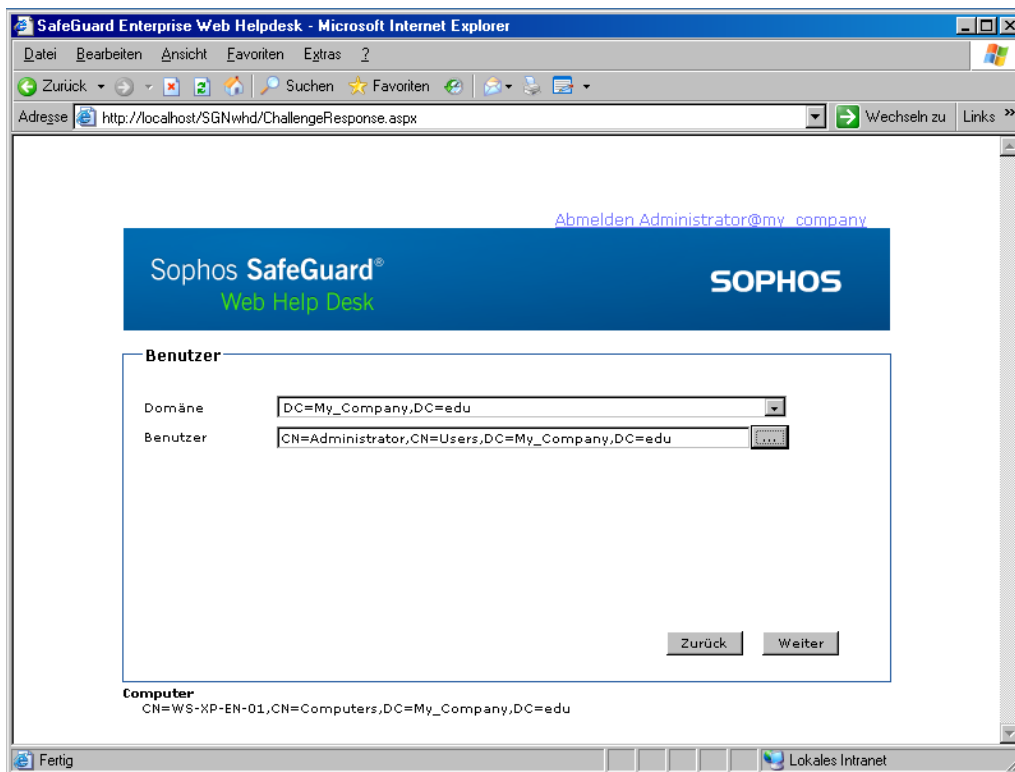
Im Falle eines nativen SafeGuard Enterprise Clients wird im nächsten Schritt die Auswahl der Benutzerinformationen verlangt.

Im Fall eines mit BitLocker verschlüsselten Computer, muss im nächsten Schritt das erforderliche Volume ausgewählt werden.

5.2.1 Response für native SafeGuard Enterprise Clients erzeugen

Im Falle eines nativen SafeGuard Enterprise Computers wird nach Auswahl des Computers in der Datenbank nun der entsprechende Benutzername und die Domäne für das Recovery eines SafeGuard Enterprise Clients benötigt.

1. Wählen Sie die Domäne des Benutzers.
2. Geben Sie den Benutzernamen ein. Hierfür gibt es mehrere Möglichkeiten:
 - Wählen Sie den Benutzernamen, indem Sie auf [...] und im Popup-Fenster auf **Suchen** klicken. Eine Liste mit Benutzernamen wird angezeigt. Wählen Sie den gewünschten Namen 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 Challenge-Code ein, den der Benutzer Ihnen genannt hat, und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft. Wenn er falsch eingegeben wurde, wird der Hinweis Ungültig unterhalb des fehlerhaften Blocks angezeigt.
5. Wenn der Challenge-Code korrekt eingegeben wurde, wird die vom SafeGuard Enterprise Client angeforderte Aktion sowie die möglichen Recovery-Aktionen auf dem Client angezeigt. Die möglichen Response-Aktionen richten sich nach den Aktionen, die auf Client-Seite beim Aufrufen der Challenge angefordert wurden. Wenn auf Client-Seite 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.
9. Ein Response-Code wird generiert. Teilen Sie den Response-Code dem Benutzer 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.

5.2.2 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. Nachdem der betreffende Computer in der Datenbank gefunden wurde, 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, aus der Liste aus und klicken Sie auf **Weiter**.
2. Der Recovery-Assistent zeigt nun den 48-stelligen Recovery-Schlüssel an. 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.

6 Recovery mit virtuellen Clients

Mit Recovery unter Verwendung virtueller Clients bietet SafeGuard Enterprise ein Recovery-Verfahren für verschlüsselte Volumes in komplexen Notfallsituationen

Das Recovery-Verfahren mit virtuellen Clients 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 auf 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 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:

Um in diesen Situationen ein Challenge/Response-Verfahren zu ermöglichen, können im SafeGuard Management Center spezifische Dateien, die als virtuelle Clients bezeichnet werden, erstellt und vor dem Challenge/Response-Verfahren an den Benutzer verteilt werden. Mit Hilfe dieser virtuellen Clients, dem Recovery-Tool RecoveryKeys.exe von der Produkt-CD sowie einem für SafeGaurd Enterprise angepassten WinPE kann dann ein Challenge/Response-Verfahren auf dem Benutzercomputer 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.

6.1 Recovery mit virtuellen Clients: Workflow

Hinweis: Ein detaillierte Beschreibung des Workflows finden Sie im SafeGuard Enterprise Administrationshandbuch.

Gehen Sie folgendermaßen vor:

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 recoverytoken.tok 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.
Als Referenz 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 Recovery-Tool zeigt dem Benutzer nun an, welche Volumes verschlüsselt sind und welche Schlüssel für die einzelnen Volumes verwendet wurden. Der Benutzer gibt diese Informationen an den Helpdesk-Beauftragten weiter.
4. Der Helpdesk-Beauftragte identifiziert den virtuellen Client in der Datenbank und wählt den erforderlichen Schlüssel aus: entweder einen einzelnen Schlüssel oder mehrere Schlüssel, die in eine Schlüsseldatei exportiert wurden. 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 wieder auf die verschlüsselten Volumes zugreifen.

6.2 Recovery-Aktionen mit virtuellen Clients

Um auf Volumes zuzugreifen, für die der Verschlüsselungsschlüssel dem Benutzer nicht zur Verfügung steht, 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

6.2.1 Einzelnen Schlüssel übertragen

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 Benutzercomputer 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.

6.2.2 Mehrere Schlüssel in einer verschlüsselten Schlüsseldatei übertragen

Die Challenge kann für die Bereitstellung eines einzelnen Schlüssels zum Zugriff auf ein verschlüsseltes Volume erzeugt werden. 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 Benutzercomputer 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.

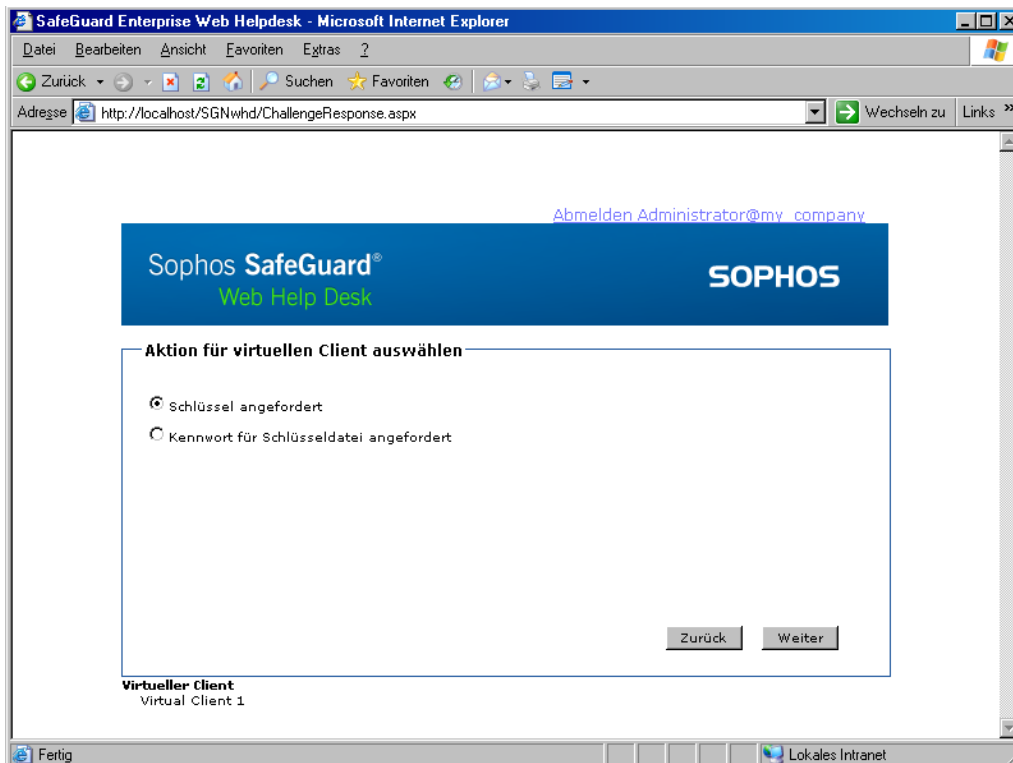
Die Schlüssel in der Schlüsseldatei werden in den Schlüsselspeicher auf dem Benutzercomputer importiert. Daraufhin kann auf alle mit den verfügbaren Schlüsseln verschlüsselten Volumes zugegriffen werden.

Hinweis: Bei der Benutzung von Web Helpdesk werden Schlüsseldateien und die entsprechenden Kennwörter nach der erfolgreichen Anwendung in einem Challenge/Response-Verfahren gelöscht.

Hinweis: In diesem Fall müssen Sie somit nach jedem erfolgreichen Challenge/Response-Verfahren eine neue Schlüsseldatei und ein neues Kennwort erzeugen.

6.3 Response mit virtuellen Clients

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



6.3.1 Voraussetzungen

Die folgenden Voraussetzungen müssen erfüllt sein:

- Der virtuelle Client muss im SafeGuard Management Center im Bereich Schlüssel & Zertifikate angelegt werden. Weitere Informationen hierzu finden Sie im Administrationshandbuch.
- 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 hierzu finden Sie im Administrationshandbuch.

- Der Benutzer muss das Schlüssel-Recovery Tool gestartet und das Challenge/Response-Verfahren eingeleitet haben.
- Eine Response-Code kann nur für zugewiesene Schlüssel erstellt werden. Ist ein Schlüssel nicht aktiv, d. h. nicht zumindest einem Benutzer zugewiesen, ist keine Response mit einem virtuellen Client möglich. In diesem Fall kann der nicht aktive Schlüssel einem beliebigen Benutzer zugewiesen werden. Daraufhin lässt sich wieder ein Response-Code für diesen Schlüssel erstellen.

6.3.2 Response mit virtuellen Clients erzeugen

Gehen Sie folgendermaßen vor:

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 mehrere 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 Namen 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 für die Auswahl der Recovery-Aktion wird angezeigt.
4. Wählen Sie den vom Benutzer durchzuführenden 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 die Schlüssel nach Schlüssel-ID oder symbolischem Namen anzeigen lassen. Klicken Sie auf **Suchen**, wählen Sie den Schlüssel aus 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 die Schaltfläche [...] und danach 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.

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. Wurde der Code nicht korrekt eingegeben, so wird unterhalb des Blocks, der den Eingabefehler enthält, der Hinweis 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 an seinem 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.

7 Recovery für SafeGuard Standalone Clients

SafeGuard Enterprise bietet auch ein Challenge/Response-Verfahren für SafeGuard Standalone Clients. SafeGuard Standalone Clients 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 SafeGuard Standalone Clients basiert daher auf der Recovery-Schlüsseldatei, die während der Konfiguration des Standalone Clients erstellt wird. Die Recovery-Datei (.xml-Datei) wird für jeden SafeGuard Standalone Clients 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.

7.1 Recovery-Aktionen für SafeGuard Standalone Clients

Ein Challenge/Response-Verfahren für einen SafeGuard Standalone Client 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 SafeGuard Standalone Client 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.

7.1.1 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.

7.1.2 Der Benutzer hat das Kennwort vergessen

Hinweis: Wir empfehlen, in erster Linie Local Self Help einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Mit Recovery über Local Self Help kann sich der Benutzer selbst das aktuelle Benutzerkennwort unter Wahrung der Vertraulichkeit in der Power-on Authentication anzeigen lassen und es weiterhin zur Anmeldung verwenden. Für weitere Informationen. 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 Booten des Computers durch die Power-on Authentication.
2. Da dem Benutzer das Kennwort nicht bekannt ist, kann er es im Windows-Dialog 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-Kennworrücksetz-DisketteAls Helpdesk-Beauftragte sollten Sie den Benutzer darüber informieren, welche Methode benutzt werden soll, und 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 Sophos SafeGuard 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. Da beim Zurücksetzen eines Kennworts ohne Angabe des alten Kennworts in SafeGuard Enterprise ein neues Zertifikat generiert werden muss, muss der Benutzer diesen Vorgang bestätigen.
6. Ein neues Benutzerzertifikat wird basierend auf dem neu gewählten Windows-Kennwort erstellt. 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 für SafeGuard Data Exchange generierte Benutzerschlüssel weiterhin verwendet werden können, müssen dem Benutzer die SafeGuard Data Exchange Passphrasen zur Reaktivierung dieser Schlüssel bekannt sein.

7.2 Response für SafeGuard Standalone Clients erzeugen

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. Als Helpdesk-Bbeauftragter wählen Sie im Fenster **Recovery-Typ** die Option **Standalone Client**.
2. Klicken Sie auf **Browse**, um die erforderliche Recovery-Datei (.xml-Datei) auszuwählen.

3. Sie werden aufgefordert, den vom Benutzer erhaltenen Challenge-Code einzugeben. Geben Sie den Challenge-Code ein.
4. Wählen Sie den vom Benutzer durchzuführenden Recovery-Aktion und klicken Sie dann auf **Weiter**.
5. Ein Response-Code wird erzeugt. Teilen Sie diesen dem Benutzer mit. Hierzu können Sie eine Buchstabierhilfe verwenden oder den Response-Code in die Zwischenablage kopieren.

Der Benutzer kann den Response-Code eingeben und wieder auf den Computer zugreifen.

8 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

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

9 Copyright

Copyright © 1996 - 2010 Sophos Group und Utimaco Safeware AG. 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 ein eingetragenes Warenzeichen von Sophos Plc und der Sophos Group. SafeGuard ist ein eingetragenes Warenzeichen von Utimaco Safeware AG - a member of the Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber.

Alle SafeGuard Produkte unterliegen dem Urheberrecht der Utimaco Safeware AG - a member of the Sophos Group, oder, sofern anwendbar, ihrer Lizenzinhaber. Alle weiteren Sophos Produkte unterliegen dem Urheberrecht der Sophos Plc oder, sofern anwendbar, ihrer Lizenzinhaber.

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