SOPHOS
Security made simple.

SafeGuard Enterprise
Web Helpdesk

Produktversion: 7
Stand: Dezember 2014

Inhalt

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 Helpdesk 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, 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 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 Endpoint berechtigt.

Typische Notfälle, in denen Hilfe beim Helpdesk angefordert wird

- Ein Benutzer hat sein Kennwort für die Anmeldung vergessen. Der Endpoint 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 Endpoint zugreifen.
- Ein Benutzer möchte auf ein Volume zugreifen, das mit einem Schlüssel verschlüsselt ist, der auf dem Endpoint nicht verfügbar ist.

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

2 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 ist über das Internet/Intranet verfügbar ohne dass SafeGuard Enterprise Software am Helpdesk Endpoint installiert sein muss. 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.

Web Helpdesk bietet Recovery für:

- Mit SafeGuard verschlüsselte Endpoints (SafeGuard Enterprise Clients, Managed)
- Virtuelle Clients
- Mit SafeGuard verschlüsselte Endpoints (SafeGuard Enterprise Clients, Standalone)

3 Installation

Web Helpdesk muss auf einem IIS-basierenden Web Server mit SafeGuard Enterprise Server installiert werden. Wenn SafeGuard Enterprise Server nicht verfügbar ist, dann wird der Benutzer aufgefordert, ihn zu installieren. 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.

3.1 Voraussetzungen

Voraussetzungen für den 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 4 mit ASP.NET 4 muss installiert sein.
- Für Windows Server 2012: Die Rolle ASP.NET muss installiert sein (Serverrollen > Webserver (IIS) > Web Server > Anwendungsentwicklung > ASP.NET 4.5).

Hinweis: Auf Windows Server 2012 trifft Folgendes zu: ASP.NET Applikationen sind vorkonfiguriert mit einem Handler-Abschnitt im web.config. Innerhalb der Delegierung von Features im IIS ist das auf schreibgeschützt gesetzt. Im IIS-Manager überprüfen Sie das unter Servername > Delegierung von Features. Wenn die Handler-Mappings auf schreibgeschützt gesetzt sind und Ihre web.configs einen Handler-Abschnitt haben, ändern Sie den Wert auf lesen/schreiben.

Voraussetzungen für den Endpoint

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

- Microsoft Internet Explorer 7 und höher
- Mozilla Firefox 2 und höher

3.2 Installation von Web Helpdesk

Das Installationspaket SGNWebHelpDesk.msi finden Sie in Ihrer Produktlieferung.

1. Doppelklicken Sie auf SGNWebHelpDesk.msi. Ein Assistent führt Sie durch die Installation. Übernehmen Sie nach Möglichkeit die Standardeinstellungen. Wenn Sie dazu aufgefordert werden, wählen Sie eine **Vollständige Installation** aus.
2. Nach der Installation ist eventuell ein Neustart erforderlich. Klicken Sie auf **Ja** oder **Fertigstellen**.

Während der Einrichtung von Web Helpdesk wird geprüft, ob SafeGuard Enterprise Server bereits auf dem IIS Server zur Verfügung steht. Wenn er nicht verfügbar ist, werden Sie dazu aufgefordert, ihn zu installieren.

3.2.1 Konfigurieren des Web Servers mit SSL

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

1. Zugang zu Web Helpdesk ausschließlich über das Intranet.

   Stellen Sie Web Helpdesk ausschließlich über das Intranet Ihres Unternehmens zur Verfügung. Stellen Sie aus Sicherheitsgründen Web Helpdesk nicht über das Internet zur Verfügung.

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 Kommunikation mit Web Helpdesk erfolgt dann über SSL.

   Folgende allgemeine Schritte sind auszuführen, 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 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 Helpdesk 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;de-de;316898
- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

3.2.2 Registrieren und Konfigurieren des SafeGuard Enterprise Servers

Wenn SafeGuard Enterprise Server nicht bereits vor der Installation von Web Helpdesk 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** 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 installiert ist als das SafeGuard Management Center, dann muss diese **`.cer`**-Datei über eine Netzwerkfreigabe oder als Kopie zugänglich sein.

   Wählen Sie nicht das MSO-Zertifikat.

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

   Wenn SSL als Tansportverschlüsselung zwischen Endpoint und SafeGuard Enterprise Server verwendet werden soll, muss der Servername, den Sie hier eingeben, mit dem Servernamen übereinstimmen, den Sie im SSL-Zertifikat vergeben haben. Andernfalls ist keine Kommunikation möglich.

5. Klicken Sie auf **OK**.

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

6. Klicken Sie auf die Registerkarte **Server-Pakete**. 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** 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** jederzeit ändern.

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

3.3 Aktualisieren von Web Helpdesk

Wenn Sie eine ältere Version von Web Helpdesk auf die aktuelle Version aktualisieren möchten, empfehlen wir Ihnen, Web Helpdesk zunächst zu deinstallieren und dann die aktuelle Version von Web Helpdesk zu installieren. Das Server-Konfigurationspaket muss nur dann neu erzeugt werden, wenn die Servereinstellungen geändert wurden.

3.4 Unterstützte Sprachen

Web Helpdesk unterstützt mehrere 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.

4 Web Helpdesk Logon für Benutzer ohne installiertem SafeGuard Enterprise Client erlauben

Es ist möglich, Web Helpdesk zu verwenden, ohne eine SafeGuard Enterprise Client installiert zu haben.

Zugriffsrechte können durch Hinzufügen oder Entfernen von Windows Benutzern oder Gruppen verwaltet werden.

Hinweis:

Diese Funktionalität verwendet Windows Authentisierung. Wenn Windows Authentisierung aktiviert ist, dann ist eine herkömmliche Anmeldung über einen höhergestuften Active Directory-Benutzer nicht länger möglich.

4.1 Voraussetzungen für die Anmeldung ohne SafeGuard Enterprise Client

Folgende Voraussetzungen müssen erfüllt sein:

1. Eine Windows Benutzergruppe muss eingerichtet und konfiguriert sein. Sie enthält Benutzer, die berechtigt sind, auf Web Helpdesk zuzugreifen (siehe *SafeGuard Enterprise Administratorhilfe*).
2. Windows Authentication beim Web Helpdesk muss aktiviert sein (**Extras - Konfigurationspakete - Registerkarte "Servers" - Win. Auth. WHD**; nähere Informationen finden Sie in der *SafeGuard Enterprise Installationsanleitung*).

4.2 Aktivieren der Windows Authentifizierung für die SafeGuard Web Helpdesk Anwendung

1. Öffnen Sie das Internetinformationsdienste (IIS) Manager Fenster.
2. Wählen Sie unter **Sites** > **Default Web Site** den Benutzerknoten, z.B. SGNWHD.
3. Wählen Sie **Authentifizierung**.
4. Wählen Sie den Eintrag **Windows-Authentifizierung** in der Liste Authentifizierung.
5. Klicken Sie **Aktivieren** in der Leiste **Aktionen** rechts.
6. Dann wählen Sie **.NET Autorisierungsregeln** aus, um drei .NET Autorisierungsregeln hinzuzufügen.

   Hinweis: In Windows Server 2008 gibt es kein Symbol im IIS für **.Net Autorisierungsregeln**. Hier ist es ein **Autorisierungsregeln** Link. Um diese Regeln bearbeiten zu können, sollte die Serverrolle **URL Authorization** installiert werden. Dazu wählt man im Server-Manager **IIS** > **Security** > **URL Authorization** aus.

7. Klicken Sie in der Leiste **Aktionen** auf **Ablehnungsregel hinzufügen...**.
8. Ein Dialog öffnet sich. Verweigern Sie den Zugriff indem Sie **Alle anonymen Benutzer** aktivieren. Bestätigen Sie mit **OK**.

9. Kehren Sie zur Leiste **Aktionen** zurück und klicken Sie auf **Zulassungsregel hinzufügen...**.
10. Ein Dialog öffnet sich. Aktivieren Sie **Bestimmte Rollen oder Benutzergruppen** und geben Sie Ihren Benutzergruppennamen inklusive Domänennamen in das Feld ein (z.B. <Domänenname>\WHD Benutzer), um Ihrer spezifischen Benutzergruppe den Zugriff zu erlauben.
11. Bestätigen Sie mit **OK**.
12. Kehren Sie zur Leiste **Aktionen** zurück und klicken Sie auf **Ablehnungsregel hinzufügen...**.
13. Ein Dialog öffnet sich. Aktivieren Sie **Alle Benutzer**, um den Zugriff für alle Benutzer zu verweigern. Bestätigen Sie mit **OK**.
14. Kontrollieren Sie die Reihenfolge der Einträge:
    - Verweigern - Anonyme Benutzer - Lokal
    - Zulassen - <Domänenname\Gruppenname> - Lokal
    - Verweigern - Alle Benutzer - Lokal
    - Zulassen - Alle Benutzer - Geerbt

Um die Funktionalität zu testen, melden Sie sich an, wie in Anmeldung mit aktivierter Windows Authentisierung (Seite 9) beschrieben. Der Willkommensbildschirm sollte erscheinen.

Wenn Sie Windows Authentifizierung deaktivieren wollen, um herkömmliche Anmeldung über einen höhergestuften Active Directory-Benutzer zu erlauben, entfernen Sie die Regel **Verweigern - Anonyme Benutzer.**

Hinweis: Sie können Windows Authentifizierung auch aktivieren, indem Sie die web.config Datei ändern. Zum Beispiel:

```
<configuration>
  <system.web>
    <authentication mode="Windows" />
     <authorization>
      <allow roles="HelpDesk" />
      <deny users="*" />
     </authorization>
  </system.web>
</configuration>
```

4.3 Anmeldung mit aktivierter Windows Authentisierung

Gehen Sie wie folgt vor:

1. Öffnen Sie den Browser und geben Sie die URL ein.
2. Um die Anwendung in Ihrem Browser aufzurufen, geben Sie folgende URL ein: **`https://<Host ID oder IP Adresse>/SGNWHD`**
3. Wählen Sie die erforderliche Option **Recovery** oder **Deaktivierung erlauben** und gehen Sie wie in Recovery-Typen - Übersicht (Seite 13) und den nachfolgenden Abschnitten beschrieben vor.

5 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 ihrem Sicherheitsbeauftragtennamen und Ihrem Kennwort entsprechend ihren Windows-Anmeldeinformationen an Web Helpdesk an.

Für Benutzer gibt es zwei Möglichkeiten zur Authentisierung:

- Benutzer, die zu Sicherheitsbeauftragten im SafeGuard Management Center höhergestuft wurden, melden sich an wie es beschrieben ist unter Anmeldung an Web Helpdesk ohne aktivierter Windows Authentisierung (Seite 10).
- Benutzer, die zu einer Web Helpdesk Benutzergruppe mit aktivierter Windows Authentisierung zugewiesen sind, melden sich an wie unter Anmeldung mit aktivierter Windows Authentisierung (Seite 9). beschrieben.

5.1 Vorbereitung im SafeGuard Management Center

Um sich ohne aktivierter Windows Authentisierung an Web Helpdesk anmelden zu können, müssen die folgenden Voraussetzungen erfüllt sein und die folgenden Vorbereitungen im SafeGuard Management Center getroffen werden. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Administrator-Hilfe*.

1. Die Web Helpdesk Benutzer müssen aus einem Active Directory in die SafeGuard Enterprise Datenbank importiert werden.
2. Benutzerzertifikate müssen diesen Benutzern zugewiesen oder für sie importiert werden und die Zertifikate (**`.p12`** Datei) müssen in der Datenbank verfügbar sein.
3. Künftige Web Helpdesk Benutzer müssen zu Sicherheitsbeauftragten gemacht werden.

   Die neuen Sicherheitsbeauftragten können sich daraufhin mit ihrem definierten Sicherheitsbeauftragtennamen, 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.
5. Darüber hinaus benötigen sie Zugriffsrechte für die Objekte, mit denen sie arbeiten müssen, z. B. Domains oder Organisationseinheiten. Weitere Informationen finden Sie in der *SafeGuard Enterprise Administratorhilfe* im Kapitel *Zuweisen von Verzeichnisobjekten zu einem Sicherheitsbeauftragten*.

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

5.2 Anmeldung an Web Helpdesk ohne aktivierter Windows Authentisierung

1. Starten Sie Ihren Browser.

2. Um die Anwendung in Ihrem Browser aufzurufen, geben Sie folgende URL ein: **`https://<Host ID oder IP Adresse>/SGNWHD`**
3. Geben Sie auf der Seite **Willkommen** Ihren Sicherheitsbeauftragten-Namen so ein, wie er im SafeGuard Management Center definiert ist: **`<Benutzername>@<DOMÄNE>`** zum Beispiel **`WHDOfficer@MYDOMAIN`**

   Achten Sie bei der Eingabe auf Groß- und Kleinschreibung. Stellen Sie sicher, dass der Benutzername korrekt geschrieben ist.

4. Geben Sie Ihr Windows-Kennwort ein.
5. Klicken Sie auf **Anmelden**.

Sie werden an Web Helpdesk angemeldet.

Hinweis: Wenn das Zertifikat erstellt wird, wenn Benutzer höhergestuft werden, müssen sie das Kennwort des Zertifikats verwenden, um sich am SafeGuard Management Center anzumelden. Es ist das Kennwort des Zertifikats einzugeben, obwohl nach dem Windows Kennwort gefragt wird.

6 Auswählen des Web Helpdesk Assistenten

1. Führen Sie auf der Seite **Home** einen der folgenden Schritte aus:
   - Um Recovery-Aktionen auf Endpoints zu autorisieren, wählen Sie **Recovery** (siehe Recovery-Typen - Übersicht (Seite 13)).
   - Um die Deaktivierung der SafeGuard Configuration Protection Richtlinie auf Endpoints zu autorisieren, wählen Sie **Deaktivierung erlauben**, siehe SafeGuard Configuration Protection (Seite 25).

7 Recovery-Typen - Übersicht

Sie können den angeforderten Recovery-Typ auswählen. Folgende Recovery-Typen stehen zur Verfügung:

- **SafeGuard Enterprise Clients (managed)**

  Recovery für die Anmeldung für zentral durch das SafeGuard Management Center verwaltete Endpoints. Zentral verwaltete Endpoints 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 werden, 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 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 Clients (Standalone)**

  Recovery für die Anmeldung für lokal verwaltete Endpoints. Diese Endpoints haben nie eine Verbindung zum SafeGuard Enterprise Server. Für jeden lokal verwalteten Sophos SafeGuard Endpoint 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.

8 Recovery für zentral verwaltete Endpoints (SafeGuard Enterprise Clients, Managed)

SafeGuard Enterprise bietet ein Recovery-Verfahren für durch SafeGuard Enterprise geschützte, zentral verwaltete Endpoints (Managed) in verschiedenen Disaster Recovery-Szenarien, z. B. Kennwort-Recovery oder Zugriff auf Daten durch Starten von einem externen Medium.

Das Programm bestimmt automatisch, ob die SafeGuard Enterprise Festplattenverschlüsselung oder die BitLocker Verschlüsselung angewendet wird und passt den Recovery Workflow entsprechend an.

8.1 Recovery-Aktionen für zentral verwaltete Endpoints

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

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

8.1.1 Wiederherstellen des Kennworts auf POA-Ebene

Eines 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 Endpoint 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 Endpoint jedoch nach Eingabe des Response-Codes bis zur Betriebssystemebene. Der Benutzer muss somit gemäß den auf der Domäne festgelegten Bedingungen 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

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 Rücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Administratorhilfe*.

- **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 darüber informiert ist.

Erzeugen Sie als SafeGuard Enterprise Helpdesk-Beauftragter eine Response für das **Booten des SGN Clients mit Benutzeranmeldung** mit der Option **Benutzerkennwort anzeigen**. Auf diese Weise wird vermieden, dass das Kennwort für den Benutzer in Active Directory zurückgesetzt werden muss. Der Benutzer kann mit dem vorhandenen Kennwort weiterarbeiten und dieses später nach Wunsch lokal ändern.

8.1.2 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 booten** gestellt wird.

8.1.3 Zugriff auf Daten durch Starten des Endpoints von externen Medien

Mit Hilfe des Challenge/Response-Verfahrens lässt sich ein Endpoint 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.com/de-de/support/knowledgebase/108805.aspx
- Der Benutzer muss den Endpoint von einem externen Medium starten. Diese Berechtigung wird erteilt, indem man im SafeGuard Management Center eine Richtlinie erstellt und diese dann dem Endpoint zuweist (Richtlinientyp **Authentisierung > Zugriff: Benutzer kann nur von interner Festplatte booten** muss auf **Nein** eingestellt sein).
- Der Endpoint muss das Starten von einem externen Medium erlauben.
- 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.

8.1.4 Wiederherstellen des SafeGuard Enterprise Policy-Cache

Ist der SafeGuard Enterprise Policy Cache beschädigt, so wird der Benutzer automatisch bei der Anmeldung an der Power-on Authentication dazu aufgefordert, ein Challenge/Response-Verfahren zu starten.

8.2 Erzeugen einer Response für zentral verwaltete Computer

Für das Erzeugen einer Response für zentral verwaltete Computer (SafeGuard Enterprise Clients) sind der Computername und der Domänenname erforderlich.

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. Hierzu 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 Computername 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 Computername 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=com`

4. Klicken Sie auf **Weiter**.

Das Programm bestimmt dann automatisch, ob die SafeGuard Enterprise Festplattenverschlüsselung oder die BitLocker Verschlüsselung auf dem Computer angewendet wird und passt den Recovery Workflow entsprechend an.

- Im Falle eines durch SafeGuard Enterprise geschützten Computers wird im nächsten Schritt die Auswahl der Benutzerinformationen verlangt.
- Im Falle eines durch BitLocker verschlüsselten Computers lässt sich ein Volume, auf das nicht mehr zugegriffen werden kann, wiederherstellen. Im nächsten Schritt muss das Volume, das entschlüsselt werden soll, ausgewählt werden.

8.2.1 Erzeugen einer Response für durch die SafeGuard Enterprise Festplattenverschlüsselung geschützte Computer

1. Wählen Sie unter **Domäne** die Domäne des Benutzers. Wählen Sie für einen lokalen Benutzer **Lokaler Benutzer auf <Computername>**.
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 Endpoint angezeigt. Die verfügbaren Response-Aktionen richten sich nach den Aktionen, die auf dem Endpoint beim Aufrufen der Challenge angefordert wurden. Wenn zum Beispiel **Crypto Token erforderlich** erforderlich ist, 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**, wie oben beschrieben, als Response-Aktion ausgewählt haben, können Sie zusätzlich auch die Option **Benutzerkennwort anzeigen** wählen, um das Kennwort auf dem Ziel-Endpoint 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 auf dem Endpoint eingeben und die autorisierte Aktion durchführen.

8.2.2 Erzeugen einer Response für durch BitLocker Drive Encryption geschützte Computer

1. Wählen Sie das Volume, auf das zugegriffen werden soll, und klicken Sie auf **Weiter**. Der Recovery-Assistent 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 Endpoint wiederherzustellen.

9 Recovery mit virtuellen Clients

Unter Verwendung virtueller Clients für Recovery-Vorgänge in SafeGuard Enterprise lässt sich der Zugriff auf verschlüsselte Volumes auch in komplexen Recovery-Situationen 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 Endpoint übertragen werden.

Hinweis: Recovery mit virtuellen Clients sollte nur in komplexen Recovery-Situationen angewendet werden. Nur wenn beide der oben genannten Sachverhalte eingetreten sind, ist ein Recovery-Vorgang mit virtuellen Clients angebracht. Wenn jedoch zum Beispiel nur der benötigte Schlüssel 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 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 Helpdesk wird Recovery mit virtuellen Clients nicht für Standalone-Endpoints (Sophos SafeGuard Client Standalone) unterstützt. Benutzen Sie stattdessen das SafeGuard Management Center.

9.1 Recovery Workflow mit virtuellen Clients

Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Administrator-Hilfe*.

1. Der Helpdesk-Beauftragte legt den virtuellen Client im Bereich **Schlüssel und Zertifikate** des SafeGuard Management Centers an und exportiert ihn in eine Datei. 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 muss dann eine SafeGuard Enterprise Recovery-CD oder eine andere CD mit einem von SafeGuard Enterprise modifizierten WinPE ohne POA-Anmeldung starten und ein Challenge/Response-Verfahren starten.

   In der SafeGuard Enterprise Datenbank wird die Recovery-Datei des virtuellen Client benutzt. Diese wird in der Challenge anstelle des Benutzer-/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 gibt diese Informationen an den Helpdesk-Beauftragten weiter.

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 wieder auf die verschlüsselten Volumes zugreifen.

9.2 Recovery-Aktionen mit virtuellen Clients

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

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

- Übertragen eines einzelnen Schlüssels
- Mehrere Schlüssel in einer verschlüsselten Schlüsseldatei übertragen

9.2.1 Übertragen eines einzelnen Schlüssels

Challenge/Response kann für die Bereitstellung eines einzelnen Schlüssels zum Zugriff auf ein verschlüsseltes Volume initialisiert 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 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.

9.2.2 Übertragen mehrerer Schlüssel in einer verschlüsselten Schlüsseldatei

Challenge/Response kann für die Bereitstellung eines einzelnen Schlüssels zum Zugriff auf ein verschlüsseltes Volume initialisiert 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 wird jeder angelegten Schlüsseldatei eindeutig zugewiesen.

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 Ziel-Endpoint 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 Ziel-Endpoint übertragen. Die Schlüsseldatei kann dann mit dem Kennwort entschlüsselt werden.

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

Hinweis: Bei der Anwendung von Web Helpdesk 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.

9.3 Response mit virtuellen Clients

9.3.1 Voraussetzungen

- Der virtuelle Client muss im SafeGuard Management Center im Bereich **Schlüssel und Zertifikate** angelegt werden. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise 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 und 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 in der *SafeGuard Enterprise Administratorhilfe*.
- 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.

9.3.2 Erzeugen einer Response mit virtuellen Clients

1. Als Helpdesk-Beauftragter wählen Sie auf der Seite **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**. Die Seite, auf der 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 benötigten 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 in **Schlüssel und Zertifikate** angelegt wurde und das Kennwort, mit dem die Datei verschlüsselt ist, in der Datenbank gespeichert wurde. Bei der Anwendung von Web Helpdesk 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**. Die Seite 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 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.

10 Recovery für Standalone-Endpoints (Sophos SafeGuard Clients Standalone)

SafeGuard Enterprise bietet auch ein Challenge/Response-Verfahren für Standalone-Endpoints (Sophos SafeGuard Clients Standalone). Diese Endpoints haben nie 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 Identifikationsdaten, die für ein Challenge/Response-Verfahren benötigt werden, zur Verfügung.

Das Challenge/Response-Verfahren für Standalone-Endpoints basiert daher auf der während der Endpoint-Konfiguration erstellten Recovery-Schlüsseldatei. Die Recovery-Datei (.xml-Datei) wird für jeden Standalone-Endpoint 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. auf einem USB-Stick oder in einem freigegebenen Netzwerkverzeichnis, kann eine Response generiert werden.

10.1 Recovery-Aktionen für Standalone-Endpoints

Ein Challenge/Response-Verfahren für Standalone-Endpoints (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 Local Cache muss repariert werden.

Für Standalone-Endpoints steht kein Benutzerschlüssel in der Datenbank zur Verfügung. Somit ist in einem Challenge/Response-Verfahren nur die Recovery-Aktion **Sophos SafeGuard 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.

10.1.1 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 Endpoint wieder benutzen.

10.1.2 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 Rücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise 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 Kennwort 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.

10.2 Erzeugen einer Response für Standalone-Computer

Um eine Response für einen Standalone-Computer zu erzeugen, wird der Name der Recovery-Datei (.xml-Datei) benötigt.

1. Wählen Sie in Web Helpdesk 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.

11 SafeGuard Configuration Protection

Das Modul SafeGuard Configuration Protection ist ab SafeGuard Enterprise 6.1 nicht mehr verfügbar. Die entsprechende Richtlinie ist im SafeGuard Management Center 6.1 noch verfügbar, um SafeGuard Enterprise 6.x Clients mit installierter Configuration Protection zu unterstützen, die über ein 6.1 Management Center verwaltet werden.

Nähere Informationen zu SafeGuard Configuration Protection finden Sie im *SafeGuard Enterprise 6 Web Helpdesk* Handbuch: http://www.sophos.com/de-de/medialibrary/PDFs/documentation/sgn_60_m_eng_web_helpdesk.pdf.

12 Protokollierung von Web Helpdesk Ereignissen

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

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

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

12.1 Aktivieren der Protokollierung von Web Helpdesk Ereignissen

Die Protokollierung für Web Helpdesk wird im SafeGuard Management Center konfiguriert.

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

1. Erzeugen Sie eine Richtlinie des Typs **Protokollierung** im SafeGuard Management Center im **Richtlinien** Navigationsbereich. 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 **Pakete für Managed Clients** 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 Helpdesk Server befindet. Aktivieren Sie nun die Richtlinie. Detaillierte Informationen hierzu finden Sie im Kapitel *Zuweisen von Richtlinien* der *SafeGuard Enterprise Administrator-Hilfe*.
5. Installieren Sie auf dem Web Helpdesk Server das zuvor erstellte Konfigurationspaket. Starten Sie den Service neu.

   Die Protokollierung von Web Helpdesk Ereignissen ist aktiviert.

6. Melden Sie sich an Web Helpdesk 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 Helpdesk protokollierten Ereignisse einzusehen.

13 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie die SophosTalk-Community unter community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation/ herunter.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/support/contact-support/support-query.aspx.

14 Rechtliche Hinweise