



# **Streamvault™-Appliance – Benutzerhandbuch**

Klicken Sie [hier](#) für die neueste Version dieses Dokuments.

Dokument zuletzt aktualisiert: 5. Juni 2025

# Rechtliche Hinweise

---

©2025 Genetec Inc. Alle Rechte vorbehalten.

Genetec Inc. vertreibt dieses Dokument mit Software, die einen Endbenutzer-Lizenzvertrag umfasst; sie wird unter Lizenz bereitgestellt und darf nur in Übereinstimmung mit den Bedingungen der Lizenzvereinbarung verwendet werden. Die Inhalte dieses Dokuments sind urheberrechtlich geschützt.

Die Inhalte dieses Handbuchs dienen ausschließlich Informationszwecken und können ohne Vorankündigung geändert werden. Genetec Inc. übernimmt keinerlei Verantwortung oder Haftung für eventuelle inhaltliche Fehler oder Ungenauigkeiten in diesem Handbuch.

Diese Publikation darf nicht kopiert, verändert oder in irgendeiner Form oder für irgendeinen Zweck reproduziert werden, noch dürfen ohne die vorherige schriftliche Genehmigung von Genetec Inc. aus dieser Publikation abgeleitete Werke erstellt werden.

Genetec Inc. behält sich das Recht vor, nach eigenem Ermessen Änderungen und Verbesserungen an seinen Produkten vorzunehmen. Dieses Dokument beschreibt den Status eines Produkts zum Zeitpunkt der letzten Dokumentenüberarbeitung und entspricht nicht unbedingt dem neuesten Produktstand.

Genetec Inc. haftet in keinem Fall gegenüber natürlichen oder juristischen Personen für Verluste oder Schäden, die zufällig oder infolge der in diesem Dokument oder in der Computer-Software beschriebenen Anweisungen und der hier beschriebenen Hardware entstehen.

Genetec™, AutoVu™, AutoVu MLC™, Citywise™, Cloud Link Roadrunner™, Community Connect™, Curb Sense™, Federation™, Flexreader™, Genetec Airport Sense™, Genetec Citigraf™, Genetec Clearance™, Genetec ClearID™, Genetec Cloudlink™, Genetec Mission Control™, Genetec Motoscan™, Genetec Patroller™, Genetec Retail Sense™, Genetec Traffic Sense™, KiwiVision™, KiwiSecurity™, Omnicast™, Privacy Protector™, Sipelia™, Stratocast™, Streamvault™, Streamvault Edge™, Synergis™, Valcri™ und ihre Logos sowie das Möbiusbandlogo sind Warenzeichen von Genetec Inc. und können in verschiedenen Gerichtsbarkeiten registriert oder zur Registrierung angemeldet sein.

Bei anderen, in diesem Dokument erwähnten Warenzeichen kann es sich um Warenzeichen oder registrierte Warenzeichen der Hersteller oder Anbieter der jeweiligen Produkte handeln.

Patent angemeldet. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™ und andere Produkte von Genetec™ wurden zum Patent angemeldet und können Gegenstand erteilter Patente sein, in den Vereinigten Staaten und in anderen Gerichtsbarkeiten weltweit.

Alle Spezifikationen können ohne vorherige Ankündigung geändert werden.

## Dokumentinformationen

Dokumenttitel: Streamvault™-Appliance – Benutzerhandbuch

Dokumentnummer original: EN.803.003

Dokumentnummer: DE.803.003

Aktualisierungsdatum des Dokuments: 5. Juni 2025

Sie können Kommentare, Korrekturen und Anregungen zu diesem Handbuch an [documentation@genetec.com](mailto:documentation@genetec.com) senden.

# Informationen über dieses Handbuch

---

Dieses Handbuch erklärt, wie Sie Ihre Streamvault-Appliance für die Zusammenarbeit mit Zutrittskontrolle und Videoüberwachung in Security Center mithilfe der aktuellen Version von SV Control Panel konfigurieren. Dieses Handbuch ergänzt das Security Center – Administratorhandbuch und das Synergis™-Appliance – Konfigurationshandbuch.

Dieser Leitfaden ist für den Integrator gedacht, der die anfängliche Einrichtung der SV-Appliance durchführt. Wir gehen davon aus, dass Sie mit der Terminologie und den Konzepten, die in Security Center verwendet werden, vertraut sind.

## Anmerkungen und Hinweise

Die folgenden Anmerkungen und Hinweise können in diesem Handbuch erscheinen:

- **Tipp:** Gibt Hinweise, wie die Information in einem Thema oder bei einem Arbeitsschritt angewendet werden kann.
- **Bemerkung:** Erläutert einen speziellen Fall oder vertieft einen wichtigen Punkt.
- **Wichtig:** Weist auf kritische Informationen über ein Thema oder einen Arbeitsschritt hin.
- **Achtung:** Zeigt an, dass eine Handlung oder ein Arbeitsschritt den Verlust von Daten, Sicherheitsprobleme oder Funktionsprobleme verursachen kann.
- **Warnung:** Zeigt an, dass eine Handlung oder ein Arbeitsschritt zu Verletzungen oder Schäden an der Hardware führen könnte.

**WICHTIG:** Inhalte in diesem Handbuch, die auf Websites von Drittanbietern verweisen, waren zum Veröffentlichungszeitpunkt korrekt. Diese Informationen können sich jedoch ohne vorherige Mitteilung von Genetec Inc. ändern.

# Inhalt

---

## Preface

|   |     |
|---|-----|
| Rechtliche Hinweise. . . . .                | ii  |
| Informationen über dieses Handbuch. . . . . | iii |

## Kapitel 1: Einführung zu Ihrer Streamvault-Appliance

|   |    |
|---|----|
| Erste Schritte mit Ihrer Streamvault Appliance. . . . .                                   | 2  |
| Von Streamvault verwendete Standardports. . . . .   | 4  |
| Informationen über das Aktualisieren der SV-Software im SV Control Panel. . . . .         | 7  |
| Komponenten der Streamvault-Appliance anschließen. . . . .                                | 8  |
| Analoge Genetec-Encoder-Karte. . . . .  | 8  |
| Kameraeingaben auf Encoder-Karten auf einer Streamvault-Appliance deaktivieren. . . . .   | 9  |
| Alarmeingaben und -Ausgaben einer Streamvault-Appliance. . . . .                          | 10 |
| Über Streamvault™-Benutzerkonten. . . . .   | 12 |
| Anmeldeinformationen für Standard-Benutzerkonten auf einer Appliance Streamvault. . . . . | 12 |
| Bei einer Streamvault-Appliance anmelden. . . . .   | 14 |
| Informationen zum Streamvault™ Service. . . . .   | 15 |
| Über Streamvault-Härtung. . . . .   | 16 |
| Appliances mit Managementfunktionen für die Härtung. . . . .                              | 16 |

## Kapitel 2: Erste Schritte mit dem SV Control Panel

|  |    |
|--|----|
| Informationen über das SV Control Panel. . . . .                                     | 19 |
| Einrichten Ihrer Appliance im SV Control Panel. . . . .                              | 19 |
| Ihre Security-Center-Lizenz auf einer Appliance aktivieren. . . . .                  | 22 |
| Manuelles Aktivieren einer Lizenz über Server Admin. . . . .                         | 24 |
| Den System Availability Monitor aktivieren. . . . .                                  | 26 |
| Security-Center-Video- und Zutrittskontrollfunktionen aktivieren. . . . .            | 27 |
| Über das Geräteregistrierungs-Tool. . . . .  | 30 |
| Öffnen des Unit Enrollment Tools. . . . .  | 30 |
| Konfigurieren von Geräteerkennungseinstellungen. . . . .                             | 30 |
| Hinzufügen von Geräten. . . . .  | 31 |
| Löschen von hinzugefügten Einheiten. . . . .   | 31 |
| Ignorieren von Geräten. . . . .  | 32 |
| Entfernen von Einheiten aus der Liste ignorierte Geräte. . . . .                     | 32 |
| Standardkameraeinstellungen konfigurieren. . . . .                                   | 33 |
| Benutzerdefinierte Aufzeichnungszeitpläne erstellen. . . . .                         | 35 |
| Informationen über Sichern und Wiederherstellen. . . . .                             | 36 |
| Ihre Directory-Datenbank sichern. . . . .  | 37 |
| Ihre Directory-Datenbank wiederherstellen. . . . .                                   | 38 |
| Die Methode für das Erstellen von Archiver-Rollen und Partitionen auswählen. . . . . | 39 |
| Archiver-Rollen im SV Control Panel hinzufügen. . . . .                              | 39 |
| Partitionen und Archiver-Rollen manuell hinzufügen. . . . .                          | 41 |
| Verschlüsseln des Betriebssystemlaufwerks. . . . .                                   | 44 |
| Erstellen eines Wiederherstellungsschlüssels. . . . .                                | 45 |
| Erfassen von Support-Protokollen. . . . .  | 48 |

## Kapitel 3: Erste Schritte mit Streamvault Maintenance

|   |    |
|---|----|
| Informationen über das Streamvault – Wartung-Plugin. . . . .              | 51 |
| Das Plugin herunterladen und installieren. . . . .                        | 52 |
| Genetec Streamvault – Berechtigungen. . . . .                             | 53 |
| Die Plugin-Rolle erstellen. . . . .                                       | 55 |
| Eine Streamvault-Hardwareüberwachungsentität konfigurieren. . . . .       | 56 |
| Eine Streamvault-Managerentität konfigurieren:. . . . .                   | 60 |
| Informationen über die Registerkarte „Management“. . . . .                | 63 |
| Die Integrität der Streamvault-Appliance überprüfen. . . . .              | 64 |
| Spalten des Berichtsbereichs für den Streamvault-Hardwaretask. . . . .    | 65 |
| Event-to-Actions für Streamvault-Integritätsereignisse erstellen. . . . . | 66 |

## Kapitel 4: SV Control Panel – Referenz

|   |    |
|---|----|
| Startseite des SV Control Panel. . . . .          | 69 |
| Konfigurationsseite des SV Control Panel. . . . . | 71 |
| Sicherheitsseite des SV Control Panels. . . . .   | 74 |
| Informationsseite des SV Control Panel. . . . .   | 78 |

## Kapitel 5: Weitere Ressourcen

|   |    |
|---|----|
| Produktgarantie für Ihre Streamvault-Appliance. . . . .                       | 81 |
| Konfigurieren des BIOS-Passworts. . . . .                                     | 82 |
| Ändern des iDRAC-Standardpassworts. . . . .                                   | 85 |
| Einen neuen iDRAC-Benutzer mit Administratorrechten hinzufügen. . . . .       | 86 |
| Deaktivieren des iDRAC-Root-Benutzers. . . . .                                | 87 |
| Neues Image für Streamvault-Appliance festlegen. . . . .                      | 88 |
| Die System-ID und Image-Version einer Streamvault™ Appliance finden. . . . .  | 89 |
| Dateifreigabe auf einer Streamvault-Appliance erlauben. . . . .               | 90 |
| Remotedesktop-Verbindungen auf einer Streamvault™-Appliance erlauben. . . . . | 91 |

## Kapitel 6: Problembehandlung

|  |     |
|--|-----|
| Eine Zurücksetzung auf Werkseinstellungen auf einer Streamvault All-in-One-Appliance durchführen. . . . .                              | 93  |
| USB-Speicher für eine Streamvault™ All-in-One-Appliance zum Zurücksetzen auf Werkseinstellungen erstellen. . . . .                     | 93  |
| Zurücksetzen des Software-Images auf einer All-in-One-Appliance. . . . .   | 95  |
| Eine Zurücksetzung auf die Werkseinstellungen auf einer Streamvault-Workstation oder Server-Appliance durchführen. . . . .             | 104 |
| Einen USB-Speicher zum Zurücksetzen auf Werkseinstellungen für eine Streamvault™-Workstation oder -Server-Appliance erstellen. . . . . | 104 |
| Das Software-Image auf einer Streamvault-Workstation- oder Server-Appliance zurücksetzen. . . . .                                      | 106 |
| Mercury-EP-Steuerungen bleiben offline, wenn TLS 1.1 deaktiviert ist.. . . .   | 109 |
| Transport Layer Security (TLS) aktivieren. . . . .   | 110 |
| Remotedesktop kann sich nicht mit einer Streamvault-Appliance verbinden. . . . .   | 113 |
| Aufhebung der Beschränkungen für Benutzerkonten von Nicht-Administratoren. . . . .   | 117 |
| Lokale Konten können nicht auf Remote Desktop, Datei-Sharing Service und Remote Management zugreifen. . . . .                          | 118 |
| Ermöglichung von Smart Card-bezogenen Diensten. . . . .  | 119 |
| Support für Mercury EP- und LP-Firmware-Controller 1.x.x aktivieren. . . . .   | 120 |
| Support für die Synergis IX-Integration aktivieren. . . . .  | 122 |
| Ändern lokaler Gruppenrichtlinienobjekte für Benutzerkonten von Nicht-Administratoren. . . . .   | 123 |
| Windows-Firewall deaktivieren. . . . .   | 126 |

## Kapitel 7: Technischer Support

|   |     |
|---|-----|
| Kontaktieren des Genetec Technical Assistance Center. . . . . | 129 |
| GTAC per Telefon kontaktieren. . . . .                        | 129 |
| Das GTAC über das GTAP kontaktieren. . . . .                  | 130 |
| Das GTAC über den Live-Chat kontaktieren. . . . .             | 130 |
| Software-Support. . . . .                                     | 132 |
| Hardware-Support. . . . .                                     | 133 |
| Spezifikationen für Streamvault. . . . .                      | 134 |
| Nutzungsbedingungen für den Streamvault-Support. . . . .      | 135 |
| Glossar . . . . .   | 136 |
| Wo finde ich Produktinformationen? . . . . .                  | 138 |

# Einführung zu Ihrer Streamvault-Appliance

Dieser Abschnitt enthält die folgenden Themen:

- ["Erste Schritte mit Ihrer Streamvault Appliance"](#) auf Seite 2
- ["Von Streamvault verwendete Standardports"](#) auf Seite 4
- [" Informationen über das Aktualisieren der SV-Software im SV Control Panel "](#) auf Seite 7
- ["Komponenten der Streamvault-Appliance anschließen"](#) auf Seite 8
- ["Über Streamvault™-Benutzerkonten"](#) auf Seite 12
- ["Bei einer Streamvault-Appliance anmelden"](#) auf Seite 14
- ["Informationen zum Streamvault™ Service"](#) auf Seite 15
- [" Über Streamvault-Härtung"](#) auf Seite 16

# Erste Schritte mit Ihrer Streamvault Appliance

Sie können Ihre Streamvault™-Appliance mit Security Center bereitstellen, indem Sie eine Reihe an Schritten befolgen.

## Bereitstellung – Übersicht

| Schritt   | Task   | Wo finde ich weitere Informationen?   |
|---|--|---|
| <b>Machen Sie sich vor der Bereitstellung mit Voraussetzungen und zentralen Themen vertraut</b> |  |   |
| 1   | Öffnen Sie die erforderlichen Netzwerkports, um die Kernsysteme in Security Center und die Streamvault-Module zu verbinden. Schließen Sie Peripheriegeräte wie Ihren Bildschirm, Ihre Tastatur, analoge Encoder-Karte und Geräte an Ihre Eingänge und Ausgänge an. Schließen Sie die Appliance an Ihr Netzwerk an. | <ul style="list-style-type: none"> <li>• <a href="#">Von Streamvault verwendete Standardports</a> auf Seite 4.</li> <li>• <a href="#">Komponenten der Streamvault-Appliance anschließen</a> auf Seite 8.</li> <li>• <a href="#">Analoge Genetec-Encoder-Karte</a> auf Seite 8.</li> <li>• <a href="#">Kameraeingaben auf Encoder-Karten auf einer Streamvault-Appliance deaktivieren</a> auf Seite 9.</li> <li>• <a href="#">Alarমেingaben und -Ausgaben einer Streamvault-Appliance</a> auf Seite 10.</li> </ul> |
| 2   | Bevor Sie Ihre Appliance in Betrieb nehmen, sollten Sie sich über den Inhalt Ihrer Image-Version informieren.  | <ul style="list-style-type: none"> <li>• <a href="#">Inhalt der einzelnen Streamvault-Image-Versionen</a>.</li> </ul>   |
| 3   | Melden Sie sich bei Windows als Admin mit dem Passwort an, das auf Ihrer Appliance gedruckt ist, und ändern Sie dann das Passwort.   | <ul style="list-style-type: none"> <li>• <a href="#">Bei einer Streamvault-Appliance anmelden</a> auf Seite 14.</li> </ul>  |
| 4   | Konfigurieren Sie das BIOS-Passwort auf Ihrer Appliance.   | <ul style="list-style-type: none"> <li>• <a href="#">Konfigurieren des BIOS-Passworts</a> auf Seite 82.</li> </ul>  |
| 5   | Wenn Ihre Appliance iDRAC unterstützt, ändern Sie umgehend das iDRAC-Standardpasswort. Für zusätzliche Sicherheit wird empfohlen, ein alternatives Benutzerkonto mit Administratorrechten zu erstellen und das Root-Benutzerkonto zu deaktivieren.   | <ul style="list-style-type: none"> <li>• <a href="#">Ändern des iDRAC-Standardpassworts</a> auf Seite 85.</li> <li>• <a href="#">Einen neuen iDRAC-Benutzer mit Administratorrechten hinzufügen</a> auf Seite 86.</li> <li>• <a href="#">Deaktivieren des iDRAC-Root-Benutzers</a> auf Seite 87.</li> </ul>   |
| <b>Einrichtungs-Assistent abschließen</b>   |  |   |
| 6   | Schließen Sie den Assistenten <i>Einrichtung von Streamvault Control Panel</i> ab.<br><b>BEMERKUNG:</b> Der Remotedesktop ist standardmäßig deaktiviert. Um den Remote Desktop zu aktivieren, aktivieren Sie die <b>Service-Einstellung Remote Desktop</b> auf der Seite <i>Sicherheit</i> des SV Control Panels.  | <ul style="list-style-type: none"> <li>• <a href="#">Einrichten Ihrer Appliance im SV Control Panel</a> auf Seite 19.</li> <li>• <a href="#">Remotedesktop-Verbindungen auf einer Streamvault™-Appliance erlauben</a> auf Seite 91.</li> </ul>  |
| 7   | Aktivieren Sie Security-Center-Lizenz. <ul style="list-style-type: none"> <li>• Wenn die Appliance mit dem Internet verbunden ist, aktivieren Sie Ihre Lizenz</li> </ul>   | <ul style="list-style-type: none"> <li>• <a href="#">Ihre Security-Center-Lizenz auf einer Appliance aktivieren</a> auf Seite 22.</li> </ul>  |

| Schritt | Task   | Wo finde ich weitere Informationen?   |
|---------|--|---|
|         | <p>mithilfe des Assistenten <i>Aktivierung von Streamvault Control Panel</i>.</p> <ul style="list-style-type: none"> <li>Wenn die Appliance nicht mit dem Internet verbunden ist, aktivieren Sie Ihre Lizenz manuell über Server Admin.</li> </ul> | <ul style="list-style-type: none"> <li><a href="#">Manuelles Aktivieren einer Lizenz über Server Admin</a> auf Seite 24.</li> </ul>   |
| 8       | Aktivieren Sie den System Availability Monitor.  | <ul style="list-style-type: none"> <li><a href="#">Den System Availability Monitor aktivieren</a> auf Seite 26.</li> </ul>  |
| 9       | Konfigurieren Sie den Genetec™ Update Service, sodass Sie die neueste Version von Security Center und des SV Control Panels erhalten können. Wenn Updates vorhanden sind, installieren Sie diese.  | <ul style="list-style-type: none"> <li><a href="#">Den Genetec™ Update Service konfigurieren</a>.</li> </ul>  |
| 10      | Wenn das SV Control Panel angibt, dass weitere Updates verfügbar sind, installieren Sie diese jetzt.   | <ul style="list-style-type: none"> <li><a href="#">Informationen über das Aktualisieren der SV-Software im SV Control Panel</a> auf Seite 7.</li> </ul>   |
| 11      | Verschlüsseln Sie das Betriebssystemlaufwerk auf Ihrer Appliance mit BitLocker und erstellen Sie einen Wiederherstellungsschlüssel.  | <ul style="list-style-type: none"> <li><a href="#">Verschlüsseln des Betriebssystemlaufwerks</a> auf Seite 44.</li> </ul>   |
| 12      | Erstellen Sie die Anzahl von Archiver-Rollen, die Sie zum Unterstützen der Kameraanzahl und der gesamten Netzwerkbandbreite benötigen, die Sie für Ihre Bereitstellung planen.   | <ul style="list-style-type: none"> <li>Für die Serien SV-1000E, SV-2000E, SV-4000E: <a href="#">Archiver-Rollen im SV Control Panel hinzufügen</a> auf Seite 39.</li> <li>Für SV-7000EX und für All-in-one: <a href="#">Partitionen und Archiver-Rollen manuell hinzufügen</a> auf Seite 41.</li> </ul> |
| 13      | Melden Sie sich bei Config Tool an und konfigurieren Sie Ihre Security-Center-Video- und Zutrittskontrollfunktionen.   | <ul style="list-style-type: none"> <li><a href="#">Security-Center-Video- und Zutrittskontrollfunktionen aktivieren</a> auf Seite 27.</li> <li><a href="#">Konfigurieren von Geräteerkennungseinstellungen</a> auf Seite 30.</li> </ul>   |
| 14      | Sichern Sie die Security-Center-Konfiguration.   | <ul style="list-style-type: none"> <li><a href="#">Ihre Directory-Datenbank sichern</a> auf Seite 37.</li> </ul>  |

## Von Streamvault verwendete Standardports

Die erforderlichen Netzwerkports müssen geöffnet sein, damit die folgenden Streamvault™-Komponenten ordnungsgemäß funktionieren.

### Erforderliche Ports für Streamvault™ Maintenance-Plugin

Der folgende Port muss in einer externen Firewall für eingehenden Datenverkehr geöffnet werden, damit das Streamvault™ Maintenance-Plugin mit der Streamvault™-Hardware kommunizieren kann. Diese Anforderung gilt nur, wenn die folgenden drei Bedingungen erfüllt sind:

- Die interne Passthrough-Verbindung zwischen dem Betriebssystem und dem iDRAC ist deaktiviert.
- Der iDRAC verwendet einen dedizierten LAN-Port.
- Zwischen dem iDRAC-Netzwerk und dem Host-Netzwerk befindet sich eine Firewall.

In jeder anderen Situation kann diese Anforderung ignoriert werden.

| Modul                           | Eingehender Port | Portnutzung  |
|---------------------------------|------------------|--|
| Streamvault-Hardwareüberwachung | 65116            | Wird für die HTTPS-Kommunikation zwischen Security Center und dem iDRAC-Baseboard-Management-Controller der Streamvault™-Hardware über das Netzwerk verwendet. |

### SV Control Panel erforderliche Anschlüsse

Die untenstehenden Ports für ausgehenden Datenverkehr müssen geöffnet sein, damit sich die Streamvault-Control-Panel-Komponenten mit Genetec™-Cloudservices verbinden können.

| Ausgehender Port | Portnutzung   | Ziel-URL   |
|------------------|---|--|
| TCP 443          | HTTPS-Kommunikation mit den Sicherungsservices von Genetec™ | svbackupservices.genetec.com<br>genetecbackupservice.blob.core.windows.net |

### Erforderliche Ports für CylancePROTECT

Die untenstehenden Ports für ausgehenden Datenverkehr müssen geöffnet sein, damit der CylancePROTECT-Desktopagent mit der Genetec-Managementkonsole kommunizieren und Agent-Updates erhalten kann.

| Ausgehender Port | Portnutzung                        | Ziel-URL   |
|------------------|------------------------------------|--|
| TCP 443          | HTTPS-Kommunikation in Nordamerika | cement.cylance.com<br>data.cylance.com<br>protect.cylance.com<br>update.cylance.com<br>api.cylance.com<br>download.cylance.com<br>venueapi.cylance.com |

| Ausgehender Port | Portnutzung   | Ziel-URL  |
|------------------|---|---|
| TCP 443          | HTTPS-Kommunikation in der Region Asien-Pazifik (Nordosten) | cement-apne1.cylance.com<br>data-apne1.cylance.com<br>protect-apne1.cylance.com<br>update-apne1.cylance.com<br>api.cylance.com<br>download.cylance.com<br>venueapi-apne1.cylance.com              |
| TCP 443          | HTTPS-Kommunikation in der Region Asien-Pazifik (Südosten)  | cement-au.cylance.com<br>cement-apse2.cylance.com<br>data-au.cylance.com<br>protect-au.cylance.com<br>update-au.cylance.com<br>api.cylance.com<br>download.cylance.com<br>venueapi-au.cylance.com |
| TCP 443          | HTTPS-Kommunikation in Mitteleuropa                         | cement-euc1.cylance.com<br>data-euc1.cylance.com<br>protect-euc1.cylance.com<br>update-euc1.cylance.com<br>api.cylance.com<br>download.cylance.com<br>venueapi-euc1.cylance.com                   |
| TCP 443          | HTTPS-Kommunikation in Südamerika                           | cement-sae1.cylance.com<br>data-sae1.cylance.com<br>protect-sae1.cylance.com<br>update-sae1.cylance.com<br>api.cylance.com<br>download.cylance.com<br>venueapi-sae1.cylance.com                   |
| TCP 443          | HTTPS-Kommunikation in GovCloud                             | cement.us.cylance.com<br>data.us.cylance.com<br>protect.us.cylance.com<br>update.us.cylance.com<br>api.us.cylance.com<br>download.cylance.com<br>download.us.cylance.com                          |

| Ausgehender Port | Portnutzung  | Ziel-URL                |
|------------------|--|-------------------------|
|                  |  | venueapi.us.cylance.com |
| TCP 443          | HTTPS-Kommunikation zur Aktivierung von Cylance nach der Neuinstallation | svservices.genetec.com  |

**BEMERKUNG:** Wenn Sie die oben genannten Verbindungen nicht öffnen möchten, kann CylancePROTECT in einen getrennten Modus wechseln. Im getrennten Modus empfängt CylancePROTECT Agentenaktualisierungen vom Genetec™ Update Service (GUS).

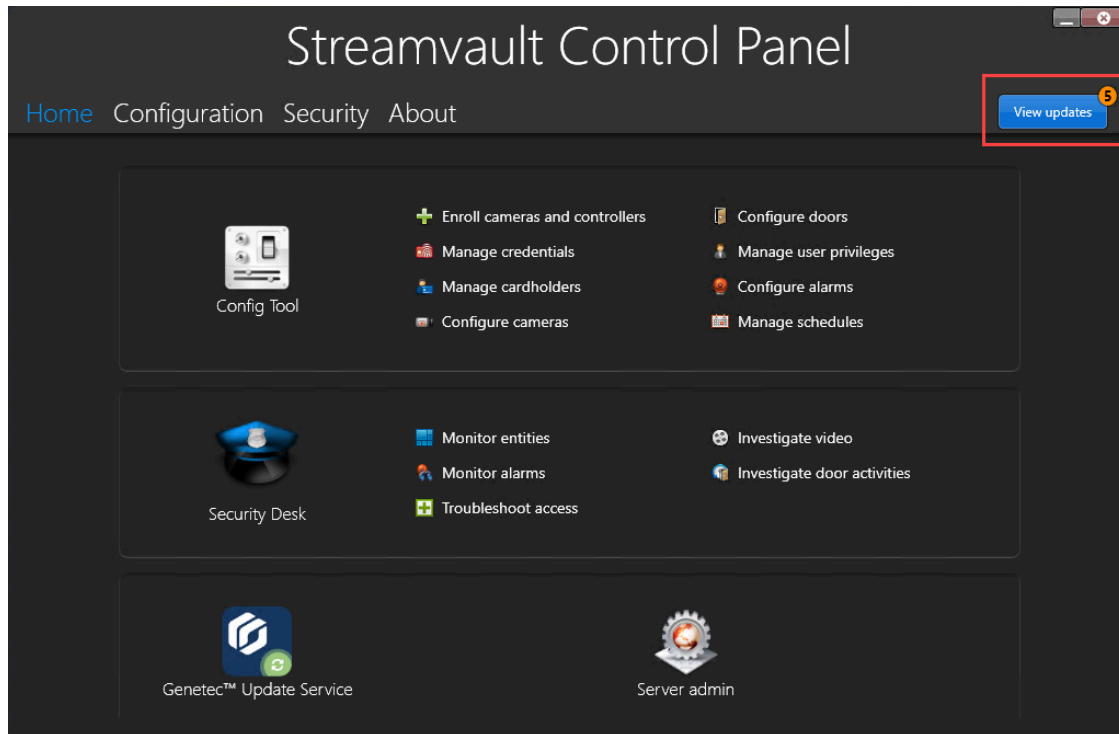
Weitere Informationen zu den Modi, in denen die Streamvault™-Appliance mit Genetec™-Verwaltungsservices kommuniziert, finden Sie unter [Sicherheitsseite des SV Control Panels](#) auf Seite 74.

# Informationen über das Aktualisieren der SV-Software im SV Control Panel

Das Genetec™ Update Service (GUS) ist in das SV Control Panel integriert, um sicherzustellen, dass die Softwarekomponenten auf Ihrer Appliance aktuell sind.

Wenn Updates verfügbar sind, wird die Taste **Updates anzeigen** zusammen mit einer Markierung, die angibt, wie viele Updates verfügbar sind. Wenn Sie auf **Updates anzeigen** klicken, wird das GUS in einem Browser geöffnet.

**BEMERKUNG:** Die Farbe der Markierung variiert basierend auf der Wichtigkeit der Updates. Eine orangefarbene Markierung weist auf empfohlene Updates hin und eine rote Markierung auf kritische Updates.



Genetec™ Update Service besitzt folgende Hauptmerkmale:

- Aktualisieren Ihrer Genetec™-Produkte, wenn eine neue Version verfügbar ist.
- Prüfen auf Aktualisierungen in regelmäßigen Abständen.
- Konfigurieren von Updates für das Herunterladen im Hintergrund; Sie müssen jedoch nach wie vor manuell installieren.
- Anzeigen, wann das letzte Mal nach Aktualisierungen gesucht wurde.
- Aktualisiert die Lizenz automatisch im Hintergrund, um sicherzustellen, dass sie gültig ist und das Ablaufdatum aktualisiert wird.
- Aktivieren unterschiedlicher Funktionen wie das Genetec Improvement Program.
- Überprüft Ihre Firmware und empfiehlt Upgrades oder benachrichtigt Sie über Schwachstellen.

Weitere Informationen über das Verwenden des GUS finden Sie im [Genetec™ Update Service – Benutzerhandbuch](#) im TechDoc Hub.

# Komponenten der Streamvault-Appliance anschließen

Um Ihre Streamvault™-Appliance für die Verwendung vorzubereiten, müssen Sie die erforderlichen Peripheriegeräte (Bildschirm, Tastatur und Maus), die optionalen Peripheriegeräte sowie eine Stromquelle anschließen.

## Bevor Sie beginnen

Machen Sie den Platz um den Ein-/Ausschaltknopf frei. Um ein Ausschalten der Appliance zu verhindern, stellen Sie sicher, dass nichts den Ein-/Ausschaltknopf berührt oder zu nahe ist.

## Prozedur

- 1 Schließen Sie das Bildschirmkabel an einen unterstützten Videoanschluss an: VGA, HDMI oder DisplayPort. Sie müssen mindestens einen Bildschirm an die Appliance anschließen. Sie können bis zu drei Bildschirme an die gleiche Appliance anschließen.
- 2 Schließen Sie den Bildschirm an das Stromnetz an und schalten Sie den Bildschirm ein.
- 3 Schließen Sie die Maus und Tastatur an einen verfügbaren USB-Anschluss an.
- 4 (Optional) Schließen Sie die optionalen Peripheriegeräte an:
  - Lautsprecher
  - [Analoge Kameras](#)
  - [Alarめingaben und -ausgaben](#)
- 5 Schließen Sie ein Ethernetkabel am Ethernetanschluss an. Schließen Sie das andere Ende des Kabels an den IP-Netzwerk-RJ-45-Anschluss an.
- 6 Schließen Sie bei Streamvault™-SV-100E-Appliances den Stromstecker am 19,5V-Eingangsanschluss und das andere Ende am Netzteil an. Schließen Sie das Kabel des Netzteils an eine Steckdose an.
- 7 Drücken Sie den Einschaltknopf, um die Streamvault-Appliance einzuschalten.

## Nach Durchführen dieser Schritte

[Melden Sie sich bei Ihrer Streamvault-Appliance an.](#)

## Analoge Genetec-Encoder-Karte

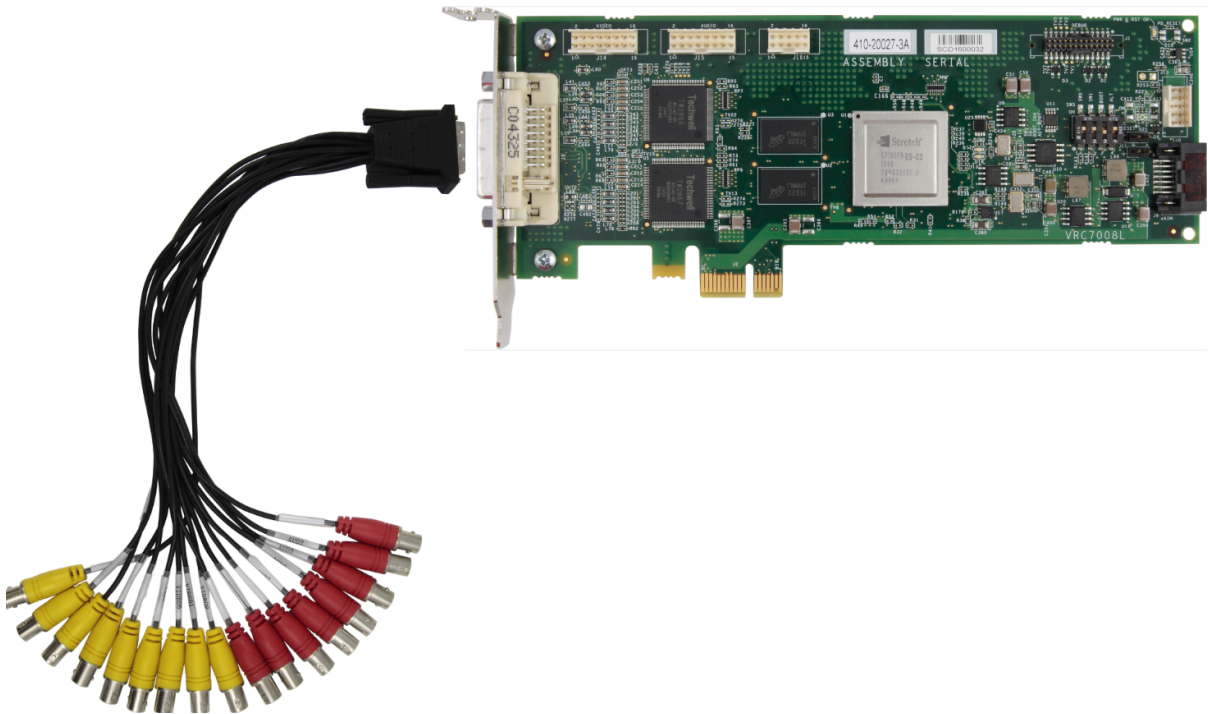
Wenn Sie eine Streamvault-Appliance verwenden, um ein Videomanagementsystem mit analogen Kameras zu implementieren, müssen Sie die Kameras mit der analogen Genetec™-Encoder-Karte auf der Appliance verbinden.

## Spezifikationen für analoge Encoder-Karten

Die folgenden Spezifikationen gelten für Streamvault-Appliances, die die analoge Videokarte enthalten.

- 8 oder 16 analoge Videoeingänge, abhängig davon, welche Karte installiert ist
- 4CIF max. Videoauflösung
- Maximale Framerate: 30 fps
- Unterstützt das H.264-Komprimierungsformat

**Einschränkungen:** Damit eine analoge Encoder-Karte aufzeichnen kann, muss Ihre Streamvault-Appliance über eine Netzwerkverbindung verfügen. Wenn keine Netzwerkverbindung verfügbar ist, müssen Sie eine Loopback-Schnittstelle konfigurieren, sodass die Encoder-Karte ordnungsgemäß funktionieren kann.



## Informationen über das Anschließen von analogen Kameras

Wenn Ihre Streamvault-Appliance die analoge Genetec-Encoder-Karte enthält, wird Sie mit einer Kabelpeitsche mit BNC-Anschlüssen geliefert. Die BNC-Anschlüsse werden verwendet, um die analogen Kameras direkt an die eingebaute Encoder-Karte anzuschließen.

## Informationen über das Hinzufügen von analogen Kameras in Security Center

Sie müssen das Geräteregistrierungs-Tool verwenden, um analoge Kameras in Security Center hinzuzufügen. Weitere Informationen finden Sie unter [Informationen über das Geräteregistrierungs-Tool](#).

Ziehen Sie folgendes in Betracht, wenn Sie analoge Kameras hinzufügen:

- Sie können analoge Kameras nicht in Security Center mithilfe der Methode *Manuell hinzufügen* hinzufügen. Verwenden Sie das Geräteregistrierungs-Tool.
- Damit Sie neue Einheiten erkennen und das Geräteregistrierungs-Tool verwenden können, müssen Sie sich vor Ort mit Config Tool verbinden.
- Wenn Sie den Hersteller einer Kamera im Geräteregistrierungs-Tool auswählen, finden Sie alle analogen Kameras unter dem Hersteller *Genetec-Encoder-Karte*.

## Kameraeingaben auf Encoder-Karten auf einer Streamvault-Appliance deaktivieren

Um eine Kameraverbindungslicenz von analog zu IP zu aktualisieren, müssen Sie die Kameraeingaben auf der Encoder-Karte deaktivieren.

### Prozedur

- 1 Klicken Sie über die Config Tool-Startseite auf die Registerkarte *Informationen*.
- 2 Klicken Sie auf die Registerkarte **Omnicast™** und überprüfen Sie die Anzahl von Kameras, die neben *Anzahl von Kameras und analogen Bildschirmen* angezeigt wird.

Beispielsweise: 16 / 16.

- 3 Öffnen Sie die Aufgabe *Video*.
- 4 Klicken Sie in der Entitätsstruktur auf die Videoeinheit, die der Encoder-Karte entspricht.
- 5 Klicken Sie auf die Registerkarte **Peripheriegeräte** und wählen Sie die Kameras aus, die Sie deaktivieren möchten.  
Sie können mehrere Kameras auswählen, indem Sie die Steuerungstaste drücken und auf die Kameras klicken.
- 6 Klicken Sie unten auf der Seite *Peripheriegeräte* auf den roten Kreis (●), um die Kameras zu deaktivieren, und klicken Sie dann auf **Anwenden**.  
Deaktivierte Kameras sind ausgegraut und links neben jeder deaktivierten Kamera in der Liste wird ein roter Punkt angezeigt.
- 7 Stellen Sie auf der Seite *Informationen* sicher, dass die Anzahl von Kameras korrekt ist.  
Sie müssen Config Tool möglicherweise neu starten, um die Anzahl der Kameras zu aktualisieren.  
**BEMERKUNG:** Wenn eine Kamera, die Sie deaktiviert haben, Video aufgezeichnet hat, wird die Kamera in der Entitätsstruktur im *Überwachungstask* in Security Desk angezeigt. Sie können Video von dieser Kamera wiedergeben.

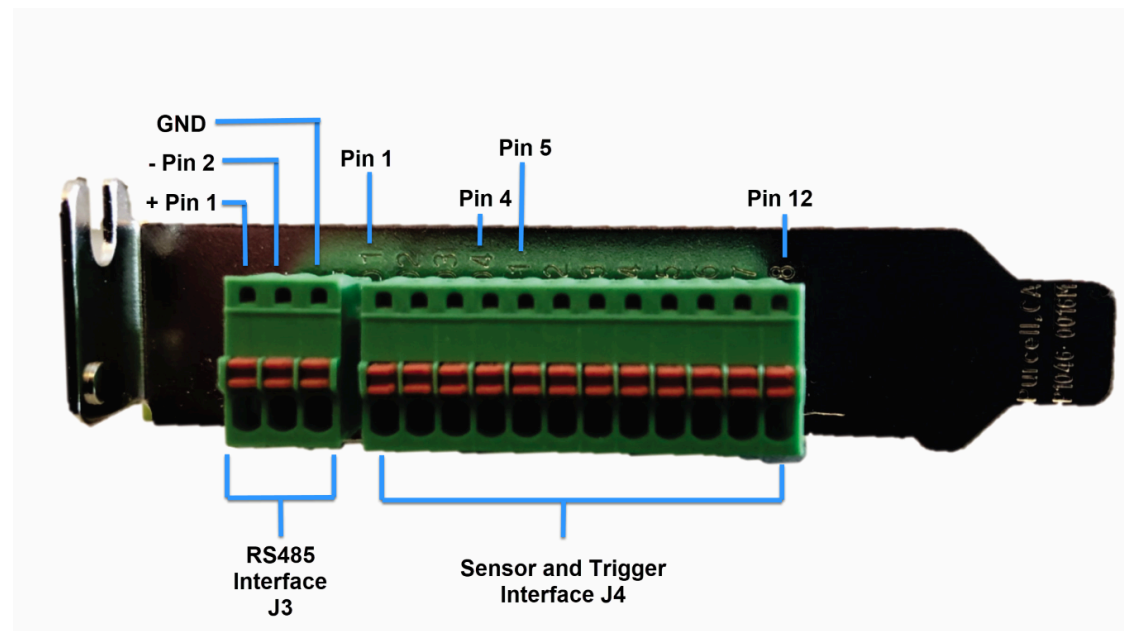
## Alarমেingaben und -Ausgaben einer Streamvault-Appliance

Wenn Sie eine Streamvault-Appliance verwenden, um ein Zutrittskontrollsystem zu implementieren, können Sie die E/A-Karte verwenden, um Hardwarealarmeingaben direkt and die Appliance anzuschließen und die Ausgaben dann mithilfe von Event-to-Actions in Security Center zu steuern.

### E/A-Kartenspezifikationen

Die folgenden Spezifikationen gelten für Streamvault-Modelle, die die E/A-Karte enthalten:

- 4 Auslöserausgaben
- 8 Alarmeingaben
- RS-485-Kommunikationsport



## Informationen über das Anschließen von E/A-Eingaben

Sie können die Eingangs- und Ausgangskabel von Hardwaregeräten direkt an die E/A-Karten auf der Rückseite der Streamvault-Appliance anschließen. Die Drähte sollten mit einem kleinen Schlitzschraubendreher eingeführt werden, um die Spannklemmen am Steckverbinder einzudrücken.

## Informationen über das Erstellen von Event-to-Actions

Informationen über das Erstellen von Event-to-Actions für Streamvault finden Sie unter [Event-to-Actions](#) im TechDoc Hub.

# Über Streamvault™-Benutzerkonten

Es gibt zwei Arten von Streamvault™-Benutzerkonten: lokale Administratoren und lokale Nicht-Administratoren. Je nachdem, mit welchem Konto Sie sich am SV Control Panel anmelden, sehen Sie nur die für Sie relevanten Funktionen.

## Lokaler Administrator

Das Benutzerkonto des lokalen Administrators (Admin) wird standardmäßig erstellt. Eine Person, die als Admin angemeldet ist, hat volle administrative Rechte für das SV Control Panel. Der Admin kann alle system- und sicherheitsrelevanten Einstellungen im SV Control Panel konfigurieren und Benutzerkonten für Nicht-Administratoren anlegen.

## Lokaler Nicht-Administrator

Das lokale Standard-Benutzerkonto für All-in-One-Appliances und Workstations, das ein Nicht-Administrator-Konto ist, ist das „Operator“-Konto. Eine Person, die als Operator angemeldet ist, hat eingeschränkten Zugriff auf die Funktionen des SV Control Panels. Der Nutzer kann das Config Tool und den Security Desk starten, System- und Lizenzierungsinformationen einsehen und auf die Produktdokumentation zugreifen.

Eine Person, die als Admin angemeldet ist, kann weitere Konten für Nicht-Administratoren anlegen, die ebenfalls einen eingeschränkten Zugang zum SV Control Panel haben.

**BEMERKUNG:** Es ist möglich, die standardmäßigen Zugriffsbeschränkungen für alle Benutzerkonten, die Nicht-Administrator-Konten sind, aufzuheben. Informationen dazu finden Sie unter [Aufhebung der Beschränkungen für Benutzerkonten von Nicht-Administratoren](#) auf Seite 117.

## Anmeldeinformationen für Standard-Benutzerkonten auf einer Appliance Streamvault

Wenn Sie Ihre Streamvault-Appliance zum ersten Mal starten, werden die Windows-Admin- und Bediener-Benutzerkonten erstellt. Diese Konten haben unterschiedliche Zugriffsrechte und Standardpasswörter. Server Admin hat auch ein Standardpasswort.

Die folgenden Standardpasswörter sind für die Erstanmeldung gedacht. Während der Einrichtung erstellen Sie Ihr eigenes Passwort für Config Tool und Security Desk.

| Benutzername  | Standardpasswor | Zugriff gewährt für   | Zugriff verweigert für   |
|---------------|-----------------|---|--|
| Administrator | admin           | Voller Systemzugriff: <ul style="list-style-type: none"> <li>Windows: alle System- und administrativen Funktionen</li> <li>Security Center</li> <li>SV Control Panel</li> </ul>   | Nicht zutreffend   |
| Operator      | Bediener        | <ul style="list-style-type: none"> <li>Papierkorb</li> <li>Bibliotheken</li> <li>Mein Computer</li> <li>C: Laufwerk</li> <li>SV-Control-Panel-Startseite, -Konfigurationsseite, nur regionale Einstellungen, - Informationsseite</li> </ul> | <ul style="list-style-type: none"> <li>Windows: herunterfahren und neu starten</li> <li>Systemeinstellungen</li> <li>Videopartition</li> </ul> |

| Benutzername     | Standardpasswor | Zugriff gewährt für  | Zugriff verweigert für   |
|------------------|-----------------|--|--|
|                  |                 | <ul style="list-style-type: none"> <li>Server Admin: Admin-Passwort für volle Rechte erforderlich</li> </ul> |  |
| Nicht zutreffend | genetecfactory  | Server Admin   | <b>BEMERKUNG:</b> Diese Option ist für Workstation-Appliances nicht verfügbar. |

Um die Passwörter für Ihr Windows-Benutzerkonto, die Client-Anwendung oder Server Admin zu ändern, melden Sie sich beim SV Control Panel mit Ihrem Windows-Admin-Benutzerkonto an. Auf der Seite *Sicherheit* im Bereich *Berechtigungen* können Sie alle Ihre Passwörter verwalten.

**BEMERKUNG:** Das Bedienerkonto wird nicht mithilfe einer Vorlage erstellt. Wenn Sie ein neues Benutzerkonto erstellen, hat es nicht standardmäßig die gleichen Einschränkungen.

## Security Center Server Admin

- Nur Admin-Benutzer können sich bei Server Admin anmelden.
- Um sich über Ihren lokalen Computer anzumelden, klicken Sie auf die **Server Admin**-Tastaturkürzel auf Ihrem Desktop.
- Damit Sie sich bei Server Admin von einem Remote-Computer aus anmelden können, müssen Sie den DNS-Namen oder die IP-Adresse des Servers, den Webserverport und das Serverpasswort kennen. Wenn Sie das Standardpasswort eingeben, werden Sie dazu aufgefordert, es zu ändern.

**WICHTIG:** Ändern Sie umgehend alle Standardpasswörter, um die Sicherheit Ihres Systems zu gewährleisten. Nutzen Sie bewährte Methoden der Branche für das Erstellen komplexer Passwörter.

## Verwandte Themen

[Ändern lokaler Gruppenrichtlinienobjekte für Benutzerkonten von Nicht-Administratoren](#) auf Seite 123

# Bei einer Streamvault-Appliance anmelden

---

Beim ersten Starten Ihrer Streamvault™-Appliance, werden Sie dazu aufgefordert, das Standard-Admin-Passwort zu ändern. Ändern Sie auch das Standard-Bedienerpasswort. Sie können sich dann als Bediener oder Admin-Benutzer anmelden.

## Bevor Sie beginnen

Erfahren Sie, über welche Zugriffsrechte die Bediener- und Admin-Konten haben.

## Was Sie noch wissen sollten

Melden Sie sich als Admin-Benutzer an, um Ihre Appliance im SV Control Panel zu konfigurieren.

**WICHTIG:** Passwörter müssen die folgenden Anforderungen erfüllen:

- Mindestens 14 Zeichen  
Die Mindestlänge beträgt 10 Zeichen für Appliances mit Image-Versionen, die nicht über den Streamvault™-Service verfügen. Informationen darüber, welche Appliances über den Streamvault™-Service verfügen und welche nicht, finden Sie unter [Appliances mit Managementfunktionen für die Härtung](#) auf Seite 16.
- Mindestens drei Zeichen aus den folgenden vier Kategorien:
  - Großbuchstaben
  - Kleinbuchstaben
  - Basisziffern (0-9)
  - Nicht-alphanumerische Zeichen (wie \$, %, !)

## Prozedur

- 1 Schalten Sie die Appliance ein.
- 2 Melden Sie sich mit dem Admin-Benutzernamen und dem Standardpasswort an, die auf der Appliance aufgedruckt sind.
- 3 Geben Sie ein neues Admin-Passwort ein.  
Sie sind nun als Admin-Benutzer angemeldet.  
**BEMERKUNG:** Einige Modelle verfügen standardmäßig nur über das Admin-Konto.
- 4 Melden Sie sich ab und melden Sie sich dann mit dem Bediener-Benutzernamen und dem Standardpasswort an, die auf der Appliance aufgedruckt sind.
- 5 Geben Sie ein neues Bedienerpasswort ein.  
Sie sind nun als Bediener-Benutzer angemeldet.
- 6 Fahren Sie als Bediener fort oder melden Sie sich ab und als Admin-Benutzer an.

## Nach Durchführen dieser Schritte

Starten Sie die anfängliche Einrichtung Ihrer Appliance.

## Informationen zum Streamvault™ Service

---

Der Streamvault Service ist ein Windows Service, der es Benutzern ermöglicht, eine Streamvault™ Appliance zu konfigurieren, wie z. B. die Anwendung von Härtingsprofilen.

Der Streamvault-Service kann die folgenden Härtingsprofile auf Appliances anwenden:

- Microsoft Sicherheits-Baselines
- Microsoft-Sicherheitsgrundlagen mit dem Profil des Center for Internet Security (CIS) Level 1
- Microsoft Sicherheits-Baselines mit dem CIS Level 2 Profil
- Microsoft-Sicherheitsgrundlagen mit dem Profil des Sicherheit Technical Implementation Guide (STIG)

Weitere Informationen zu den Härtingsprofilen finden Sie unter [Über Streamvault-Härtung](#) auf Seite 16.

Wenn ein Admin-Benutzer ein Härtingsprofil im SV Control Panel auswählt, wendet der Streamvault™-Service das Profil auf die Appliance an.

Updates für den Streamvault-Service sind in regelmäßigen Abständen verfügbar und können über den Genetec™ Update Service (GUS) oder das Genetec Technical Assistance Portal (GTAP) angewendet werden. Wenn ein Update verfügbar ist, erscheint eine Benachrichtigung im SV Control Panel. Die Anwendung von Updates ist optional, wird aber empfohlen, um Zugriff auf neue Versionen der Härtingsprofile zu erhalten.

## Über Streamvault-Härtung

Die Härtung erweitert die Sicherheit Ihrer Streamvault™ Appliance durch die Anwendung einer spezifischen Einstellung von Sicherheitseinstellungen.

Wenn Sie Ihre Appliance härten, optimieren Sie sie für mehr Sicherheit, aber möglicherweise auf Kosten von Benutzerfreundlichkeit oder Leistung. Wie stark Sie Ihre Appliance härten, hängt von Ihrem Bedrohungsmodell und der Sensibilität Ihrer Daten ab.

Die Härtung wird auf der Seite *Sicherheit* des SV Control Panels vorgenommen. Es stehen vier vordefinierte Profile für die Härtung zur Auswahl.

Standardmäßig werden alle Appliances mit dem Härtungsprofil Microsoft mit CIS Level 2 ausgeliefert.

| Profil für die Härtung    | Beschreibung   |
|---------------------------|--|
| Microsoft (nur)           | <p>Dieses Profil für die Härtung wendet Microsoft-Sicherheitsgrundlagen auf Ihr System an. Microsoft Security Baselines sind eine Gruppe von Microsoft-empfohlenen Konfigurationseinstellungen, die auf dem Feedback von Microsoft Security Engineering Teams, Produktgruppen, Partnern und Kunden basieren.</p> <p>Die Microsoft-Baselines, die auf Streamvault™-Appliances bereitgestellt werden, sind die Windows-Baseline und die Microsoft Edge-Baseline.</p> |
| Microsoft mit CIS Stufe 1 | <p>Dieses Härtungsprofil wendet die Microsoft-Sicherheitsbaselines und das Profil des Center for Internet Security (CIS) Level 1 (CIS L1) auf Ihr System an. Das CIS L1 bietet grundlegende Sicherheitsanforderungen, die auf jedem System mit geringen oder gar keinen Leistungseinbußen oder Funktionseinschränkungen implementiert werden können.</p>   |
| Microsoft mit CIS Stufe 2 | <p>Dieses Härtungsprofil wendet die Microsoft-Sicherheitsbaselines und die Profile CIS L1 und Level 2 (L2) auf Ihr System an. Das Profil CIS L2 bietet die höchste Sicherheitsstufe und ist für Organisationen gedacht, in denen Sicherheit von größter Bedeutung ist.</p> <p>Die strenge Sicherheit, die dieses Härtungsprofil mit sich bringt, kann die Systemfunktionalität einschränken und das Remote Management von Servern erschweren.</p>                  |
| Microsoft mit STIG        | <p>Dieses Profil zur Härtung wendet die Microsoft-Sicherheitsbaselines und die Sicherheit Technical Implementation Guides (STIGs) der Defense Information Systems Agency (DISA) auf Ihr System an. Die DISA STIGs basieren auf den Standards des National Institute of Standards and Technology (NIST) und bieten fortschrittlichen Sicherheitsschutz für Windows-Systeme für die Abteilung des US-Verteidigungsministeriums.</p>                                  |

**BEMERKUNG:** Profile zur Härtung sind nur auf Appliances verfügbar, die über die [Streamvault™ Service](#) verfügen. Weitere Informationen dazu finden Sie unter [Informationen zum Streamvault™ Service](#) auf Seite 15.

## Appliances mit Managementfunktionen für die Härtung

Nur Appliances mit dem Streamvault™ Service verfügen über Funktionen für das Härtungsmanagement. Der Typ der Appliance und das Image bestimmen, ob der Streamvault™ Service verfügbar ist.

In der folgenden Tabelle ist aufgeführt, welche Appliances über den Streamvault™ Service verfügen und welche nicht.

| Appliance-Typ                  | Image-Versionen mit dem Streamvault™ Service                                   | Image-Versionen ohne den Streamvault™ Service  |
|--------------------------------|--|--|
| All-in-One                     | <ul style="list-style-type: none"> <li>11.2024.2</li> </ul>                    | <ul style="list-style-type: none"> <li>16</li> <li>17</li> <li>18</li> <li>19</li> </ul>   |
| SVW                            | <ul style="list-style-type: none"> <li>11.2024.2</li> </ul>                    | <ul style="list-style-type: none"> <li>0010.4</li> <li>0011.2</li> <li>0012.2</li> <li>0013.2</li> </ul>                         |
| SVA                            | <ul style="list-style-type: none"> <li>11.2024.2</li> </ul>                    | <ul style="list-style-type: none"> <li>0010.4</li> <li>0011.2</li> <li>0012.2</li> <li>0013.2</li> </ul>                         |
| SVR                            | <ul style="list-style-type: none"> <li>10.2021.2</li> <li>11.2024.2</li> </ul> | <ul style="list-style-type: none"> <li>0012.2.X</li> </ul>   |
| Andere Streamvault™ Appliances | <ul style="list-style-type: none"> <li>WS.2022.1</li> </ul>                    | <ul style="list-style-type: none"> <li>2016.1.B</li> <li>2016.1.C</li> <li>2019.1</li> <li>2019.4.C</li> <li>2022.1.C</li> </ul> |

**BEMERKUNG:** Informationen zur Ermittlung der Image-Version Ihrer Appliance finden Sie unter [Die System-ID und Image-Version einer Streamvault™ Appliance finden](#) auf Seite 89.

# Erste Schritte mit dem SV Control Panel

Die ersten Schritte stellen das SV Control Panel vor und bieten Informationen über das Einrichten Ihrer Streamvault-Appliance.

Dieser Abschnitt enthält die folgenden Themen:

- ["Informationen über das SV Control Panel"](#) auf Seite 19
- [" Ihre Security-Center-Lizenz auf einer Appliance aktivieren "](#) auf Seite 22
- [" Manuelles Aktivieren einer Lizenz über Server Admin "](#) auf Seite 24
- ["Den System Availability Monitor aktivieren"](#) auf Seite 26
- [" Security-Center-Video- und Zutrittskontrollfunktionen aktivieren "](#) auf Seite 27
- ["Über das Geräteregistrierungs-Tool"](#) auf Seite 30
- [" Standardkameraeinstellungen konfigurieren "](#) auf Seite 33
- [" Benutzerdefinierte Aufzeichnungszeitpläne erstellen "](#) auf Seite 35
- [" Informationen über Sichern und Wiederherstellen "](#) auf Seite 36
- [" Die Methode für das Erstellen von Archiver-Rollen und Partitionen auswählen "](#) auf Seite 39
- [" Verschlüsseln des Betriebssystems "](#) auf Seite 44
- [" Erfassen von Support-Protokollen "](#) auf Seite 48

# Informationen über das SV Control Panel

Das SV Control Panel ist eine Oberflächenanwendung, mit der Sie die Streamvault™-Appliance für die Zusammenarbeit mit Zutrittskontrolle und Videoüberwachung in Security Center konfigurieren können.

**ACHTUNG:** Konfigurationsänderungen, die Sie auf dem SV Control Panel vornehmen, werden Konfigurationsänderungen überschreiben, die außerhalb des SV Control Panel durchgeführt wurden, einschließlich benutzerdefinierter Windows-Einstellungen.

Das SV Control Panel kann in den folgenden Modi ausgeführt werden:

- Erweiterungsmodus für Einrichtungen, die auf einem Erweiterungsserver ausgeführt werden.
- Client-Modus für Einrichtungen, die auf Workstation-Appliances ausgeführt werden.
- Directory-Modus für Einrichtungen, die auf dem Hauptserver ausgeführt werden.

Das SV Control Panel umfasst die folgenden Funktionen:

- Den Assistenten *Einrichtung des Streamvault Control Panel*, um Ihre Appliance schnell einzurichten.
- Den Assistenten *Aktivierung des Streamvault Control Panel*, um Ihre Appliance zu aktivieren.
- Den *Security-Center-Installationsassistenten*, den Sie zum Konfigurieren von Security Center verwenden können.
- Die Assistenten *Streamvault Control Panel – Sichern* und *Streamvault Control Panel – Wiederherstellen* helfen Ihnen dabei, Sicherungen Ihrer Directory-Datenbank und Konfigurationen zu erstellen und diese Dateien bei Bedarf in Ihrem System wiederherzustellen.
- Der Genetec™ Update Service (GUS), der regelmäßig nach Software-Updates sucht.
- Tastaturkürzel für häufig verwendete Tasks in Config Tool und Security Desk.
- Links zum Genetec Technical Assistance Portal (GTAP) und zur Produktdokumentation.
- Die Option zur Auswahl des Betriebsmodus für die mit Ihrer Streamvault™ Appliance gelieferte Cylance Antivirus Software. Die Optionen sind auf der Seite Konfiguration der *Sicherheit* aufgeführt.
- Die Möglichkeit, weitere Archiver-Rollen und Partitionen für Einrichtungen auf Erweiterungsservern zu erstellen.

## BEMERKUNG:

- Diese Anleitung gilt für SV Control Panel Version 3.2.1, die Sie von GTAP herunterladen können.
- SV Control Panel Version 3.0 und höher ist mit Appliances kompatibel, die nicht über den Streamvault™-Service verfügen. Diese Appliances haben jedoch keinen Zugriff auf die Härtingsprofile.

## Einrichten Ihrer Appliance im SV Control Panel

Wenn Sie sich das erste Mal bei Ihrer Streamvault™-Appliance anmelden, öffnet das SV Control Panel den Assistenten *Einrichtung des Streamvault Control Panel*, um Sie durch die Ersteinrichtung zu führen.

### Bevor Sie beginnen

Verbinden Sie die Appliance mit dem Internet.

### Was Sie noch wissen sollten


- Die Einstellungen, die im Assistenten angewendet wurden, können später auf der Seite *Konfiguration* des SV Control Panel geändert werden.
- Bei einem Archiver, Analytik, einer Workstation oder einer anderen Appliance, bei der es sich um einen Security-Center-Erweiterungsserver handelt, werden Sie nicht zur Änderung von Benutzerpasswörtern aufgefordert.

## Prozedur

- 1 Starten Sie Ihre Appliance.

Das SV Control Panel startet mit dem geöffneten Assistenten *Einrichtung des Streamvault Control Panel*.

**BEMERKUNG:** Das SV Control Panel wird automatisch geöffnet, wenn die Appliance zum ersten Mal gestartet wird. Bei nachfolgenden Neustarts müssen sich Benutzer mit ihren Admin-Anmeldedaten anmelden und SV Control Panel starten.

- 2 Klicken Sie auf der Seite *Einführung* auf **Weiter**.
- 3 Konfigurieren Sie auf der Seite *Netzwerk* die IP-Verbindungseinstellungen:
  - a) Wenn Sie DHCP verwenden, um die IP-Adresse automatisch (Standard) zu erhalten, und die IP-Adresse fehlt, klicken Sie auf **Aktualisieren** , um eine neue IP-Adresse zu erhalten. Klicken Sie dann auf **Erneut versuchen**.
  - b) Wenn das Feld **Status** etwas anderes als „Mit dem Internet verbunden“ anzeigt, klicken Sie auf **Erneut versuchen**.
  - c) Wenn das Feld **Status** „Mit dem Internet verbunden“ anzeigt, klicken Sie auf **Weiter**.
- 4 Füllen Sie auf der Seite *Computereinrichtung* die Felder in den Abschnitten *Allgemeine Informationen* und *Regionale Einstellungen* aus.
- 5 So ändern Sie die Sprache der Benutzeroberfläche:
  - a) Wählen Sie unter **Produktsprache** Ihre Sprache aus.
  - b) Starten Sie SV Control Panel neu.
  - c) Wenn der Assistent *Einrichtung des Streamvault Control Panel* erneut geöffnet wird, klicken Sie auf **Weiter** auf der Seite *Computereinrichtung*.
- 6 Wählen Sie auf der Seite *CylancePROTECT konfigurieren* einen Kommunikationsmodus aus:
  - **Online (empfohlen):** Bei Internetverbindung kommuniziert der CylancePROTECT Agent mit Genetec, um über neue Bedrohungen zu berichten, den Agenten zu aktualisieren und Daten für die Verbesserung der mathematischen Modelle zu senden. Diese Option bietet die höchste Schutzstufe.
  - **Getrennt:** Der getrennte Modus ist für eine Appliance ohne Internetverbindung gedacht. In diesem Modus kann sich CylanceProtect nicht mit Genetec™-Verwaltungsservices in der Cloud verbinden und Informationen an sie senden. Ihre Appliance ist vor den meisten Gefahren geschützt. Wartung und Updates sind über den Genetec™ Update Service (GUS) verfügbar.
  - **Ausschalten:** Wählen Sie diesen Modus aus, um CylancePROTECT dauerhaft von Ihrer Appliance zu deinstallieren. Ihre Appliance verwendet Microsoft Defender als Bedrohungsschutz und -erkennung. Es wird nicht empfohlen, CylancePROTECT auszuschalten, wenn die Appliance keine Updates der Virendefinitionen für Microsoft Defender empfangen kann.
- 7 Klicken Sie auf **Quarantäne-Management aktivieren**, um dem Cylance-Symbol in der Taskleiste zusätzliche Funktionen hinzuzufügen, darunter die Option **Quarantäne löschen**, um Dateien zu löschen, die Cylance in Quarantäne gestellt hat.
- 8 Klicken Sie auf der Seite *Berechtigungen* auf **Kennwort modifizieren**, um die Kennwörter für die folgenden Anwendungen zu modifizieren:
  - **Security Center (Admin-Benutzer):** Das Passwort des Admin-Benutzers für Security Desk, Config Tool und Genetec™ Update Service.
  - **Server Admin:** Das Passwort für die Genetec™-Server-Admin-Anwendung.

Wenn es sich bei Ihrer Appliance um einen Erweiterungsserver des Security Centers handelt, werden Sie nicht aufgefordert, Passwörter zu ändern. Wählen Sie **Diesen Schritt überspringen** aus, wenn Sie keine neuen Kennwörter festlegen möchten.
- 9 Wählen Sie auf der Seite *Härtung* eines der folgenden Profile für die Härtung aus:
  - **Microsoft (nur):** Dieses Profil für die Härtung wendet Microsoft-Sicherheitsgrundlagen auf Ihr System an. Microsoft Sicherheits-Baselines sind eine Gruppe von Microsoft-empfohlenen Konfigurationseinstellungen, die auf dem Feedback von Microsoft Security Engineering Teams, Produktgruppen, Partnern und Kunden basieren.
  - **Microsoft mit CIS Stufe 1:** Dieses Härtungsprofil wendet die Microsoft-Sicherheitsbaselines und das Profil des Center for Internet Security (CIS) Level 1 (CIS L1) auf Ihr System an. Das CIS L1 bietet

grundlegende Sicherheitsanforderungen, die auf jedem System mit geringen oder gar keinen Leistungseinbußen oder Funktionseinschränkungen implementiert werden können.

- **Microsoft mit CIS Stufe 2:** Dieses Härtingsprofil wendet die Microsoft-Sicherheitsbaselines und die Profile CIS L1 und Level 2 (L2) auf Ihr System an. Das Profil CIS L2 bietet die höchste Sicherheitsstufe und ist für Organisationen gedacht, in denen Sicherheit von größter Bedeutung ist.

**BEMERKUNG:** Die strenge Sicherheit, die dieses Härtingsprofil mit sich bringt, kann die Systemfunktionalität einschränken und das Remote Management von Servern erschweren.

- **Microsoft mit STIG:** Dieses Profil zur Härtung wendet die Microsoft-Sicherheitsbaselines und die Sicherheit Technical Implementation Guides (STIGs) der Defense Information Systems Agency (DISA) auf Ihr System an. Die DISA STIGs basieren auf den Standards des National Institute of Standards and Technology (NIST) und bieten fortschrittlichen Sicherheitsschutz für Windows-Systeme für die Abteilung des US-Verteidigungsministeriums.

**BEMERKUNG:** Die Seite *Härtung* ist nur für Appliances mit dem Streamvault™ Service verfügbar.

10 Wählen Sie auf der Seite *System Availability Monitor* eine Methode zur Datenerfassung aus:

- **Do not collect data:** Der System Availability Monitor Agent wird installiert, sammelt jedoch keine Daten.
- **Daten werden anonym gesammelt:** Es wird kein Aktivierungscode benötigt. Integritätsdaten werden an einen dedizierten Integritätsüberwachungsdienst gesendet. Dort werden die Objektnamen unkenntlich gemacht und können nicht rückverfolgt werden. Diese Daten werden von Genetec Inc. nur für statistische Zwecke erfasst und sind nicht über GTAP zugänglich.
- **Daten werden gesammelt und mit meinem System verknüpft:** Ein Aktivierungscode ist erforderlich. Die erfassten Integritätsdaten werden mit einem System verknüpft, das mit einer aktiven Systemwartungsvereinbarung registriert ist.

11 Lesen Sie die Vertraulichkeitsvereinbarung, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen in der Vertraulichkeitsvereinbarung** und klicken Sie auf **Anwenden**.

12 Klicken Sie auf der Seite *Zusammenfassung* auf **Schließen**.

Die Option **Aktivierungsassistent nach der Einrichtung starten** ist standardmäßig ausgewählt. Wenn Sie es löschen, werden Sie daran erinnert, das Produkt zu aktivieren.

## Nach Durchführen dieser Schritte

Aktivieren Sie Ihre Appliance vor der Verwendung.

# Ihre Security-Center-Lizenz auf einer Appliance aktivieren

Der Assistent *Aktivieren des Streamvault Control Panel activation* hilft Ihnen dabei, Ihre Security-Center-Lizenz auf Ihrer Streamvault™-Appliance zu aktivieren.

## Bevor Sie beginnen

- Verbinden Sie Ihre Appliance mit dem Internet.
- Vergewissern Sie sich, dass Sie die System-ID und das Passwort haben, die Ihnen nach dem Kauf Ihrer Lizenz zugeschickt wurden.

## Was Sie noch wissen sollten

- Dieser Task gilt nur für Appliances mit einer Internetverbindung. Aktivieren Sie bei Appliances ohne Internetverbindung [Ihre Security-Center-Lizenz manuell über Server Admin](#).
- Sie müssen die Security-Center-Lizenz nur auf der Appliance aktivieren, die die Directory-Rolle hostet, und nicht auf Appliances, bei denen es sich um Erweiterungsserver oder Workstations handelt.

## Prozedur

- 1 Klicken Sie im SV Control Panel auf **Das System ist nicht aktiviert. Klicken Sie hier zum Aktivieren**.  
Der Assistent *Aktivierung des Streamvault Control Panel* wird geöffnet.  
**BEMERKUNG:** Wenn Sie die Meldung *Internetverbindung ist für die Aktivierung erforderlich* sehen, ist Ihre Appliance derzeit nicht mit dem Internet verbunden. Verbinden Sie Ihre Appliance entweder jetzt oder aktivieren Sie Ihre Lizenz manuell über Server Admin.
- 2 Klicken Sie auf der Seite *Aktivierung* auf **System-ID** und dann auf **Weiter**.
- 3 Geben Sie auf der Seite *System-ID* Ihre System-ID ein und klicken Sie dann auf **Weiter**.
- 4 Überprüfen Sie auf der Seite *Zusammenfassung*, ob die System-ID korrekt ist und klicken Sie auf **Aktivieren**.  
Die Seite *Ergebnis* wird geöffnet und zeigt an, dass die Aktivierung erfolgreich war.
- 5 Klicken Sie auf **Weiter**.
- 6 (Optional) Führen Sie auf der Seite *Updates* eine der folgenden Optionen durch:
  - Wenn keine Updates verfügbar sind, klicken Sie auf **Security-Center-Installationsassistent öffnen**.
  - Wenn Updates verfügbar sind, klicken Sie auf **Updates anzeigen**, um den Genetec™ Update Service zu öffnen, und installieren Sie die Updates.
  - Wenn die Update-Überprüfung fehlgeschlagen ist, weil das Directory nicht reagiert, klicken Sie auf **Server Admin öffnen** und stellen Sie sicher, dass das Directory bereit ist.**BEMERKUNG:** Wenn der Genetec Update Service nicht bereit war, kann die Update-Überprüfung fehlschlagen. Sie sehen die Meldung: *Es kann derzeit nicht nach Updates gesucht werden. Wir versuchen es später erneut*.
- 7 Aktivieren oder deaktivieren Sie Synergis™ Software und Genetec™ Mobile auf der Seite *Zusätzliche Funktionen*.  
Diese Funktionen werden nur angezeigt, wenn sie auf Ihrer Appliance installiert sind. Die Genetec-Mobile-Funktion ist nur für Security Center 5.8 und älter verfügbar.
- 8 Schließen Sie den Assistenten *Aktivierung des Streamvault Control Panel*.

## Nach Durchführen dieser Schritte

- (Optional) [Aktivieren Sie den System-Availability-Monitor-Agenten](#).
- [Ihre Security-Center-Einstellungen mithilfe des Security-Center-Installationsassistenten konfigurieren](#)

## Verwandte Themen

[Manuelles Aktivieren einer Lizenz über Server Admin](#) auf Seite 24

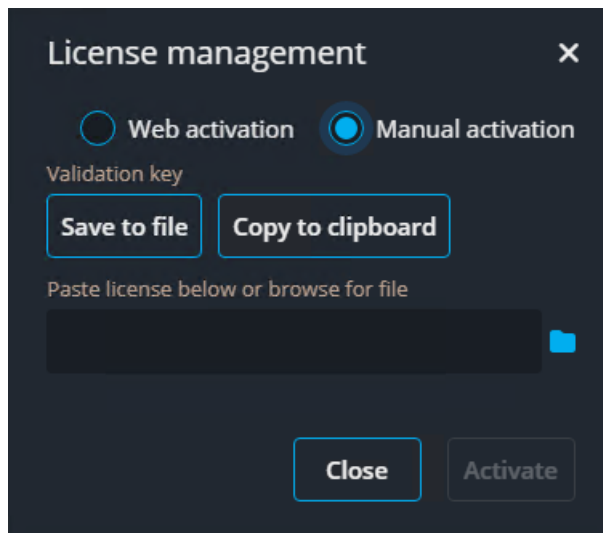
[Informationsseite des SV Control Panel](#) auf Seite 78

# Manuelles Aktivieren einer Lizenz über Server Admin

Wenn Ihre Streamvault™-Appliance keine Internetverbindung hat, müssen Sie Ihre Security-Center-Lizenz manuell über Server Admin aktivieren.

## Prozedur

- 1 Speichern Sie den Validierungsschlüssel:
  - a) Öffnen Sie auf Ihrer Appliance SV Control Panel.
  - b) Klicken Sie auf der Startseite auf das Symbol **Server Admin**.
  - c) Melden Sie sich im Server Admin an.  
Wenn Ihr Server-Admin-Passwort vom Windows-Admin-Passwort abweicht, melden Sie sich bei Server Admin mit den Anmeldedaten an, die im Assistenten *Einrichtung des Streamvault Control Panel* festgelegt sind.
  - d) Klicken Sie auf der Seite *Lizenz* auf **Ändern**.
  - e) Klicken Sie im Dialogfeld *Lizenzmanagement* auf **Manuelle Aktivierung** > **Als Datei speichern**.  
Der Standardname der Datei lautet *validation.vk*.



- f) Kopieren Sie die Datei *validation.vk* auf einen USB-Schlüssel.
  - g) Werfen Sie den USB-Schlüssel auf dem Computer aus.

- 2 Rufen Sie die Lizenz über das Genetec™ Technical Assistance Portal (GTAP) ab:
  - a) Schließen Sie den USB-Schlüssel an einem anderen Computer an, der über eine Internetverbindung verfügt.
  - b) Melden Sie sich beim [GTAP](#) an.
  - c) Geben Sie auf der *GTAP-Anmeldungsseite* die System-ID und das Passwort ein, die Ihnen beim Kauf Ihrer Lizenz zugewiesen wurden, und klicken Sie auf **Anmelden**.
  - d) Klicken Sie auf der Seite *Systeminformationen* auf **Lizenz aktivieren** im Abschnitt *Lizenzinformationen*.
  - e) Geben Sie im Dialogfeld, das geöffnet wird, den Validierungsschlüssel ein oder suchen Sie nach der Datei.
  - f) Suchen Sie im Dialogfenster *Aktivierung* nach der Datei *validation.vk* auf dem USB-Schlüssel und klicken Sie auf **Absenden**.  
Die Meldung *Ihre Lizenz wurde erfolgreich aktiviert* wird angezeigt.
  - g) Klicken Sie auf **Lizenz herunterladen** und speichern Sie dann den Lizenzschlüssel.  
Der Standardname ist Ihre System-ID, gefolgt von *\_Directory\_License.lic*.
  - h) Kopieren Sie die Datei *\_Directory\_License.lic* auf den USB-Schlüssel.
  - i) Werfen Sie den USB-Schlüssel auf dem Computer aus.
- 3 Aktivieren Sie Ihre Lizenz:
  - a) Schließen Sie den USB-Schlüssel an Ihre Appliance an.
  - b) Kehren Sie zu Server Admin zurück.
  - c) Klicken Sie auf der Seite *Lizenz* auf **Ändern**.
  - d) Klicken Sie im Dialogfeld *Lizenzmanagement* auf **Manuelle Aktivierung**.
  - e) Fügen Sie Ihre Lizenzinformationen aus der Datei *License.lic* ein (kann mit einem Textbearbeitungsprogramm geöffnet werden) oder suchen Sie nach der Datei *License.lic* und klicken Sie auf **Öffnen**.
  - f) Klicken Sie auf **Aktivieren**.

## Verwandte Themen

[Ihre Security-Center-Lizenz auf einer Appliance aktivieren](#) auf Seite 22

# Den System Availability Monitor aktivieren

---

Um die Systemverfügbarkeit und Integritätsprobleme im GTAP zu überwachen, können Sie den System Availability Monitor so einrichten, dass er Daten über Ihre Appliance erfasst und sie an Health Monitoring Services sendet.

## Bevor Sie beginnen

Um Integritätsinformationen über Ihre Appliance zu erfassen und zu berichten, müssen Sie einen Aktivierungscode im [GTAP](#) erstellen. Weitere Informationen zum Vorgehen hierfür finden Sie unter [Aktivierungscode für den System Availability Monitor Agent erstellen](#) im TechDoc Hub.

## Prozedur

- 1 Öffnen Sie SV Control Panel.
- 2 Klicken Sie auf der Seite *Konfiguration* im Abschnitt *System Availability Monitor* auf **Konfigurieren**.
- 3 Klicken Sie im Fenster *Genetec System Availability Monitor Agent* auf **Ändern**.
- 4 Stellen Sie sicher, dass das Kontrollkästchen **Daten werden erfasst und mit meinem System verknüpft** aktiviert ist.
- 5 Geben Sie im Feld **Aktivierungscode** den Code für Ihre Appliance ein.
- 6 Klicken Sie auf **OK**.

# Security-Center-Video- und Zutrittskontrollfunktionen aktivieren

Der *Security-Center-Installationsassistent* führt Sie durch die Einrichtung der Hauptfunktionen von Videomanagement und Zutrittskontrolle.

## Was Sie noch wissen sollten

Einstellungen, die Sie im Assistenten anwenden, können später in Config Tool geändert werden.

**Gilt für:** Appliances, die die Directory-Rolle hosten, wie All-in-One-Appliances.

## Prozedur

- 1 Melden Sie sich als Admin-Benutzer an.

**TIPP:** Wenn Ihr Security-Center-Passwort vom Windows-Admin-Passwort abweicht, melden Sie sich bei Security Center mit den Anmeldedaten an, die im Assistenten *Einrichtung des Streamvault Control Panel* festgelegt sind.

Der Security-Center-Installationsassistent wird geöffnet.

- 2 Nachdem Sie die Seite *Intro* gelesen haben, klicken Sie auf **Weiter**.

- 3 Wählen Sie auf der Seite *Verfügbare Funktionen* die gewünschten Funktionen aus und klicken Sie auf **Weiter**.

Grundlegende Funktionen sind standardmäßig aktiviert. Sie können Funktionen später auf der Seite *Funktionen* in der Ansicht **Allgemeine Einstellungen** des Tasks System aktivieren und deaktivieren.

**BEMERKUNG:** Wenn Ihre Lizenz eine Funktion nicht unterstützt, scheint die Funktion nicht in der Liste auf.

- 4 Geben Sie auf der Seite *Kamerasicherheit* den Standardbenutzernamen und das Passwort an, die für alle Ihre Kameras verwendet werden, und klicken Sie dann auf **Weiter**.

**TIPP:** Wählen Sie für zusätzliche Sicherheit die Option **HTTPS verwenden** aus.


- 5 Konfigurieren Sie auf der Seite *Kameraqualitätseinstellungen* die folgenden Optionen:

- **Auflösung:**
  - **Hoch:** 1280x720 und höher
  - **Standard:** Höher als 320x240 und niedriger als 1280x720
  - **Niedrig:** 320x240 und niedriger
  - **Standard:** Standardeinstellungen des Herstellers.

Die Kamera wählt immer die höchste Auflösung, die sie unterstützen kann, aus der ausgewählten Kategorie. Wenn die Kamera keine Auflösungen aus der ausgewählten Kamera unterstützt, verwendet es die höchste Auflösung, die sie unterstützen kann, aus der nächsten Kategorie. Wenn die Kamera keine hohe Auflösung unterstützen kann, verwendet sie die höchste Auflösung aus der Standardgruppe, die sie unterstützen kann.

Die Einstellungen auf dieser Seite können später auf der Seite *Standardkameraeinstellungen* der Archiver-Rolle geändert werden.

- 6 Wählen Sie auf der Seite *Aufzeichnungseinstellungen* die Standardaufzeichnungseinstellungen aus, die auf alle Kameras angewendet werden:
  - **Aus:** Aufzeichnung ist deaktiviert.
  - **Fortlaufend:** Kameras zeichnen fortlaufend auf. Dies ist die Voreinstellung.
  - **Bei Bewegung/Manuell:** Kameras zeichnen auf, wenn die Aufzeichnung durch eine Aktion (wie Aufzeichnung starten, Lesezeichen hinzufügen, Alarm auslösen), Bewegungserkennung oder manuell durch einen Benutzer ausgelöst wird.
  - **Manuell:** Kameras zeichnen auf, wenn die Aufzeichnung durch eine Aktion (wie Aufzeichnung starten, Lesezeichen hinzufügen, Alarm auslösen) oder manuell durch einen Benutzer ausgelöst wird.  
**BEMERKUNG:** Wenn die Einstellung **Manuell** verwendet wird, dann löst Bewegung keine Aufzeichnung aus.
  - **Benutzerdefiniert:** Sie können einen Zeitplan für die Aufzeichnung festlegen.
- 7 Klicken Sie auf **Weiter**.
- 8 Geben Sie auf der Seite *Zutrittskontroll-Einheitensicherheit* dem Standardbenutzernamen und das Passwort für alle Ihre Zutrittskontrollereinheiten an und klicken Sie auf **Weiter**.
- 9 Wählen Sie auf der Seite *Karteneinhaber* aus, wie Sie Berechtigungsnachweise (Karten) und Karteneinhaber hinzufügen möchten.
  - a) Wählen Sie aus, ob Sie Karteneinhaber (wenn der Security-Center-Installationsassistent geschlossen wird) über den Task *Karteneinhaberverwaltung* oder über das Import-Tool hinzufügen möchten.
  - b) Klicken Sie auf **Weiter**.
- 10 Fügen Sie auf der Seite *Benutzer* weitere Benutzer zu Ihrem System hinzu:
  - a) Geben Sie den Benutzernamen ein.
  - b) Wählen Sie den **Benutzertyp** aus:
    - **Operator:** Ein Bediener kann den Task *Überwachung* verwenden, Video anzeigen und Besucher in Security Desk verwalten.
    - **Berichte:** Ein berichtender Benutzer kann die Security-Desk-Anwendung verwenden und die Standardberichtstasks ausführen, außer Tasks für AutoVu™ ALPR. Ein Benutzer, der nur über Berichtsberechtigungen verfügt, kann kein Video anzeigen, physische Geräte steuern oder Vorfälle berichten.
    - **Ermittler:** Ein Ermittler kann den Task *Überwachung nutzen*, um Videos anzuzeigen, PTZ-Kameras zu steuern, Videos aufzuzeichnen und zu exportieren, Lesezeichen und Ereignisse hinzuzufügen, Untersuchungstasks zu nutzen, Alarme und Besucher zu verwalten, Zeitpläne für die Entriegelung von Türen zu überschreiben, Tasks zu speichern und so weiter.
    - **Supervisor:** Ein Supervisor kann den Task *Überwachung nutzen*, um Videos anzuzeigen, PTZ-Kameras zu steuern, Videos aufzuzeichnen und zu exportieren, Lesezeichen und Ereignisse hinzuzufügen, Untersuchungstasks zu nutzen, Alarme und Besucher zu verwalten, Zeitpläne für die Entriegelung von Türen zu überschreiben, Tasks zu speichern und so weiter. Ein Supervisor kann auch die Wartungstasks verwenden, Karteneinhaber und Berechtigungsnachweise verwalten, benutzerdefinierte Felder bearbeiten, Bedrohungsstufen festlegen, Kameras blockieren und Personenzählungen durchführen.
    - **Inbetriebnahme:** Der Benutzer, der die Inbetriebnahme durchführt, hat die meisten Konfigurationsberechtigungen mit folgenden Ausnahmen: Verwalten von Rollen, Makros, Benutzern, Benutzergruppen, benutzerdefinierten Ereignissen, Aktivitätspfaden, Bedrohungsstufen und Audiodateien. Beim Benutzer, der die Inbetriebnahme durchführt, handelt es sich üblicherweise um den Systemeinstallateur.
    - **Einfacher AutoVu-Bediener:** Dieser Benutzertyp ist für Bediener gedacht, die AutoVu ALPR benutzen. Der einfache AutoVu-Benutzer kann ALPR-Tasks verwenden, ALPR-Entitäten konfigurieren, ALPR-Regeln erstellen, ALPR-Ereignisse überwachen usw.
    - **Patroller-Benutzer:** Dieser Benutzertyp ist für Genetec-Patroller™-Benutzer gedacht, die AutoVu ALPR benutzen. Der Patroller-Benutzer kann ALPR-Tasks verwenden, ALPR-Entitäten konfigurieren, ALPR-Regeln erstellen, ALPR-Ereignisse überwachen usw. Ein Patroller-Benutzer hat keinen Zugriff auf andere Security-Center-Anwendungen, beispielsweise Config Tool und Security Desk. Der Patroller-Benutzer kann Berichte nicht bearbeiten oder das Patroller-Passwort ändern.

- 11 Geben Sie das **Passwort** ein und bestätigen Sie es. Klicken Sie anschließend auf **Hinzufügen**.  
Der neue Benutzer wird zur Benutzerliste auf der rechten Seite des Dialogfensters hinzugefügt. Um einen Benutzer zu löschen, wählen Sie einen Benutzer aus der Liste aus und klicken Sie auf .  
Sie können die Benutzerprofile in der Ansicht **Benutzer** des Tasks *Benutzerverwaltung* ändern. Weitere Informationen finden Sie im [Security Center – Administratorhandbuch](#) im TechDoc Hub.
- 12 Klicken Sie auf **Weiter**.
- 13 Bestätigen Sie, dass die Informationen auf der Seite *Zusammenfassung* korrekt sind und klicken Sie dann auf **Anwenden** oder klicken Sie auf **Zurück**, um etwaige Fehler zu korrigieren.
- 14 Klicken Sie auf der Seite *Zusammenfassung* auf **Neu starten**.  
Config Tool startet neu, um Ihre Einstellungen zu übernehmen.  
**BEMERKUNG:** Die Option **Geräteregistrierungs-Tool nach dem Schließen des Assistenten öffnen** ist standardmäßig ausgewählt. Sie können diese Option deaktivieren und das Geräteregistrierungs-Tool zu einem späteren Zeitpunkt öffnen, indem Sie auf die Verknüpfung **Kameras und Steuerungen registrieren** auf der *Startseite* des SV Control Panel klicken.

## Nach Durchführen dieser Schritte

[Fügen Sie Einheiten zu Ihrem System hinzu](#) mithilfe des Geräteregistrierungs-Tools.

## Verwandte Themen

[Standardkameraeinstellungen konfigurieren](#) auf Seite 33

[Benutzerdefinierte Aufzeichnungszeitpläne erstellen](#) auf Seite 35

[Startseite des SV Control Panel](#) auf Seite 69

# Über das Geräteregistrierungs-Tool

Mit dem Tool „Geräteregistrierung“ können Sie IP-Einheiten (Video und Zutrittskontrolle) ermitteln, die an Ihr Netzwerk angeschlossen sind. Die Erkennung kann auf dem Hersteller und auf den Netzwerkeigenschaften (Erkennungspoint, IP-Adressbereich, Kennwort, usw.) basieren. Nachdem Sie eine Einheit entdeckt haben, können Sie sie zu Ihrem System hinzufügen.

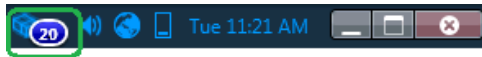
- Das Geräteregistrierungs-Tool öffnet sich automatisch nach dem *Security Center Installationsassistenten*, es sei denn, Sie haben die Option **Geräteanmeldung nach Assistent öffnen** deaktiviert.
- Beim Hinzufügen von Zutrittskontrollgeräten können mit dem Tool zur Geräteregistrierung nur HID- und Synergis™-Einheiten registriert werden. Umfassende Informationen über die Registrierung von Synergis-Einheiten finden Sie im *Synergis™ Appliance – Konfigurationsleitfaden*.

## Öffnen des Unit Enrollment Tools

Es gibt drei Möglichkeiten, um das Unit Enrollment Tool zu öffnen.

### Prozedur

- Führen Sie eine der folgenden Aktionen aus:
  - Klicken Sie auf der Startseite des SV Control Panel auf **+ Kameras und Steuerungen registrieren**.
  - Klicken Sie auf der Startseite des SV Control Panel auf das **Config Tool**-Symbol und klicken Sie dann auf **Tasks > Unit Enrollment**.
  - Klicken Sie auf der Startseite des SV Control Panel auf das **Config Tool**-Symbol und klicken Sie dann auf das **Einheitenstatus hinzufügen**-Symbol in the Config Tool in der Config-Tool-Benachrichtigungsleiste.



## Konfigurieren von Geräteerkennungseinstellungen

Über die Schaltfläche **Einstellungen und Hersteller** im Unit Enrollment Tool können Sie angeben, welche Hersteller in die Suche nach neuen Einheiten aufgenommen werden sollen. Sie können auch die Erkennungseinstellungen für Geräte konfigurieren und Benutzernamen und Passwörter für Geräte festlegen, um die Geräteerkennung zu vereinfachen.


### Prozedur

- 1 Klicken Sie auf der Startseite auf **Tools > Unit Enrollment**.
- 2 Klicken Sie im Dialogfeld *Geräteerkennung* auf **Einstellungen und Hersteller** ( ).
- 3 Verwenden Sie die Option **Basis-Authentifizierung ablehnen**, um die Basis-Authentifizierung zu aktivieren oder zu deaktivieren (nur bei Videoeinheiten). Dies ist dann nützlich, wenn Sie im Security Center InstallShield die Basic-Authentifizierung ausgeschaltet haben, diese jedoch wieder anschalten müssen, um ein Firmware-Upgrade auszuführen oder eine Kamera anzumelden, die nur Basic-Authentifizierung unterstützt. Um die Basis-Authentifizierung wieder zu aktivieren, müssen Sie die Option **Basis-Authentifizierung ablehnen** auf **AUS** setzen.

**BEMERKUNG:** Diese Option ist nur für Benutzer mit Administratorrechten verfügbar.

- 4 Klicken Sie auf **Hersteller hinzufügen** (+), um einen Hersteller in die Liste der zu erfassenden Geräte aufzunehmen.


Um einen Hersteller aus der Liste zu entfernen, wählen Sie ihn aus und klicken Sie auf ✖.

- 5 Konfigurieren Sie die speziellen Einstellungen für jeden Hersteller, den Sie hinzugefügt haben. Wählen Sie hierfür den Hersteller aus und klicken Sie auf .
- WICHTIG:** Sie müssen den richtigen Benutzernamen und das Passwort eingeben, damit das Gerät ordnungsgemäß angemeldet wird.
- 6 (Optional) Entfernen Sie Geräte aus der Liste ignorierte Geräte (siehe [Entfernen von Einheiten aus der Liste ignorierte Geräte](#) auf Seite 32).
- 7 Klicken Sie auf **Speichern**.

## Hinzufügen von Geräten

Sobald neue Geräte ermittelt wurden, können Sie diese Geräte mithilfe des Tools für Geräteerkennung Ihrem System hinzufügen.

### Prozedur

- 1 Klicken Sie auf der Startseite auf **Tools > Unit Enrollment**.
- 2 Es gibt drei Möglichkeiten, neu ermittelte Geräte hinzuzufügen:
  - Sie können all neu ermittelten Geräte gleichzeitig hinzufügen. Klicken Sie hierfür auf die Schaltfläche **Alle hinzufügen** () im Dialogfeld unten rechts.
  - Klicken Sie auf eine einzelne Einheit in der Liste und dann in der Spalte **Status** auf **Hinzufügen**.
  - Rechtsklicken Sie auf ein einzelnes Gerät in der Liste und klicken Sie auf **Hinzufügen oder Gerät hinzufügen....**

Wenn Benutzername und Passwort einer Videoeinheit nicht korrekt sind, wird der **Status** der Einheit als **Ungültige Anmeldung** aufgeführt und Sie werden aufgefordert, beim Hinzufügen der Einheit die richtigen Informationen einzugeben. Wenn Sie für alle Kameras in Ihrem System den gleichen Benutzernamen und das gleiche Passwort verwenden möchten, wählen Sie die Option **Als Standard-Authentifizierung für alle Hersteller speichern**.

Sie können eine Einheit auch manuell hinzufügen, indem Sie auf die Schaltfläche **Manuell hinzufügen** klicken, die sich unten im Dialogfeld *Unit Enrollment Tool* befindet.

#### BEMERKUNG:

- Bei Videoeinheiten, bei denen die hinzugefügte Kamera ein Codierer mit Mehrfachstreaming-Option ist, wird jeder Stream mit der *Kamera - n*-Zeichenfolge an den Kameranamen angehängt, wobei *n* für die Streamnummer steht. Bei IP-Kameras, die nur einen Stream liefern können, wird der Kameraname nicht geändert.
- Wenn Sie eine SharpV hinzufügen, enthalten die Kameraeinheiten standardmäßig ein selbstsigniertes Zertifikat, das den allgemeinen Namen der SharpV verwendet (z. B. SharpV12345). Um die SharpV zum Archiver hinzuzufügen, müssen Sie ein neues Zertifikat (signiert oder selbstsigniert) generieren, das die IP-Adresse der Kamera anstelle des allgemeinen Namens verwendet.

## Löschen von hinzugefügten Einheiten

Sie können Einheiten löschen, die bereits auf dem System hinzugefügt wurden, damit sie nicht jedes Mal angezeigt werden, wenn Sie mit dem Tool für Geräteerkennung nach Einheiten auf Ihrem System suchen.

### Was Sie noch wissen sollten

Die Option **Fertiggestellte löschen** im Unit Enrollment Tool ist dauerhaft und kann nicht rückgängig gemacht werden.

### Prozedur

- 1 Fügen Sie die erkannten Einheiten zu Ihrem System hinzu, siehe [Hinzufügen von Geräten](#) auf Seite 31.
- 2 Klicken Sie nach dem Hinzufügen auf **Fertiggestellte löschen**.  
Jede Einheit, bei der **Hinzugefügt** in der **Status**-Spalte angezeigt wird, wird aus der Liste der erkannten Einheiten gelöscht.

## Ignorieren von Geräten

Sie können Geräte ignorieren, sodass diese nicht in der Liste der erkannten Geräte des Tools für Geräteerkennung erscheinen.

### Prozedur

- 1 Klicken Sie auf der Startseite auf **Tools > Unit Enrollment**.  
Das Tool Geräteerkennung öffnet sich und zeigt eine Liste der Geräte, die im System erkannt wurden.
- 2 Rechtsklicken Sie auf das Gerät, das ignoriert werden soll und wählen Sie **Ignorieren**.  
Das Gerät wird aus der Liste entfernt und ignoriert, wenn das Tool Geräteerkennung neue Geräte erkennt. Weitere Informationen über das Entfernen von Geräten aus der Liste ignoriierter Geräte, siehe [Entfernen von Einheiten aus der Liste ignoriierter Geräte](#) auf Seite 32.

## Entfernen von Einheiten aus der Liste ignoriierter Geräte

Sie können eine Einheit aus der Liste der ignorierten Geräte entfernen. Diese Einheit wird dann ignoriert, wenn das Tool Geräteerkennung eine Suche durchführt.

### Prozedur

- 1 Klicken Sie auf der Startseite auf **Tools > Unit Enrollment**.
- 2 Klicken Sie in der oberen rechten Ecke des Dialogfelds *Geräteerkennung* auf **Einstellungen und Hersteller** (⚙️).
- 3 Klicken Sie auf **Ignorierte Geräte** und dann auf **Alle ignorierten Geräte entfernen**. Oder wählen Sie eine Einheit aus und klicken Sie auf **Ignoriertes Gerät entfernen** (✖️).

# Standardkameraeinstellungen konfigurieren


Sie können unter *Standardkameraeinstellungen* die Standardaufzeichnungs- und Videoqualitätseinstellungen bearbeiten, die auf alle Kameras angewendet werden, die vom Archiver gesteuert werden. Anfänglich werden diese Einstellungen auf der Seite *Kameraqualitätseinstellungen* im Security-Center-Installationsassistenten konfiguriert.

## Was Sie noch wissen sollten

Sie können auch Video- und Aufzeichnungseinstellungen für eine Kamera in Config Tool mithilfe der Registerkarte **Video und Aufzeichnung** der Einheit anwenden. Einstellungen, die für eine individuelle Kamera festgelegt wurden, haben Vorrang vor den Einstellungen, die im Security-Center-Installationsassistenten oder auf der Seite *Standardkameraeinstellungen* angewendet wurden.

## Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Video*.
- 2 Wählen Sie die Archiver-Rolle aus und klicken Sie auf die Registerkarte **Standardkameraeinstellungen**.
- 3 Konfigurieren Sie unter **Videoqualität (für alle Archiver gleich)** Folgendes:
  - **Auflösung:**
    - **Hoch:** 1280x720 und höher
    - **Standard:** Höher als 320x240 und niedriger als 1280x720
    - **Niedrig:** 320x240 und niedriger
    - **Standard:** Standardeinstellungen des Herstellers.

Die Kamera wählt immer die höchste Auflösung, die sie unterstützen kann, aus der ausgewählten Kategorie. Wenn die Kamera keine Auflösungen aus der ausgewählten Kamera unterstützt, verwendet es die höchste Auflösung, die sie unterstützen kann, aus der nächsten Kategorie. Wenn die Kamera keine hohe Auflösung unterstützen kann, verwendet sie die höchste Auflösung aus der Standardgruppe, die sie unterstützen kann.
- 4 Klicken Sie unter **Aufzeichnung** auf , um einen Zeitplan hinzuzufügen.  
Verfügbare Zeitpläne umfassen:
  - Zeitpläne, die mithilfe der Ansicht **Zeitpläne** im Task *System* erstellt wurden.
  - Einen benutzerdefinierten Zeitplan, wenn einer im Security-Center-Installationsassistenten erstellt wurde.
- 5 Wählen Sie im Drop-down-Menü **Modus** einen Modus für den Aufzeichnungszeitplan aus.
  - **Aus:** Aufzeichnung ist deaktiviert.
  - **Fortlaufend:** Kameras zeichnen fortlaufend auf. Dies ist die Voreinstellung.
  - **Bei Bewegung/Manuell:** Kameras zeichnen auf, wenn die Aufzeichnung durch eine Aktion (wie Aufzeichnung starten, Lesezeichen hinzufügen, Alarm auslösen), Bewegungserkennung oder manuell durch einen Benutzer ausgelöst wird.
  - **Manuell:** Kameras zeichnen auf, wenn die Aufzeichnung durch eine Aktion (wie Aufzeichnung starten, Lesezeichen hinzufügen, Alarm auslösen) oder manuell durch einen Benutzer ausgelöst wird.

**BEMERKUNG:** Wenn die Einstellung **Manuell** verwendet wird, dann löst Bewegung keine Aufzeichnung aus.

  - **Benutzerdefiniert:** Sie können einen Zeitplan für die Aufzeichnung festlegen.

6 Stellen Sie folgende Optionen ein:

- **Audio aufzeichnen:** Aktivieren Sie diese Option, wenn Sie Audio zusammen mit Video aufzeichnen möchten. Damit diese Option funktioniert, müssen Ihre Kameras mit Mikrofonen ausgestattet sein.
- **Redundante Archivierung:** Aktivieren Sie diese Option, wenn Sie möchten, dass sowohl der primäre als auch der sekundäre Server Video gleichzeitig archivieren. Diese Einstellung ist nur dann wirksam, wenn Failover konfiguriert ist.
- **Automatische Bereinigung:** Aktivieren Sie diese Option, wenn Sie Video nach einer bestimmten Anzahl von Tagen löschen möchten. Video wird gelöscht, ob der Archiver-Speicher voll ist oder nicht.
- **Aufzuzeichnende Zeit vor einem Ereignis:** Legen Sie mit dem Schieberegler die Anzahl der Sekunden fest, die vor einem Ereignis aufgezeichnet werden sollen. Bei jedem Beginn einer Aufzeichnung wird dieser Puffer gespeichert. Das stellt sicher, dass der auslösende Faktor der Aufzeichnung ebenfalls auf Video erfasst wird.
- **Aufzuzeichnende Zeit nach Bewegung:** Legen Sie die Anzahl der Sekunden fest, die nach einem Bewegungsereignis aufgezeichnet werden sollen. In diesem Zeitraum kann der Benutzer die Aufzeichnung nicht anhalten.
- **Standard für manuelle Aufzeichnungsdauer :** Legen Sie die Anzahl der Minuten fest, wie lange eine Aufzeichnung dauern soll, wenn sie von einem Benutzer gestartet wird. Der Benutzer kann die Aufzeichnung jederzeit anhalten, bevor die Dauer abläuft. Dieser Wert wird auch von der Aktion „Aufzeichnung starten“ verwendet, wenn die Standardaufzeichnungslänge ausgewählt ist.

7 Klicken Sie auf **Übernehmen**.

8 Wenn Sie die neuen Einstellungen auf alle vorhandenen Kameras anwenden möchten, klicken Sie auf **Ja**.


## Verwandte Themen

[Security-Center-Video- und Zutrittskontrollfunktionen aktivieren](#) auf Seite 27

# Benutzerdefinierte Aufzeichnungszeitpläne erstellen


Erstellen Sie im Security-Center-Installationsassistenten benutzerdefinierte Aufzeichnungszeitpläne, damit Kameras in unterschiedlichen Aufzeichnungsmodi für einen bestimmten Zeitbereich aufzeichnen.

## Prozedur

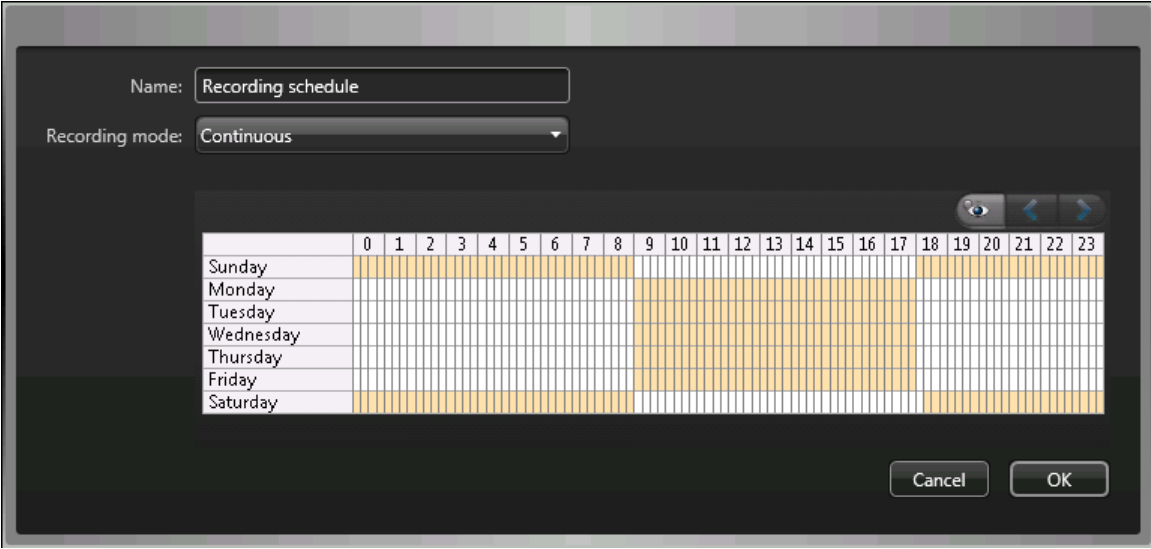
- 1 Klicken Sie auf der Seite *Aufzeichnungseinstellungen* auf  unter **Aufzeichnungszeitplan**.
- 2 Geben Sie einen Namen für den neuen Zeitplan ein.
- 3 Wählen Sie aus der Liste **Aufzeichnungsmodus** eine der folgenden Optionen aus:
  - **Aus:** Aufzeichnung ist deaktiviert.
  - **Fortlaufend:** Kameras zeichnen fortlaufend auf. Dies ist die Voreinstellung.
  - **Bei Bewegung/Manuell:** Kameras zeichnen auf, wenn die Aufzeichnung durch eine Aktion (wie Aufzeichnung starten, Lesezeichen hinzufügen, Alarm auslösen), Bewegungserkennung oder manuell durch einen Benutzer ausgelöst wird.
  - **Manuell:** Kameras zeichnen auf, wenn die Aufzeichnung durch eine Aktion (wie Aufzeichnung starten, Lesezeichen hinzufügen, Alarm auslösen) oder manuell durch einen Benutzer ausgelöst wird.

**BEMERKUNG:** Wenn die Einstellung **Manuell** verwendet wird, dann löst Bewegung keine Aufzeichnung aus.

  - **Benutzerdefiniert:** Sie können einen Zeitplan für die Aufzeichnung festlegen.
- 4 Geben Sie für jeden Wochentag einen Zeitbereich für die Aufzeichnung an:
  - Klicken und ziehen Sie, um einen Zeitblock auszuwählen.
  - Klicken Sie mit der rechten Maustaste und ziehen Sie, um einen Zeitblock zu löschen.
  - Verwenden Sie die Pfeiltasten, um in der 24-Stunden-Zeitleiste zu scrollen.

**TIPP:** Um zum Hochauflösungsmodus zu wechseln, wobei jeder Block für eine Minute steht, klicken Sie auf .

Das folgende Beispiel zeigt einen Zeitplan, wobei die Aufzeichnung durchgehend von 18:00 bis 09:00 Uhr an Wochenenden und von 09:00 bis 17:00 Uhr an Wochentagen erfolgt.



## Verwandte Themen

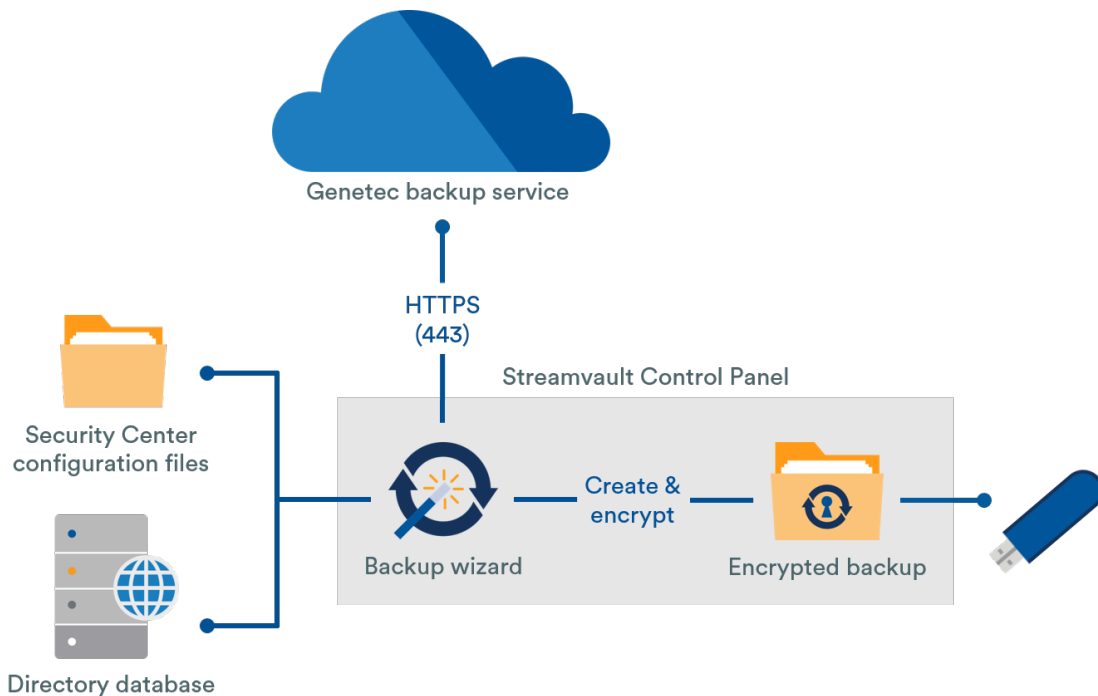
[Security-Center-Video- und Zutrittskontrollfunktionen aktivieren](#) auf Seite 27

# Informationen über Sichern und Wiederherstellen

Mithilfe des SV Control Panel können Sie Ihre Directory-Datenbank und Konfigurationsdateien sichern. Sie können sie später im Fall eines Systemausfalls oder System-Upgrades auf die gleiche System-ID wiederherstellen.

## So funktioniert das Sichern und Wiederherstellen in SV Control Panel

Sie erstellen Sicherungen Ihrer Directory-Datenbank und Ihrer Konfigurationsdateien und speichern Sie lokal oder in der Cloud. Das folgende Architekturdiagramm zeigt, wie Sicherungen im SV Control Panel funktionieren:



## Vorteile von Sicherung und Wiederherstellung

- Mithilfe des Assistenten *Wiederherstellen* können Sie jede der fünf Cloud-Sicherungen oder jede Ihrer lokalen Sicherungen auf der gleichen System-ID wiederherstellen.
- Alle Sicherungsdateien können verschlüsselt werden.
- Das System wird nach fünf fehlgeschlagenen Anmeldeversuchen gesperrt.
- Sie müssen nicht im Genetec™-Advantage-Programm registriert sein, um diese Funktion zu verwenden.

## Einschränkungen von Sicherung und Wiederherstellung

- Eine Sicherung schließt ihre Lizenzdateien, Videoarchiver oder andere Datenbanken aus.
- Sie können eine Sicherung nicht auf einer älteren Version von Security Center wiederherstellen. Sie können beispielsweise keine Sicherung von einem Security-Center-5.10-System auf einem Security-Center-5.9-System wiederherstellen.
- Sie können die Konfigurationsdateien nicht wiederherstellen, wenn Sie zwischen Hauptversionen von Security Center wiederherstellen. Sie können beispielsweise keine Konfigurationsdateien von einer Sicherung eines Security-Center-5.9-Systems auf einem Security-Center-5.10-System wiederherstellen.

## Verwandte Themen

[Ihre Directory-Datenbank sichern](#) auf Seite 37

[Ihre Directory-Datenbank wiederherstellen](#) auf Seite 38

## Ihre Directory-Datenbank sichern

Sie können Sichern und Wiederherstellen verwenden, um Ihre Directory-Datenbank und Konfigurationsdateien zu sichern. Sichern und Wiederherstellen erleichtert das Konfigurieren Ihres Systems nach einem Hardware-Upgrade und kann Ihre Konfigurationen nach einem Systemausfall wiederherstellen.

### Bevor Sie beginnen

Stellen Sie Folgendes sicher:

- Security Center 5.9 oder neuer ist installiert.
- Genetec™ Server wird ausgeführt
- Sie haben eine gültige und aktive Lizenz.

### Was Sie noch wissen sollten

- 
- Nur Administratoren können eine Sicherung durchführen und alle Sicherungen in der Cloud müssen authentifiziert werden.

### Prozedur

- 1 Klicken Sie im SV Control Panel auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie unter *Directory und Konfigurationen sichern/wiederherstellen* auf **Sicherungsassistent > Weiter**.
- 3 Wählen Sie auf der Seite *Sicherungsmethode* entweder **Cloud** oder **Lokal** aus und klicken Sie dann auf **Weiter**.
  - Wenn Sie **Cloud** ausgewählt haben, führen Sie die folgenden Schritte durch:
    - a. Geben Sie auf der Seite *Authentifizierung* entweder Ihre System-ID oder Ihre GTAP-Anmeldedaten ein, um die Sicherung zu authentifizieren.  
**BEMERKUNG:** Wenn Sie Ihre Anmeldedaten das erste Mal eingegeben haben, werden Sie bei zukünftigen Sicherungen nicht mehr gefragt.
    - b. Wählen Sie auf der Seite *Sicherheit* eine der folgenden zwei Optionen aus:
      - **Genetec meine Sicherheit verwalten lassen:** Sie müssen kein Passwort eingeben. Der Sicherungs-Cloud-Service von Genetec Inc. verschlüsselt Ihre Daten.
      - **Mein eigenes Passwort verwenden:** Erstellen Sie Ihr eigenes Passwort und merken Sie es sich, um es später für die Verschlüsselung Ihrer Sicherungsdateien zu verwenden.  
**WICHTIG:** Wenn Sie Ihr Passwort verlieren oder vergessen, kann Genetec Inc. das verlorene Passwort nicht wiederherstellen.
  - Wenn Sie **Lokal** ausgewählt haben, führen Sie die folgenden Schritte aus:
    - a. Geben Sie auf der Seite *Zielordner* einen Namen für das Backup ein und navigieren Sie zum Ordner, in dem Sie die Sicherung speichern möchten.
    - b. Erstellen Sie auf der Seite *Sicherheit*, um Ihre Sicherungsdatei zu verschlüsseln. Sie können auch **Meine Sicherung nicht verschlüsseln** auswählen, obwohl das nicht empfehlenswert ist.
- 4 Befolgen Sie die restlichen Schritte im Assistenten, um Ihre Sicherung abzuschließen.

## Verwandte Themen

[Informationen über Sichern und Wiederherstellen](#) auf Seite 36

[Ihre Directory-Datenbank wiederherstellen](#) auf Seite 38

## Ihre Directory-Datenbank wiederherstellen

Wenn Sie Ihre Directory-Datenbank und Konfigurationsdateien mithilfe von Sichern und Wiederherstellen im SV Control Panel gesichert haben, können Sie Ihre Sicherungsdateien zur gleichen System-ID wiederherstellen. Sicherungsdateien können im Fall eines Systemausfalls oder eines Hardware-Upgrades wiederhergestellt werden.

### Bevor Sie beginnen

Stellen Sie Folgendes sicher:

- Security Center 5.9 oder neuer ist installiert.
- Genetec™ Server wird ausgeführt
- Sie haben eine gültige und aktive Lizenz.

### Was Sie noch wissen sollten

- Wenn Sie Ihre Dateien in der Cloud gesichert haben, können Sie jede der letzten fünf Sicherungen auf der gleichen System-ID wiederherstellen.
- Wenn Sie Ihre Dateien lokal gesichert haben, können Sie jede Ihrer Sicherungen auf der gleichen System-ID wiederherstellen.
- Wenn Sie während des Sicherungsvorgangs Ihr eigenes Passwort für Ihre verschlüsselten Sicherungsdateien erstellt haben, benötigen Sie es zum Wiederherstellen Ihrer Dateien.

### Prozedur

- 1 Klicken Sie im SV Control Panel auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie unter *Directory und Konfigurationen sichern/wiederherstellen* auf **Wiederherstellungsassistent > Weiter**.
- 3 Wählen Sie auf der Seite *Wiederherstellungsmethode* entweder **Cloud** oder **Lokal** aus.  
Wenn Sie **Cloud** ausgewählt haben, geben Sie auf der Seite *Authentifizierung* entweder Ihre System-ID oder GTAP-Anmeldedaten ein, abhängig davon, was Sie für die Authentifizierung der Sicherung verwendet haben. Wenn Sie Ihre GTAP-Anmeldedaten verwenden, wird ein Aktivierungscode an Ihre E-Mail-Adresse gesendet.
- 4 Wählen Sie auf der Seite *Sicherungsauswahl* die Datei aus, die Sie auf Ihrem System wiederherstellen möchten.
- 5 Wenn Sie beim Sicherungsvorgang ein Passwort wählen, müssen Sie auf der Seite *Wiederherstellen* das Passwort eingeben.
- 6 Befolgen Sie die restlichen Schritte im Assistenten, um den Wiederherstellungsvorgang abzuschließen.

## Verwandte Themen

[Ihre Directory-Datenbank sichern](#) auf Seite 37

[Informationen über Sichern und Wiederherstellen](#) auf Seite 36

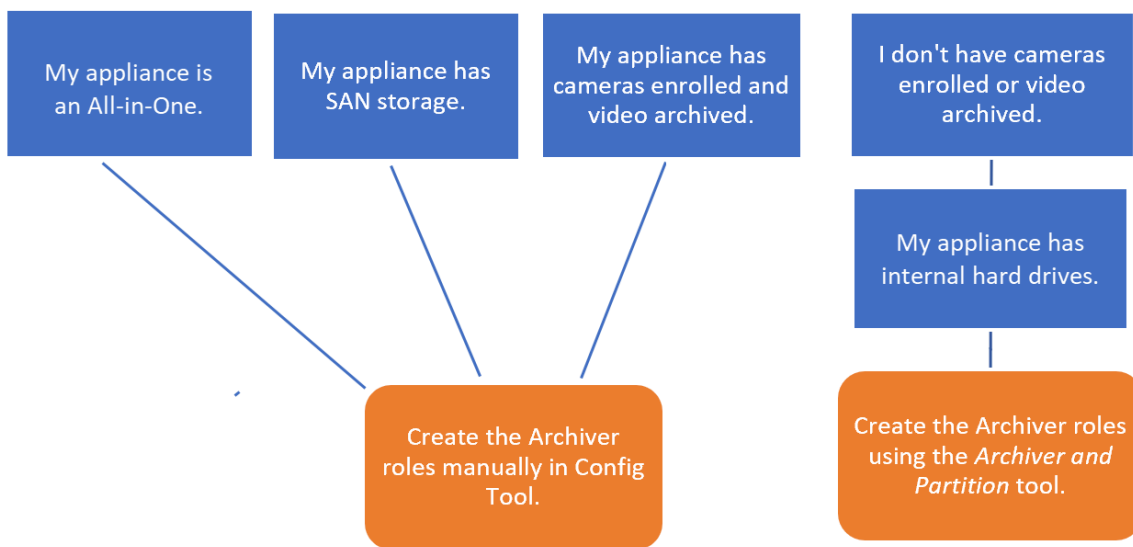
# Die Methode für das Erstellen von Archiver-Rollen und Partitionen auswählen

Um Ihre Appliance für die erwartete Anzahl von Kameras und Bandbreitenauslastung einzurichten, möchten Sie ausreichend Archiver-Rollen erstellen. Abhängig vom Typ und Status Ihrer Appliance können Sie zwischen zwei Methoden wählen.

- [Das Tool für Archiver Rollen und Partitionen verwenden.](#)
- [Partitionen und Archiver-Rollen manuell erstellen.](#)

## Die Methode für Ihre Situation auswählen

Verwenden Sie den folgenden Entscheidungsbaum, um zu entscheiden, welche Methode Sie verwenden sollen:



## Informationen über das Tool für Archiver-Rollen und Partitionen

Sie können auf das Tool für Archiver-Rollen und Partitionen im SV Control Panel zugreifen. Das Tool berechnet, wie viele Archiver-Rollen Sie benötigen, basierend auf der Anzahl der Kameras, die Sie bereitstellen möchten, sowie ihrer erwarteten Bandbreite.

Dieses Tool ist nur auf Streamvault™-Modellen verfügbar, die eine interne Festplatte haben. Wenn Sie ein externes Speichergerät wie eine SAN- oder Streamvault™-SV-7000EX-Appliance einrichten, befolgen Sie die Schritte unter [Partitionen und Archiver-Rollen manuell hinzufügen](#) auf Seite 41.

Wenn das Tool Partitionen erstellt, werden alle lokalen Laufwerke außer C: gelöscht und vorhandene Archiver-Rollen und registrierte Kameras werden aus Security Center entfernt. Wenn Ihre Appliance also über Kameras und aufgezeichnetes Video verfügt, das Sie behalten möchten, [fügen Sie die Partitionen und Archiver-Rollen manuell hinzu](#).

## Archiver-Rollen im SV Control Panel hinzufügen

Verwenden Sie das Tool für Archiver-Rollen und Partitionen, um ausreichend Archiver-Rollen hinzuzufügen, um den erwarteten Videodatenverkehr zu unterstützen. Dieses Tool ist auf Archiver-Appliances der Streamvault™-Serien 1000, 2000 und 4000 verfügbar.

## Bevor Sie beginnen

- Wählen Sie die entsprechende Methode für das Erstellen von Archiver-Rollen und Partitionen aus.
- Sichern Sie die wichtigen Daten auf der Festplatte, auf der Sie eine Partition erstellen möchten.  
**ACHTUNG:** Das Tool für Archiver-Rollen und Partitionen kann bestehende Daten löschen, einschließlich der Archiver-Rollenkonfiguration und aller Dateien auf dem D:-Laufwerk.

## Prozedur

- 1 Klicken Sie im SV Control Panel auf die Registerkarte **Konfiguration**.
- 2 Klicken Sie unter *Archiver-Rollen und Partitionen* auf **Konfigurieren**.

Das Dialogfeld *Archiver-Rollen und Partitionen* wird geöffnet.

- 3 Wählen Sie eine der folgenden Optionen aus, um die Anzahl der Archiver-Rollen und Partitionen zu konfigurieren:
  - Damit das Tool die Anzahl der Rollen und Partitionen sowie die Partitionsgröße, die Sie benötigen, berechnen kann, wählen Sie **Empfohlenes Szenario** aus. Geben Sie die Anzahl von Kameras ein, die Sie voraussichtlich bereitstellen werden, sowie den erwarteten Durchsatz jeder Kamera.
  - Um die Anzahl der Archiver-Rollen und Partitionen anzugeben, die erstellt werden sollen, wählen Sie **Benutzerdefiniertes Szenario** aus. Geben Sie die Anzahl der Archiver-Rollen, die Anzahl der Partitionen und die Partitionsgröße an.

Die Anzahl der Partitionen muss ein Mehrfaches der Anzahl der Archiver-Rollen sein.

**ACHTUNG:** Dateien auf der Festplatte, auf der Sie eine Partition erstellen, werden gelöscht.

- 4 Klicken Sie auf **Partitionen und Rollen erstellen**.

**Archiver Roles and Partitions**

An Archiver role can support:

- 300 cameras
- Throughput of 500 Mbps
- Partitions with a maximum size of 30 TB

Your model (SV-1000-R14-72T-8-210) supports:

- 400 cameras
- 400 Mbps

☒ Suggested scenario

Number of cameras:  Number of roles:

Camera throughput:  Number of partitions:

Size of partitions (TB):

☐ Custom scenario

Number of roles:  Total disk space (TB):

Number of partitions:  Used disk space (TB):

Size of partitions (TB):  Free disk space (TB):

Create partitions/roles

- 5 Aktivieren Sie im Fenster *Warnung* das Kontrollkästchen, um zu bestätigen, dass Sie fortfahren möchten.

- 6 Klicken Sie auf **OK**.

Das Fenster *Ergebnis* wird geöffnet und die Namen und Standorte der Archiver-Rollen und Partitionen werden angezeigt. Jeder Archiver-Rolle wird automatisch ein Laufwerksbuchstabe zugewiesen.

## Partitionen und Archiver-Rollen manuell hinzufügen

Um Ihre Streamvault™-SV-7000EX- oder Streamvault™-SV-300E-All-in-One-Appliance zum ersten Mal einzurichten, müssen Sie manuell Partitionen erstellen. Sie können Archiver-Rollen auch manuell zu einer Appliance hinzufügen, auf der sich bereits Daten befinden, damit die Daten nicht verloren gehen.

### Bevor Sie beginnen

[Wählen Sie eine Methode für das Erstellen von Partitionen auf Ihrer Appliance aus.](#)

### Was Sie noch wissen sollten

Beim Formatieren eines Laufwerks werden die Daten auf der Partition gelöscht. Um Daten aufzubewahren, verkleinern Sie das Laufwerk und erstellen Sie neue Laufwerke.

### Prozedur

- 1 Führen Sie Folgendes durch, wenn auf der Appliance bereits Kameras registriert, Videos archiviert oder Zutrittskontrolldaten vorhanden sind.
  - a) [Sichern Sie die Directory-Datenbank mithilfe des SV Control Panel.](#)
  - b) Erstellen Sie einen Bericht *Kamerakonfiguration*, um einen Schnappschuss Ihrer aktuellen Kamerakonfiguration zu machen. Weitere Informationen finden Sie unter [Kameraeinstellungen anzeigen](#) im TechDoc Hub.
- 2 Erstellen Sie die Laufwerke, die Sie für die Archiver-Rollen benötigen, die Sie auf der Appliance erstellen möchten.
  - Erstellen Sie auf Appliances, die mit SAN-Speicher verbunden sind, wie SV-7000EX, eine logische Einheitennummer (Logical Unit Number, LUN) für jede Archiver-Rolle.
  - Verwenden Sie bei Appliances, wie SV-1000E, SV-2000E und SV-4000E, das Windows-Tool *Datenträgerverwaltung*, um die Laufwerke einzurichten.

- 3 Erstellen Sie eine Archiver-Rolle in Security Center:
  - a) Öffnen Sie auf der Config Tool-Startseite den *System*-Task und klicken Sie auf die Ansicht **Rollen**.
  - b) Klicken Sie auf **Eine Entität hinzufügen** und wählen Sie **Archiver** aus.  
Der Assistent für die Archiver-Rollenkonfiguration wird geöffnet.
  - c) Geben Sie auf der Seite *Spezifische Informationen* einen Namen für die Archiver-Rollen**datenbank** ein und klicken Sie auf **Weiter**.  
Jede Archiver-Rolle muss eine dedizierte Datenbank haben.

Creating a role: Archiver

**Specific info**

Basic information

Creation summary

Entity creation outcome

Database server: (local)\SQLEXPRESS

Database: Archiver5

- d) Geben Sie im Abschnitt **Basisinformation** den **Entitätsnamen** ein und klicken Sie auf **Weiter**.  
Es ist eine bewährte Methode, dass der Datenbankname der Archiver-Rolle dem Entitätsnamen entspricht.

Creating a role: Archiver

Specific info

**Basic information**

Creation summary

Entity creation outcome

Fill in the following fields. The entity description is optional.

Entity name: Archiver5

Entity description:


- e) Vergewissern Sie sich, dass die Informationen, die auf der Seite *Zusammenfassung des Anlegens* gezeigt werden, korrekt sind und klicken Sie dann auf **Erstellen**.
- 4 Konfigurieren Sie die Archiver-Rolle.
  - a) Wählen Sie im Entitäts-Browser Ihre neue Archiver-Rolle aus und klicken Sie auf **Ressourcen**.
  - b) Klicken Sie auf **+**, um den Bereich *Server* zu erweitern, und wählen Sie eine Netzwerkschnittstellenkarte (NIC) aus der Liste **Netzwerkarte** aus.  
Alle Archiver-Rollen müssen die gleiche NIC verwenden.

Server: VM9084

Network card: 10.2.110.157 - Ethernet0

RTSP port: 558 and 608 Telnet port: 5605

- c) Wählen Sie unter *Aufzeichnung* eine **Festplattengruppe** oder einen **Netzwerkort** für die Archiver-Rolle aus oder erstellen Sie diese/n.  
Jede Archiver-Rolle benötigt einen dedizierten Aufzeichnungsort. Wenn Archiver A auf die Festplatten A, B und C schreibt, sollte Archiver B auf die Festplatten D, E und F schreiben. Eine Rolle kann mehrere Partitionen haben, aber es sollten niemals zwei Rollen die gleiche Partition verwenden.
  - d) Klicken Sie auf **Übernehmen**.
- 5 Wiederholen Sie Schritte 3 und 4, um jede Archiver-Rolle zu erstellen.

- 6 Fügen Sie Ihre Kameras zu ihrer dedizierten Archiver-Rolle hinzu:
  - a) Öffnen Sie auf der Config-Tool-Startseite den Task *Video*.
  - b) Wählen Sie im Entitäts-Browser die Archiver-Rolle aus, der Sie die Kamera zuweisen möchten, und klicken Sie auf **Videoeinheit** .
  - c) Geben Sie im Dialogfeld, das geöffnet wird, die erforderlichen Informationen zur Kamera ein und klicken Sie auf **OK**.

**BEMERKUNG:** Das Hinzufügen der Kameras dauert einige Sekunden. Wenn die Rolle eine Kamera nicht in der vorgegebenen Zeit hinzufügen kann, wird ein Fehlerstatus gemeldet und die Kamera entfernt.
  - d) Klicken Sie auf **Übernehmen**.

# Verschlüsseln des Betriebssystemlaufwerks

Um Ihre Streamvault™-Appliance und Ihr Windows-Administratorpasswort zu schützen, müssen Sie das Betriebssystemlaufwerk (C:) mit BitLocker verschlüsseln.

## Bevor Sie beginnen

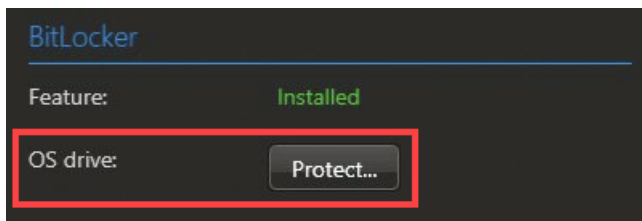
Wenn das Betriebssystemlaufwerk mit BitLocker verschlüsselt ist, wird der Entschlüsselungsschlüssel auf einem TPM (Trusted Platform Module)-Chip gespeichert, der sich auf der Systemplatine der Streamvault™-Appliance befindet. Wenn das Betriebssystemlaufwerk entfernt oder die Systemplatine ausgetauscht würde, gingen die Informationen auf dem Betriebssystemlaufwerk verloren. Das Betriebssystemlaufwerk kann nicht auf den Entschlüsselungsschlüssel auf dem TPM zugreifen. In diesen Szenarien können Sie einen Wiederherstellungsschlüssel erstellen, der zum Entschlüsseln des Laufwerks verwendet werden kann. Ohne Wiederherstellungsschlüssel muss für die Appliance ein neues Image erstellt und die Software neu installiert werden.

Der Speicherdatenträger wird in erster Linie zum Speichern von Videoarchiven verwendet und ist nicht mit BitLocker verschlüsselt. Sie können die Funktionen von Security Center verwenden, um Videoarchive im Ruhezustand zu verschlüsseln.

**BEMERKUNG:** Die BitLocker-Funktion ist ab SV Control Panel 3.2 verfügbar. Mit dieser Funktion wird auch ein Update des Härtingsprofils für [Appliances mit Funktionen für das Härtingsmanagement](#) eingeführt. Sie können dieses Update herunterladen, indem Sie das [Streamvault™ Service](#) vom Genetec™ Update Service (GUS) oder GTAP herunterladen. Um die BitLocker-Funktion in vollem Umfang nutzen zu können, empfehlen wir Ihnen, sowohl das Betriebssystemlaufwerk zu verschlüsseln als auch ggf. das Update des Härtingsprofils anzuwenden.

## Prozedur

- 1 Klicken Sie im SV Control Panel auf die Registerkarte **Sicherheit**.
- 2 Klicken Sie im Abschnitt *BitLocker* neben dem Feld **Betriebssystemlaufwerk** auf **Schützen**.



**BEMERKUNG:** Wenn das Betriebssystemlaufwerk bereits verschlüsselt ist, wird die Schaltfläche **Schützen** durch den Status *Geschützt* ersetzt.

- 3 Wenn Sie gefragt werden, ob Sie BitLocker aktivieren möchten, klicken Sie auf **Ja**.  
Das Betriebssystemlaufwerk wird verschlüsselt, der Entschlüsselungsschlüssel wird auf dem TPM gespeichert, und ein Wiederherstellungsschlüssel wird erstellt. Standardmäßig wird der Wiederherstellungsschlüssel auf einem festen Datenträger gespeichert. Wenn kein festes Datenlaufwerk vorhanden ist (z. B. auf einer Workstation), wird der Wiederherstellungsschlüssel auf einem USB-Stick gespeichert.
- WICHTIG:** Wenn Sie den Wiederherstellungsschlüssel auf einem festen Datenträger speichern, stellen Sie sicher, dass Sie den Schlüssel an einen sicheren Ort verschieben und von der Appliance löschen.

- 4 (Optional) Wenn kein festes Datenlaufwerk oder kein USB-Schlüssel vorhanden ist, können Sie auswählen, ob Sie mit der Verschlüsselung fortfahren möchten, ohne einen Wiederherstellungsschlüssel zu erstellen. Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf **Ja**, um fortzufahren, ohne einen Wiederherstellungsschlüssel zu erstellen.
- Klicken Sie auf **Nein**, um die Verschlüsselung abubrechen.

**BEMERKUNG:** Wenn Sie keinen Wiederherstellungsschlüssel erstellen, können Sie später einen erstellen. Weitere Informationen dazu finden Sie unter [Erstellen eines Wiederherstellungsschlüssels](#) auf Seite 45.

## Erstellen eines Wiederherstellungsschlüssels

Wenn Sie das Betriebssystemlaufwerk auf Ihrer Streamvault™-Appliance mit BitLocker verschlüsselt, aber keinen Wiederherstellungsschlüssel gespeichert haben, können Sie mit der Windows BitLocker-Laufwerkverschlüsselung ein Laufwerk erstellen.

### Was Sie noch wissen sollten

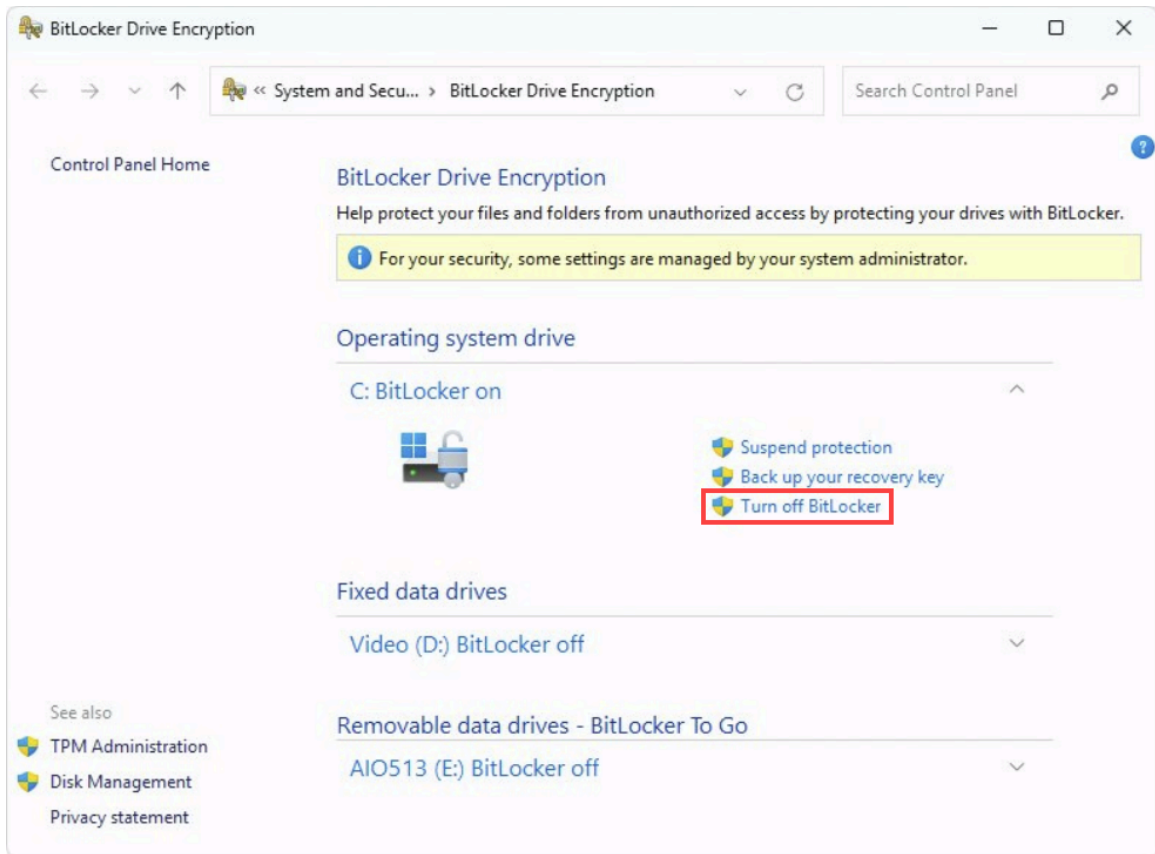
Bei diesem Verfahren wird davon ausgegangen, dass Sie das Betriebssystemlaufwerk über das SV Control Panel verschlüsselt haben.

### Prozedur

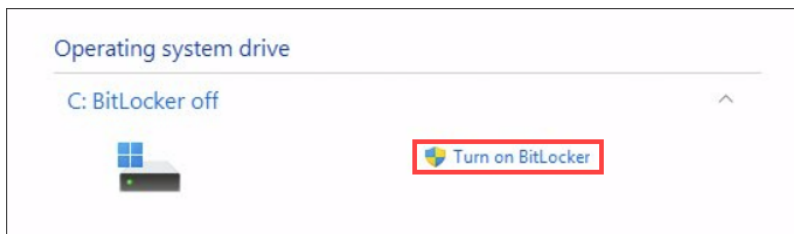
- 1 Geben Sie im Windows-Startmenü BitLocker ein, und wählen Sie in den Ergebnissen die Option **BitLocker verwalten** aus.

Das Fenster *BitLocker-Laufwerkverschlüsselung* wird geöffnet. Alle Laufwerke, die mit der Appliance verbunden sind, werden aufgelistet.

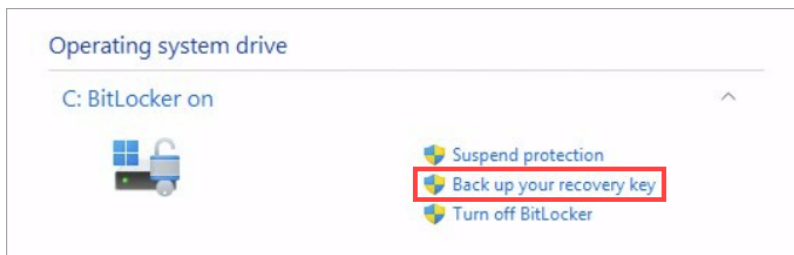
- 2 Klicken Sie im Abschnitt *Betriebssystemlaufwerk* auf **BitLocker deaktivieren** und warten Sie, bis das Betriebssystemlaufwerk entschlüsselt ist. Dieser Vorgang dauert einige Minuten.



- 3 Sobald das Betriebssystemlaufwerk entschlüsselt ist, klicken Sie auf **BitLocker aktivieren** und warten Sie, bis das Betriebssystemlaufwerk erneut mit BitLocker verschlüsselt wurde.



- 4 Sobald das Betriebssystemlaufwerk verschlüsselt ist, klicken Sie neben dem Betriebssystemlaufwerk (C:) auf **Wiederherstellungsschlüssel sichern**.

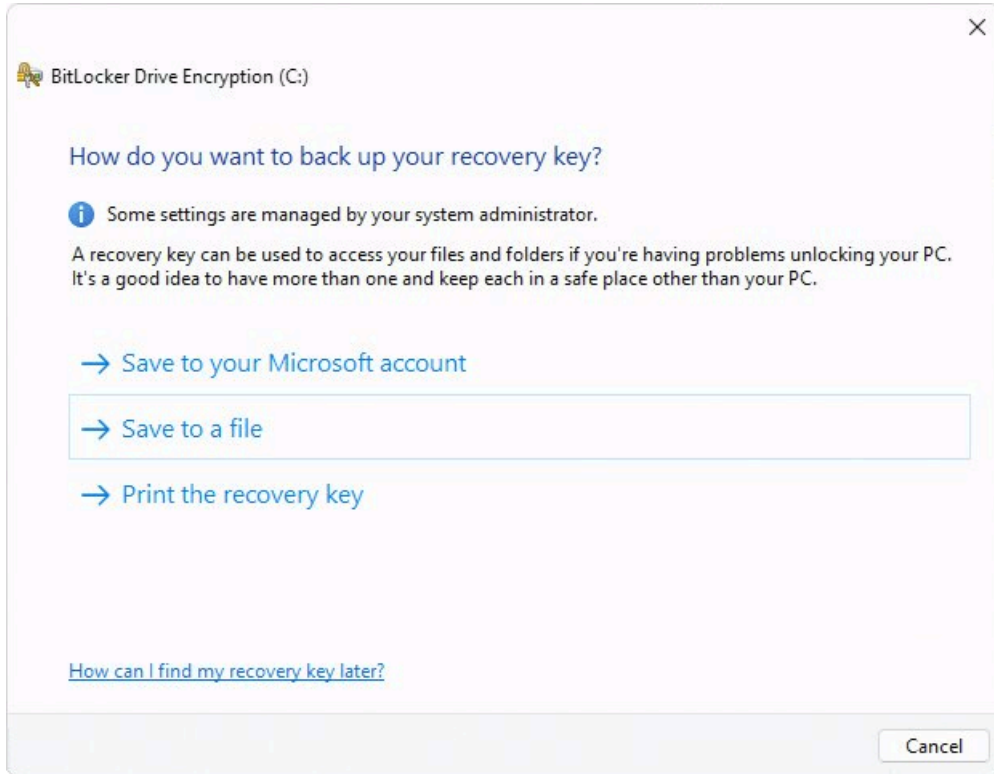


Der Assistent *BitLocker-Laufwerkverschlüsselung* wird geöffnet.

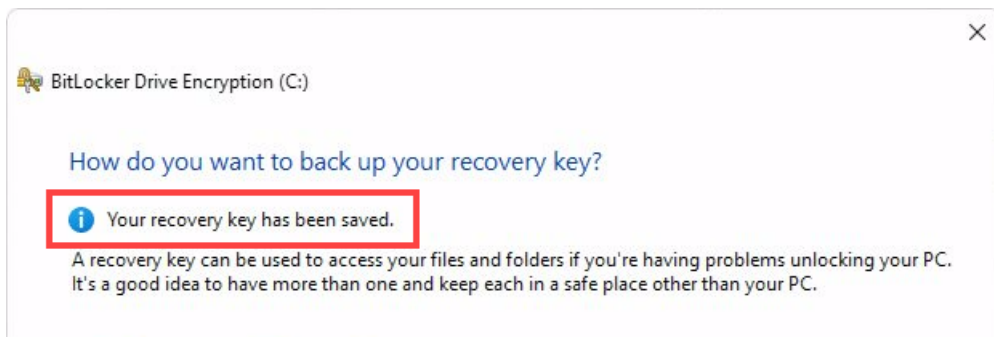
5 Wählen Sie aus, wie Sie Ihren Wiederherstellungsschlüssel sichern möchten:

- **In Ihrem Microsoft-Konto speichern:** Speichern Sie den Wiederherstellungsschlüssel in der *Bibliothek für Wiederherstellungsschlüssel* Ihres Microsoft-Kontos.
- **In einer Datei speichern:** Speichern Sie Ihren Wiederherstellungsschlüssel als Klartextdatei auf einem unverschlüsselten Festplattenlaufwerk der Appliance oder auf einem USB-Schlüssel.
- **Wiederherstellungsschlüssel ausdrucken:** Drucken Sie eine Kopie Ihres Wiederherstellungsschlüssels aus.

**BEMERKUNG:** Wenn Sie **In einer Datei speichern** auswählen, stellen Sie sicher, dass ein festes Datenlaufwerk oder ein USB-Schlüssel zum Speichern des Wiederherstellungsschlüssels verfügbar ist.



6 Wenn Sie den Wiederherstellungsschlüssel in einer Datei speichern, wählen Sie den Speicherort aus, an dem Sie den Schlüssel speichern möchten, und klicken Sie auf **Speichern**. Sie werden benachrichtigt, dass die Wiederherstellung gespeichert wurde.



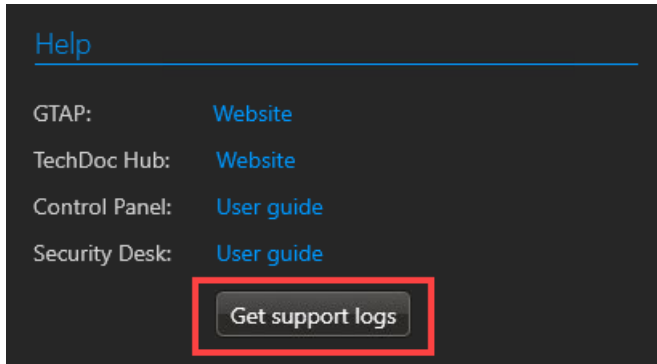
7 Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

# Erfassen von Support-Protokollen

Das Genetec™ Technical Assistance Center (GTAC) kann Ihre Streamvault™-Protokolle und andere Anwendungsprotokolle nutzen, um Probleme auf Ihrer Appliance zu beheben. Sie können diese Support-Protokolle vom SV Control Panel herunterladen.

## Prozedur

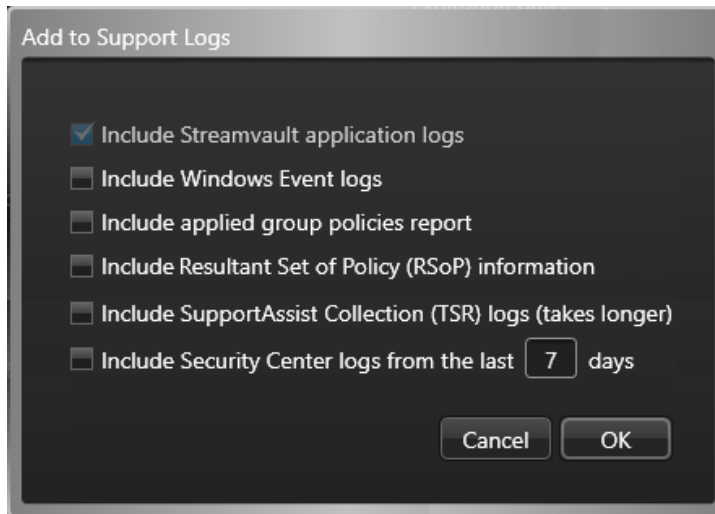
- 1 Klicken Sie im SV Control Panel auf die Registerkarte **Informationen**.
- 2 Klicken Sie im Abschnitt *Hilfe* auf **Support-Protokolle abrufen**.



- 3 Wählen Sie im Dialogfeld *Zu Support-Protokollen hinzufügen* die Protokolle aus, die Sie herunterladen möchten:
  - **Streamvault-Anwendungsprotokolle:** Diese Protokolle enthalten Cylance-, OEM-, Policy-, Software- und SV Control-Panel-Protokolldateien. Diese Option ist standardmäßig ausgewählt und kann nicht deaktiviert werden.
  - **Windows-Ereignisprotokolle:** Diese Protokolle umfassen Windows-Anwendungs-, Sicherheits- und Systemereignisse.
  - **Bericht über angewendete Gruppenrichtlinien:** Dieser Bericht bezieht sich auf Systeme, die Teil der Domäne sind. Der Bericht listet alle Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) auf, die derzeit erzwungen werden, und gibt an, ob sie auf lokaler Ebene oder Domänenebene angewandt werden.
  - **Resultant Set of Policy (RSOP)-Informationen:** Dieser HTML-Bericht enthält alle Systemeinstellungen, die über Gruppenrichtlinien konfiguriert wurden. Bei Systemen, die nicht mit einer Domäne verbunden sind, ist diese Option standardmäßig aktiviert. Bei Systemen, die mit einer Domäne verbunden sind, ist diese Option standardmäßig deaktiviert, da der Bericht vertrauliche Informationen enthält (wie den Domänennamen, den Hostnamen der Appliance usw.).
  - **SupportAssist Collection-Protokolle (TSR):** Diese Protokolle gelten für Systeme, die eine SupportAssist-Sammlung erstellen können, die auch als Technical Support Report (TSR) bezeichnet wird. Dell PowerEdge-Server, z. B. Streamvault-Server der Serien 1000, 2000, 4000 und 7000, können

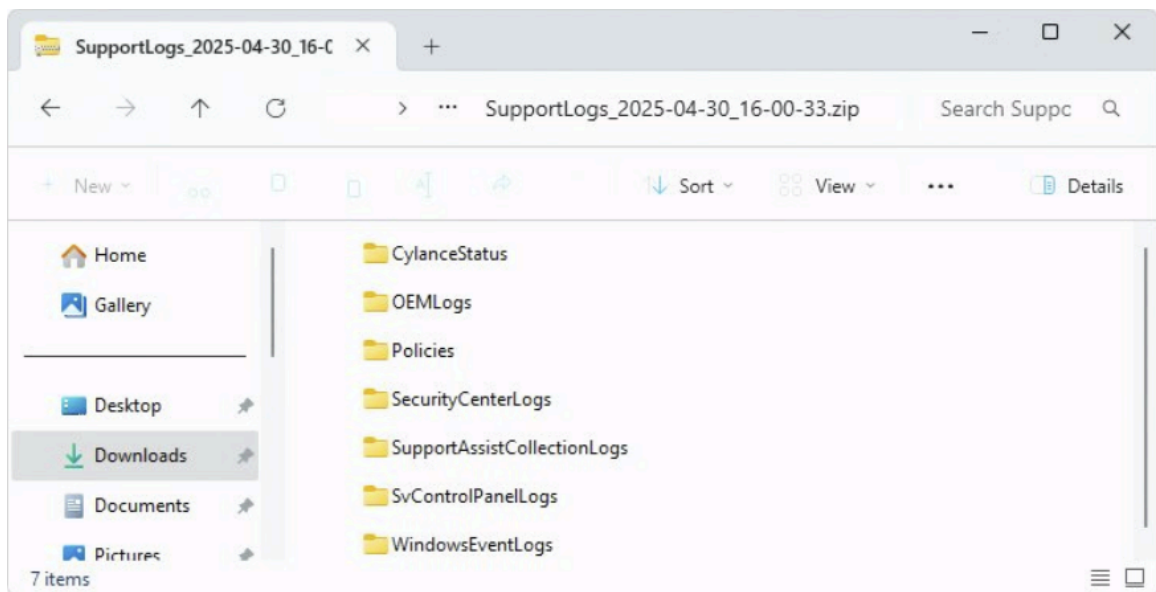
SupportAssist-Sammlungen erstellen. Diese Option ist nur für Streamvault-Server verfügbar, die iDRAC unterstützen.

- **Security Center-Protokolle der letzten X Tage:** Standardmäßig werden die Security Center-Protokolle der letzten 7 Tage erfasst. Geben Sie die gewünschte Anzahl von Tagen ein.



- 4 Klicken Sie auf **OK**.
- 5 Wählen Sie im Dialogfeld *Ordner suchen* den Ordner aus, in dem Sie Ihre Protokolle speichern möchten, und klicken Sie dann auf **OK**.

Ihre Support-Protokolle werden in einem *.zip*-Ordner gespeichert.



# Erste Schritte mit Streamvault Maintenance

Die ersten Schritte stellen das Streamvault – Wartung-Plugin vor und bieten Informationen über das Einrichten des Plugins.

Dieser Abschnitt enthält die folgenden Themen:

- ["Informationen über das Streamvault – Wartung-Plugin"](#) auf Seite 51
- ["Das Plugin herunterladen und installieren"](#) auf Seite 52
- ["Genetec Streamvault – Berechtigungen"](#) auf Seite 53
- [" Die Plugin-Rolle erstellen "](#) auf Seite 55
- ["Eine Streamvault-Hardwareüberwachungsentität konfigurieren"](#) auf Seite 56
- ["Eine Streamvault-Managerentität konfigurieren:"](#) auf Seite 60
- [" Informationen über die Registerkarte „Management“ "](#) auf Seite 63
- ["Die Integrität der Streamvault-Appliance überprüfen"](#) auf Seite 64
- ["Spalten des Berichtsbereichs für den Streamvault-Hardwaretask"](#) auf Seite 65
- ["Event-to-Actions für Streamvault-Integritätsereignisse erstellen"](#) auf Seite 66

# Informationen über das Streamvault – Wartung-Plugin

Das Streamvault™-Maintenance-Plugin hilft bei der Überwachung des Status Ihrer Streamvault™-Appliance und benachrichtigt Sie, wenn Probleme auftreten.

**BEMERKUNG:** Dieses Handbuch gilt für das Streamvault-Maintenance-Plugin 2.0.

Das Streamvault – Wartung-Plugin enthält die folgenden Komponenten:

- **Streamvault-Rolle:** Die Plugin-Rolle, die verwendet wird, um die Hardwareüberwachungs- oder Managerentität auszuführen. Eine Rolle pro Streamvault-Appliance, die Sie überwachen möchten, ist erforderlich.
- **Streamvault™-Hardwareüberwachung:** Entität zum Definieren der Alarmkonfigurationen für jede Streamvault-Appliance.
- **Streamvault™-Manager:** Entität zum stapelweisen Steuern von Konfigurationen für eine Gruppe von Streamvault-Appliances. Nur eine Streamvault-Manager-Instanz kann erstellt werden.
- **Streamvault™-Hardware:** Berichtstask in Security Center, den Sie verwenden können, um eine Liste von Integritätsproblemen anzuzeigen, die bei Ihren Streamvault™-Appliances auftreten können.

Die Plugin-Entitätskonfigurationen bestehen aus den folgenden Einstellungen:

- **Alarmkonfigurationen:** definieren die Typen von **Ereignissen**, den **Schweregrad** und **Benachrichtigungstypen**, die Alarime in Bezug auf den Integritätsstatus Ihrer Streamvault-Server beeinflussen.
- **E-Mail-Empfänger:** wählen Sie aus, welche Benutzer und Benutzergruppen E-Mail-Benachrichtigungen erhalten.
- **Berechtigungsnachweise für das Remote-Management:** steuern die Erstellung von Benutzerprofilen in iDRAC.
- **Integration des Integrated Dell Remote Access Controller (iDRAC)** (für Streamvault-Modelle, die iDRAC unterstützen): wird für eine präzisere Steuerung der Berechtigungsnachweisverwaltung verwendet. Diese Funktion befindet sich auf der Registerkarte **Management** des Plugins.

Weitere Information über iDRAC finden Sie unter <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

## WICHTIG:

- Bei Systemen mit iDRAC-fähigen Server, muss die iDRAC-Firmware Version 6.0 oder neuer sein.
- Für iDRAC-unterstützte Geräte greift das Streamvault – Wartung-Plugin auf Integritätsdaten mithilfe einer internen Verbindung zu, solange die iSM (iDRAC Service Module)-Software installiert ist. iSM ist standardmäßig auf Modellen installiert, die iDRAC unterstützen.

Wenn iSM nicht verfügbar ist, verwendet das Plugin Out-of-Band-Kommunikation mit iDRAC. In diesem Fall muss eine Netzwerkverbindung zwischen dem dedizierten iDRAC-Port und mindestens einem LAN-Port existieren, wenn Portteilung nicht verwendet wird. Der dedizierte iDRAC-Port ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter: <https://www.dell.com/support/kbdoc/en-ca/000177212/dell-powerededge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip>.

## Das Plugin herunterladen und installieren

Um das Streamvault™-Maintenance-Plugin in Security Center zu ignorieren, müssen Sie das Plugin auf einem Directory-Server, den Streamvault™-Server, die Sie überwachen möchten, sowie auf allen Client-Workstations, über die Sie das Plugin konfigurieren möchten, installieren.

### Bevor Sie beginnen

Stellen Sie sicher, dass eine kompatible Version von Security Center installiert ist. Weitere Informationen finden Sie unter [Unterstützte Plugins in Security Center](#).

### Was Sie noch wissen sollten

- **BEST-PRACTICE:** Installieren Sie die Streamvault-Rolle auf jedem Server, den Sie überwachen möchten.
- **WICHTIG:** Stellen Sie sicher, dass das iDRAC-Modul jedes Servers mit Ihrem Netzwerk verbunden ist und mit dem Host-System kommunizieren kann. Standardmäßig verwendet das iDRAC-Modul den gleichen LAN-Port wie das Host-System und ist konfiguriert, um eine IP-Adresse mithilfe von DHCP zu erhalten.
- **WICHTIG:** Stellen Sie vor dem Fortfahren sicher, dass das iDRAC-Modul auf Firmware 6.00 oder neuer aktualisiert ist und dass das Server-BIOS auf die neueste Version aktualisiert ist.
- Das Plugin wird nur auf Servern unterstützt, die die Security-Center-Serversoftware ausführen.
- **BEMERKUNG:** Das [Streamvault – Wartung-Plugin](#) ist auf allen kompatiblen Streamvault-Servern vorab installiert. Deshalb müssen die meisten Benutzer nur die Rollen und Entitäten in Security Center erstellen. Wenn Ihr Server versendet wurde, bevor das Plugin verfügbar gemacht wurde oder wenn es deinstalliert wurde, befolgen Sie diese Schritte zur Installation.

### Prozedur

- 1 Öffnen Sie die GTAP-Seite [Produktdownload](#).
- 2 Wählen Sie unter **Download Finder** Ihre Version von Security Center aus.
- 3 Laden Sie im Abschnitt *Genetec Plugins* das Paket für Ihr Produkt herunter.
- 4 Führen Sie die .exe-Datei aus und entpacken Sie dann die Datei.  
Standardmäßig wird die Datei nach C:\Genetec entpackt.
- 5 Öffnen Sie den extrahierten Ordner, klicken Sie mit der rechten Maustaste auf die Datei *setup.exe* und klicken Sie auf **Als Administrator ausführen**.
- 6 Befolgen Sie die Installationsanweisungen.
- 7 Klicken Sie auf der Seite *Installationsassistent abgeschlossen* auf **Fertigstellen**.  
**WICHTIG:** Die Option **Genetec™ Server neu starten** ist standardmäßig ausgewählt. Sie können diese Option deaktivieren, wenn Sie den Genetec™ Server nicht sofort neu starten möchten. Sie müssen jedoch den Genetec Server neu starten, um die Installation abzuschließen.
- 8 Schließen und öffnen Sie alle Instanzen von Config Tool und Security Desk.

# Genetec Streamvault – Berechtigungen

Damit Sie die Tasks *Hardwareüberwachung* und *Manager* im Zusammenhang mit der Streamvault™-Appliance verwenden können, müssen Benutzerkonten die erforderlichen Berechtigungen zugewiesen sein.

## Benutzerberechtigungen für Streamvault konfigurieren

Einigen Benutzergruppen wie Administratoren sind Standardrechte zugewiesen.

Im Config-Tool-Task *Benutzerverwaltung* können Sie die Rechte für den Benutzer oder die Benutzergruppe auf der Seite *Rechte* des Benutzers oder der Benutzergruppe konfigurieren oder ändern.

Weitere Informationen zur Rechtehierarchie sowie der Vererbung und Zuweisung von Rechten finden Sie im [Security Center – Administratorhandbuch](#) und im [Security Center – Härtingsleitfaden](#) im TechDoc Hub.

**BEMERKUNG:** Eine Liste der verfügbaren Security-Center-Berechtigungen finden Sie in der Tabelle [Security-Center-Berechtigungen](#). Sie können diese Liste nach Bedarf sortieren und filtern.

## Berechtigungen für die Streamvault-Plugin-Rolle

Streamvault-Plugin-Rollenberechtigungen gewähren Zugriff auf Tasks, die mit der Streamvault *Hardwareüberwachung* und dem Streamvault *Manager* zusammenhängen.

Standardmäßig können Administratoren auf alle Rechte zugreifen. Wenn Sie ein Benutzerkonto über eine der anderen Berechtigungsvorlagen erstellen, erfordert das Benutzerkonto die folgenden Streamvault-Plugin-Rollenberechtigungen für Config Tool in Streamvault.

| Unterkategorie von Berechtigungen | Umfasst Berechtigungen für     | Aktionen, die ausgeführt werden können  |
|-----------------------------------|--------------------------------|---|
| Hardwareüberwachung               | Hardwareüberwachung bearbeiten | <ul style="list-style-type: none"> <li>Alarmkonfigurationen bearbeiten</li> <li>E-Mail-Empfänger bearbeiten</li> <li>Remote-Management-Benachrichtigungsnachweise bearbeiten</li> <li>Porteinstellungen ändern</li> </ul> |
|                                   | Hardwareüberwachung hinzufügen | Eine neue Hardwareüberwachungsentität erstellen und sie zu einem Streamvault-Server zuweisen  |
|                                   | Hardwareüberwachung löschen    | Eine bestehende Hardwareüberwachungsentität löschen   |
|                                   | Hardwareüberwachung anzeigen   | Eine Hardwareüberwachungskonfiguration anzeigen   |
| Manager                           | Manager bearbeiten             | <ul style="list-style-type: none"> <li>Alarmkonfigurationen stapelweise bearbeiten</li> <li>E-Mail-Empfänger stapelweise bearbeiten</li> </ul>  |

| Unterkategorie von Berechtigungen | Umfasst Berechtigungen für | Aktionen, die ausgeführt werden können                                |
|-----------------------------------|----------------------------|---|
|                                   | Manager hinzufügen         | Die Managerentität erstellen und zu einem Streamvault-Server zuweisen |
|                                   | Manager löschen            | Die Managerentität löschen  |
|                                   | Manager anzeigen           | Die Managerkonfiguration anzeigen                                     |

# Die Plugin-Rolle erstellen

Bevor Sie das -Plugin konfigurieren und verwenden können, müssen Sie die Streamvault™-Maintenance-Pluginrolle in Config Tool erstellen.

## Bevor Sie beginnen

Laden Sie das Plugin herunter und installieren Sie es.

## Was Sie noch wissen sollten

Das Streamvault – Wartung-Plugin enthält zwei Plugin-Rollen:

- **Streamvault™-Hardwareüberwachung:** Die Streamvault™-Hardwareüberwachungsentität hilft bei der Überwachung des Status Ihrer Streamvault™-Appliance und benachrichtigt Sie, wenn Probleme auftreten. Es ist eine Streamvault™-Hardwareüberwachung pro Streamvault™-Appliance erforderlich.
- **Streamvault™Manager:** Die Streamvault™-Managerentität wird zum Steuern der Alarmkonfigurationen für eine Gruppe von Streamvault™-Agent-Entitäten verwendet. Nur ein Streamvault™-Manager ist pro System erlaubt.
- **BEMERKUNG:** Wenn es sich bei den Directory-Servern um virtuelle Computer oder Nicht-Streamvault-Server handelt, erstellen Sie eine Rolle für diese Server nur dann, wenn Sie die Manager-Entität verwenden möchten.

## Prozedur

- 1 Öffnen Sie auf der Config Tool-Startseite den Task *Plugins*.
- 2 Klicken Sie in der Task *Plugins* auf **Eine Entität hinzufügen** (+) und wählen Sie **Plugin** aus.  
Der Plugin-Erstellungsassistent wird geöffnet.
- 3 Wählen Sie auf der Seite *Spezifische Informationen* den Server aus, auf dem die Plugin-Rolle gehostet wird, sowie den Plugin-Typ und klicken Sie dann auf **Weiter**.  
Wenn Sie keine Erweiterungsserver in Ihrem System verwenden, wird die Option **Server** nicht angezeigt.
- 4 Geben Sie auf der Seite *Basisinformationen* die Rolleninformationen an:
  - a) Geben Sie den **Entitätsnamen** ein.
  - b) Geben Sie die **Entitätsbeschreibung** ein.
  - c) Wählen Sie die **Partition** für die Plugin-Rolle aus.  
Wenn Sie in Ihrem System keine Partitionen verwenden, wird die Option **Partition** nicht angezeigt. Partitionen sind logische Gruppierungen, welche die Sichtbarkeit von Entitäten steuern. Nur Benutzer, die Mitglied dieser Partition sind, können diese Rolle anzeigen oder bearbeiten.
  - d) Klicken Sie auf **Weiter**.
- 5 Prüfen Sie auf der Seite *Zusammenfassung* die Informationen und klicken Sie dann auf **Erstellen** oder **Zurück**, um Änderungen vorzunehmen.  
Nachdem die Plugin-Rolle erstellt wurde, wird die folgende Meldung angezeigt: Aktion war erfolgreich.
- 6 Klicken Sie auf **Schließen**.

## Nach Durchführen dieser Schritte

- Konfigurieren Sie die Streamvault-Hardwareüberwachungsentität.
- Konfigurieren Sie die Streamvault-Managerentität.

# Eine Streamvault-Hardwareüberwachungsentität konfigurieren

Sie können die Streamvault™-Hardwareüberwachungsentität konfigurieren, um den Zustand einer Streamvault™-Appliance zu beobachten und Benachrichtigungen einzurichten, die ausgelöst werden, wenn Probleme auftreten.

## Bevor Sie beginnen

- Registrieren Sie Ihre Streamvault-Appliances.
- [Erstellen Sie die Streamvault-Plugin-Rolle.](#)  
**WICHTIG:** Eine Streamvault-Hardwareüberwachung wird automatisch auf jedem Streamvault-Server erstellt, der eine Streamvault-Rolle hostet. Wenn die Hardwareüberwachungsentität in Ihrem System nicht vorhanden ist, nachdem Sie die Rolle erstellt haben, müssen Sie die Hardwareüberwachung manuell erstellen. Die Hardware-Überwachung kann nur auf einem Streamvault-Server ausgeführt werden.

## Was Sie noch wissen sollten

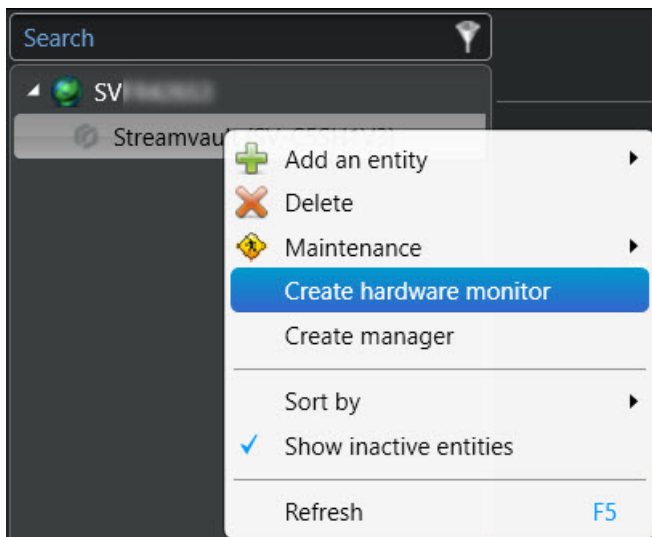
Die Konfigurationsoptionen unterscheiden sich je nachdem, ob Sie iDRAC-fähige Server oder andere Nicht-iDRAC-Server haben.

- [Einen iDRAC-fähigen Server konfigurieren.](#)
- [Nicht-iDRAC-Server konfigurieren.](#)

## Prozedur

### So konfigurieren Sie einen iDRAC-fähigen Server:

- 1 Navigieren Sie in Config Tool zum Task *Plugins* und wählen Sie die Streamvault-Plugin-Rolle aus.
- 2 Klicken Sie mit der rechten Maustaste auf die Streamvault-Plugin-Rolle und klicken Sie auf **Hardwareüberwachung erstellen**.



- 3 Geben Sie auf der Registerkarte **Identität** einen Namen für die Streamvault-Hardwareüberwachung im Feld **Name** ein.
- 4 Wählen Sie die Registerkarte **Allgemein** aus.

- 5 (Optional) Wenn Sie eine Streamvault™-Managerentität für Ihr System erstellt haben, wählen Sie das Kontrollkästchen **Managereinstellungen verwenden** aus, um die Benachrichtigungskonfigurations-Profileinstellungen des Streamvault-Managers zu verwenden.
- 6 Aktivieren Sie im Abschnitt *Alarmkonfigurationsprofil* das Kontrollkästchen **Hardwareüberwachung verwaltet iDRAC-Alarmkonfigurationen**, um Alarmkonfigurationen über die Streamvault-Hardwareüberwachung zu verwalten.
- 7 Aktivieren Sie die Kontrollkästchen, die den **Ereignistypen**, **Schweregrad** und **Benachrichtigungstypen** entsprechen, die Sie für diese Streamvault-Hardwareüberwachung einschließen möchten.

| Events     | Severity                            |                                     |                          | Notification                        |                                     |
|------------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|
|            | Critical                            | Warning                             | Information              | Email                               | Event                               |
|            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Cooling    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| CPU        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Memory     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Networking | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Power      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Storage    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| System     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

- 8 Wählen Sie im Abschnitt *E-Mail-Empfänger* aus, welche Benutzer und Benutzergruppen E-Mail-Benachrichtigungen erhalten, wenn eine Bedingung im Abschnitt *Alarmkonfigurationsprofil* erfüllt wird.

| Email recipients  |
|---|
| <input type="checkbox"/> Admin  |
| <input checked="" type="checkbox"/> Administrators <span style="color: yellow;">No email configured for this group</span> |
| <input type="checkbox"/> AutoVu   |
| <input type="checkbox"/> AutoVu operators   |
| <input type="checkbox"/> Patroller  |
| <input type="checkbox"/> Patroller users  |

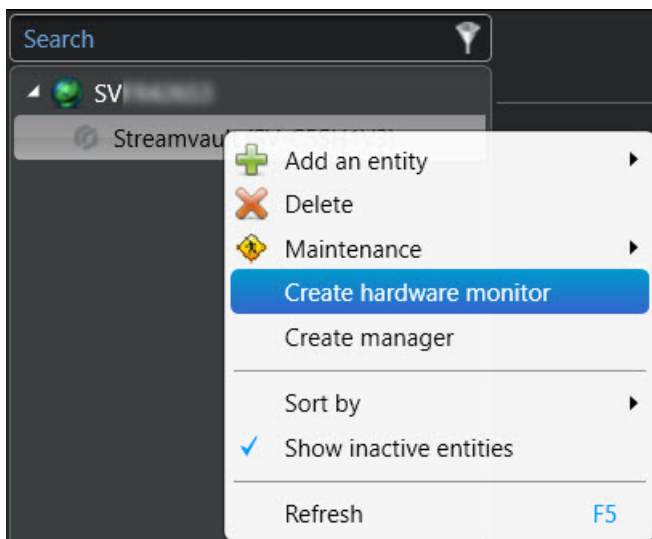
- 9 Führen Sie im Abschnitt *Remote-Managementberechtigungs-nachweise* eine der folgenden Optionen durch:
  - Aktivieren Sie das Kontrollkästchen **Hardwareüberwachung verwaltet iDRAC-Konten**, um Berechtigungsnachweise direkt über das Plugin zu verwalten.
  - Deaktivieren Sie das Kontrollkästchen **Hardwareüberwachung verwaltet iDRAC-Konten**, um iDRAC zum Steuern der Benutzer- und Passwörterstellung zu verwenden.
- 10 (Optional) Wenn Sie das Kontrollkästchen **Hardwareüberwachung verwaltet iDRAC-Konten** deaktiviert haben, navigieren Sie zur Registerkarte **Management** und konfigurieren Sie die Anmeldedaten direkt in iDRAC.

- 11 (Optional) Sie können im Abschnitt *Einstellungen* den **Standardeingangsport** von 65115 zu einem Port Ihrer Wahl ändern. Weitere Informationen dazu finden Sie unter [Von Streamvault verwendete Standardports](#) auf Seite 4.

- 12 Klicken Sie auf **Anwenden**.

### So konfigurieren Sie einen Nicht-iDRAC-Server:

- 1 Navigieren Sie in Config Tool zum Task *Plugins* und wählen Sie die Streamvault-Plugin-Rolle aus.
- 2 Klicken Sie mit der rechten Maustaste auf die Streamvault-Plugin-Rolle und klicken Sie auf **Hardwareüberwachung erstellen**.



- 3 Geben Sie auf der Registerkarte **Identität** einen Namen für die Streamvault-Hardwareüberwachung im Feld **Name** ein.
- 4 Wählen Sie die Registerkarte **Allgemein** aus.
- 5 (Optional) Wenn Sie eine Streamvault-Managerentität für Ihr System erstellt haben, wählen Sie das Kontrollkästchen **Managereinstellungen verwenden** aus, um die Benachrichtigungskonfigurations-Profileinstellungen des Streamvault-Managers zu verwenden.
- 6 Aktivieren Sie im Abschnitt *Alarmkonfigurationsprofil* die Kontrollkästchen, die den **Ereignis-** und **Benachrichtigungstypen** entsprechen, die Sie auf die Streamvault – Wartung-Plugin-Instanzen anwenden möchten, die vom Streamvault-Manager gesteuert werden.
- 7 Legen Sie unter **Konfiguration** den **Schwellenwert %** der Solid-State-Festplatte (SSD) fest, wann Sie eine Benachrichtigung erhalten möchten, dass Sie die SSD bald ersetzen müssen.

- 8 Wählen Sie im Abschnitt *E-Mail-Empfänger* aus, welche Benutzer und Benutzergruppen E-Mail-Benachrichtigungen erhalten, wenn eine Bedingung im Abschnitt *Alarmkonfigurationsprofil* erfüllt wird.

☐ Use manager settings

### Alert configuration profile

| Events                   | Notification                        | Event                               | Status                                     | Configuration                               |
|--------------------------|-------------------------------------|-------------------------------------|--|---|
|                          | Email                               | Event                               |  |   |
| Predictive drive failure | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> Normal | Threshold % <input type="text" value="90"/> |
| SSD wear                 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> Normal |   |
| Offline drive            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |   |

### Email recipients

- ☐ Admin
- ☒ Administrators No email configured for this group
- ☐ AutoVu
- ☐ AutoVu operators
- ☐ Patroller
- ☐ Patroller users

- 9 Klicken Sie auf **Übernehmen**.

## Verwandte Themen

[Informationen über die Registerkarte „Management“](#) auf Seite 63

## Eine Streamvault-Managerentität konfigurieren:

Sie können die Streamvault™-Managerentität konfigurieren, um die Alarmkonfiguration einer Gruppe von Streamvault-Hardwareüberwachungen von einem einzelnen Ort aus zu steuern. Sie können auch Benachrichtigungen einrichten, die über auftretende Probleme informieren. Das Verwenden der Streamvault-Managerentität ist optional.

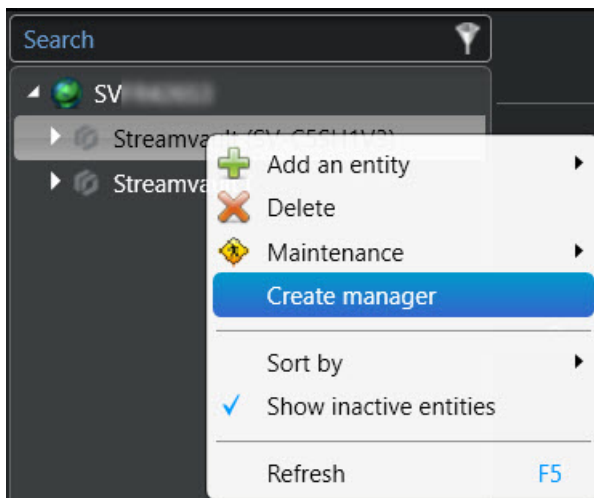
### Bevor Sie beginnen

- Registrieren Sie Ihre Streamvault™-Geräte.
- [Erstellen Sie die Streamvault-Plugin-Rolle.](#)

**BEMERKUNG:** Die Streamvault™ Manager-Einheit kann auf jedem Server (Streamvault™ oder Nicht-Streamvault™) oder jeder VM in Ihrem Security Center-System ausgeführt werden. Es kann nur eine Streamvault-Managerentität zum System hinzugefügt werden.

### Prozedur

- 1 Navigieren Sie in Config Tool zum Task *Plugins* und wählen Sie die Streamvault-Plugin-Rolle aus.
- 2 Klicken Sie mit der rechten Maustaste auf die Streamvault-Plugin-Rolle und klicken Sie auf **Manager erstellen**.



- 3 Wählen Sie die Streamvault-Managerentität aus und klicken Sie auf die Registerkarte **Allgemein**. Die folgenden Abschnitte werden angezeigt:
  - Der Abschnitt *iDRAC-Alarmkonfigurationsprofil* verwaltet iDRAC-fähige Server in Ihrem System.
  - Der Abschnitt *Nicht-iDRAC-Alarmkonfigurationsprofil* wird zum Verwalten von anderen Nicht-iDRAC-Servern im System verwendet.

Beide Abschnitte werden immer angezeigt, unabhängig davon, ob Sie ein iDRAC- oder Nicht-iDRAC-System haben.

- 4 (Falls zutreffend) Konfigurieren Sie Folgendes im Abschnitt *iDRAC-Benachrichtigungskonfigurationsprofil*:
- Um iDRAC-Alarmkonfigurationen über die Streamvault-Hardwareüberwachung des ausgewählten Servers zu verwalten, aktivieren Sie das Kontrollkästchen **Hardwareüberwachung verwaltet die iDRAC-Alarmkonfigurationen**.
  - Aktivieren Sie die Kontrollkästchen, die den **Ereignistypen**, **Schweregraden** und **Benachrichtigungstypen** entsprechen, die Sie auf den Streamvault – Wartung-Plugin-Instanzen anwenden möchten, die vom Streamvault-Manager gesteuert werden.

**iDRAC alert configuration profile**

☒ Hardware monitor manages iDRAC alert configurations

| Events     | Severity                            |                                     |                          | Notification                        |                                     |
|------------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|
|            | Critical                            | Warning                             | Information              | Email                               | Event                               |
| Cooling    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| CPU        | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Memory     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Networking | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Power      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Storage    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| System     | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Hardware monitors using Streamvault™ manager configuration

Streamvault (SV-C5SH1V3) - Streamvault™ hardware monitor

**BEMERKUNG:** Hardwareüberwachungen, deren Konfigurationen vom Streamvault-Manager festgelegt werden, werden unter **Hardwareüberwachungen, die die Streamvault™-Managerkonfiguration verwenden**. Hardwareüberwachungen die ihre eigenen Konfigurationen verwenden, werden unter **Hardwareüberwachungen, die eine benutzerdefinierte Konfiguration verwenden** aufgelistet.

- 5 (Falls zutreffend) Konfigurieren Sie Folgendes im Abschnitt *Nicht-iDRAC-Benachrichtigungskonfigurationsprofil*:
- Aktivieren Sie die Kontrollkästchen, die den **Ereignis**- und **Benachrichtigungstypen** entsprechen, die Sie auf den Streamvault – Wartung-Plugin-Instanzen anwenden möchten, die vom Streamvault-Manager gesteuert werden.
  - Legen Sie unter **Konfiguration** den **Schwellenwert %** der Solid-State-Festplatte (SSD) fest, wann Sie eine Benachrichtigung erhalten möchten, dass Sie die SSD bald ersetzen müssen.

| Events                   | Notification                        |                                     | Configuration  |
|--------------------------|-------------------------------------|-------------------------------------|----------------|
|                          | Email                               | Event                               |                |
| Predictive drive failure | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | Threshold % 90 |
| SSD wear                 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                |
| Offline drive            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |                |

Hardware monitors using Streamvault™ manager configuration

- Streamvault (SVFR426S3) - Streamvault™ hardware monitor

**BEMERKUNG:** Hardwareüberwachungen, deren Konfigurationen vom Streamvault-Manager festgelegt werden, werden unter **Hardwareüberwachungen, die die Streamvault™-Managerkonfiguration verwenden**. Hardwareüberwachungen die ihre eigenen Konfigurationen verwenden, werden unter **Hardwareüberwachungen, die eine benutzerdefinierte Konfiguration verwenden** aufgelistet.

- 6 Wählen Sie im Abschnitt *E-Mail-Empfänger* aus, welche Benutzer und Benutzergruppen E-Mail-Benachrichtigungen erhalten, wenn eine Bedingung im Abschnitt **iDRAC-Alarmkonfigurationsprofil** oder **Nicht-iDRAC-Alarmkonfigurationsprofil** erfüllt wird.

| Email recipients                                   |
|--|
| <input type="checkbox"/> Admin                     |
| <input checked="" type="checkbox"/> Administrators |
| <input type="checkbox"/> AutoVu                    |
| <input type="checkbox"/> AutoVu operators          |
| <input type="checkbox"/> Patroller                 |
| <input type="checkbox"/> Patroller users           |

No email configured for this group

- 7 Klicken Sie auf **Übernehmen**.

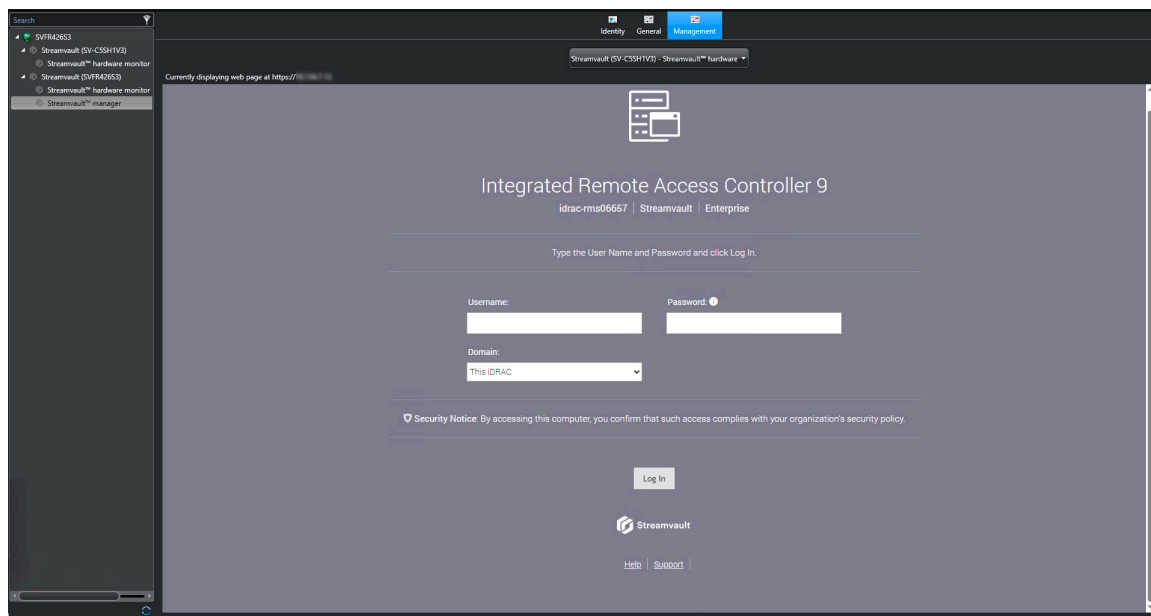
## Informationen über die Registerkarte „Management“

Die Registerkarte **Management** zeigt eine iDRAC-Webseite an, auf der Sie Ihre iDRAC-Server-Anmeldedaten konfigurieren und verwalten können. Sie finden ebenfalls weitere Informationen über Ihren iDRAC-Server und können andere Optionen konfigurieren, die nicht auf der Streamvault™-Plugin-Benutzeroberfläche verfügbar sind.

Sie können auf die Registerkarte **Management** über die Streamvault™-Hardwareüberwachung jedes iDRAC-fähigen Servers oder über den Streamvault™-Manager zugreifen.

Wenn Sie auf die Registerkarte **Management** über den Streamvault-Manager zugreifen, wird ein Drop-down-Menü oben auf der Seite angezeigt. Sie können es verwenden, um von einem iDRAC-Server zu einem anderen zu wechseln, anstatt manuell von einer Hardwareüberwachung zu einer anderen umzuschalten. Jeder iDRAC-Server hat seine eigene iDRAC-Webseite.

Um Anmeldeinformationen zu erhalten, klicken Sie auf **Hilfe** unten auf der Website.



**BEMERKUNG:** Um auf die iDRAC-Seite zuzugreifen, benötigen Sie eine Netzwerkverbindung zwischen dem Clientsystem, das Config Tool ausführt, und der IP-Adresse des iDRAC-Servers. Wenn eine Netzwerkverbindung nicht verfügbar ist, verwenden Sie die Config-Tool-Seite direkt von der Streamvault-Appliance über eine Remotedesktop- oder lokale Konsolensitzung.

Wenn in Ihrem System keine iDRAC-Server vorhanden sind, ist die Registerkarte **Management** leer. Eine Meldung gibt an, dass es keine verfügbaren Streamvault-Hardwareüberwachungen mit iDRAC-Managementfunktion gibt.

**BEMERKUNG:** Wenn die iDRAC-Webseite nicht lädt, klicken Sie auf eine andere Registerkarte und gehen Sie dann zur Registerkarte **Management** zurück.

### Verwandte Themen

[Eine Streamvault-Hardwareüberwachungsentität konfigurieren](#) auf Seite 56

[Eine Streamvault-Managerentität konfigurieren:](#) auf Seite 60

## Die Integrität der Streamvault-Appliance überprüfen

---

Verwenden Sie den Streamvault™-Hardwaretask, um eine Liste an Integritätsproblemen anzuzeigen, die bei Ihren Streamvault™-Appliances auftreten können.

### Prozedur

- 1 Öffnen Sie auf der Startseite den Task *Streamvault-Hardware*.
- 2 **Zeitbereich**-Abfragefilter, definieren Sie den Zeitbereich, der im Bericht enthalten sein soll.
- 3 Klicken Sie auf **Bericht erstellen**.  
Die Eigenschaften der Einheiten sind im Berichtsbereich aufgelistet.

## Spalten des Berichtsbereichs für den Streamvault-Hardwaretask

---

Nachdem ein Bericht erstellt wurde, werden die Ergebnisse Ihrer Abfrage im Berichtsfenster aufgelistet. Dieser Abschnitt listet die Spalten auf, die für den Streamvault™-Hardwaretask verfügbar sind.

- **Bild:** Symbol für den Problemtyp.
- **Schweregrad:** Mit dem Problem verknüpfter Schweregrad.
- **Zeitstempel:** Datum und Uhrzeit des Auftretens des Problems.
- **Quelle:** Vom Problem betroffene Streamvault-Appliance.
- **MessageID:** Identifizierende, alphanumerische, mit dem berichteten Problem verknüpfte Sequenz.
- **Nachricht:** Beschreibung des Problems.
- **Beschreibung:** Beschreibung der Problemursache.

**BEMERKUNG:** Weitere Informationen über das Erstellen von Berichten finden Sie unter [Überblick über den Berichtstask-Arbeitsbereich](#) im TechDoc Hub.

# Event-to-Actions für Streamvault-Integritätsereignisse erstellen

Mithilfe eines Event-to-Actions können Sie Aktionen festlegen, die durchgeführt werden, wenn ein Streamvault™-Hardwareproblem erkannt wird.

## Bevor Sie beginnen

- Erstellen Sie die Streamvault-Maintenance-Plugin-Rolle.
- konfigurieren Sie eine Streamvault-Hardwareüberwachungsentität.

## Prozedur

- 1 Klicken Sie auf der Config-Tool-Startseite auf den Task *Automation* und klicken Sie auf die Ansicht **Aktionen**.
- 2 Klicken Sie auf **Element hinzufügen** (+).
- 3 Konfigurieren Sie Ihr Event-to-Action:
  - a) Wählen Sie im Drop-down-Menü **Wann** die Option **Streamvault-Hardwareproblem erkannt** aus.
  - b) Klicken Sie auf **Bedingung festlegen** und geben Sie den iDRAC-Fehlercode ein. Sie können auch die ganze ID eingeben, um falsche Auslöser zu verhindern.

Im Screenshot unten lautet der Fehlercode beispielsweise TMP0103 und die volle ID ist IDRAC.2.8.TMP0103.

- c) (Optional) Wählen Sie in der Option **Von** Ihr Streamvault-Plugin oder Ihre Hardwareüberwachung aus.

**BEMERKUNG:** Da das Streamvault™ Plugin benutzerdefinierte Vorfälle verwendet, die nur für sich selbst von Bedeutung sind, ist es nicht notwendig, eine Quelle zuzuweisen.

Wenn Sie das Streamvault™-Plugin als Einheit auswählen, werden alle verknüpften Automatisierungsregeln gelöscht, wenn die Plugin-Rolle jemals gelöscht wird. Wenn keine Einheit

als Absender angegeben ist und die Rolle gelöscht wird, bleiben die Regeln für die Automatisierung bestehen.

- d) Wählen Sie aus der Drop-down-Liste **Aktion** einen Aktionstyp aus und konfigurieren Sie dessen Parameter.
  - e) (Optional) Klicken Sie in der Option **Gültig** auf **Immer**, und wählen Sie einen Zeitplan, wann das Event-to-Action aktiv ist.  
Wenn das Ereignis außerhalb des definierten Zeitplans auftritt, wird die Aktion nicht ausgelöst.
- 4 Stellen Sie sicher, dass das Event-to-Action aktiviert ist.
  - 5 Klicken Sie auf **Speichern**.

**BEMERKUNG:** Eine vollständige Liste der iDRAC-Fehlercodes finden Sie unter <https://developer.dell.com/apis/2978/versions/5.xx/docs/Error%20Codes/EEMIRegistry.md>.

# SV Control Panel – Referenz

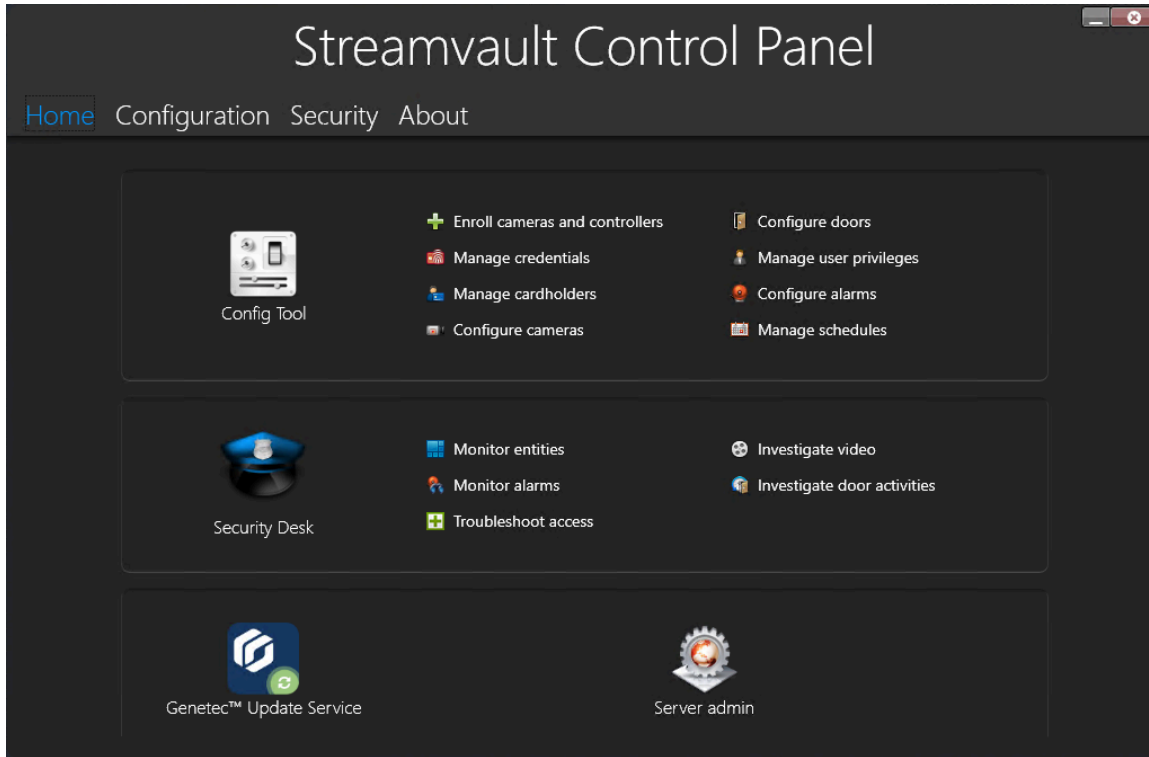
Diese Referenzseiten helfen Ihnen dabei, das SV Control Panel zu verstehen.

Dieser Abschnitt enthält die folgenden Themen:

- ["Startseite des SV Control Panel"](#) auf Seite 69
- ["Konfigurationsseite des SV Control Panel"](#) auf Seite 71
- ["Sicherheitsseite des SV Control Panels"](#) auf Seite 74
- ["Informationsseite des SV Control Panel"](#) auf Seite 78

## Startseite des SV Control Panel

Verwenden Sie die Startseite im SV Control Panel, um auf die Standardtasks zuzugreifen, die für das Konfigurieren und Verwenden Ihres Systems erforderlich sind. Sie können auf die Symbole auf der Benutzeroberfläche klicken, um auf die Anwendungen Config Tool, Security Desk, Server Admin oder Genetec™ Update Service zuzugreifen.



Alternativ können Sie auf die Config-Tool- oder Security-Desk-Tastaturkürzel klicken, um die entsprechenden Tasks zu öffnen.

Bei Systemen, die im Client-Modus ausgeführt werden, ist das Server-Admin-Tastaturkürzel nicht verfügbar. Ebenso sind die Tastaturkürzel für Config Tool und Security Desk eingeschränkt.

**BEMERKUNG:** Hinweis: Wenn Ihr System nicht aktiviert ist, erscheint ein rotes Banner, um Sie darauf hinzuweisen. Klicken Sie auf **Das System ist nicht aktiviert. Klicken Sie hier, um es zu aktivieren.**, um den Assistenten zur Aktivierung des Streamvault™ Control Panels zu öffnen.

### Config Tool-Tastaturkürzel

Verwenden Sie die Tastaturkürzel zum Öffnen der Haupttasks in Config Tool. Die verfügbaren Tastaturkürzel hängen von Ihren Lizenzoptionen ab.

| Tastaturkürzel                  | Aktion  |
|---------------------------------|---|
| Config Tool                     | Öffnet das Config Tool.   |
| Kameras und Controller anmelden | Öffnet das Unit Enrollment Tool, in dem Sie Ihre Kameras und Controller registrieren können.                          |
| Berechtigungen verwalten        | Öffnet den Task <i>Berechtigungsnachweisverwaltung</i> , in dem Sie die Berechtigungen der Benutzer verwalten können. |

| Tastaturkürzel           | Aktion   |
|--------------------------|--|
| Karteninhaber verwalten  | Öffnet den Task <i>Karteninhaberverwaltung</i> , in dem Sie Karteninhaber verwalten können.            |
| Kameras konfigurieren    | Öffnet den Task <i>Video</i> , in dem Sie Kameras hinzufügen und verwalten können.                     |
| Türen konfigurieren      | Öffnet den Task <i>Bereichsansicht</i> , in dem Sie Türen hinzufügen und verwalten können.             |
| Benutzerrechte verwalten | Öffnet den Task <i>Benutzerverwaltung</i> , in dem Sie Benutzerrechte hinzufügen und verwalten können. |
| Alarmer konfigurieren    | Öffnet die Task <i>Alarmer</i> , in der Sie Alarmer konfigurieren können.                              |
| Zeitpläne verwalten      | Öffnet den Task <i>System</i> , in dem Sie Zeitpläne erstellen und verwalten können.                   |

## Tastaturkürzel für Security Desk

Verwenden Sie die Tastaturkürzel, um die Haupttasks in der Security-Desk-Anwendung zu öffnen. Die verfügbaren Tastaturkürzel hängen von Ihren Lizenzoptionen ab.

| Tastaturkürzel             | Aktion  |
|----------------------------|---|
| Security Desk              | Öffnet Security Desk.   |
| Einheiten überwachen       | Öffnet den Task <i>Überwachung</i> , in dem Sie Systemereignisse in Echtzeit überwachen können.   |
| Alarmer überwachen         | Öffnet den Task <i>Alarmüberwachung</i> , in dem Sie aktive Alarmer überwachen und darauf reagieren sowie vergangene Alarmer anzeigen können.   |
| Zutrittsfehlerbehebung     | Öffnet das Werkzeug für die Zutrittsfehlerbehebung, mit dem Sie Probleme bei der Konfiguration des Zutritts diagnostizieren und beheben können.<br><b>BEMERKUNG:</b> Diese Tastaturkürzel ist nicht für Systeme verfügbar, die im Client-Modus ausgeführt werden. |
| Video untersuchen          | Öffnet den Task <i>Archive</i> , in dem Sie nach Videoarchiven suchen können.<br><b>BEMERKUNG:</b> Diese Tastaturkürzel ist nicht für Systeme verfügbar, die im Client-Modus ausgeführt werden.   |
| Türaktivitäten untersuchen | Öffnet den Task <i>Türaktivitäten</i> , in dem Sie die Ereignisse an ausgewählten Türen untersuchen können.<br><b>BEMERKUNG:</b> Dieser Tastaturkürzel ist nicht für Systeme verfügbar, die im Client-Modus ausgeführt werden.                                    |

## Genetec Update Service-Tastaturkürzel

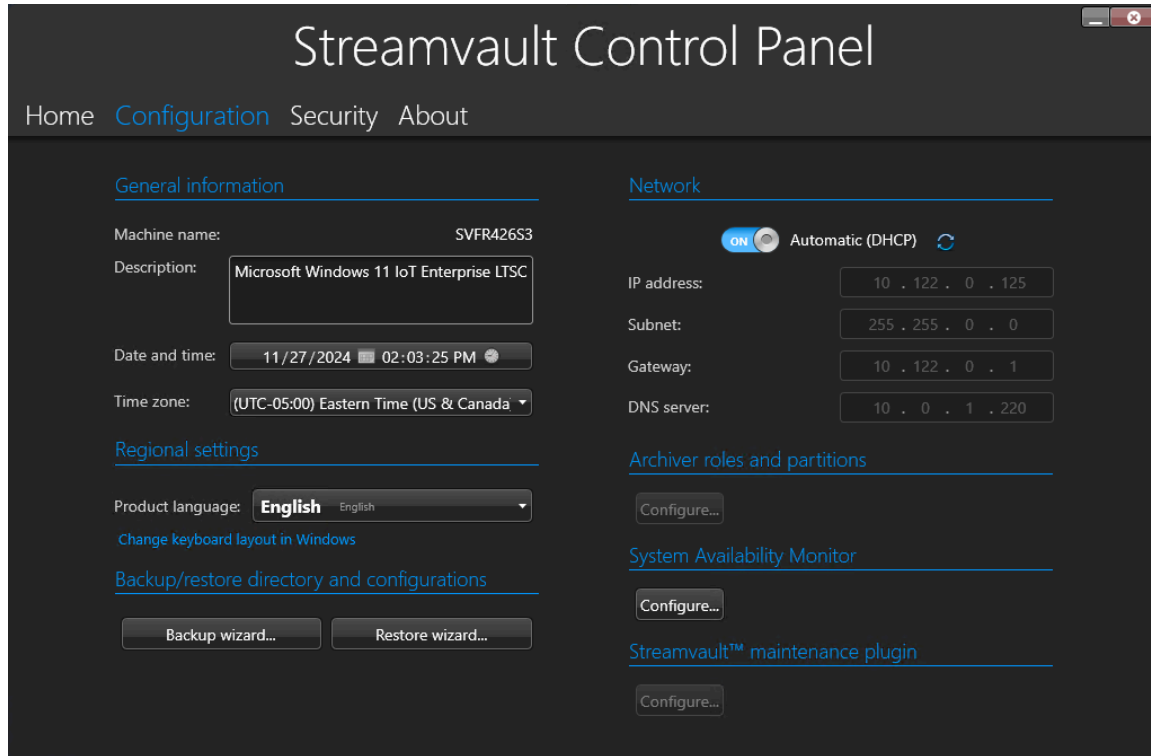
Verwenden Sie den Genetec Update Service, um sicherzustellen, dass die Softwarekomponenten auf Ihrer Appliance aktuell sind.

## Server Admin-Tastaturkürzel

Verwenden Sie die Server-Admin-Anwendung, um eine Lizenz manuell anzuwenden oder die Konfiguration des Servers anzuzeigen und zu ändern.

# Konfigurationsseite des SV Control Panel

Verwenden Sie die *Konfigurationsseite* des Streamvault™ Control Panel, um allgemeine Einstellungen zu modifizieren, z. B. die *regionalen Einstellungen*, die *Netzwerkeinstellungen* und die *Einstellungen für den System Availability Monitor*.



Für Systeme, die auf einem Erweiterungsserver oder im Clientmodus laufen, sind die Abschnitte *System Availability Monitor* und *Verzeichnis und Konfigurationen sichern/wiederherstellen* nicht verfügbar.

## Einstellungen für allgemeine Informationen

Verwenden Sie den Abschnitt *Allgemeine Informationen*, um allgemeine Einstellungen zu ändern, z. B. den Namen Ihrer Streamvault™-Appliance.

- **Computername:** Zeigt den Namen des SV-Computers an.
- **Beschreibung:** Geben Sie eine aussagekräftige Beschreibung ein, um den Computer zu identifizieren.
- **Datum / Uhrzeit:** Klicken Sie auf das Feld, um die Daten- und Zeitwerte zu konfigurieren, die auf dem Rechner angezeigt werden. Alternativ können Sie auf den Kalender oder das Uhrensymbol im Feld klicken, um die Einstellungen zu konfigurieren.
- **Zeitzone:** Wählen Sie eine Zeitzone aus dem Drop-down-Menü aus.

## Regionale Einstellungen

Verwenden Sie den Abschnitt *Regionale Einstellungen*, um die Spracheinstellungen des Layouts Ihrer Systemtastatur zu ändern.

- **Produktsprache:** Wählen Sie eine Sprache aus der Liste aus, um die Sprache von Config Tool und Security Desk aus.
- WICHTIG:** Damit die Änderungen übernommen werden, müssen Sie Ihre Security-Center-Anwendungen neu starten.

- **Tastatur-Layout in Windows ändern:** Klicken Sie auf diese Option, um die Windows Einstellungsseite für *Sprache & Region* zu öffnen und das Layout Ihrer Tastatur zu ändern.
- WICHTIG:** Damit die Änderungen übernommen werden, müssen Sie Ihren Computer neu starten.
- BEMERKUNG:** Die SV Control Panel ist in Englisch, Französisch und Spanisch verfügbar.

## Backup und Wiederherstellen

Verwenden Sie den Abschnitt *Verzeichnis und Konfigurationen sichern/wiederherstellen*, um auf den Assistenten zum *Sichern* und *Wiederherstellen* zuzugreifen.

Das Sichern und Wiederherstellen ist eine Funktion des SV Control Panel. Sie können damit Ihre Directory-Datenbank und Konfigurationsdateien sichern und später für die gleiche System-ID wiederherstellen. Sichern und Wiederherstellen kann im Fall eines Systemausfalls oder eines Hardware-Upgrades verwendet werden. Diese Funktion sichert Ihre Lizenzdatei, Videoarchive oder andere Datenbanken nicht.

Dieser Abschnitt ist nicht für Systeme verfügbar, die auf einem Erweiterungsserver oder im Client-Modus ausgeführt werden.


- **Sicherungsassistent:** Klicken Sie auf **Sicherungsassistent**, um eine Sicherung Ihrer Directory-Datenbank und Konfigurationsdateien zu erstellen.
- **Wiederherstellungsassistent:** Klicken Sie auf **Wiederherstellungsassistent**, um eine Sicherung Ihrer Directory-Datenbank und Konfigurationsdateien in Ihrem System wiederherzustellen.

**WICHTIG:** Sie müssen den erforderlichen Port öffnen, um sicherzustellen, dass die Funktion *Directory und Konfigurationen* mit dem SV Control Panel kommunizieren kann. Weitere Informationen dazu finden Sie unter [Von Streamvault verwendete Standardports](#) auf Seite 4.

## Netzwerkeinstellungen

Im Abschnitt *Netzwerk* können Sie die Netzwerkeinstellungen ändern, z. B. die IP-Adresse Ihrer Streamvault™-Appliance.

- **Automatisches DHCP:** Das Dynamic Host Configuration Protocol (DHCP) wird verwendet, um die IP-Adresse, das Subnetz, Gateway und den DNS-Server automatisch zuzuweisen. Deaktivieren Sie diese Option, wenn Sie nicht möchten, dass die IP-Adresse dynamisch von Ihrem DHCP-Server zugewiesen wird.

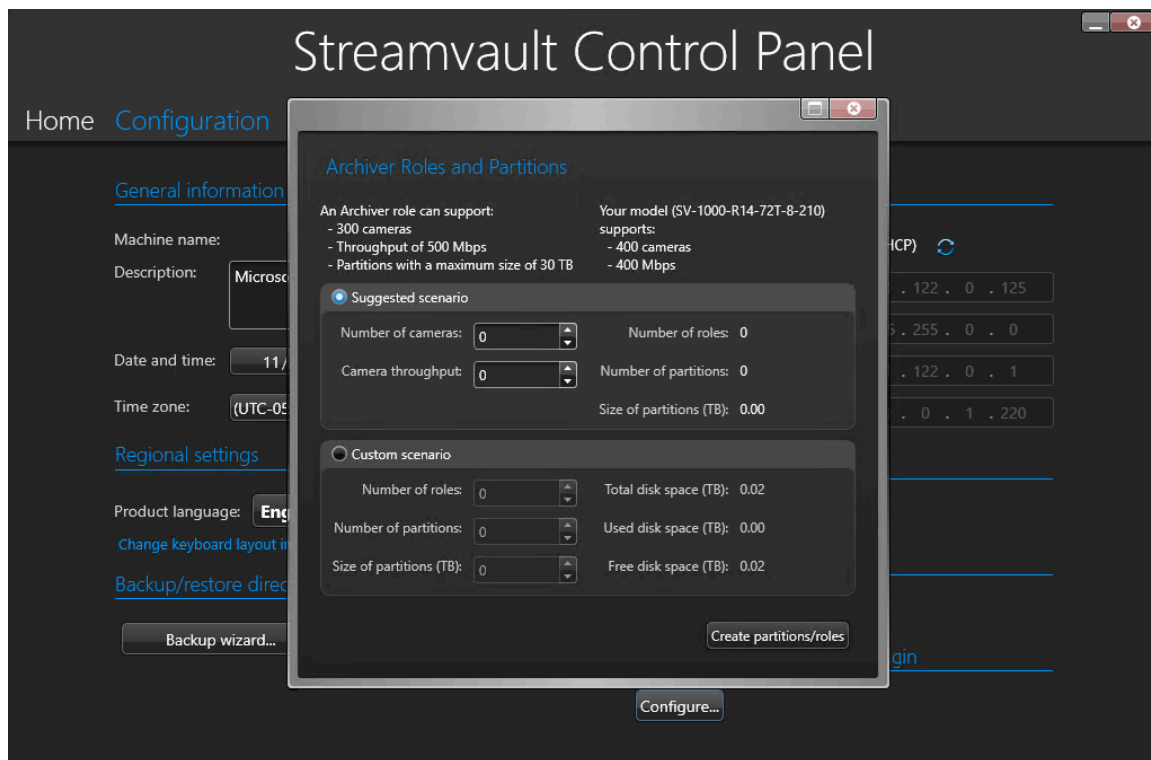
Klicken Sie auf **Aktualisieren** , um Ihre DHCP-Einstellungen zu aktualisieren und eine neue IP-Adresse zu erhalten.

- **IP-Adresse:** Die IP-Adresse des Computers.
- **Subnetz:** Die Subnetzmaske des Computers.
- **Gateway:** Die IP-Adresse des Gateway.
- **DNS-Server:** Die IP-Adresse des DNS-Servers.

## Archivierungrollen und Partitionen

Verwenden Sie den Abschnitt *Archivierungrollen und Partitionen*, um Systeme zu konfigurieren, die mehr als die maximale Anzahl von Kameras und den maximalen Durchsatz benötigen, die von einem einzelnen Archiver unterstützt werden.

Dieser Abschnitt ist für Systeme verfügbar, die Security Center 5.9 und neuer auf einem Erweiterungsserver ausführen.



- **Eine Archiver-Rolle kann Folgendes unterstützen:** Zeigt die maximale Anzahl von Kameras, die Durchsatzmenge und die Partitionsgröße an, die von einer einzelnen Archiver-Rolle unterstützt werden.
- **Ihr Modell unterstützt:** Zeigt die maximale Anzahl von Kameras und die Durchsatzmenge an, die von Ihrem Streamvault-Appliance-Modell unterstützt werden.
- **Empfohlenes Szenario:** Kalkuliert die Anzahl von Rollen und Partitionen sowie die Partitionsgröße, die für Ihre gewünschte Menge an Kameras und Durchsatz erforderlich sind.
- **Benutzerdefiniertes Szenario:** Wählen Sie die Anzahl von Rollen, Partitionen und Partitionsgrößen für Ihre Systemkonfiguration aus.

Weitere Informationen zu dieser Funktion finden Sie unter [Archiver-Rollen im SV Control Panel hinzufügen](#) auf Seite 39.

## System Availability Monitor-Einstellungen

Verwenden Sie den Abschnitt *System Availability Monitor*, um die Einstellungen für den System Availability Monitor Agent auf Ihrer Streamvault™ Appliance zu konfigurieren. Beispielsweise das Festlegen der Datenerfassungsmethode oder Aktivieren des Agenten.

Sie können auch Folgendes überprüfen:

- Ob die Appliance mit Security Center kommuniziert
- Wann der letzte Kontrollpunkt aufgetreten ist
- Welche Fehler und Warnungen kürzlich in den Anwendungs- und Serviceprotokollen berichtet wurden

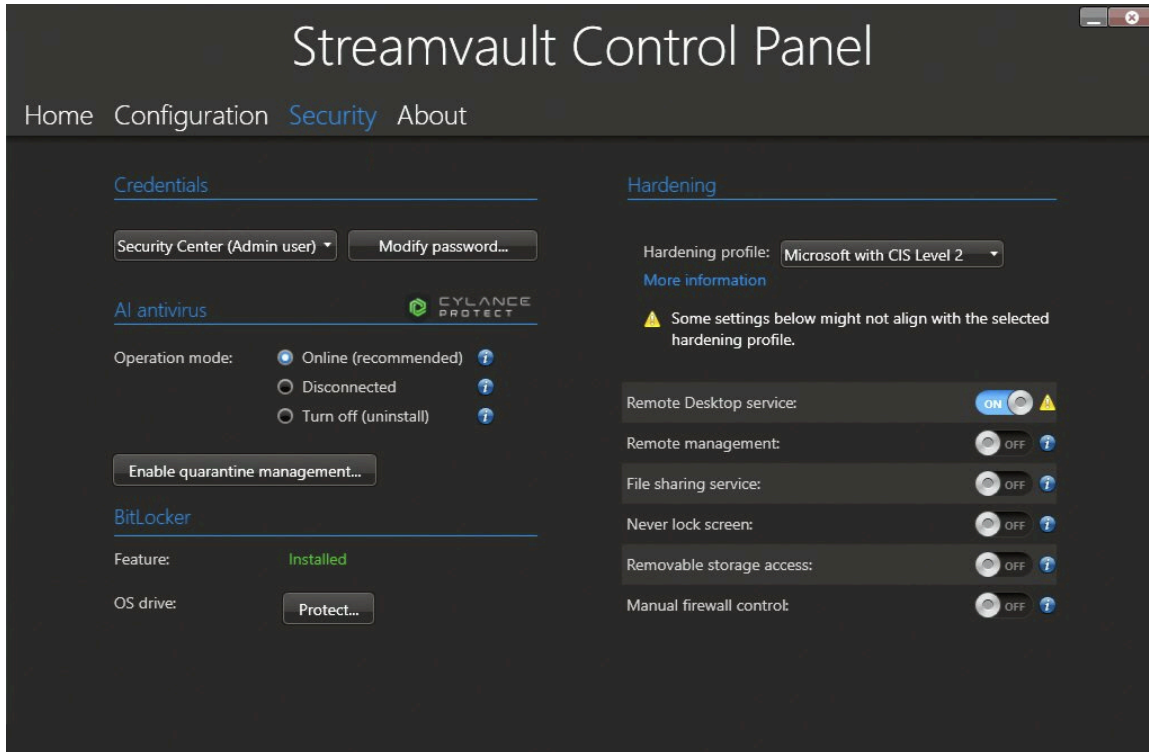
Dieser Abschnitt ist nicht für Systeme verfügbar, die auf einem Erweiterungsserver oder im Client-Modus ausgeführt werden.

## Streamvault Maintenance-Plugin-Einstellungen

Verwenden Sie den Abschnitt *Streamvault™-Wartungs-Plugins*, um das Plugin im Security Center zu registrieren, wenn es noch nicht registriert ist.

## Sicherheitsseite des SV Control Panels

Auf der Seite *Sicherheit* können Sie Benutzer-Passwörter modifizieren, den Kommunikationsmodus zwischen dem CylancePROTECT Agent und Genetec™ auswählen und Härtingsprofile und System-Sicherheitseinstellungen auf Ihre Streamvault™ Appliance anwenden.



### Passworteinstellungen

Verwenden Sie den Abschnitt *Berechtigungen* auf der Seite *Sicherheit*, um die Passwörter der Benutzerkonten für Ihre Streamvault™ Appliance zu ändern.

**BEMERKUNG:** Für den aktuellen Benutzer sind auf einem Haupt- und Erweiterungsserver unterschiedliche Passwortoptionen verfügbar. Auf einem Erweiterungsserver kann der Admin nur die Windows-Passwörter, nicht die Passwörter für Security-Center-Anwendungen ändern.

Definieren Sie für jeden Benutzer ein Passwort:

- **Security Center (Admin-Benutzer):** Das Passwort des Admin-Benutzers für Security Desk, Config Tool und Genetec™ Update Service.
- **Server Admin:** Das Passwort für die Genetec™-Server-Admin-Anwendung.
- **Windows-Bediener:** Klicken Sie auf **Passwort ändern**, um das Bedienerpasswort für Windows zu ändern.

### Antivirus-Einstellungen

Im Abschnitt *AI-Antivirus* können Sie den Modus auswählen, in dem der CylancePROTECT Agent mit Genetec kommuniziert.

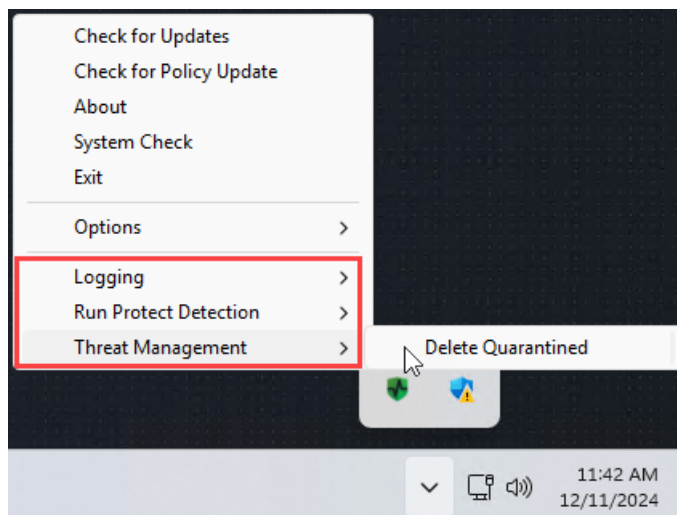
CylancePROTECT ist die KI-gestützte Antiviren-Software zum Schutz vor Bedrohungen und deren Erkennung.

Sie können zwischen den folgenden Betriebsarten wählen:

- **Online (empfohlen):** Bei Internetverbindung kommuniziert der CylancePROTECT Agent mit Genetec, um über neue Bedrohungen zu berichten, den Agenten zu aktualisieren und Daten für die Verbesserung der mathematischen Modelle zu senden. Diese Option bietet die höchste Schutzstufe.
- **Getrennt:** Der getrennte Modus ist für eine Appliance ohne Internetverbindung gedacht. In diesem Modus kann sich CylanceProtect nicht mit Genetec™-Verwaltungsservices in der Cloud verbinden und Informationen an sie senden. Ihre Appliance ist vor den meisten Gefahren geschützt. Wartung und Updates sind über den Genetec™ Update Service (GUS) verfügbar.
- **Ausschalten:** Wählen Sie diesen Modus aus, um CylancePROTECT dauerhaft von Ihrer Appliance zu deinstallieren. Ihre Appliance verwendet Microsoft Defender als Bedrohungsschutz und -erkennung. Es wird nicht empfohlen, CylancePROTECT auszuschalten, wenn die Appliance keine Updates der Virendefinitionen für Microsoft Defender empfangen kann.

**ACHTUNG:** Das Wechseln zwischen Optionen erfordert möglicherweise einen Neustart des Computers, was einen Ausfall des Systems verursacht.

Klicken Sie auf **Quarantäneverwaltung aktivieren**, um das **Bedrohungsmanagement** zum Rechtsklickmenü des Cylance-Symbols in der Windows Taskleiste hinzuzufügen. Mit dieser Option können Sie unter Quarantäne gestellte Objekte löschen. Die Funktionen **Logging** und **Run Protect Detection** wurden ebenfalls dem Rechtsklickmenü hinzugefügt. Mit diesen Optionen können Sie auf Protokolle zugreifen bzw. Scans auslösen.



## Verschlüsselungseinstellungen

Verwenden Sie den Abschnitt *BitLocker*, um die BitLocker-Funktion zu installieren und das Betriebssystemlaufwerk auf Ihrer Streamvault™-Appliance zu verschlüsseln.

- **Funktion:** Die BitLocker-Funktion ist unter Windows 10 und Windows 11 vorinstalliert. Wenn Sie Windows Server installiert haben, müssen Sie auf **Installieren** klicken, um die Funktion zu installieren.
- **Betriebssystemlaufwerk:** Klicken Sie auf **Schützen**, um das Betriebssystemlaufwerk (C:) mit BitLocker zu verschlüsseln. Der Entschlüsselungsschlüssel wird auf einem TPM (Trusted Platform Module)-Chip gespeichert, der sich auf der Systemplatine der Streamvault™-Appliance befindet. Wenn das Betriebssystemlaufwerk entfernt oder die Systemplatine ausgetauscht würde, gingen die Informationen auf dem Betriebssystemlaufwerk verloren. Das Betriebssystemlaufwerk kann nicht auf den Entschlüsselungsschlüssel auf dem TPM zugreifen. In diesen Szenarien können Sie einen Wiederherstellungsschlüssel erstellen, der zum Entschlüsseln des Laufwerks verwendet werden kann. Ohne Wiederherstellungsschlüssel muss für die Appliance ein neues Image erstellt und die Software neu installiert werden. Durch die Verschlüsselung des Betriebssystemlaufwerks wird auch das Windows-Administrator Kennwort vor unbefugtem Zugriff geschützt.

Weitere Informationen finden Sie unter [Verschlüsseln des Betriebssystemlaufwerks](#).

## Einstellungen für die Härtung

Verwenden Sie den Abschnitt *Härtung*, um ein Härtingsprofil auszuwählen und die Einstellungen für die Systemsicherheit Ihrer Streamvault™ Appliance festzulegen.

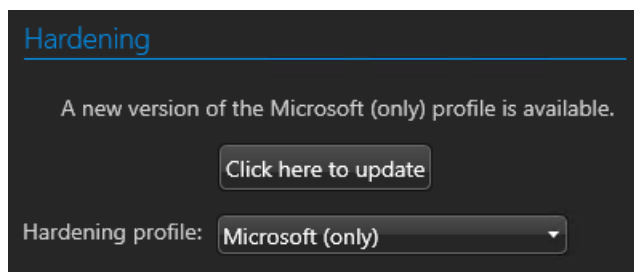
**BEMERKUNG:** Die Härtingsprofile sind nur auf Appliances verfügbar, die über die [Streamvault™ Service](#) verfügen. Weitere Informationen dazu finden Sie unter [Informationen zum Streamvault™ Service](#) auf Seite 15.

Es gibt vier vordefinierte Härtingsprofile:

- **Microsoft (nur):** Dieses Profil für die Härtung wendet Microsoft-Sicherheitsgrundlagen auf Ihr System an. Microsoft Sicherheits-Baselines sind eine Gruppe von Microsoft-empfohlenen Konfigurationseinstellungen, die auf dem Feedback von Microsoft Security Engineering Teams, Produktgruppen, Partnern und Kunden basieren.
  - **Microsoft mit CIS Stufe 1:** Dieses Härtingsprofil wendet die Microsoft-Sicherheitsbaselines und das Profil des Center for Internet Security (CIS) Level 1 (CIS L1) auf Ihr System an. Das CIS L1 bietet grundlegende Sicherheitsanforderungen, die auf jedem System mit geringen oder gar keinen Leistungseinbußen oder Funktionseinschränkungen implementiert werden können.
  - **Microsoft mit CIS Stufe 2:** Dieses Härtingsprofil wendet die Microsoft-Sicherheitsbaselines und die Profile CIS L1 und Level 2 (L2) auf Ihr System an. Das Profil CIS L2 bietet die höchste Sicherheitsstufe und ist für Organisationen gedacht, in denen Sicherheit von größter Bedeutung ist.
- BEMERKUNG:** Die strenge Sicherheit, die dieses Härtingsprofil mit sich bringt, kann die Systemfunktionalität einschränken und das Remote Management von Servern erschweren.
- **Microsoft mit STIG:** Dieses Profil zur Härtung wendet die Microsoft-Sicherheitsbaselines und die Sicherheit Technical Implementation Guides (STIGs) der Defense Information Systems Agency (DISA) auf Ihr System an. Die DISA STIGs basieren auf den Standards des National Institute of Standards and Technology (NIST) und bieten fortschrittlichen Sicherheitsschutz für Windows-Systeme für die Abteilung des US-Verteidigungsministeriums.

**BEMERKUNG:** Standardmäßig werden alle Appliances mit dem Härtingsprofil Microsoft mit CIS Level 2 ausgeliefert.

Wenn eine neue Version des von Ihnen ausgewählten Härtingsprofils verfügbar ist, wird eine Schaltfläche **Hier klicken, um zu aktualisieren** angezeigt. Klicken Sie auf die Schaltfläche, um die Aktualisierung zu übernehmen.



Zusätzlich zu den Härtingsprofilen können die folgenden Sicherheitseinstellungen für das System festgelegt werden:

- **Remote Desktop Service:** Erlauben Sie Personen in Ihrem Netzwerk, sich bei der Appliance mithilfe der Anwendung *Remotedesktop* anzumelden. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Remote Management:** Aktivieren Sie den Remote Support für Microsoft Management Werkzeuge wie Windows Admin Center, Microsoft Server Manager und Remote PowerShell.
- **Datei-Sharing Service:** Erlauben Sie Personen in Ihrem Netzwerk, Dateien und Ordner zu teilen, die sich auf der Appliance befinden. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Bildschirm nie sperren:** Wenn diese Option aktiviert ist, bleibt ein Benutzer auch dann angemeldet, wenn er 15 Minuten lang nicht aktiv war.

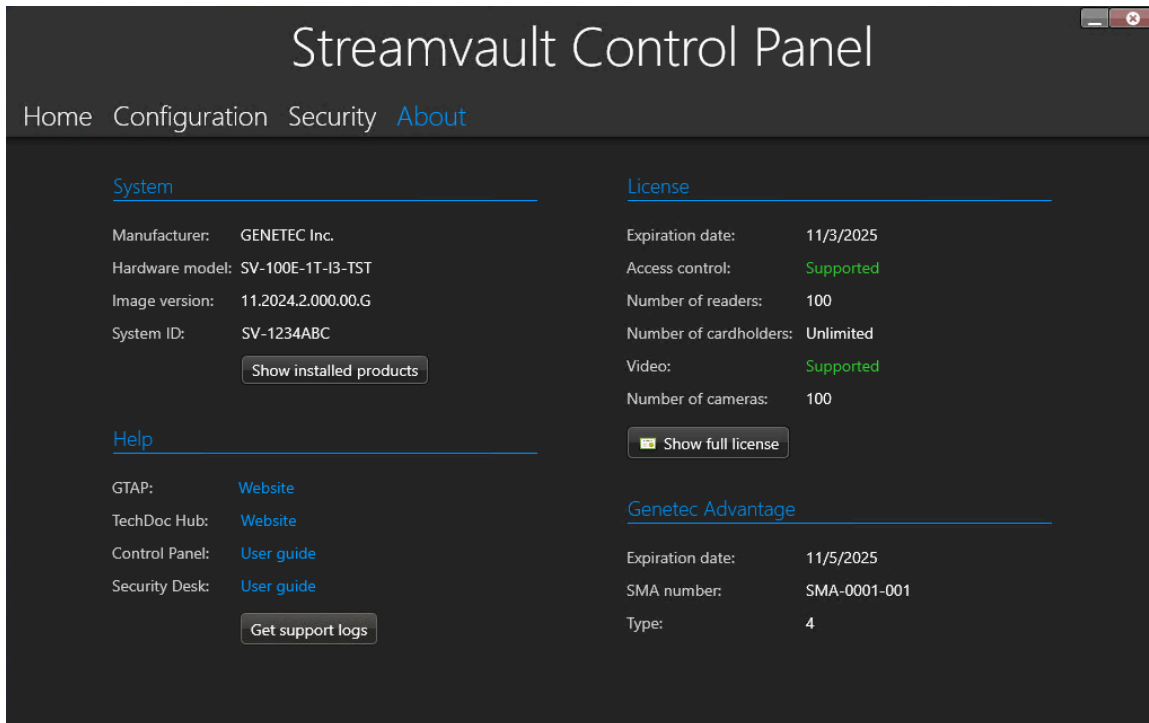
- **Zugriff auf Wechselmedien:** Aktivieren Sie den Zugriff auf einen angeschlossenen USB-Schlüssel oder eine USB-Festplatte über Windows zu erlauben.  
**BEMERKUNG:** Benutzer mit administrativen Berechtigungen haben automatisch Zugriff auf Wechselmedien.
- **Manuelle Firewall-Steuerung:** Standardmäßig verwendet die Windows Defender-Firewall Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) aus den Härtingsprofilen, um das System zu sichern. Aktivieren Sie diese Option, um die Firewall-Richtlinien manuell zu steuern. Alle Gruppenrichtlinienobjekte werden deaktiviert.

Weitere Informationen dazu finden Sie unter [Windows-Firewall deaktivieren](#) auf Seite 126.

# Informationsseite des SV Control Panel

Verwenden Sie die Seite *Informationen*, um hilfreiche Informationen anzuzeigen, wenn Sie Unterstützung bei Ihrer Streamvault™-Appliance benötigen. Die Seite *Informationen* enthält Systeminformationen, Links zum Genetec™ Technical Assistance Portal (GTAP) und zur Produktdokumentation, Lizenzinformationen und Informationen zum Software Maintenance Agreement (SMA).

In Systemen, die auf einem Erweiterungsserver ausgeführt werden oder sich im Client-Modus befinden, sind nur die Abschnitte *System* und *Hilfe* verfügbar.



## Systeminformationen

Verwenden Sie den Abschnitt *System*, um Informationen über das System anzuzeigen.

- **Hersteller:** Zeigt den Hardwarehersteller an.
- **Hardware-Modell:** Zeigt das Hardware-Modell an.
- **Image-Version:** Zeigt die Software-Image-Version an.
- **System-ID:** Zeigt die System-ID-Nummer an.
- **Installierte Produkte anzeigen:** Klicken Sie, um die Softwareversion der auf der Appliance installierten Genetec-Komponenten anzuzeigen.

## Hilfe-Informationen

Im *Hilfereich* finden Sie nützliche Links zur GTAP- und Produktdokumentation.

- **GTAP:** Klicken Sie auf den Link, um [GTAP](#) und Support-Foren zu öffnen.  
**BEMERKUNG:** Sie benötigen einen gültigen Benutzernamen und ein Passwort, um sich bei GTAP anzumelden.
- **TechDoc Hub:** Klicken Sie auf den Link, um den [Genetec TechDoc Hub](#) zu öffnen.
- **Control Panel:** Klicken Sie auf den Link, um das *Streamvault-Appliance – Benutzerhandbuch* zu öffnen, das Informationen zu SV Control Panel enthält.

- **Security Desk:** Klicken Sie hier, um das *Security Center – Benutzerhandbuch* zu öffnen.
- **Support-Protokolle abrufen:** Klicken Sie hier, um auszuwählen, welche Support-Protokolle Sie zur Fehlerbehebung herunterladen möchten.

## Lizenzinformation

Verwenden Sie den Abschnitt *Lizenz*, um Informationen über die Lizenz anzuzeigen. Die angezeigte Informationen hängen von Ihren Lizenzoptionen ab.

- **Ablaufdatum:** Zeigt an, wann Ihre Security-Center-Lizenz abläuft.
- **Zutrittskontrolle:** Zeigt an, ob Zutrittskontrollfunktionen unterstützt werden oder nicht.
- **Anzahl der Lesegeräte:** Zeigt an, wie viele Lesegeräte in Ihrem System unterstützt werden.
- **Anzahl der Karteninhaber:** Zeigt an, wie viele Karteninhaber in Ihrem System unterstützt werden.
- **Video:** Zeigt an, ob Videofunktionen unterstützt werden oder nicht.
- **Anzahl der Kameras:** Zeigt an, wie viele Kameras in Ihrem System unterstützt werden.
- **Ganze Lizenz anzeigen:** Klicken Sie, um weitere Lizenzinformationen anzuzeigen.

Dieser Abschnitt ist nicht für Systeme verfügbar, die auf einem Erweiterungsserver oder im Client-Modus ausgeführt werden.

## Genetec Advantage Informationen

Verwenden Sie den Abschnitt *Genetec Advantage*, um Informationen über die SMA anzuzeigen.

- **Ablaufdatum:** Zeigt das Ablaufdatum des Software-Wartungsvertrags an.
- **SMA-Nummer:** Zeigt die SMA-Nummer an.
- **Typ:** Zeigt den SMA-Typ an.

Dieser Abschnitt ist nicht für Systeme verfügbar, die auf einem Erweiterungsserver oder im Client-Modus ausgeführt werden.

## Weitere Ressourcen

Dieser Abschnitt enthält die folgenden Themen:

- ["Produktgarantie für Ihre Streamvault-Appliance"](#) auf Seite 81
- [" Konfigurieren des BIOS-Passworts "](#) auf Seite 82
- [" Ändern des iDRAC-Standardpassworts "](#) auf Seite 85
- ["Einen neuen iDRAC-Benutzer mit Administratorrechten hinzufügen"](#) auf Seite 86
- ["Deaktivieren des iDRAC-Root-Benutzers"](#) auf Seite 87
- ["Neues Image für Streamvault-Appliance festlegen"](#) auf Seite 88
- ["Die System-ID und Image-Version einer Streamvault™ Appliance finden"](#) auf Seite 89
- ["Dateifreigabe auf einer Streamvault-Appliance erlauben"](#) auf Seite 90
- ["Remotedesktop-Verbindungen auf einer Streamvault™-Appliance erlauben"](#) auf Seite 91

## Produktgarantie für Ihre Streamvault-Appliance

---

Ihre Streamvault™-Appliance ist durch eine Standard-Hardware- und -Softwaregarantie abgedeckt, mit einer optionalen zweijährigen Erweiterung.

Detaillierte Beschreibungen der Nutzungsbedingungen der Genetec™-Produktgarantie finden Sie im [Überblick über die Genetec™-Produktgarantie](#).

# Konfigurieren des BIOS-Passworts

Um die Daten auf Ihrer Streamvault™-Appliance vor unbefugtem Zugriff zu schützen, müssen Sie ein BIOS-Passwort festlegen.

## Was Sie noch wissen sollten

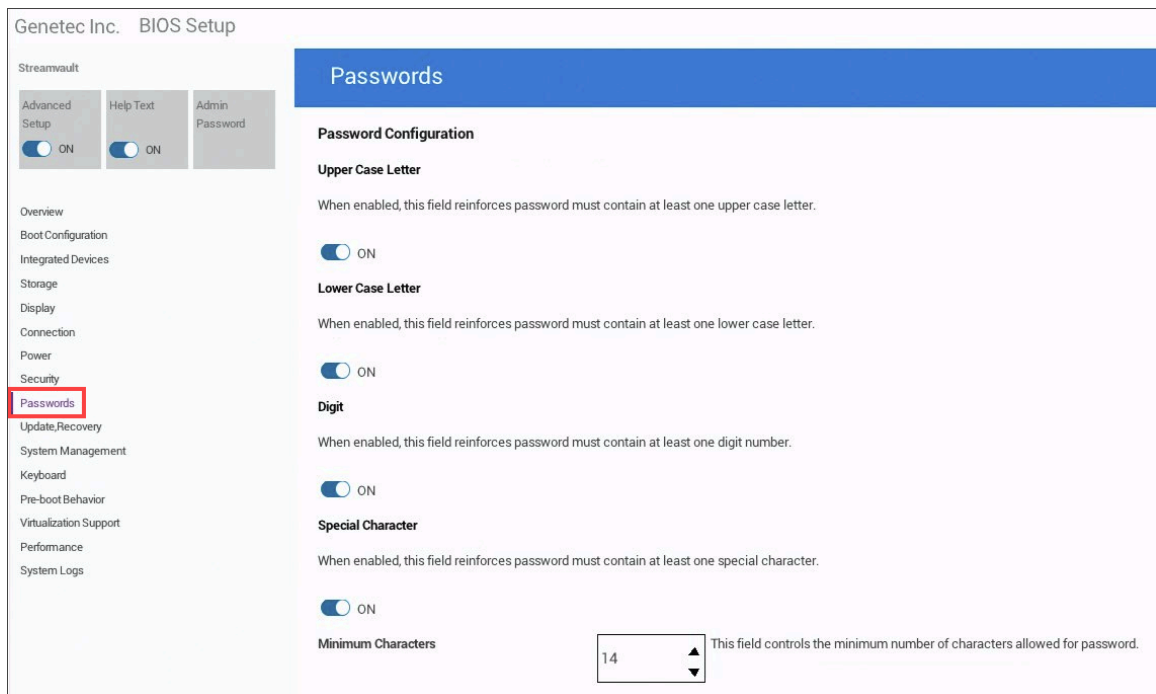
Die Schritte zum Konfigurieren eines BIOS-Passworts unterscheiden sich je nach Appliance-Modell. Befolgen Sie die für Ihre Appliance geltende Vorgehensweise.

- [Legen Sie das BIOS-Passwort für Ihre Streamvault™ All-in-One-Appliance oder -Workstation fest.](#)
- [Legen Sie das BIOS-Passwort auf Ihrer Appliance der Serie SV-1000, SV-2000, SV-4000 oder SV-7000 \(PowerEdge\) fest.](#)

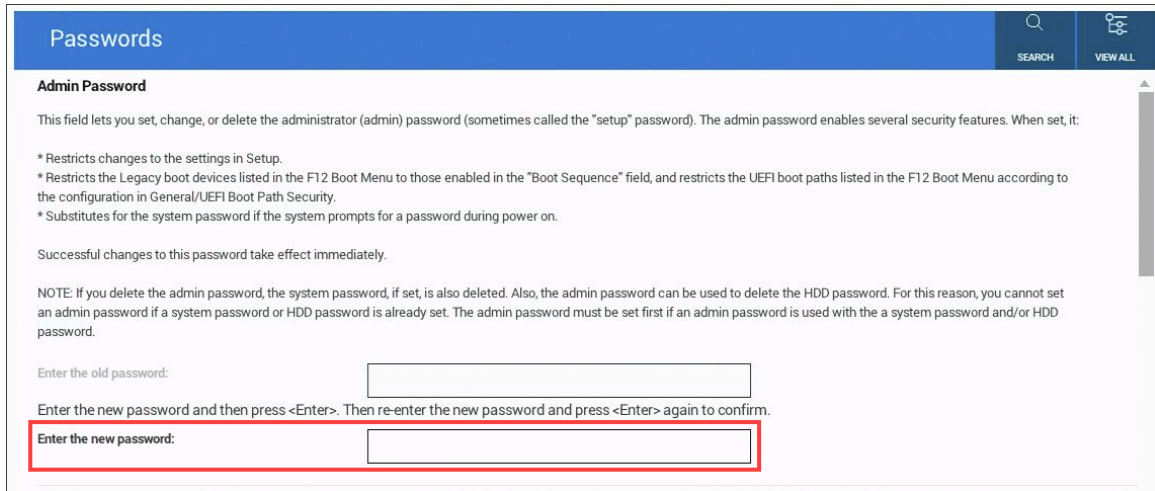
## Prozedur

### So legen Sie das BIOS-Passwort für Ihre Streamvault™ All-in-One-Appliance oder -Workstation fest:

- 1 Schalten Sie die Appliance ein oder starten Sie sie neu, und drücken Sie wiederholt F2, bis das Menü *BIOS-Setup* angezeigt wird.
- 2 Wählen Sie **Passwörter** aus dem Menü auf der linken Seite des Bildschirms aus.
- 3 Scrollen Sie auf der Seite *Passwörter* nach unten zum Abschnitt *Passwortkonfiguration* und konfigurieren Sie die folgenden Einstellungen:
  - Aktivieren Sie die Optionen **Großbuchstabe**, **Kleinbuchstabe**, **Ziffer** und **Sonderzeichen**.
  - Setzen Sie das Feld **Minimale Zeichen** auf 14.



- 4 Scrollen Sie zum Anfang der Seite *Passwörter* und geben Sie unter **Admin-Passwort** ein neues BIOS-Passwort ein.



**Passwords**

**Admin Password**

This field lets you set, change, or delete the administrator (admin) password (sometimes called the "setup" password). The admin password enables several security features. When set, it:

- \* Restricts changes to the settings in Setup.
- \* Restricts the Legacy boot devices listed in the F12 Boot Menu to those enabled in the "Boot Sequence" field, and restricts the UEFI boot paths listed in the F12 Boot Menu according to the configuration in General/UEFI Boot Path Security.
- \* Substitutes for the system password if the system prompts for a password during power on.

Successful changes to this password take effect immediately.

NOTE: If you delete the admin password, the system password, if set, is also deleted. Also, the admin password can be used to delete the HDD password. For this reason, you cannot set an admin password if a system password or HDD password is already set. The admin password must be set first if an admin password is used with the a system password and/or HDD password.

Enter the old password:

Enter the new password and then press <Enter>. Then re-enter the new password and press <Enter> again to confirm.

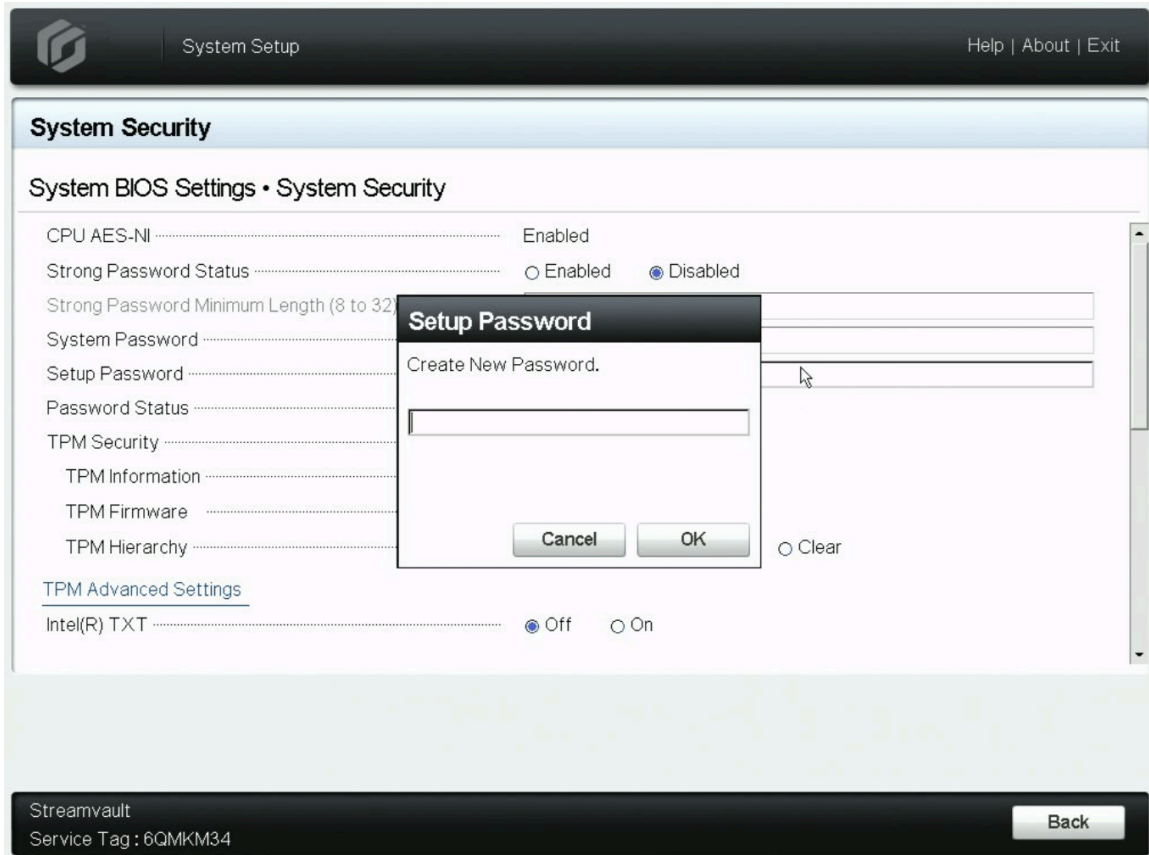
Enter the new password:

- 5 Klicken Sie auf **Beenden**.  
Ihre Änderungen werden gespeichert und die Appliance wird neu gestartet.

### So legen Sie das BIOS-Passwort für Ihre Appliance der Serie SV-1000, SV-2000, SV-4000 oder SV-7000 (PowerEdge) fest:

- 1 Schalten Sie die Appliance ein oder starten Sie sie neu und drücken Sie wiederholt F2, bis das Menü *System-Setup* erscheint.
- 2 Klicken Sie im *Hauptmenü des System-Setups* auf **System-BIOS**.
- 3 Klicken Sie in den *System-BIOS-Einstellungen* auf **Systemsicherheit**.
- 4 Klicken Sie im Feld **Setup-Passwort** in das Textfeld.

- 5 Geben Sie im sich öffnenden Dialogfeld *Setup-Passwort* ein neues Passwort ein und klicken Sie auf **OK**.



- 6 Wählen Sie im Feld **Passwortstatus** die Option **Gesperrt** aus, damit das Setup-Passwort vor dem Ändern des Systempassworts eingegeben werden muss.
- 7 Klicken Sie auf **Zurück > Fertig stellen > Fertig stellen**.  
Ihre Änderungen werden gespeichert und die Appliance wird neu gestartet.

# Ändern des iDRAC-Standardpassworts

---

Wenn Ihre Streamvault™-Appliance iDRAC unterstützt, sollten Sie das iDRAC-Standardpasswort für den Root-Benutzer sofort ändern, um unbefugten Zugriff auf Ihre Appliance zu verhindern.

## Prozedur

- 1 Starten Sie den Webbrowser „Microsoft Edge“ und öffnen Sie `https://idrac.local`.
- 2 Verwenden Sie auf der Anmeldeseite des *Integrated Remote Access Controller* den Standardbenutzernamen und das Standardkennwort, um sich anzumelden:
  - Geben Sie unter **Benutzername** das Wort `root` ein.
  - Geben Sie unter **Passwort** das Passwort ein, das sich auf dem Serviceschild Ihrer Appliance befindet.
- 3 Sobald Sie angemeldet sind, werden Sie aufgefordert, ein neues Passwort für den Root-Benutzer zu konfigurieren. Wählen Sie **Standardpasswort ändern** aus, geben Sie das neue Passwort ein und bestätigen Sie es. Klicken Sie anschließend auf **Weiter**, um Ihre Änderungen zu speichern.

## Nach Durchführen dieser Schritte

Zusätzlich zum Ändern des Standardpassworts für den Root-Benutzer ist es empfehlenswert, einen alternativen iDRAC-Benutzer mit administrativen Rechten zu erstellen und den Root-Benutzer zu deaktivieren. Weitere Informationen finden Sie unter [Hinzufügen eines neuen iDRAC-Benutzers mit Administratorrechten](#).

# Einen neuen iDRAC-Benutzer mit Administratorrechten hinzufügen

---

Der iDRAC-Root-Benutzer ist bekannt und seine Verwendung stellt ein Sicherheitsrisiko dar, selbst wenn Sie das Standardpasswort geändert haben. Daher wird empfohlen, einen neuen Benutzer mit Administratorrechten für den Zugriff auf iDRAC hinzuzufügen.

## Was Sie noch wissen sollten

Sie können einen lokalen Benutzer hinzufügen oder Microsoft Active Directory verwenden, um ein Benutzerkonto zu erstellen.

## Prozedur

- Fügen Sie einen neuen Benutzer auf eine der folgenden Arten hinzu:
  - Informationen zum Hinzufügen eines lokalen Benutzers finden Sie unter [Konfigurieren lokaler Benutzer mithilfe der iDRAC-Webschnittstelle](#) im Dell *iDRAC-Benutzerhandbuch*.
  - Informationen zur Verwendung von Microsoft Active Directory zum Erstellen eines neuen Benutzers finden Sie unter [Konfigurieren von Active Directory-Benutzern](#) im Dell *iDRAC-Benutzerhandbuch*.

**BEMERKUNG:** Stellen Sie bei der Konfiguration der Benutzerberechtigungen sicher, dass die **Benutzerrolle** auf **Administrator** festgelegt ist.

## Nach Durchführen dieser Schritte

[Deaktivieren Sie den iDRAC-Root-Benutzer](#) für zusätzliche Sicherheit.

# Deaktivieren des iDRAC-Root-Benutzers

---

Wenn Sie einen neuen iDRAC-Benutzer mit Administratorrechten erstellt haben, deaktivieren Sie den Root-Benutzer, um sicherzustellen, dass sich niemand mit diesem Benutzernamen anmelden kann.

## Bevor Sie beginnen

- Ändern Sie das iDRAC-Standardpasswort auf Ihrer Streamvault™-Appliance.
- Fügen Sie einen neuen iDRAC-Benutzer mit Administratorrechten hinzu.

## Was Sie noch wissen sollten

Sie können den Root-Benutzer deaktivieren, indem Sie die Rechte des Benutzers bearbeiten.

## Prozedur

- Ausführliche Informationen zum Bearbeiten der iDRAC-Root-Benutzerberechtigungen finden Sie unter [Konfigurieren lokaler Benutzer mithilfe der iDRAC-Webschnittstelle](#) im Dell *iDRAC-Benutzerhandbuch*.

**BEMERKUNG:** Stellen Sie beim Bearbeiten der Rechte des Root-Benutzers sicher, dass Sie Folgendes konfigurieren:

- Legen Sie die **Benutzerrolle** auf **Keine** fest.
- Setzen Sie die **LAN-Berechtigungsstufe** auf **Kein Zugriff**.
- Setzen Sie die **Berechtigungsstufe für die serielle Schnittstelle** auf **Kein Zugriff**.
- Setzen Sie **Seriell über LAN** auf **Deaktiviert**.

## Neues Image für Streamvault-Appliance festlegen

Um ein neues Image für eine Streamvault™-Appliance festzulegen, benötigen Sie das zugehörige Microsoft [Certificate of Authenticity \(Echtheitszertifikat, COA\)](#), um zu bestimmen, welches Image mit der Appliance verwendet werden kann. An jeder Streamvault-Appliance ist ein COA-Kennzeichen angebracht, das die Windows-Edition angibt, die auf der Appliance ausgeführt wird.

Eine Liste der Images, die basierend auf der jeweiligen Windows-Edition mit Ihrer Appliance kompatibel sind, finden Sie in den [Streamvault-Versionshinweisen](#). Verwenden Sie Ihr Software-Image nicht, wenn auf Ihrer Appliance eine andere Windows-Edition als in den Versionshinweisen angegeben ausgeführt wird.

Das folgende Beispiel zeigt ein typisches COA-Etikett mit Windows-Edition und Zertifikatsinformationen. Produkte, die eingebettete Version von Microsoft-Software enthalten, haben ein COA-Etikett.



**BEMERKUNG:** Jedes Streamvault-Image arbeitet mit der jeweiligen Security-Center-Version, wie in den [Streamvault-Versionshinweisen](#) angegeben. Für ein Downgrade von Security Center auf eine frühere Version muss unter Umständen die Härtingsebene der Appliance reduziert werden.

Eine Übersicht über die Produktverfügbarkeit, den Support und verfügbare Services finden Sie auf der [Seite Product Lifecycle im GTAP](#).

# Die System-ID und Image-Version einer Streamvault™ Appliance finden

---

Wenn Sie das Genetec™ Technical Assistance Center (GTAC) kontaktieren, benötigen Sie die System-ID und die Image-Version der Genetec-Software, die auf der Appliance installiert ist.

## Bevor Sie beginnen

Melden Sie sich bei Windows als Administrator an.

## Was Sie noch wissen sollten

Zusätzlich zur System-ID und Image-Version fordert der GTAC möglicherweise auch die Zertifizierungsnummer und die Seriennummer an. Diese Informationen finden Sie auf einem Etikett auf der Streamvault-Appliance.

## Prozedur

- 1 Öffnen Sie über den Windows-Desktop **Genetec™ SV Control Panel**.
- 2 Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für den Admin-Benutzer ein.
- 3 Klicken Sie auf **Info**.
- 4 Im Abschnitt *System* finden Sie die **System-ID** und die **Image-Version**.

## Verwandte Themen

[Eine Zurücksetzung auf Werkseinstellungen auf einer Streamvault All-in-One-Appliance durchführen](#) auf Seite 93

[Eine Zurücksetzung auf die Werkseinstellungen auf einer Streamvault-Workstation oder Server-Appliance durchführen](#) auf Seite 104

# Dateifreigabe auf einer Streamvault-Appliance erlauben

---

Um Dateien und Ordner mit Menschen in Ihrem Netzwerk zu teilen, müssen Sie die Dateifreigabe im SV Control Panel aktivieren.

## Bevor Sie beginnen

Melden Sie sich auf der Appliance als Admin-Benutzer bei Windows an.

## Was Sie noch wissen sollten

- Für maximale Sicherheit ist die Dateifreigabe standardmäßig deaktiviert.
- Die Remote-Computer und Ihre Appliance müssen mit dem gleichen IP-Netzwerk verbunden sein.

## Prozedur

- 1 Aktivieren Sie auf der Seite *Sicherheit* des SV Control Panels die Option **Datei-Sharing Service**.
- 2 Klicken Sie auf **Übernehmen**.
- 3 Um einen Ordner oder eine Datei mit jemandem zu teilen, klicken Sie mit der rechten Maustaste auf einen Ordner oder eine Datei im Windows Datei-Explorer und klicken Sie auf **Teilen**.

# Remotedesktop-Verbindungen auf einer Streamvault™-Appliance erlauben

---

Damit Sie eine Appliance über einen Computer oder einen virtuellen Computer im Netzwerk steuern könne, müssen Sie zunächst Remote-Zugriff auf der Appliance aktivieren.

## Bevor Sie beginnen

Melden Sie sich auf der Appliance als Admin-Benutzer bei Windows an.

## Was Sie noch wissen sollten

- Für maximale Sicherheit ist Remote-Zugriff standardmäßig deaktiviert.
- Die Appliance und der Remote-Computer müssen mit dem gleichen Netzwerk verbunden sein.

## Prozedur

- 1 Aktivieren Sie auf der Seite *Sicherheit* des SV Control Panels die Option **Remote Desktop Service**.
- 2 Klicken Sie auf **Übernehmen**.

## Verwandte Themen

[Remotedesktop kann sich nicht mit einer Streamvault-Appliance verbinden](#) auf Seite 113

# Problembehandlung

Dieser Abschnitt enthält die folgenden Themen:

- ["Eine Zurücksetzung auf Werkseinstellungen auf einer Streamvault All-in-One-Appliance durchführen" auf Seite 93](#)
- ["Eine Zurücksetzung auf die Werkseinstellungen auf einer Streamvault-Workstation oder Server-Appliance durchführen" auf Seite 104](#)
- ["Mercury-EP-Steuerungen bleiben offline, wenn TLS 1.1 deaktiviert ist." auf Seite 109](#)
- ["Transport Layer Security \(TLS\) aktivieren" auf Seite 110](#)
- ["Remotedesktop kann sich nicht mit einer Streamvault-Appliance verbinden" auf Seite 113](#)
- ["Aufhebung der Beschränkungen für Benutzerkonten von Nicht-Administratoren" auf Seite 117](#)
- ["Lokale Konten können nicht auf Remote Desktop, Datei-Sharing Service und Remote Management zugreifen" auf Seite 118](#)
- ["Ermöglichung von Smart Card-bezogenen Diensten" auf Seite 119](#)
- ["Support für Mercury EP- und LP-Firmware-Controller 1.x.x aktivieren" auf Seite 120](#)
- ["Support für die Synergis IX-Integration aktivieren" auf Seite 122](#)
- ["Ändern lokaler Gruppenrichtlinienobjekte für Benutzerkonten von Nicht-Administratoren" auf Seite 123](#)
- ["Windows-Firewall deaktivieren" auf Seite 126](#)

# Eine Zurücksetzung auf Werkseinstellungen auf einer Streamvault All-in-One-Appliance durchführen

Wenn die Software einer Streamvault™ All-in-One-Appliance nicht startet oder nicht wie erwartet funktioniert, können Sie die Appliance mithilfe eines USB-Speichers auf Werkseinstellungen zurücksetzen.

## Bevor Sie beginnen

- [Ihre Directly-Datenbank im SV Control Panel sichern](#)
- Haben Sie die richtige Lizenz für die Version für Security Center, die Sie wiederherstellen oder installieren möchten.
- Haben Sie die System-ID und das Passwort, das Ihnen per E-Mail beim Kauf der Appliance gesendet wurde. Siehe [Die System-ID und Image-Version einer Streamvault™ Appliance finden](#) auf Seite 89.
- (Empfohlen) Verbinden Sie Ihre Appliance mit dem Internet mithilfe einer Ethernet-Verbindung, sodass das System die Verbindung bestätigen kann.  
**BEMERKUNG:** Die Validierung schlägt fehl, wenn keine Internetverbindung vorhanden ist, aber Sie können Ihre Appliance weiterhin verwenden.

## Was Sie noch wissen sollten

Eine Zurücksetzung auf die Werkseinstellungen löscht und überschreibt alle Daten, die sich aktuell auf dem Windows-Laufwerk (C:) befinden, einschließlich Datenbanken und Protokolle. Videodateien auf anderen Datenträgern sind davon nicht betroffen.

## Prozedur

- 1 [Erstellen Sie einen USB-Schlüssel zum Zurücksetzen auf die Werkseinstellungen, der das Software-Image enthält.](#)
- 2 [Setzen Sie mithilfe des USB-Schlüssels das Image auf Ihrer Appliance zurück.](#)

## Nach Durchführen dieser Schritte

[Konfigurieren Sie Ihre Appliance neu.](#)

## Verwandte Themen

[Die System-ID und Image-Version einer Streamvault™ Appliance finden](#) auf Seite 89

## USB-Speicher für eine Streamvault™ All-in-One-Appliance zum Zurücksetzen auf Werkseinstellungen erstellen

Bevor Sie das Image einer Streamvault™ All-in-One-Appliance zurücksetzen können, müssen Sie einen bootfähigen USB-Speicher vorbereiten, der das erforderliche Streamvault™-Software-Image enthält.

## Bevor Sie beginnen

- Sie benötigen einen USB-Schlüssel mit mindestens 32 GB an Speicher. Einige USB-Schlüssel können das Image nicht booten. Wenn dies der Fall ist, versuchen Sie eine andere Marke oder ein anderes Modell.  
**ACHTUNG:** Alle Daten auf dem USB-Schlüssel werden gelöscht, wenn Sie ein bootfähiges Laufwerk erstellen.

## Prozedur

- 1 Wenden Sie sich an das [Genetec™ Technical Assistance Center \(GTAC\)](#), um das Image zur Wiederherstellung zu erhalten.

Das Image zur Wiederherstellung liegt in einem der folgenden drei Formate vor:

- eine *.zip* Datei, die *.swm-Dateien* enthält,
- eine *.iso* Datei, die die *.swm-Dateien* und die *Benutzeroberfläche des Streamvault™-Hilfsprogramms für Werksreset* enthält, mit der Sie das Software-Image zurücksetzen,
- eine *.iso* Datei, die den *Windows Setup-Assistenten* enthält, mit dem Sie das Software-Image zurücksetzen.

- 2 Wenn es sich bei Ihrem Image zur Wiederherstellung um eine *.zip*-Datei handelt, entpacken Sie den Inhalt in einen beliebigen Windows-Ordner.

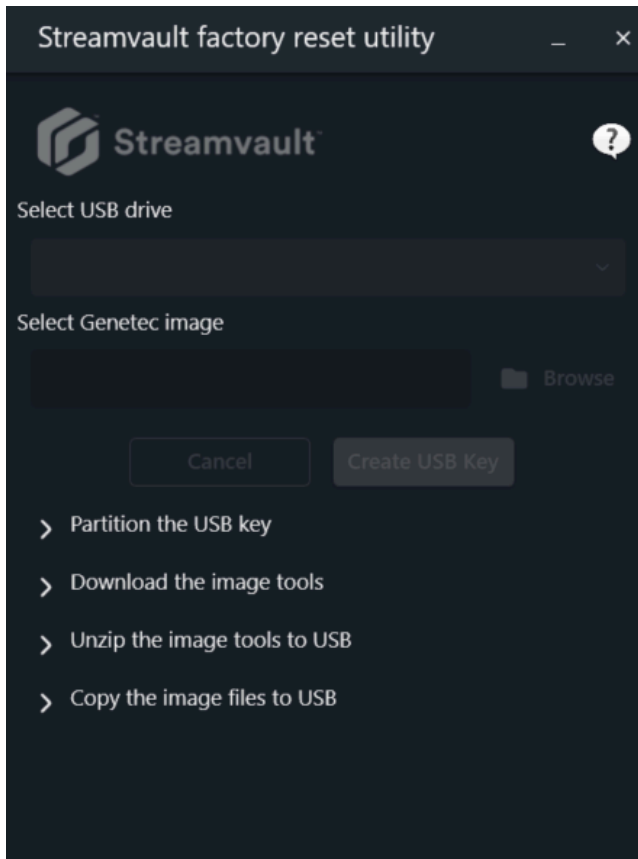
- 3 Laden Sie auf der Seite [Product Download](#) im GTAP den USB Creator für das *Streamvault™-Hilfsprogramm für Werksreset* herunter.

- a) Wählen Sie in der Liste *Download Finder* Ihre Version von Security Center aus.
- b) Laden Sie in der Liste *Andere* das Paket *Streamvault™-Hilfsprogramm für Werksreset* herunter.

|   |   |
|---|---|
| <b>Other</b>  |   |
| Genetec Video Player  |  |
| Streamvault All-in-One image for Windows 11 LTSC (SHA1: D399117267BDC481D70E5A713711C1F4DB6C7A7D) |  |
| Streamvault Control Panel 3.1.0   |  |
| <b>Streamvault Factory Reset Utility</b>  |  |

- 4 Schließen Sie den USB-Speicher an einen USB-Anschluss an.
- 5 Öffnen Sie den USB Creator für das *Streamvault™-Hilfsprogramm für Werksreset*, der Sie aus dem TechDoc Hub heruntergeladen haben.

- 6 Wählen Sie in der Liste **USB-Laufwerk** einen USB-Schlüssel aus, der über mindestens 32 GB an Speicher verfügt.



- 7 Klicken Sie im Abschnitt *Genetec-Image auswählen* auf **Durchsuchen** und wählen Sie die heruntergeladene *.swm*- oder *.iso*-Datei aus.

**BEMERKUNG:** Wenn Sie eine *.swm*-Datei benötigen, wählen Sie eine der entpackten Dateien aus dem *wim*-Ordner aus. Alle *.swm*-Dateien in diesem Ordner werden auf den USB-Schlüssel kopiert.

- 8 Klicken Sie auf **USB-Schlüssel erstellen**.

Das *Streamvault™-Hilfsprogramm für Werksreset* beginnt die Partitionierung des USB-Schlüssels, lädt die Image-Tools herunter und kopiert die Image-Dateien.

Wenn der Download abgeschlossen ist, wird die folgende Meldung angezeigt: Der USB-Speicher wurde erfolgreich erstellt.

Das folgende Video zeigt, wie Sie einen USB-Schlüssel zum Zurücksetzen auf die Werkseinstellungen mit einer *.iso* Datei erstellen.



## Nach Durchführen dieser Schritte

Setzen Sie das Software-Image Ihrer Streamvault All-in-One-Appliance zurück.

## Zurücksetzen des Software-Images auf einer All-in-One-Appliance

Nachdem Sie einen bootfähigen USB-Speicher mit dem erforderlichen Streamvault™-Software-Image vorbereitet haben, können Sie ihn zum Zurücksetzen des Software-Images auf einer Streamvault™ All-In-One-Appliance verwenden.

## Bevor Sie beginnen

- Stellen Sie sicher, dass Sie über den USB-Schlüssel verfügen, der die Wiederherstellungssoftware für Ihre Appliance enthält.

## Was Sie noch wissen sollten

- Das Zurücksetzen dauert ungefähr 20 bis 30 Minuten. In dieser Zeit werden mehrere Skripte ausgeführt und die Appliance wird mehrmals neu gestartet.
- Unterbrechen Sie den Zurücksetzungsvorgang nicht. Das manuelle Ausschalten oder Herunterfahren der Appliance kann die Wiederherstellung unterbrechen.

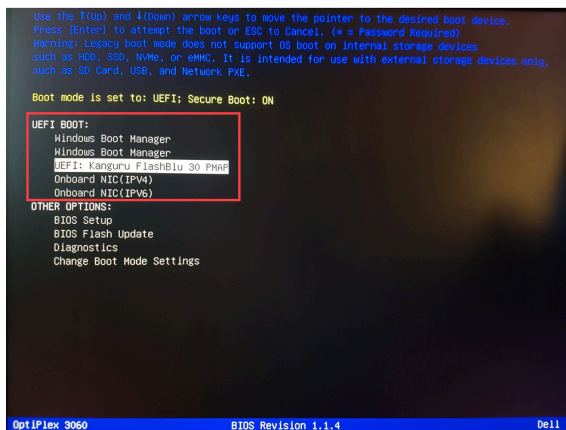
## Prozedur

### So setzen Sie das Software-Image zurück:

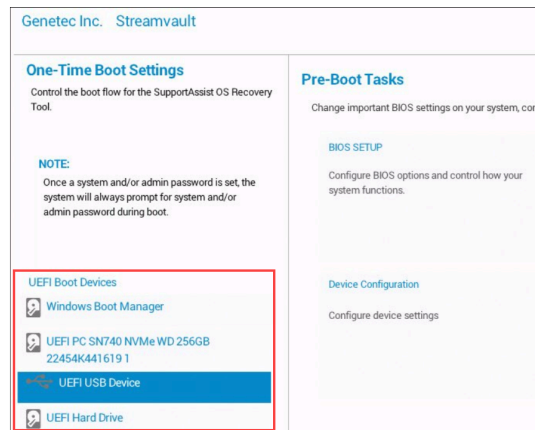
- 1 Schalten Sie die Appliance aus.
- 2 Schließen Sie den von Ihnen erstellten USB-Schlüssel an einen USB-Anschluss an.
- 3 Schalten Sie die SV-Appliance ein und drücken Sie wiederholt F12, bis das Startmenü erscheint. Abhängig von Ihrer Appliance wird entweder das UEFI-Startmenü oder das Streamvault™-Menü für einmaligen Start geöffnet.

- 4 Wählen Sie das USB-Laufwerk aus und drücken Sie die Eingabetaste.

**BEMERKUNG:** Das Erscheinungsbild des Startmenüs kann abweichen.



UEFI Boot menu



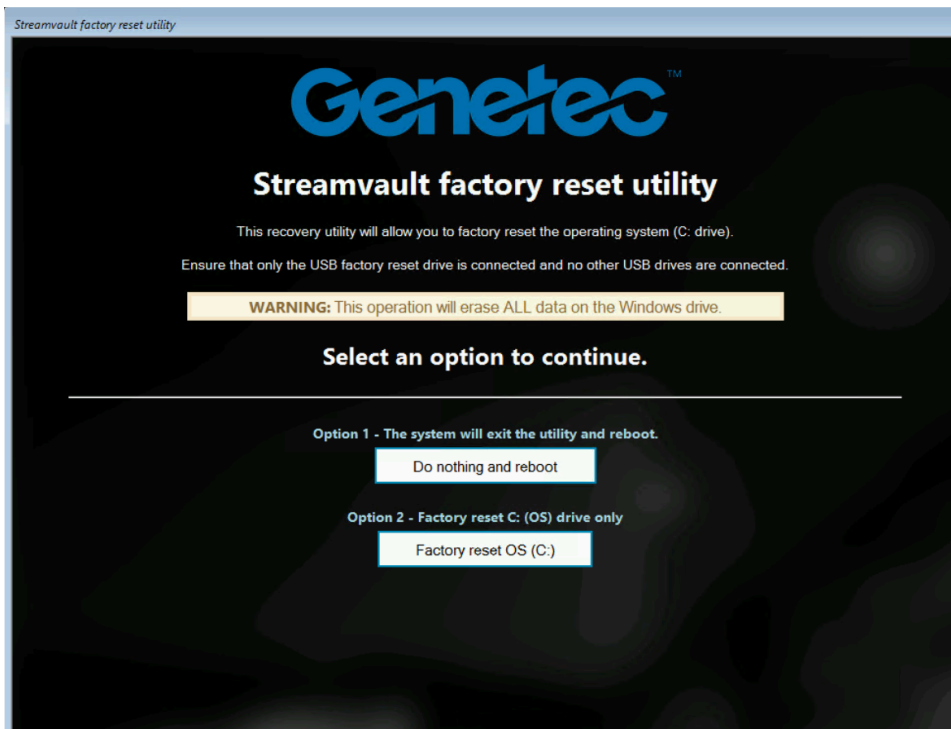
Streamvault One-time Boot menu

Je nach Software-Image wird entweder das *Streamvault™-Hilfsprogramm für Werksreset* oder der *Windows Setup-Assistent* geöffnet.

- 5 Setzen Sie das Software-Image mit dem Tool zurück, das auf Ihrer Appliance vorhanden ist:
  - *Streamvault™-Hilfsprogramm für Werksreset*
  - *Windows-Setup-Assistent*

### So setzen Sie das Software-Image mit dem Streamvault™-Hilfsprogramm für Werksreset zurück:

- 1 Wenn der USB-Speicher im Wiederherstellungsmodus startet, wählen Sie **Betriebssystem (C:) auf Werkseinstellungen zurücksetzen**, um das Systemlaufwerk der Appliance zu formatieren und erneut zu installieren.



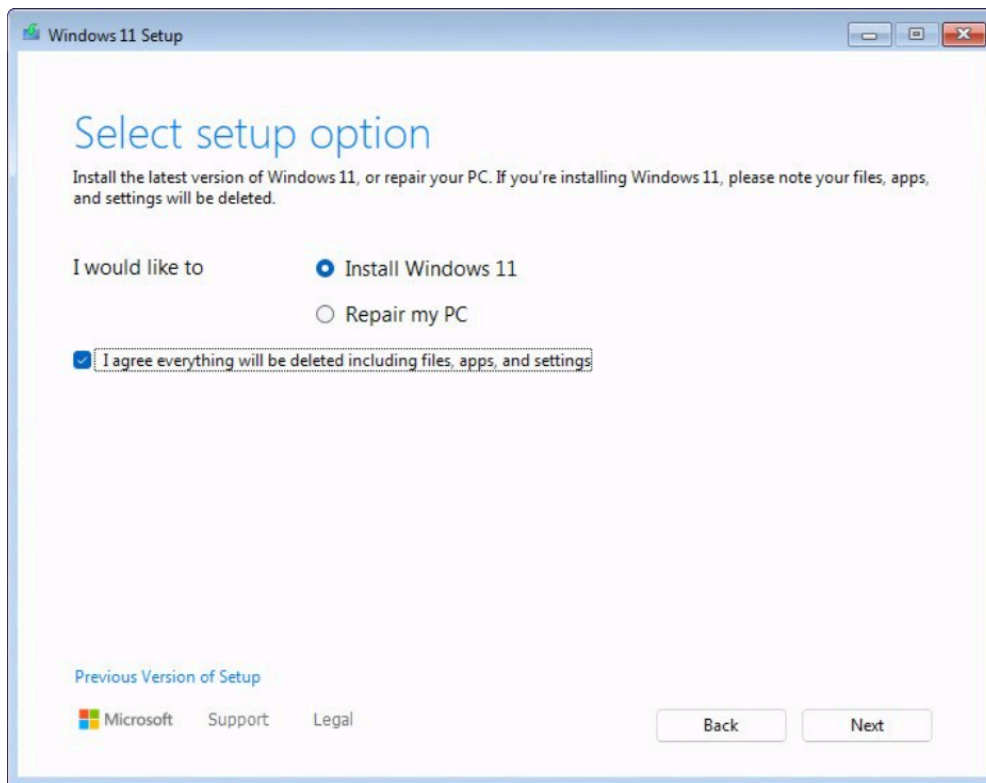
- 2 Wenn Sie dazu aufgefordert werden, tippen Sie Yes und drücken Sie die Eingabetaste. Warten Sie, bis das Zurücksetzen auf Werkseinstellungen abgeschlossen ist.
- 3 Wenn das Zurücksetzen auf die Werkseinstellungen abgeschlossen ist, entfernen Sie den USB-Schlüssel aus der Appliance und drücken Sie die Eingabetaste, um einen Neustart durchzuführen.
- 4 Geben Sie im Dialogfeld *Genetec™ Product Validator* die Teilenummer (Produktnummer) der Appliance und die Genetec™-Seriennummer ein.  
Diese Nummern befinden sich auf dem Genetec-Etikett, das oben auf der Appliance angebracht ist. Wenn es kein Etikett gibt, können Sie einen beliebigen Text zum Fortfahren eingeben.  
Die **Start**-Taste wird angezeigt
- 5 Klicken Sie auf **Start**.  
Eine der folgenden Statusmeldungen wird angezeigt:
  - **BESTANDEN:** Der Vorgang war erfolgreich. Fahren Sie mit dem nächsten Schritt fort.
  - **FEHLGESCHLAGEN – Keine Übertragung:** Der Vorgang war erfolgreich; zu diesem Zeitpunkt bestand jedoch keine Internetverbindung. Fahren Sie mit dem nächsten Schritt fort.
  - **FEHLGESCHLAGEN:** Der Vorgang war nicht erfolgreich. Kontaktieren Sie das [Genetec™ Technical Assistance Center \(GTAC\)](#).
- 6 Wenn Sie eine Meldung **BESTANDEN** oder **BESTANDEN – Keine Übertragung** erhalten, schließen Sie das Fenster *Genetec™ Product Validator*.
- 7 Warten Sie darauf, dass das Hintergrundskript geschlossen wird, und starten Sie die Appliance neu.

### So setzen Sie das Software-Image mithilfe des Windows-Setup-Assistenten zurück:

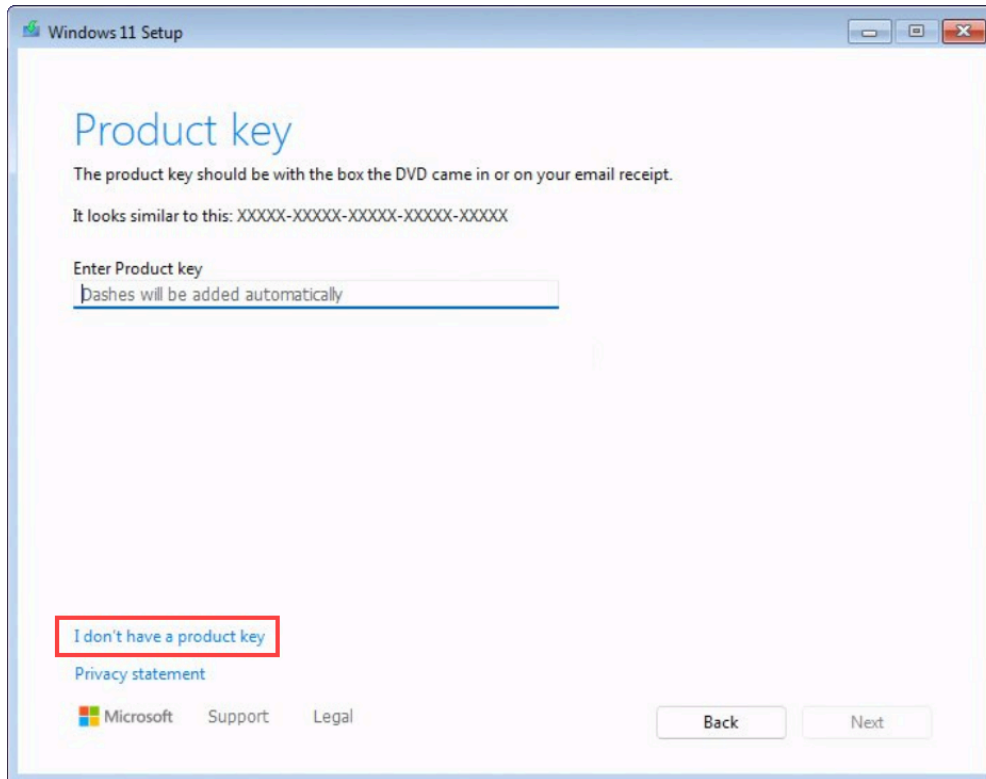
- 1 Wählen Sie auf dem Bildschirm *Spracheinstellungen auswählen* Ihre bevorzugten Sprach- und Zeiteinstellungen aus, und klicken Sie auf **Weiter**.
- 2 Wählen Sie auf dem Bildschirm *Tastatureinstellungen auswählen* Ihre bevorzugte Tastatur aus, und klicken Sie auf **Weiter**.

- 3 Wählen Sie auf dem Bildschirm *Setup-Option auswählen* die Option **Windows X installieren** aus, wobei X für die Windows-Version steht, die Sie installieren. Bestätigen Sie, dass Ihre Dateien, Apps und Einstellungen gelöscht werden, und klicken Sie auf **Weiter**.

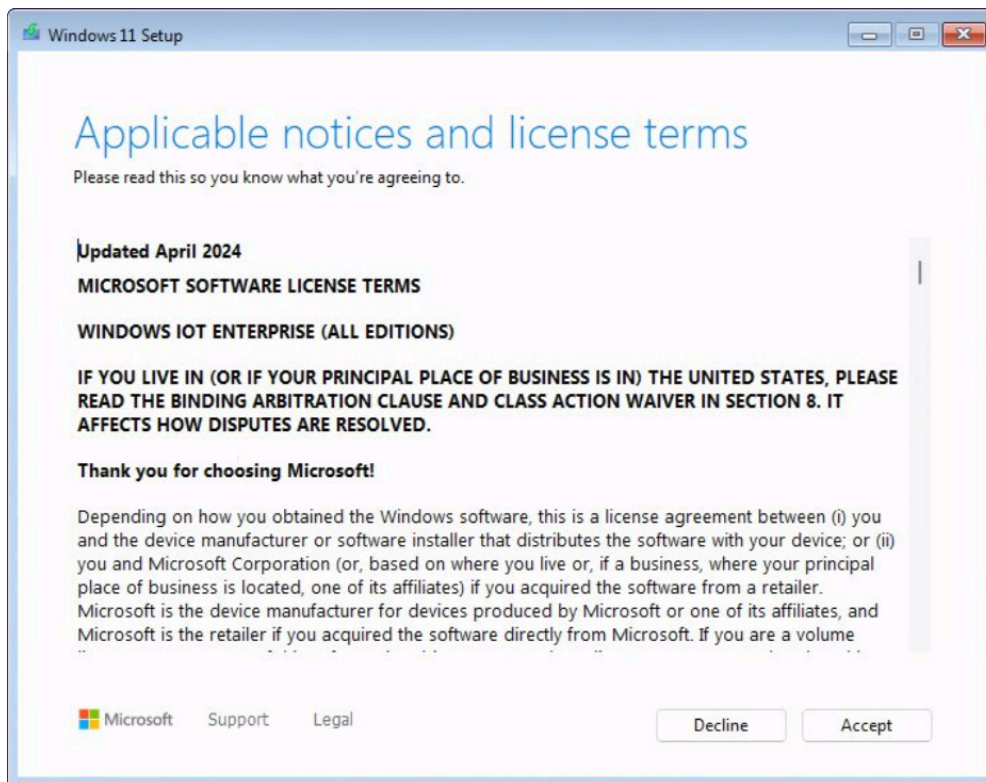
**BEMERKUNG:** Die auf dem sekundären Videodatenträger gespeicherten Videoarchive sind davon nicht betroffen. Es werden nur die Dateien auf dem Datenträger des Betriebssystems gelöscht.



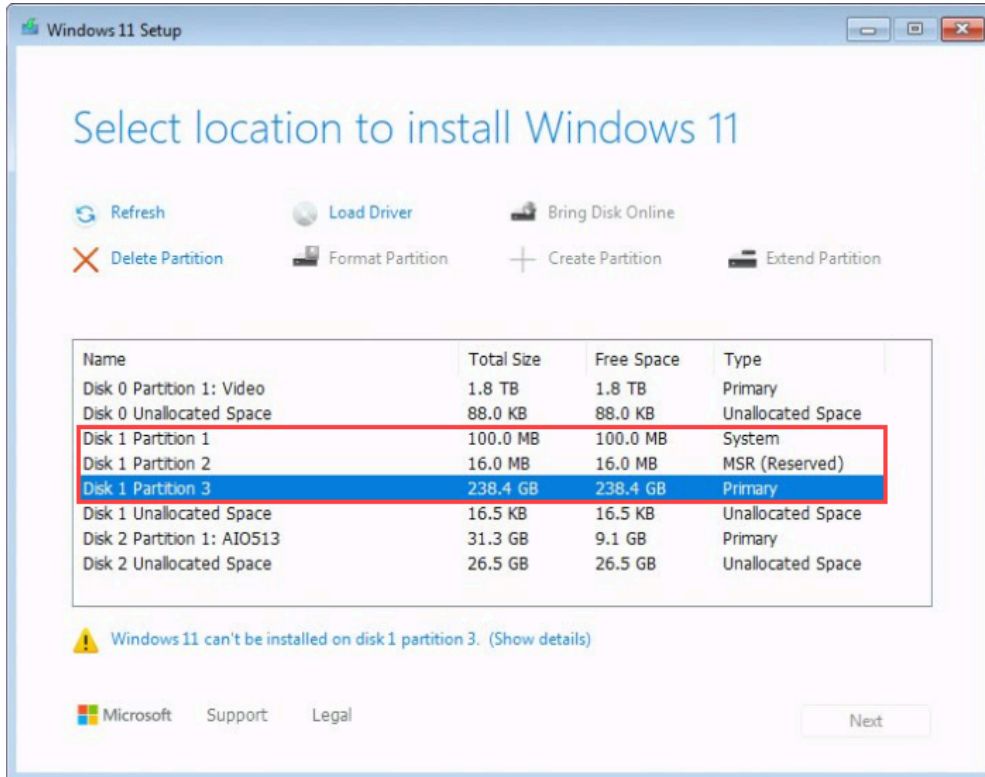
- 4 Führen Sie auf dem Bildschirm *Produktschlüssel* eine der folgenden Optionen aus:
- Wenn die Appliance mit dem Internet verbunden ist, klicken Sie auf **Ich habe keinen Produktschlüssel**, um fortzufahren. Die Appliance ruft ihre Aktivierungsdaten automatisch von Microsoft ab.
  - Wenn die Appliance nicht mit dem Internet verbunden ist, geben Sie den Lizenzschlüssel ein, der sich auf dem Etikett des [Echtheitszertifikats](#) auf Ihrer Appliance befindet, und klicken Sie auf **Weiter**.



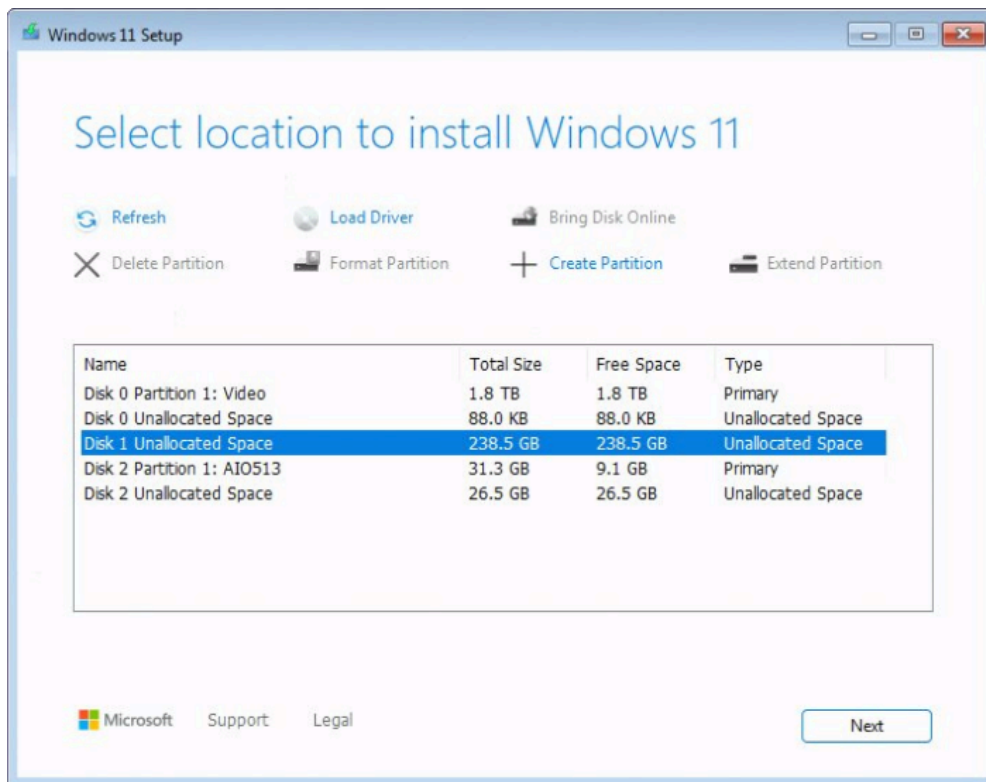
- 5 Lesen Sie auf dem Bildschirm *Anwendbare Hinweise und Lizenzbedingungen* die Lizenzbedingungen und klicken Sie auf **Akzeptieren**.



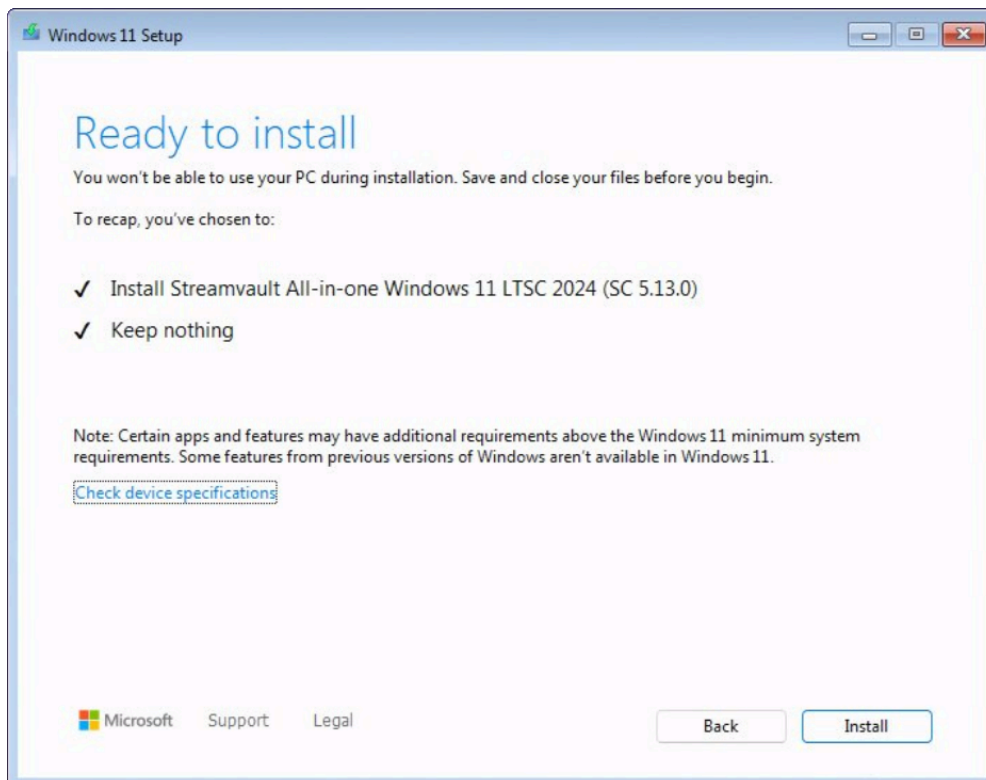
- 6 Löschen Sie auf dem Bildschirm *Speicherort für die Installation von Windows X auswählen* die primären Partitionen, die Systempartition und die MSR-Partition (falls zutreffend) auf dem Betriebssystemlaufwerk. Auf dem Betriebssystemlaufwerk verbleibt nur nicht zugewiesener Speicherplatz, und der Windows-Setup-Assistent erstellt die gelöschten Partitionen während des Installationsvorgangs automatisch neu.
- ACHTUNG:** Die primäre Partition auf dem Betriebssystemdatenträger ist in der Regel kleiner als 1 TB. Löschen Sie nicht die primäre Partition auf dem Videospeicherdatenträger, auf der Ihre Videoarchive gespeichert sind.



- 7 Wählen Sie den nicht zugewiesenen Speicherplatz auf dem Betriebssystemlaufwerk aus und klicken Sie auf **Weiter**.



- 8 Klicken Sie auf dem Bildschirm *Bereit zum Installieren* auf **Installieren**.



- 9 Wenn die Installation abgeschlossen ist, startet das System mit Windows neu und ein Skript wird automatisch ausgeführt, um die Installation abzuschließen. Wenn die Ausführung des Skripts beendet ist, starten Sie die Appliance neu.

Sehen Sie sich dieses Video an, um zu erfahren, wie Sie das Software-Image auf einer All-in-One-Appliance mithilfe eines bootfähigen USB-Speichers mit .swm-Dateien zurücksetzen.



### Nach Durchführen dieser Schritte

- Melden Sie sich bei Windows mit dem Standardbenutzernamen und dem Passwort an, die sich auf einem Sticker auf der Appliance befinden.
- [Aktivieren Sie Ihre Security Center-Lizenz.](#)
- Wenn Sie Security Center-Konfigurationen vor dem Zurücksetzen auf die Werkseinstellungen gesichert haben, [stellen Sie die Konfiguration mithilfe des SV Control Panel wieder her.](#)
- [Konfigurieren Sie Ihre Appliance neu.](#)

# Eine Zurücksetzung auf die Werkseinstellungen auf einer Streamvault-Workstation oder Server-Appliance durchführen

Wenn die Software auf Ihrem Streamvault™-Server oder Ihrer -Workstation nicht startet oder nicht wie erwartet funktioniert, können Sie die Appliance auf die Werkseinstellungen mithilfe eines USB-Schlüssels zurücksetzen.

## Bevor Sie beginnen

- Sichern Sie alle Security-Center-Konfigurationen mithilfe von SV Control Panel. Weitere Informationen, siehe [Ihre Directory-Datenbank sichern](#) auf Seite 37.
- Sie benötigen einen USB-Schlüssel mit mindestens 32 GB an Speicher. Einige USB-Schlüssel können das Image nicht booten. Wenn dies der Fall ist, versuchen Sie eine andere Marke oder ein anderes Modell.  
**ACHTUNG:** Alle Daten auf dem USB-Schlüssel werden gelöscht, wenn Sie ein bootfähiges Laufwerk erstellen.
- Haben Sie die richtige Lizenz für die Version für Security Center, die Sie wiederherstellen oder installieren möchten.
- Haben Sie die System-ID und das Passwort, das Ihnen per E-Mail beim Kauf der Appliance gesendet wurde.

## Was Sie noch wissen sollten

- **Gilt für:** Alle Modelle, die mit SVW, SVR und SVA beginnen und alle Server mit den Modellnummern SV-1000E und höher.
- Sehen Sie für All-in-One-Appliances unter [Eine Zurücksetzung auf Werkseinstellungen auf einer Streamvault All-in-One-Appliance durchführen](#) auf Seite 93 nach.
- Eine Zurücksetzung auf die Werkseinstellungen löscht alle Daten, die sich auf dem Systemlaufwerk befindet, hat aber keinen Einfluss auf die Standard-Werks-RAID-Laufwerkeinstellungen.
- Das Zurücksetzen schlägt möglicherweise fehl, wenn die Standardwerkseinstellungen von Festplatten, RAID-Laufwerken oder Partitionen auf der Appliance geändert wurden. Kontaktieren Sie in solchen Fällen das [Genetec™ Technical Assistance Center \(GTAC\)](#).

## Prozedur

- 1 Erstellen Sie einen USB-Schlüssel für eine Zurücksetzung auf die Werkseinstellungen.
- 2 Setzen Sie mithilfe des USB-Schlüssels das Image auf Ihrer Appliance zurück.

## Nach Durchführen dieser Schritte

[Richten Sie Ihre Appliance ein.](#)

## Verwandte Themen

[Die System-ID und Image-Version einer Streamvault™ Appliance finden](#) auf Seite 89

## Einen USB-Speicher zum Zurücksetzen auf Werkseinstellungen für eine Streamvault™-Workstation oder -Server-Appliance erstellen

Bevor Sie das Image einer Streamvault™-Workstation oder -Server-Appliance zurücksetzen können, müssen Sie einen bootfähigen USB-Speicher vorbereiten, der das erforderliche Streamvault-Software-Image enthält.

## Bevor Sie beginnen

Sie benötigen einen USB-Schlüssel mit mindestens 32 GB an Speicher. Einige USB-Schlüssel können das Image nicht booten. Wenn dies der Fall ist, versuchen Sie eine andere Marke oder ein anderes Modell.

**ACHTUNG:** Alle Daten auf dem USB-Schlüssel werden gelöscht, wenn Sie ein bootfähiges Laufwerk erstellen.

## Prozedur

- 1 Wenden Sie sich an das [Genetec™ Technical Assistance Center \(GTAC\)](#), um das Image zur Wiederherstellung zu erhalten.





Das Image zur Wiederherstellung liegt in einem der folgenden drei Formate vor:

- eine *.zip* Datei, die *.swm-Dateien* enthält,
- eine *.iso* Datei, die die *.swm-Dateien* und die *Benutzeroberfläche des Streamvault™-Hilfsprogramms für Werksreset* enthält, mit der Sie das Software-Image zurücksetzen,
- eine *.iso* Datei, die den *Windows Setup-Assistenten* enthält, mit dem Sie das Software-Image zurücksetzen.

- 2 Wenn es sich bei Ihrem Image zur Wiederherstellung um eine *.zip*-Datei handelt, entpacken Sie den Inhalt in einen beliebigen Windows-Ordner.

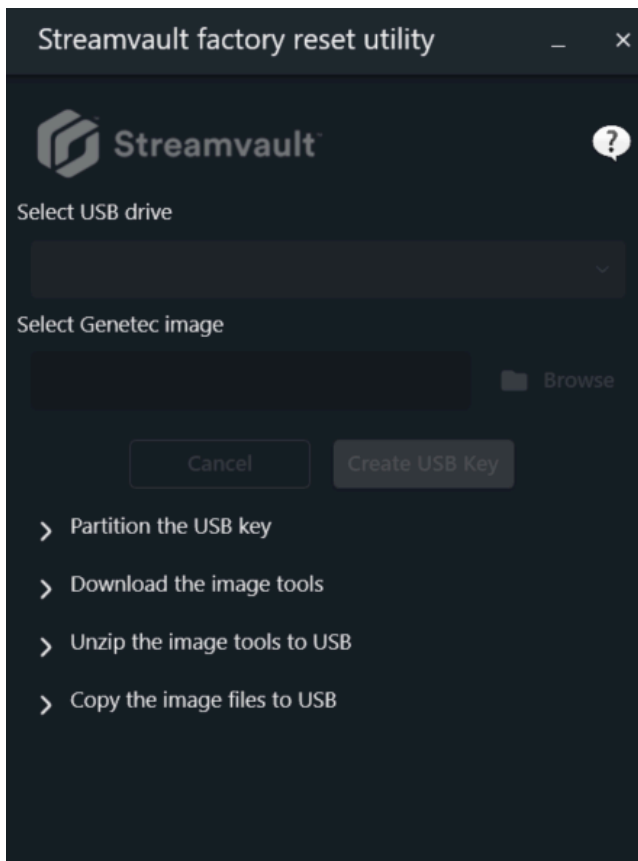
- 3 Laden Sie auf der Seite [Product Download](#) im GTAP den USB Creator für das *Streamvault™-Hilfsprogramm für Werksreset* herunter.

- a) Wählen Sie in der Liste *Download Finder* Ihre Version von Security Center aus.
- b) Laden Sie in der Liste *Andere* das Paket *Streamvault™-Hilfsprogramm für Werksreset* herunter.

| Other   |   |
|---|---|
| Genetec Video Player  |    |
| Streamvault All-in-One image for Windows 11 LTSC (SHA1: D399117267BDC481D70E5A713711C1F4DB6C7A7D) |   |
| Streamvault Control Panel 3.1.0   |  |
| Streamvault Factory Reset Utility   |  |

- 4 Schließen Sie den USB-Speicher an einen USB-Anschluss an.
- 5 Öffnen Sie den USB Creator für das *Streamvault™-Hilfsprogramm für Werksreset*.

- 6 Wählen Sie in der Liste **USB-Laufwerk** einen USB-Schlüssel aus, der über mindestens 32 GB an Speicher verfügt.



- 7 Klicken Sie im Abschnitt *Genetec-Image auswählen* auf **Durchsuchen** und wählen Sie die heruntergeladene *.swm*- oder *.iso*-Datei aus.

Wenn Sie eine *.swm*-Datei benötigen, wählen Sie das erforderliche Image im Ordner *<Service-Tag-Nummer>* aus.

- 8 Klicken Sie auf **USB-Schlüssel erstellen**.

Das *Streamvault™-Hilfsprogramm für Werksreset* beginnt die Partitionierung des USB-Schlüssels, lädt die Image-Tools herunter und kopiert die Image-Dateien.

Wenn der Download abgeschlossen ist, wird die folgende Meldung angezeigt: Der USB-Speicher wurde erfolgreich erstellt.

Das folgende Video zeigt, wie Sie einen USB-Schlüssel zum Zurücksetzen auf die Werkseinstellungen mit einer *.iso* Datei erstellen.



## Nach Durchführen dieser Schritte

Setzen Sie das Software-Image Ihrer Streamvault-Workstation oder -Server-Appliance zurück.

## Das Software-Image auf einer Streamvault-Workstation- oder Server-Appliance zurücksetzen

Nachdem Sie einen bootfähigen USB-Speicher mit dem erforderlichen Streamvault™-Software-Image vorbereitet haben, können Sie ihn zum Zurücksetzen des Software-Images auf einer Workstation oder Server-Appliance verwenden.

## Bevor Sie beginnen

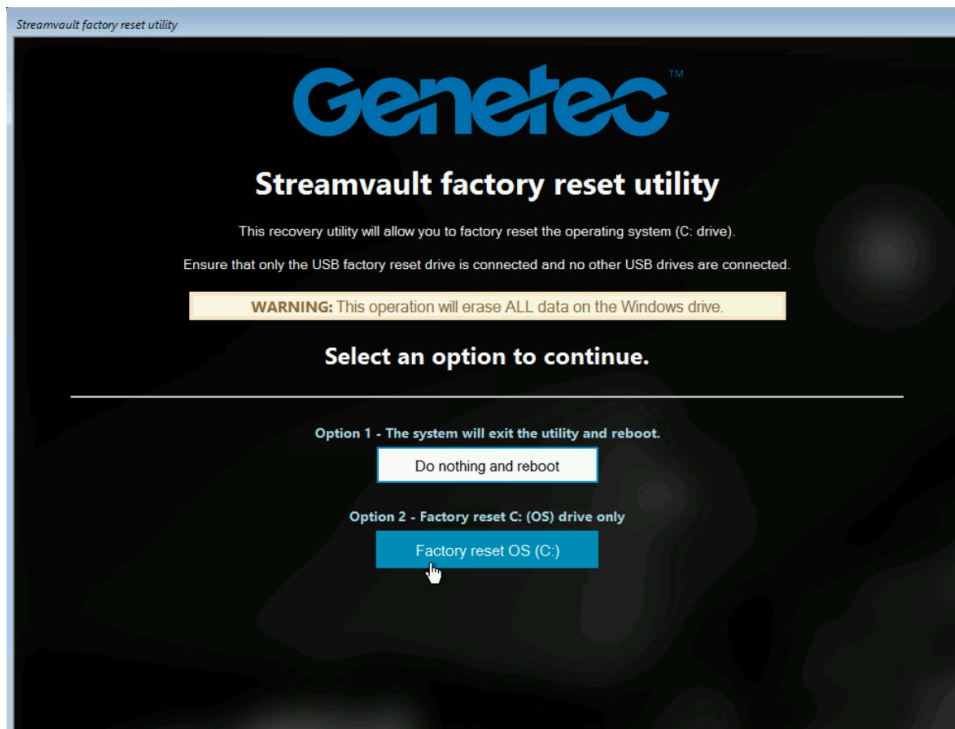
- Stellen Sie sicher, dass Sie über den USB-Schlüssel verfügen, der die Wiederherstellungssoftware für Ihre Appliance enthält.

## Was Sie noch wissen sollten

- Das Zurücksetzen beeinträchtigt nicht die standardmäßigen Werkseinstellungen des RAID-Laufwerks.
- Das Zurücksetzen schlägt möglicherweise fehl, wenn die Standardwerkseinstellungen von Festplatten, RAID-Laufwerken oder Partitionen auf der Appliance geändert wurden. Kontaktieren Sie in solchen Fällen das [Genetec™ Technical Assistance Center \(GTAC\)](#).

## Prozedur

- 1 Schalten Sie die Appliance aus.
- 2 Schließen Sie den von Ihnen erstellten bootfähigen USB-Schlüssel an einen USB-Anschluss an.
- 3 Schalten Sie die Streamvault-Appliance ein.
- 4 Wenn Sie dazu aufgefordert werden, drücken Sie F12.  
Der *Boot Manager* wird geöffnet. Klicken Sie auf das Menü **UEFI-Einmalstart**.
- 5 Wählen Sie Ihr USB-Laufwerk auf und drücken Sie dann Eingabe.  
Das *Streamvault™-Hilfsprogramm für Werksreset* wird geöffnet.
- 6 Klicken Sie auf **Betriebssystem (C:) auf die Werkseinstellungen zurücksetzen**.



Eine Eingabeaufforderung wird geöffnet, und das *Streamvault™-Hilfsprogramm für Werksreset* analysiert das System, um das Systemlaufwerk zu erkennen.

- 7 Geben Sie in der Eingabeaufforderung Yes ein, um zu bestätigen, dass die richtige Festplatte erkannt wurde, und drücken Sie dann die Eingabetaste, um das Zurücksetzen auf die Werkseinstellungen zu starten.

**WICHTIG:** Während des Re-Imaging-Vorgangs dürfen Sie die Workstation nicht unterbrechen, ausschalten oder neu starten. Dies kann bis zu 20 Minuten dauern, abhängig von der Geschwindigkeit Ihres USB-Schlüssels.

- 8 Wenn das Zurücksetzen auf die Werkseinstellungen abgeschlossen ist und Sie dazu aufgefordert werden, die Workstation neuzustarten, drücken Sie die Eingabetaste.
- 9 Entfernen Sie den USB-Schlüssel aus dem USB-Port.

Die Workstation wurde nun zum Standardzustand zurückgesetzt.

Sehen Sie sich dieses Video an, um zu erfahren, wie man ein Software-Image auf einer Streamvault-Workstation oder -Server-Appliance zurücksetzt.



### Nach Durchführen dieser Schritte

- Melden Sie sich bei Windows mit dem Standardbenutzernamen und dem Passwort an, die sich auf einem Sticker auf der Appliance befinden.
- [Aktivieren Sie Ihre Security Center-Lizenz.](#)
- Wenn Sie Security Center-Konfigurationen vor dem Zurücksetzen auf die Werkseinstellungen gesichert haben, [stellen Sie die Konfiguration mithilfe des SV Control Panel wieder her.](#)
- [Konfigurieren Sie Ihre Appliance neu.](#)

## Mercury-EP-Steuerungen bleiben offline, wenn TLS 1.1 deaktiviert ist.

---

Nachdem eine Mercury-EP-Steuerung in Security Center registriert wurde, geht die Einheit nicht wieder online.

Sie erhalten keine Fehler oder Warnungen zu diesem Fehler.

**Gilt für:**

- Streamvault™ SV-100E 16.3 und neuer
- Streamvault™ SV-300E 16.3 und neuer
- Streamvault™ SV-350E 16.3 und neuer

**Ursache**

Alle Mercury-EP-Steuerungen erfordern das TLS (Transport Layer Security)-Protokoll 1.1 für die Kommunikation mit Security Center. Das Protokoll ist jedoch auf Streamvault™-All-in-One-Appliances 16.3 und neuer deaktiviert.

**Lösung**

[Aktivieren Sie TLS 1.1.](#)

# Transport Layer Security (TLS) aktivieren

Die TLS (Transport Layer Security)-Protokolle 1.0 und 1.1 protocols haben schwerwiegende Sicherheitslücken, weshalb sie auf Streamvault™-Appliances deaktiviert sind. Wenn ein in Security Center registriertes Gerät eines dieser Protokolle zur Kommunikation benötigt, müssen Sie das Protokoll auf Ihrer Appliance aktivieren.

## Was Sie noch wissen sollten

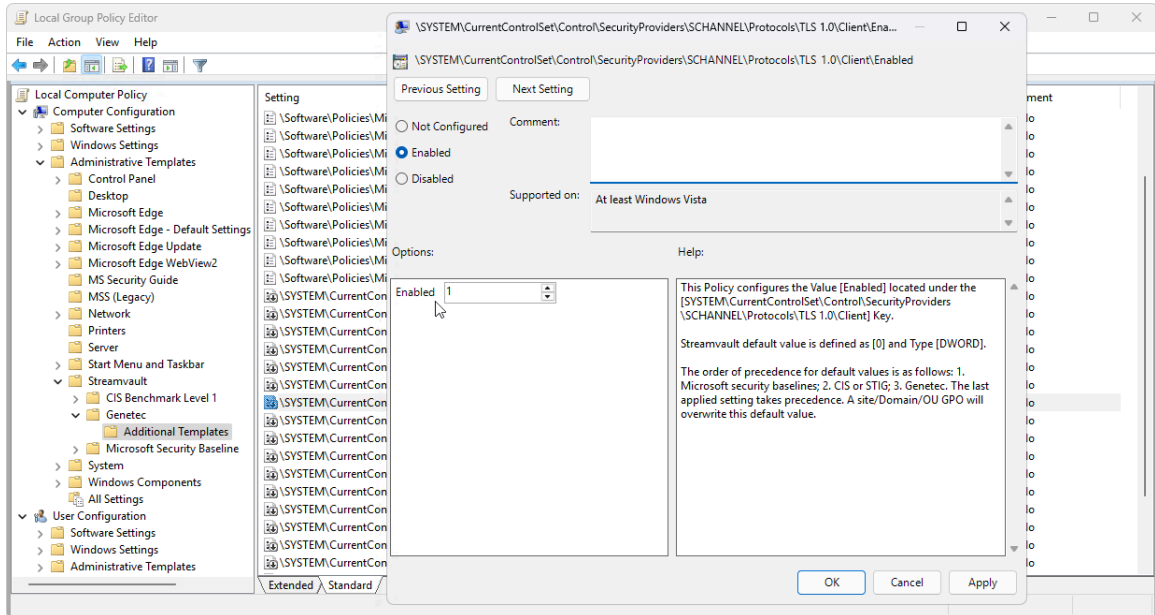
- TLS 1.1 ist im Streamvault-Software-Image 16.3 und neuer deaktiviert.
- TLS 1.0 ist im Streamvault-Software-Image 16.0 und neuer deaktiviert.
- Aktivieren Sie nur die Version von TLS, die Ihr Gerät erfordert.
- Aktivieren Sie TLS auf den Server- (eingehend) und Clientknoten (ausgehend).
- Aus Sicherheitsgründen sind die Optionen für Interneteigenschaften auf Appliances deaktiviert. Wenn Ihre Appliance über den Streamvault™-Service verfügt, können Sie Transport Layer Security über den Editor für lokale Gruppenrichtlinien aktivieren. Wenn Ihre Appliance nicht über den Streamvault™-Service verfügt, können Sie Transport Layer Security nur über den Windows-Registrierungseditor aktivieren.

## Prozedur

### So aktivieren Sie Transport Layer Security auf einer Appliance mit dem Streamvault™ Service:

- 1 Öffnen Sie die Eingabeaufforderung als Administrator und führen Sie `gpedit.msc` aus.  
Der Editor für lokale Gruppenrichtlinien wird geöffnet.
- 2 Öffnen Sie **Computerkonfiguration > Administrative Vorlagen > Streamvault™ > Genetec > Zusätzliche Vorlagen**.
- 3 Aktivieren Sie Transport Layer Security 1. *n* auf dem Client, wobei *n* die Nummer der Nebenversion darstellt:
  - a) Klicken Sie mit der rechten Maustaste auf `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Transport Layer Security 1.n\Client\Enabled`, und klicken Sie auf **Bearbeiten**.
  - b) Setzen Sie **Enabled** auf 1 und klicken Sie auf **Anwenden > OK**.
  - c) Klicken Sie mit der rechten Maustaste auf `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Transport Layer Security 1.n\Client\DisabledByDefault`, und klicken Sie auf **Bearbeiten**.
  - d) Setzen Sie **DisabledByDefault** auf 0, und klicken Sie auf **Anwenden > OK**.

- 4 Aktivieren Sie Transport Layer Security 1. *n* auf dem Server:
  - a) Klicken Sie mit der rechten Maustaste auf `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Transport Layer Security 1.n\Server\Enabled` und klicken Sie auf **Bearbeiten**.
  - b) Setzen Sie **Aktiviert** auf 1 und klicken Sie auf **Anwenden** > **OK**.
  - c) Klicken Sie mit der rechten Maustaste auf `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Transport Layer Security 1.n\Server\DisabledByDefault` und klicken Sie auf **Bearbeiten**.
  - d) Setzen Sie **DisabledByDefault** auf 0 und klicken Sie auf **Anwenden** > **OK**.



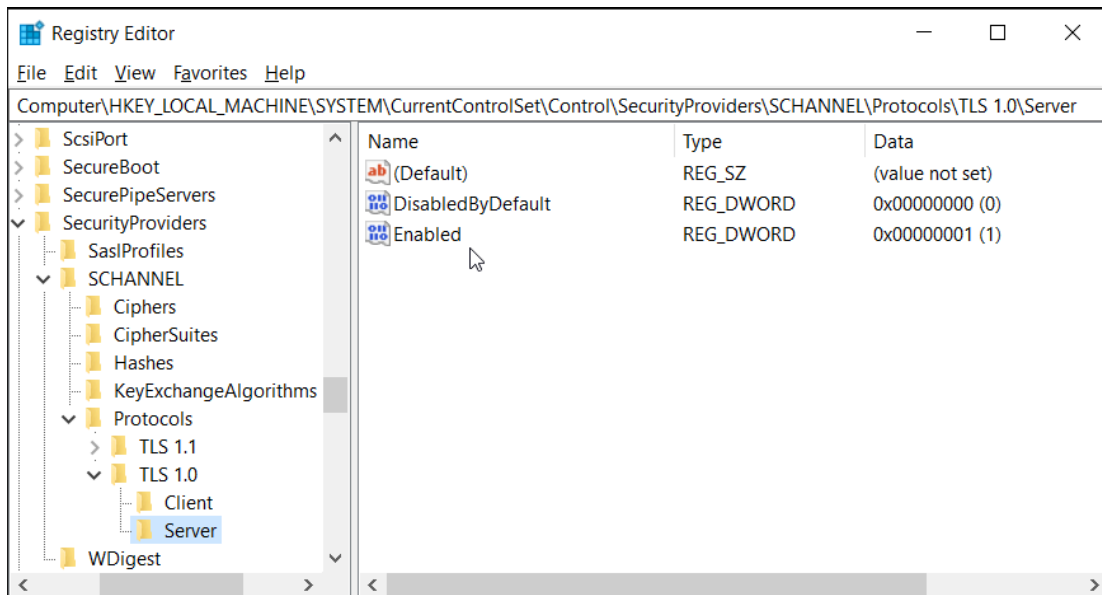
- 5 Starten Sie Windows neu.

## So aktivieren Sie Transport Layer Security auf einer Appliance ohne den Streamvault™ Service:

- 1 Öffnen Sie den Windows Registrierungseditor.

2 Aktivieren Sie TLS 1.*n*, wobei *n* für die Nebenversionsnummer steht:

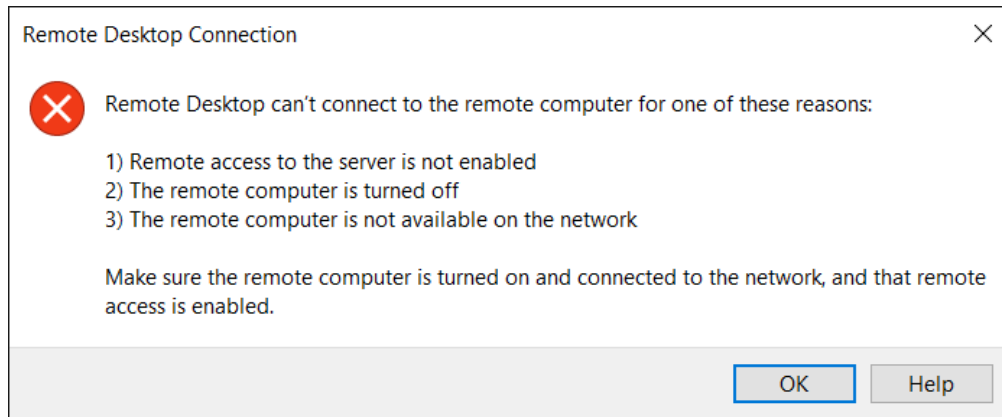
- a) Navigieren Sie zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n`.
- b) Wählen Sie den Knoten **Server** aus, legen Sie **DisabledByDefault** auf 0 und **Aktiviert** auf 1 fest.
- c) Wählen Sie den Knoten **Client** aus, legen Sie **DisabledByDefault** auf 0 und **Aktiviert** auf 1 fest.



3 Starten Sie Windows neu.

# Remotedesktop kann sich nicht mit einer Streamvault-Appliance verbinden

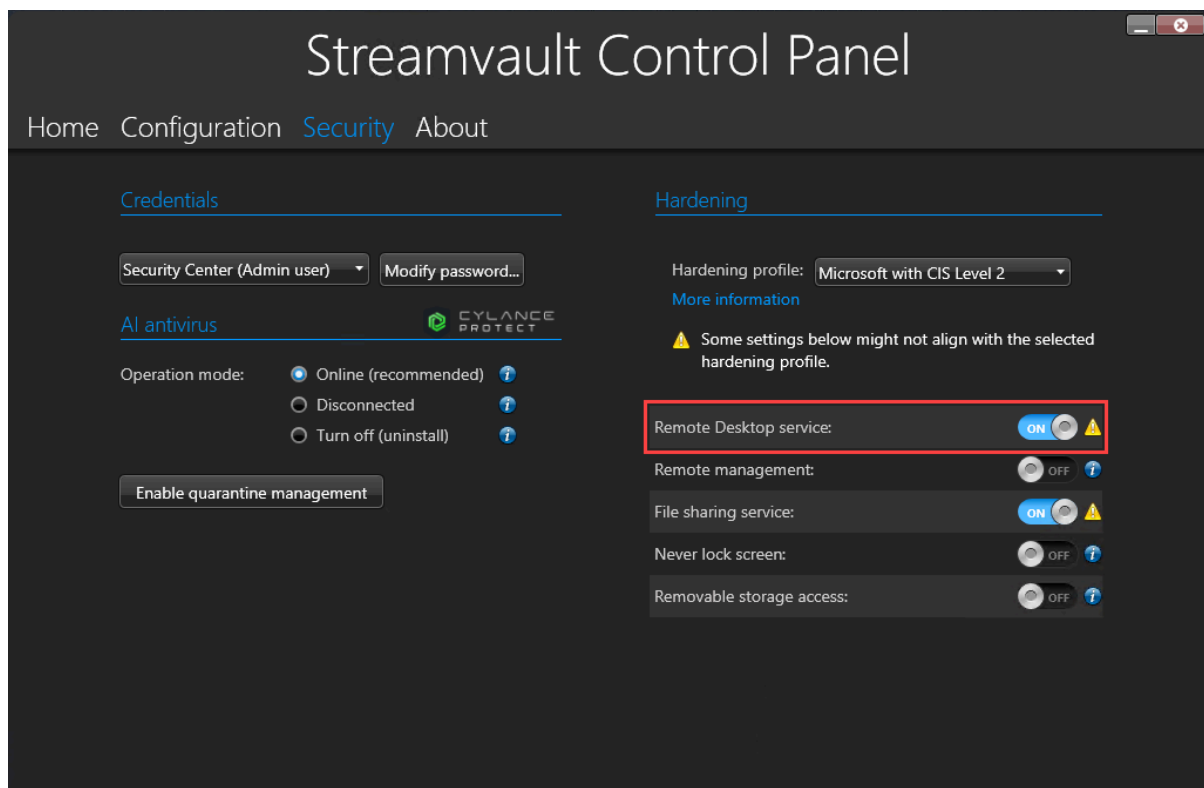
Wenn Sie versuchen, mithilfe von Remotedesktop auf eine Streamvault™-Appliance zuzugreifen, erhalten Sie eine Meldung, dass sich Remotedesktop nicht mit dem Remote-Computer verbinden kann.



## Remote Desktop Service ist in der SV Control Panel deaktiviert

**Beschreibung:** Standardmäßig ist der Remote-Zugriff auf einer Appliance deaktiviert, um maximale Sicherheit zu gewährleisten.

**Lösung:** [Aktivieren Sie Remote-Zugriff auf der Appliance](#). Schalten Sie auf der Seite *Sicherheit* des SV Control Panels den **Remote Desktop Service** ein.



## Remote Desktop ist unter Windows nicht erlaubt

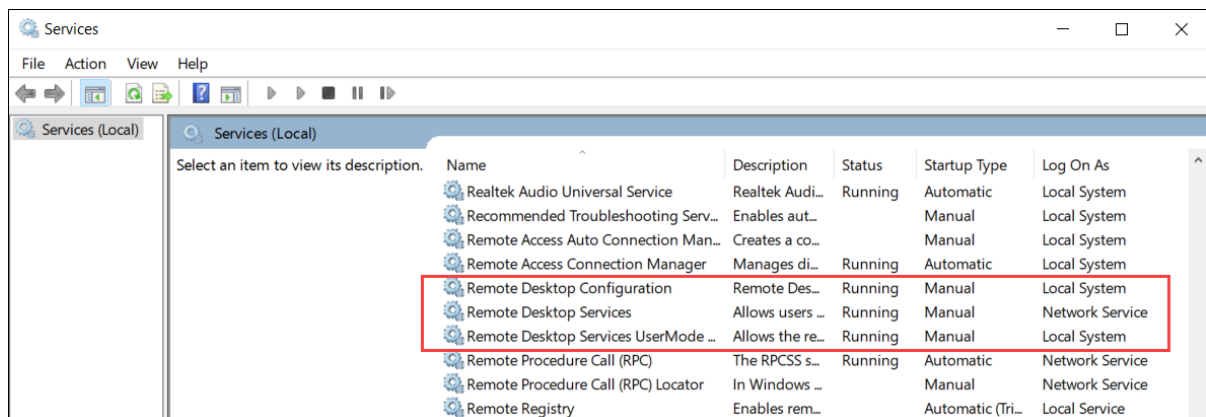
**Beschreibung:** Obwohl der **Remote Desktop Service** in der SV Control Panel aktiviert ist, ist diese Einstellung derzeit in Windows nicht erlaubt.

**Lösung:** Überschreiben Sie die Windows-Einstellung, indem Sie die Option **Remote Desktop Service** aus- und dann wieder einschalten.

## Remotedesktopdienste werden nicht ausgeführt

**Beschreibung:** Die Remotedesktopdienste wurden in Windows angehalten.

**Lösung:** Öffnen Sie die Windows-Services-Konsole, stellen Sie sicher, dass **Remotedesktopdienste** als **Netzwerkdienstbenutzer** angemeldet ist und stellen Sie sicher, dass die anderen Remotedesktopdienste ausgeführt werden.

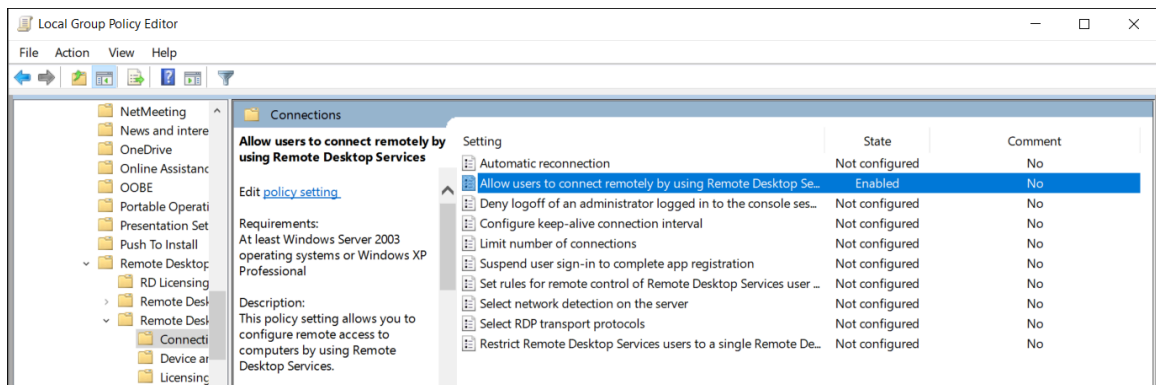


## Remote Desktop Services werden verweigert

**Beschreibung:** Windows ist konfiguriert, um für Remote-Benutzer Zugriff zu Remotedesktopdiensten verweigern.

**Lösung:** Erlauben Sie Remote-Benutzern Zugriff zur Appliance mithilfe von Remotedesktopdiensten:

1. Öffnen Sie die Eingabeaufforderung als Administrator und führen Sie `gpedit.msc` aus.
2. Navigieren Sie zu **Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Remotedesktopdienste > Remotedesktop-Sitzungshost > Verbindungen**.
3. Aktivieren Sie **Benutzern eine Remote-Verbindung über Remotedesktopdienste erlauben**.

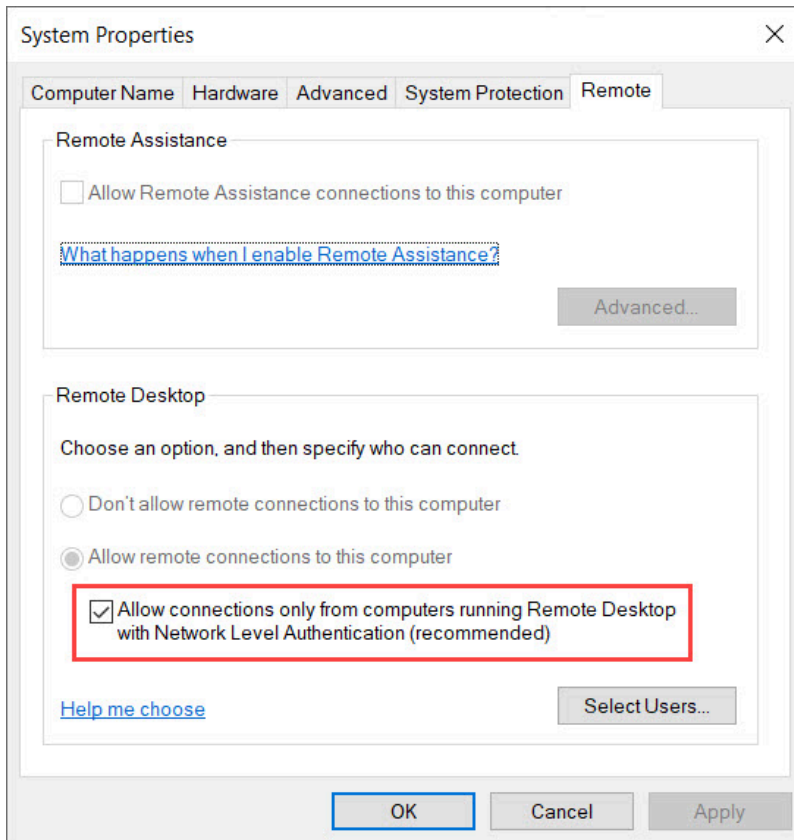


4. Führen Sie in der Eingabeaufforderung `gpupdate /force` aus.

5. Gehen Sie im Windows Control Panel zu **System und Sicherheit > Remote-Zugriff erlauben**.

Das Fenster *Systemeigenschaften* wird auf der Registerkarte **Remote** geöffnet.

6. Stellen Sie sicher, dass im Abschnitt *Remotedesktop* die Option **Verbindungen nur von Computern erlauben, die Remotedesktop mit Authentifizierung auf Netzwerkebene ausführen (empfehlen)** ausgewählt ist.



## Lokale Gruppenrichtlinien verweigern Remote-Zugriff

**Beschreibung:** Die lokalen Windows-Gruppenrichtlinien sind konfiguriert, um Remote-Zugriff auf Ihre Appliance zu verweigern.

**Lösung:** Konfigurieren Sie die Gruppenrichtlinien auf Ihrer Appliance, um Remote-Zugriff zu erlauben:

1. Öffnen Sie die Eingabeaufforderung als Administrator und führen Sie `gpedit.msc` aus.
2. Gehen Sie zu **Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Zuweisung von Benutzerrechten**.
3. Überprüfen Sie die folgenden Einstellungen für Gruppenrichtlinien:
  - **Anmeldung über Remotedesktopdienste erlauben** ist festgelegt auf **Administratoren**.
  - **Zugriff auf diesen Computer über das Netzwerk** ist auf **Gäste** festgelegt.
  - **Anmeldung über Remotedesktopdienste verweigern** ist festgelegt auf **Gäste**.

## NTLMv2-Authentifizierung wird nicht unterstützt

**Beschreibung:** Die Appliance oder der Remote-Computer unterstützen NTLMv2-Authentifizierung nicht.

**BEMERKUNG:** Wenn alle Client-Computer NTLMv2 unterstützen, empfehlen Microsoft und mehrere unabhängige Organisationen die Richtlinie *Nur NTLMv2-Antwort senden*. Sehen Sie in den

bewährten Methoden und Sicherheitsüberlegungen von Windows für [Netzwerksicherheit: LAN-Managerauthentifizierungsebene](#) nach, bevor Sie Ihre Einstellungen ändern.

**Lösung:** So stellen Sie sicher, dass Ihre Umgebung NTLMv2-Authentifizierung erlaubt:

1. Öffnen Sie die Eingabeaufforderung als Administrator und führen Sie `gpedit.msc` aus.
2. Gehen Sie zu **Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen > Netzwerksicherheit: LAN-Managerauthentifizierungsebene**.
3. Legen Sie die Richtlinie fest auf **LM & NTLM senden – NTLMv2-Sitzungssicherheit verwenden, wenn ausgehandelt**.

## Kontakt

**Lösung:** Wenn Remotedesktopverbindung weiterhin keine Verbindung herstellen kann, [kontaktieren Sie das Genetec Technical Assistance Center \(GTAC\)](#).

## Verwandte Themen

[Remotedesktop-Verbindungen auf einer Streamvault™-Appliance erlauben](#) auf Seite 91

# Aufhebung der Beschränkungen für Benutzerkonten von Nicht-Administratoren

---

Standardmäßig haben Benutzerkonten von Nicht-Administratoren, einschließlich des Operators, nur eingeschränkten Zugriff auf die Funktionen des Streamvault™-Control Panels. Sie können die Beschränkungen für diese Konten aufheben, um ihnen mehr Zugriff zu den Funktionen zu geben.

## Bevor Sie beginnen

- Nur eine Person, die als Administrator angemeldet ist, kann Einschränkungen für Nicht-Administrator-Konten aufheben.
- Beschränkungen können nur auf Systemen mit dem Streamvault™ Service aufgehoben werden.

## Prozedur

- 1 Öffnen Sie den Datei-Explorer und navigieren zu `C:\Windows\System32\GroupPolicyUsers`.
- 2 Löschen Sie das Verzeichnis `S-1-5-32-545` und seinen gesamten Inhalt. Dieses Verzeichnis enthält die Einschränkungen für Nicht-Administratoren.
- 3 Starten Sie Windows neu.

## Lokale Konten können nicht auf Remote Desktop, Datei-Sharing Service und Remote Management zugreifen

---

Wenn die Optionen für den **Remote Desktop Service**, das **Remote Management** oder den **Datei-Sharing Service** in der SV Control Panel aktiviert sind, können lokale Konten trotzdem nicht auf die Funktionen zugreifen.

Dieses Verhalten gilt für Windows Server-Produkte, die mit SV Control Panel 3.0 und höher ausgestattet sind:

- Streamvault™ SV-1000E Serie
- Streamvault™ SV-2000E Serie
- Streamvault™ SV-4000EX Serie
- Streamvault™ SV-7000EX Serie

Standardmäßig sind der Remote Desktop Service, das Remote Management und der Datei Sharing-Service für den lokalen Administrator und lokale Konten, wie z. B. Operator, deaktiviert. Bei früheren Versionen des SV Control Panels hatten der lokale Administrator und die lokalen Konten Zugriff auf diese Funktionen, wenn sie aktiviert waren. Ab SV Control Panel 3.0 erhält nur der lokale Administrator Zugriff, wenn die Funktionen aktiviert sind.

Dieses neue Verhalten wird durch die Option **Zugriff auf diesen Computer verweigern aus der Sicherheitsrichtlinie für das Netzwerk** gesteuert und entspricht den Sicherheitsgrundsätzen von Microsoft für Windows Server.

# Ermöglichung von Smart Card-bezogenen Diensten

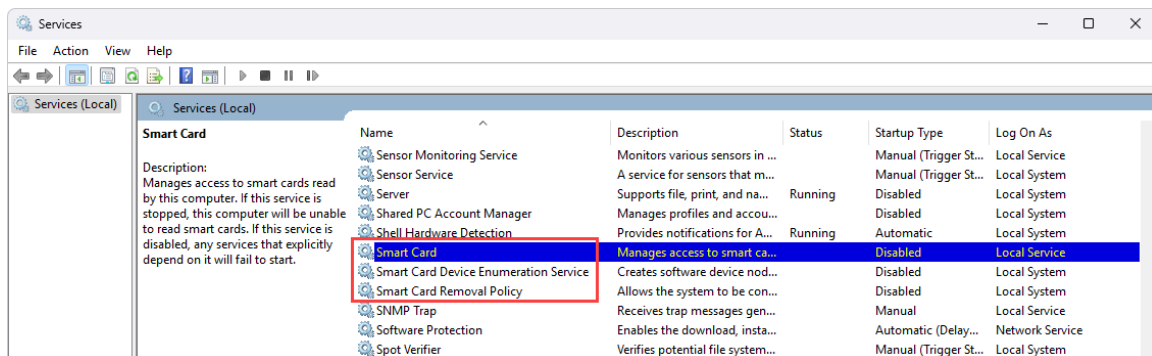
Wenn Sie von einer älteren Version auf SV Control Panel 3.0 aktualisiert haben und Smart Card-bezogene Services aktivieren möchten, können Sie dies über die Anwendung Windows Services tun.

## Was Sie noch wissen sollten

Die Option **Support für Speicherkarten aktivieren** ist in SV Control Panel 3.0 nicht verfügbar, da die Smart Card Services standardmäßig aktiviert sind.

## Prozedur

- 1 Führen Sie unter Windows *services.msc* aus, um die *Services*-Anwendung zu öffnen.
- 2 Aktivieren Sie den **Smart Card-Service**.
  - a) Klicken Sie mit der rechten Maustaste auf den **Smart Card-Service** und wählen Sie **Eigenschaften**.  
Das Dialogfeld *Eigenschaften* wird geöffnet.
  - b) Suchen Sie auf der Registerkarte **Allgemein** das Feld **Starttyp**, und wählen Sie **Automatisch**.
  - c) Klicken Sie auf **Anwenden** > **OK**.
- 3 Aktivieren Sie den **Smart Card Device Enumeration Service**.
  - a) Klicken Sie mit der rechten Maustaste auf **Smart Card Device Enumeration Service**, und wählen Sie **Eigenschaften**.  
Das Dialogfeld *Eigenschaften* wird geöffnet.
  - b) Suchen Sie auf der Registerkarte **Allgemein** das Feld **Starttyp**, und wählen Sie **Handbuch**.
  - c) Klicken Sie auf **Anwenden** > **OK**.
- 4 Aktivieren Sie den **Smart Card Device Enumeration Service**.
  - a) Klicken Sie mit der rechten Maustaste auf den Service **Smart Card Removal Policy**, und wählen Sie **Eigenschaften**.  
Das Dialogfeld *Eigenschaften* wird geöffnet.
  - b) Suchen Sie auf der Registerkarte **Allgemein** das Feld **Starttyp**, und wählen Sie **Handbuch**.
  - c) Klicken Sie auf **Anwenden** > **OK**.



# Support für Mercury EP- und LP-Firmware-Controller 1.x.x aktivieren

---

Bevor Sie Mercury EP- oder LP-Firmware-Controller 1.x.x in Ihre Streamvault™ Appliance integrieren können, müssen Sie eine ältere SSL Cipher Suite aktivieren.

## Was Sie noch wissen sollten

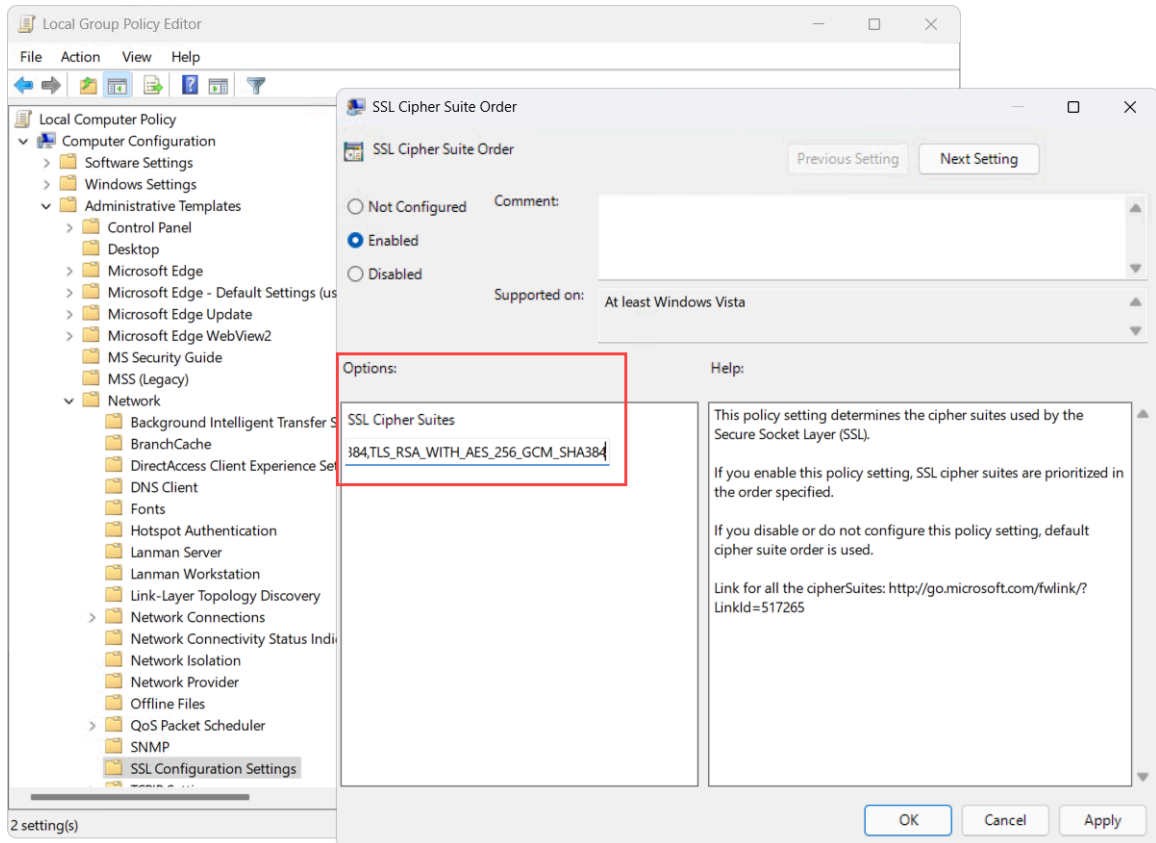
Abhängig von Ihrer Integration muss eine der folgenden Cipher Suites hinzugefügt werden, damit die Einheiten mit der Appliance kommunizieren können:

- **Integration von Mercury LP-Controllern in Firmware 1.31 und früher:**
  - TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
  - TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- **Integration von Mercury EP-Controllern in Firmware 1.29.7 und älter:**
  - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

## Prozedur

- 1 Führen Sie unter Windows `gpedit.msc` aus, um den *Editor für lokale Gruppenrichtlinien* zu öffnen.
- 2 Navigieren Sie zu **Computer Konfiguration > Verwaltungsvorlagen > Netzwerk > Secure Socket Layer Konfiguration Einstellungen**.
- 3 Doppelklicken Sie auf **Secure Socket Layer Cipher Suite Order**.
- 4 Fügen Sie im Bereich *Optionen* im Feld **SSL Cipher Suites** ein Komma am Ende der Liste hinzu, gefolgt von der für Ihre Integration geltenden Cipher Suite. Fügen Sie keine Leerzeichen ein.

- 5 Klicken Sie auf **OK**, um das Gruppenrichtlinienobjekt (GPO) zu speichern.



- 6 Starten Sie den Software Service oder die Appliance neu.

# Support für die Synergis IX-Integration aktivieren

Bevor Sie Synergis™ IX-Controller auf Ihrer Streamvault™-Appliance registrieren können, müssen Sie eine zusätzliche SSL Cipher Suite hinzufügen.

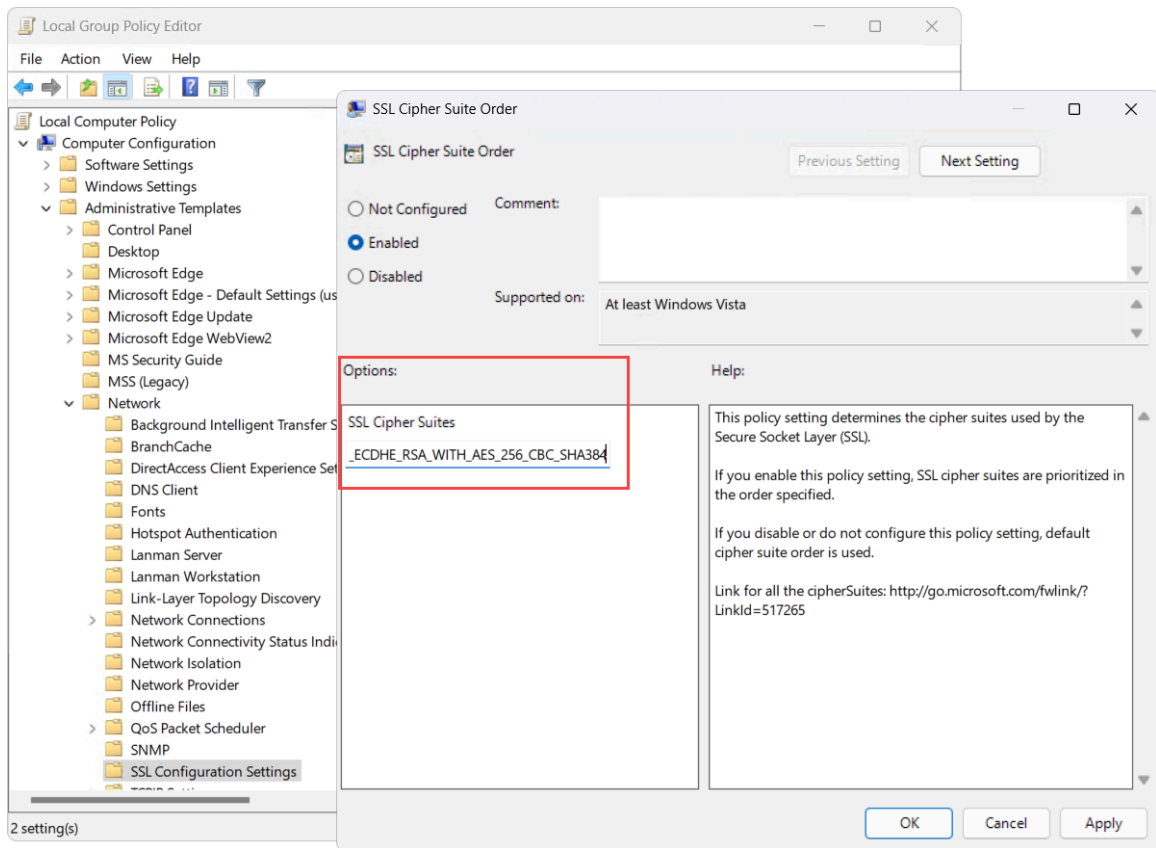
## Was Sie noch wissen sollten

Eine der folgenden Cipher Suites muss hinzugefügt werden, um Synergis IX-Controller auf Ihrer Streamvault™-Appliance zu registrieren:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

## Prozedur

- 1 Führen Sie unter Windows `gpedit.msc` aus, um den *Editor für lokale Gruppenrichtlinien* zu öffnen.
- 2 Navigieren Sie zu **Computer Konfiguration** > **Verwaltungsvorlagen** > **Netzwerk** > **Secure Socket Layer Konfiguration Einstellungen**.
- 3 Doppelklicken Sie auf **Secure Socket Layer Cipher Suite Order**.
- 4 Fügen Sie im Bereich *Optionen* im Feld **SSL Cipher Suites** ein Komma am Ende der Liste hinzu, gefolgt von `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384` oder `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256`. Fügen Sie keine Leerzeichen ein.
- 5 Klicken Sie auf **OK**, um das Gruppenrichtlinienobjekt (GPO) zu speichern.



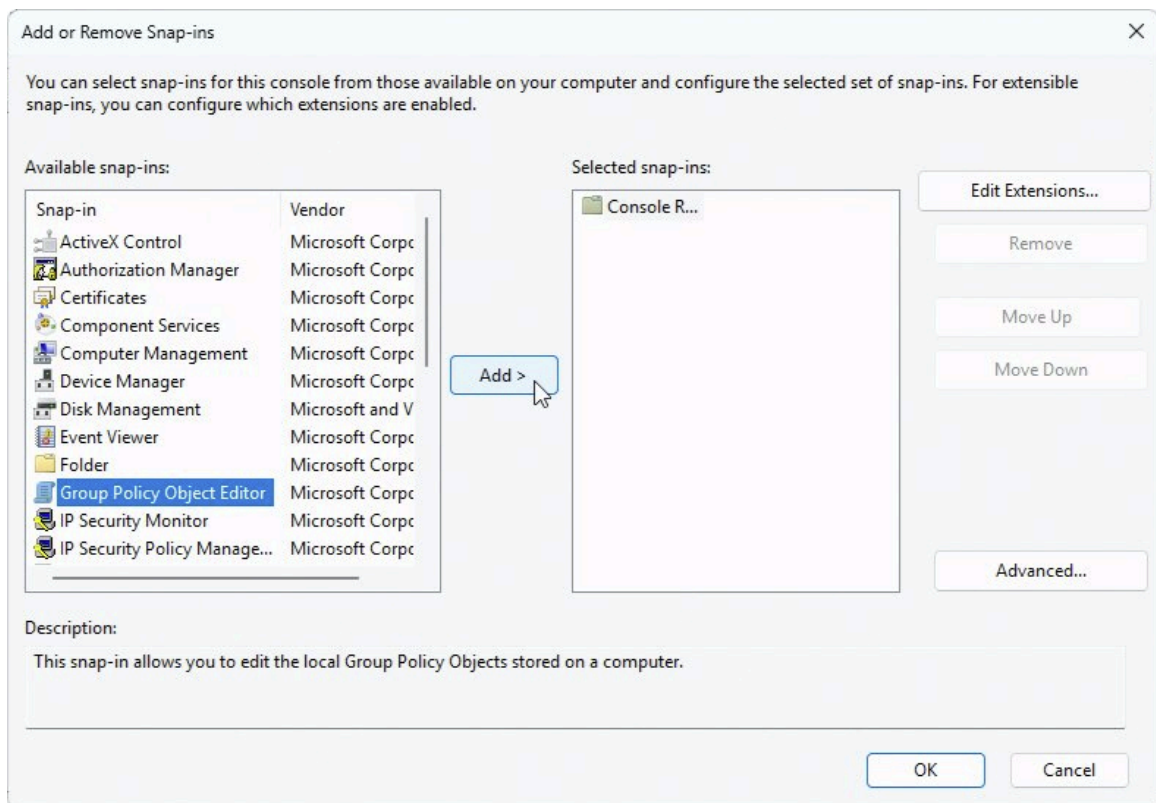
- 6 Starten Sie den Software Service oder die Appliance neu.

# Ändern lokaler Gruppenrichtlinienobjekte für Benutzerkonten von Nicht-Administratoren

Standardmäßig haben Konten von Benutzern, die keine Administratoren sind, eingeschränkten Zugriff auf die Funktionen der Streamvault™-Appliance. Um deren Berechtigungen anzupassen, können Sie die lokalen Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) für die Gruppe **Nicht-Administratoren** über die Microsoft Management Console ändern.

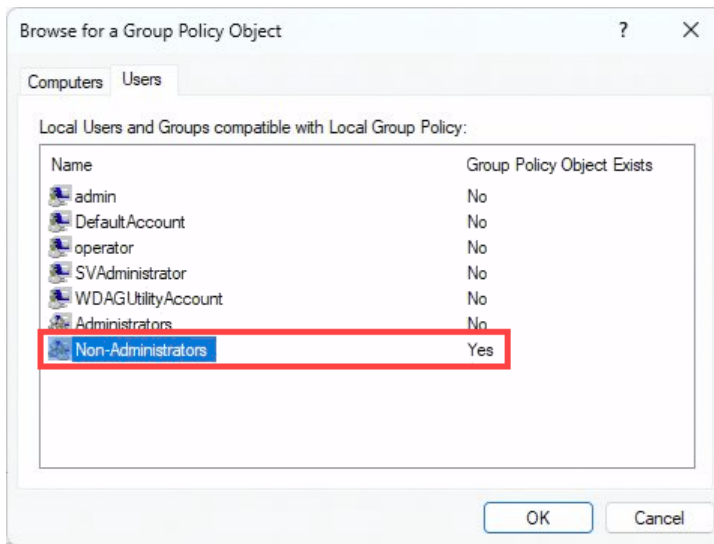
## Prozedur

- 1 Wählen Sie im Windows-Startmenü die Option **Ausführen**, geben Sie `mmc . exe` ein und klicken Sie auf **OK**. Das Fenster *Microsoft Management Console* wird geöffnet.
- 2 Klicken Sie im linken Bereich auf **Datei > Snap-In hinzufügen/entfernen**. Das Dialogfeld *Snap-Ins hinzufügen oder entfernen* wird geöffnet.
- 3 Wählen Sie im Abschnitt **Verfügbare Snap-Ins** die Option **Gruppenrichtlinienobjekt-Editor** aus, und klicken Sie auf **Hinzufügen**.

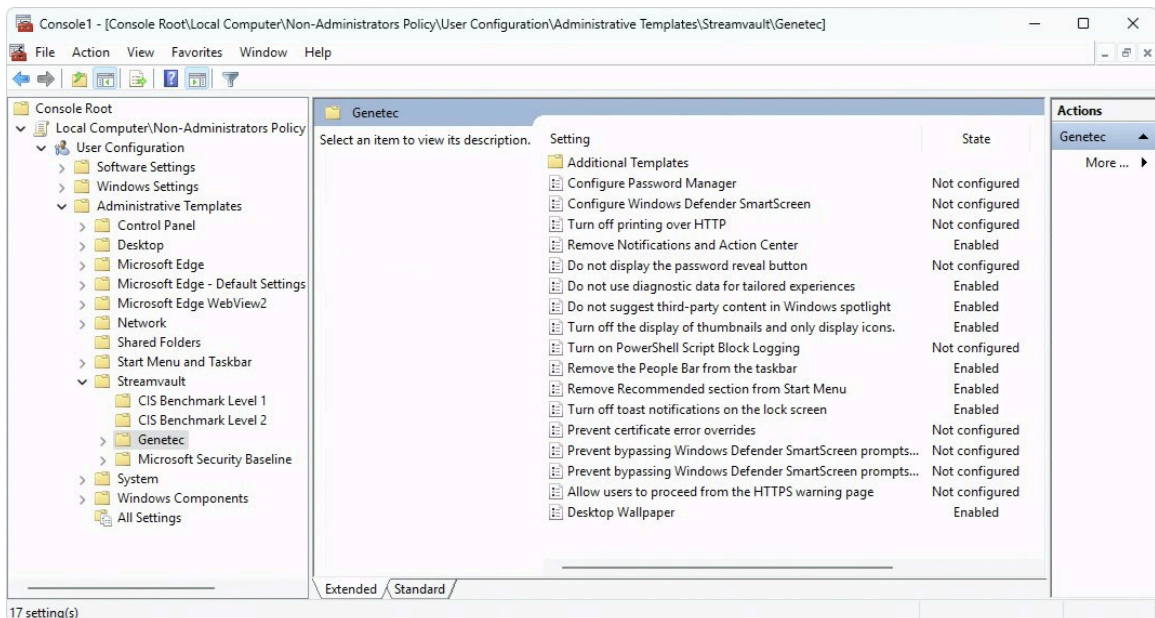


- 4 Klicken Sie im Assistenten *Gruppenrichtlinienobjekt* auf **Durchsuchen**.

- 5 Klicken Sie im Dialogfeld *Nach Gruppenrichtlinienobjekt suchen* auf die Registerkarte **Benutzer**, wählen Sie die Gruppe **Nicht-Administratoren** aus, für die ein lokales Gruppenrichtlinienobjekt vorhanden ist, und klicken Sie auf **OK**.



- 6 Klicken Sie im Dialogfeld *Gruppenrichtlinienobjekt auswählen* auf **Fertig stellen**.
- 7 Klicken Sie im Dialogfeld *Snap-Ins hinzufügen oder entfernen* auf **OK**.
- 8 Wählen Sie im Fenster *Microsoft Management Console* die Option **Konsolenstamm > Lokaler Computer > Richtlinie für Nicht-Administratoren > Benutzerkonfiguration > Administrative Vorlagen > Streamvault > <Härtungsprofil>**.  
Dabei steht <Härtungsprofil> für eines der vier vordefinierten Härtingsprofile: CIS Benchmark Level 1, CIS Benchmark Level 2, Genetec™ und Microsoft Security Baseline.  
Alle GPOs, die für Nicht-Administrator-Konten konfiguriert sind, werden im ausgewählten Härtingsprofil aufgelistet.  
**BEMERKUNG:** Ein Gruppenrichtlinienobjekt wird konfiguriert, wenn sein Status *Aktiviert* oder *Deaktiviert* ist. Ein Gruppenrichtlinienobjekt mit dem Status *Nicht konfiguriert* wird nicht von Streamvault™ gesteuert.



- 9 Doppelklicken Sie auf die einzelnen Gruppenrichtlinienobjekte, um sie anzuzeigen oder zu bearbeiten.

## Verwandte Themen

[Anmeldeinformationen für Standard-Benutzerkonten auf einer Appliance Streamvault](#) auf Seite 12

# Windows-Firewall deaktivieren

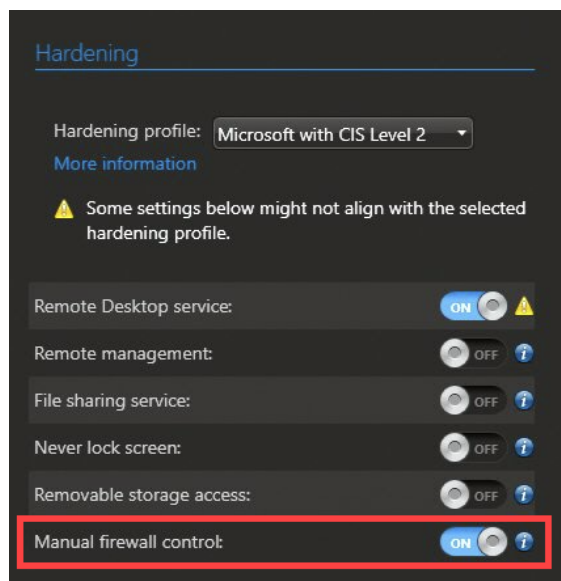
Standardmäßig verwendet die Windows-Firewall lokale Gruppenrichtlinienobjekte (Group Policy Objects, GPOs) aus den Härtingsprofilen, um die Streamvault™-Appliance zu sichern. Wenn Sie die Windows-Firewall zur Fehlerbehebung deaktivieren möchten, müssen Sie zuerst die manuelle Firewall-Steuerung im SV Control Panel aktivieren.

## Prozedur

- 1 Öffnen Sie das SV Control Panel und rufen Sie die Seite *Sicherheit* auf.
- 2 Aktivieren Sie im Abschnitt *Härtung* die Option **Manuelle Firewall-Steuerung** und klicken Sie auf **Anwenden**.

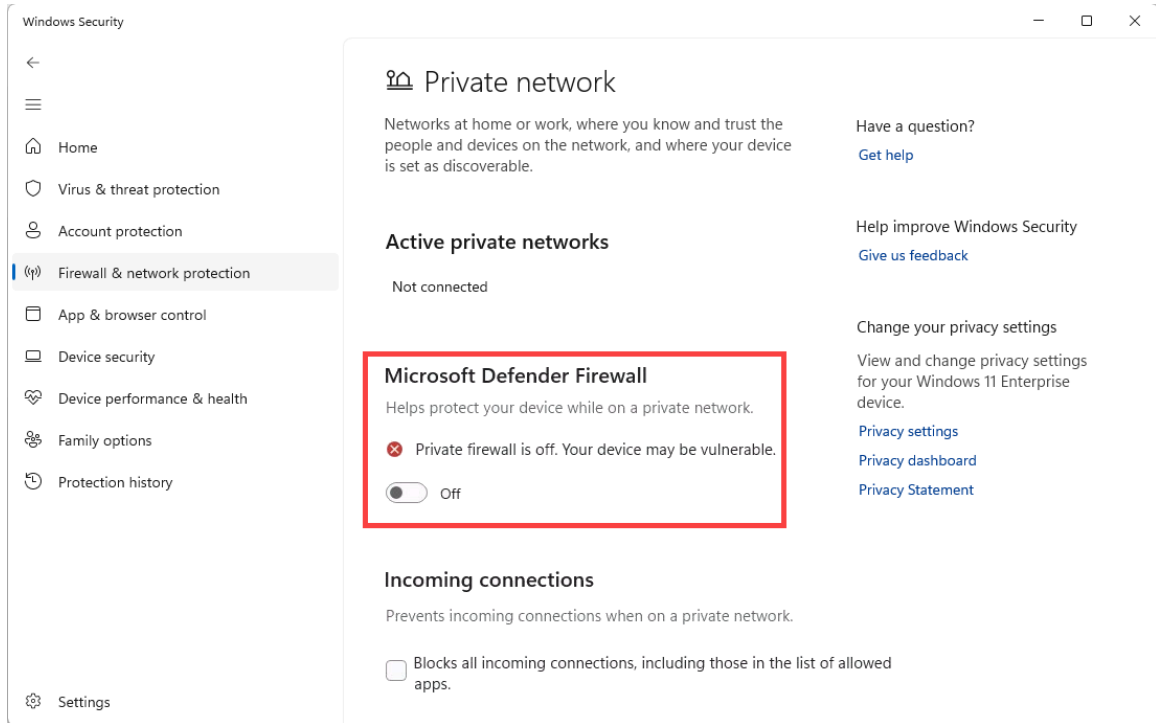
Warten Sie, bis die Einstellung angewendet wird.

**BEMERKUNG:** Wenn diese Option aktiviert ist, werden alle lokalen GPOs deaktiviert. Davon sind keine Firewall-Regeln betroffen.



- 3 Wählen Sie im Windows-Startmenü die Option **Firewall und Netzwerkschutz**.
- 4 Wählen Sie das Netzwerk aus, für das Sie die Firewall deaktivieren möchten.

5 Deaktivieren Sie im Abschnitt *Microsoft Defender-Firewall* die Firewall.



**BEMERKUNG:** Sie können die Firewall auch über die *Windows Defender-Firewall mit erweiterter Sicherheit* deaktivieren.

# Technischer Support

Dieser Abschnitt enthält die folgenden Themen:

- ["Kontaktieren des Genetec Technical Assistance Center"](#) auf Seite 129
- ["Software-Support"](#) auf Seite 132
- ["Hardware-Support"](#) auf Seite 133
- ["Spezifikationen für Streamvault"](#) auf Seite 134
- ["Nutzungsbedingungen für den Streamvault-Support"](#) auf Seite 135

# Kontaktieren des Genetec Technical Assistance Center

Das Genetec™ Technical Assistance Center (GTAC) hilft Ihnen bei allen Software- und Hardwareproblemen bei Streamvault™.

**BEMERKUNG:** Bei Anfragen zu Softwareproblemen bei Genetec™ Security Center wird technische Unterstützung über unsere reguläre technische Hilfstelefonlinie angeboten. Sie finden die GTAC-Telefonnummer und Geschäftszeiten für Ihre Region auf der Seite [Genetec Technical Assistance Center Kontaktieren Sie uns](#).

## Nützliche Informationen

Halten Sie die folgenden Informationen bereit, wenn Sie einen Supportfall öffnen:

- Die System-ID Ihrer Security Center-Lizenz. Weitere Informationen erhalten Sie unter [Wo finde ich meine System-ID?](#).
- Ihre Genetec-Seriennummer oder das Hardware-Servicetag.
- Ihren Genetec-Code, den Sie auf dem Gehäuse finden (gilt nicht für All-in-One-Appliances). Der Code ist erforderlich, wenn Sie den administrativen Zugriff auf das System verloren haben und ein Werks-Image benötigen.



- Ihre Diagnostik-TSR-Protokolldatei (falls zutreffend). Weitere Informationen finden Sie unter [Erfassen von Support-Protokollen](#).

## GTAC per Telefon kontaktieren

Telefonsupport bei Streamvault™-Problemen ist für alle Kunden während der Geschäftszeiten in ihrer Region verfügbar.

### Für Kunden in Nordamerika, Europa, dem mittlerem Osten und Afrika:

1. Sie finden die GTAC-Telefonnummer und die Geschäftszeiten für Ihre Region unter [Genetec Technical Assistance Center \(GTAC\) Kontaktieren Sie uns](#).
2. Rufen Sie unter der GTAC-Telefonnummer an und wählen Sie Option Nr. 2.

### Für Kunden in der Region Asien-Pazifik:

Support für die APAC-Region ist über das [Genetec Technical Assistance Portal \(GTAP\)](#) per Live-Chat und Support-Fälle verfügbar. Die Geschäftszeiten sind Montag bis Freitag, 08:00 bis 20:00 Uhr (Ortszeit).

### So kontaktieren Sie uns über den 24/7-Notfall-Support außerhalb der Geschäftszeiten:

1. Rufen Sie die GTAC-Nummer für Ihre Region an.
2. Geben Sie Ihre Genetec-Zertifizierungs-ID-Nummer ein.
3. Geben Sie die Genetec-Advantage-Vertragsnummer oder die Genetec-Abonnementnummer ein.
4. Wählen Sie das Produkt aus.

5. Hinterlassen Sie eine Nachricht mit Ihrem Namen, Ihrer Telefonnummer und einer Beschreibung des Problems.

Der Techniker im Dienst wird Sie innerhalb von 30 Minuten kontaktieren.

**WICHTIG:** Rund-um-die-Uhr-Notfallsupport ist nur für Kunden verfügbar, die diese Option in ihren Genetec Advantage-Vertrag aufgenommen haben. Um weitere Informationen zu erhalten, kontaktieren Sie [advantage@genetec.com](mailto:advantage@genetec.com).

Kunden ohne Advantage-Deckung müssen einen Fall über das [Genetec Technical Assistance Portal \(GTAP\)](#) öffnen.

## Das GTAC über das GTAP kontaktieren

Support bei allen Streamvault™-Problemen ist für alle Kunden während der Geschäftszeiten in Ihrer Region über Online-Support-Fälle im [Genetec™ Technical Assistance Portal \(GTAP\)](#) verfügbar.

Bei Kunden ohne Genetec™-Advantage-Garantie muss ein Fall über das [Genetec Technical Assistance Portal \(GTAP\)](#) geöffnet werden. Um weitere Informationen über Genetec Advantage zu erhalten, kontaktieren Sie [advantage@genetec.com](mailto:advantage@genetec.com).

So reichen Sie einen Fall über das Online-Portal ein:

1. Navigieren Sie zum [Genetec Technical Assistance Portal](#).
2. Melden Sie sich mit Ihrer Unternehmens-E-Mail an.
3. Klicken Sie auf **+ Fall erstellen**.



4. Wählen Sie in der Liste **System-ID** das betroffene System aus.
5. Fügen Sie bei Hardwarerückgaben und -reparaturen **Antrag auf Warenrücksendegenehmigung** in den Titel hinzu, damit unser Team diese Anfragen einfach erkennen kann.

### Description of the issue

#### Please Note:

- If you have more than one issue to report, please open one case for each
- If you have a problem with an order and/or its license parts, please contact [customerservice@Genetec.com](mailto:customerservice@Genetec.com)
- If you have any sales-related questions, please contact [sales@Genetec.com](mailto:sales@Genetec.com)
- If you are reporting a hardware issue with a StreamVault™ appliance, please type 'RMA' in the Title.

Title:

RMA Request [your title here]

Description:

[Your description here]

6. Fügen Sie die Seriennummer Ihres Produkts, den Genetec-Code und die Diagnose-TSR-Protokolldatei (wenn verfügbar) hinzu.
7. Klicken Sie auf **Fall absenden**.

Sie erhalten eine Fallbestätigung per E-Mail zusammen mit der geschätzten Antwortzeit.

## Das GTAC über den Live-Chat kontaktieren

Kunden mit Genetec™ Advantage erhalten Unterstützung bei Streamvault™-Problemen über den Live-Chat im [Genetec Technical Assistance Portal \(GTAP\)](#). Kunden erhalten Support während der Geschäftszeiten in ihrer Region.

Bei Kunden ohne Genetec-Advantage-Garantie muss ein Fall über das [Genetec Technical Assistance Portal \(GTAP\)](#) geöffnet werden. Um weitere Informationen über Genetec Advantage zu erhalten, kontaktieren Sie [advantage@genetec.com](mailto:advantage@genetec.com).

So starten Sie einen Live-Chat:

1. Gehen Sie zum [Genetec Technical Assistance Portal](#).
2. Melden Sie sich mit Ihrer Unternehmens-E-Mail an.
3. Klicken Sie auf die Taste **Zum Chatten klicken**.



4. Wählen Sie Ihre bevorzugte Sprache aus.
5. Geben Sie die vollständige System-ID (GSC-xxxxxx-xxxxxx) ein und klicken Sie dann auf **System-ID überprüfen**.
6. Wählen Sie aus, ob Sie bezüglich eines neuen oder bestehenden Falls chatten.
7. Wählen Sie das Produkt aus.
8. Klicken Sie auf **Chat starten**.

9. Um eine Warenrücksendungsgenehmigung anzufordern, fügen Sie die Seriennummer Ihres Produkts, den Genetec-Code und die Diagnose-TSR-Protokolldatei (wenn verfügbar) hinzu.

Antwortzeit (verfügbar nur während der Geschäftszeiten in Ihrer Region): Üblicherweise innerhalb von 5 Minuten.

# Software-Support

---

Die Streamvault™-Windows-Image-Software enthält die neueste Version der Security-Center-Software und der Control Panel zum Zeitpunkt der Erstellung des Image. Support für das Windows-Image und die Security-Center-Software werden separat behandelt.

## Streamvault-Software

- Ein Streamvault-Windows-Image wird von Ihrer Streamvault-Garantie für den gesamten Lebenszyklus Ihrer Appliance abgedeckt.  
**WICHTIG:** Upgrades Ihres Windows-Betriebssystems werden nicht durch Ihre Garantie abgedeckt. Beim Upgrade des Windows-Betriebssystems werden die erforderlichen Treiber, Härtung und Software gelöscht, die mit dem Image installiert wurden.
- Die für das Streamvault-Appliance-Re-Imaging bereitgestellte Sicherung enthält das Betriebssystem und Image, die beim Kauf der Appliance mitgeliefert wurden.
- Das Streamvault-Windows-Image wird von Ihrer Streamvault-Garantie abgedeckt, unabhängig von Ihrem Genetec™-Advantage-Status.

## Security-Center-Software

Probleme mit der Security-Center-Software sind vom Service-Level-Agreement (SLA) und in den folgenden Genetec-Lifecycle-Management (GLM)-Dokumenten beschriebenen Supportverfahren abgedeckt: [Genetec Advantage – Beschreibung](#).

## Hardware-Support

---

HP- und [Dell-ProSupport](#)-Garantien sind über Genetec™ verfügbar. Bei Hardwareproblemen hilft Ihnen das Genetec Technical Assistance Center (GTAC) bei der Diagnostizierung des Problems und bei der Koordination mit HP und Dell ProSupport.

Einzelheiten zu den von Genetec™ angebotenen Garantien für Streamvault-Hardware finden Sie in der [Übersicht der Genetec-Hardwaregarantien](#).

# Spezifikationen für Streamvault

---

Beachten Sie die folgenden technischen, mechanischen und umweltbezogenen Daten beim Planen und Bereitstellen Ihrer Streamvault™-Appliance.

## Technische, mechanische und umweltbezogene Daten

All-in-One-Appliances:

- [SV-300E-Datenblatt](#)

Rackmontage-Appliances:

- [Datenblatt der SV-1000E-Serie](#)
- [Datenblatt der SV-2000E-Serie](#)
- [Datenblatt der SV-4000E-Serie](#)

Zentralisierter Speicher mit hoher Verfügbarkeit:

- [Datenblatt der SV-7000EX-Serie](#)

Workstations:

- [Datenblatt der Serie SVW-100E](#)
- [Datenblatt der SVW-300E-Serie](#)
- [Datenblatt der SVW-500E-Serie](#)

All-in-One-Vehicle Monitoring-Appliances:

- [Datenblatt der SVR-300A-Serie](#)
- [Datenblatt der SVR-300AR-Serie](#)
- [Datenblatt der SVR-500A-Serie](#)

## Nutzungsbedingungen für den Streamvault-Support

---

Die Genetec™ Standard- und Erweiterte Garantie für Hardware unterliegen den in der [Übersicht über die Genetec Hardware-Garantie](#) beschriebenen Laufzeiten und Bedingungen.

# Glossar

## Produktions-Image

Ein Produktions-Image ist ein Streamvault™-Image, das beim Kauf einer Appliance an den Kunden ausgeliefert wird. Die auf diesem Image installierten Software-Versionen variieren je nach Kundenauftrag.

## Streamvault-Hilfsprogramm für Werksreset

Das Streamvault-Hilfsprogramm für Werksreset ist ein Tool, über das Sie eine Streamvault-Appliance auf die Werkseinstellungen zurücksetzen. Anhand des Tools können Sie einen bootfähigen USB-Schlüssel mit dem erforderlichen Streamvault-Software-Image erstellen.

## Streamvault™-Hardware

Streamvault™-Hardware ist ein Berichtstask in Security Center, den Sie verwenden können, um eine Liste von Integritätsproblemen anzuzeigen, die bei Ihren Streamvault™-Appliances auftreten können.

## Streamvault™-Hardwareüberwachung

Die Streamvault™-Hardwareüberwachungsentität hilft bei der Überwachung des Status Ihrer Streamvault™-Appliance und benachrichtigt Sie, wenn Probleme auftreten. Es ist eine Streamvault™-Hardwareüberwachung pro Streamvault™-Appliance erforderlich.

## Streamvault™-Manager

Die Streamvault™-Managerentität wird zum Steuern der Alarmkonfigurationen für eine Gruppe von Streamvault™-Agent-Entitäten verwendet. Nur ein Streamvault™-Manager ist pro System erlaubt.

## Streamvault™ Service

Der Streamvault Service ist ein Windows Service, der es Benutzern ermöglicht, eine Streamvault™ Appliance zu konfigurieren, wie z. B. die Anwendung von Härtingsprofilen.

## SV-1000E

SV-1000E ist eine kosteneffiziente Rackmontage-Sicherheits-Appliance für mittlere Sicherheitssysteme. Sie hilft Ihnen beim Umstieg auf ein einheitliches Sicherheitssystem, indem sie Videoüberwachung, Zutrittssteuerung, automatische Nummernschilderkennung, Kommunikation, Einbrucherkennung und Analytik in einer einzigen Appliance vereint. SV-1000E wird mit vorinstalliertem Security Center und SV Control Panel geliefert.

## SV-100E

SV-100E ist eine subkompakte, komplette Appliance, die mit vorinstalliertem Microsoft Windows, Security Center und SV Control Panel geliefert wird. SV-100E ist für kleine Anlagen mit einem einzigen Server konzipiert und kann sowohl Kameras als auch Zutrittskontroll-Lesegeräte unterstützen.

## SV-2000E

SV-2000E ist eine Sicherheits-Appliance für die Rackmontage, mit der Sie ein einheitliches System bereitstellen können, das Videoüberwachung, Zutrittskontrolle, automatische Nummernschilderkennung und Kommunikation kombiniert. SV-2000E wird mit vorinstalliertem Security Center und SV Control Panel geliefert.

## SV-300E

SV-300E ist eine kompakte, komplette und schlüsselfertige Appliance, die mit vorinstalliertem Microsoft Windows, Security Center und SV Control Panel geliefert wird. Dank der integrierten analogen Encoder-Erfassungskarten können Sie die Appliance verwenden, um schnell ein alleinstehendes Videoüberwachungs- oder Zutrittskontrollsystem oder aber ein einheitliches System bereitzustellen.

## SV-350E

SV-350E ist eine schlüsselfertige All-in-One-Sicherheits-Appliance, die Ihnen beim Umstieg zu einem einheitlichen System hilft, das Videoüberwachung, Zutrittskontrolle, Einbrucherkennung und Kommunikation kombiniert. Die Appliance wird mit vorinstalliertem Microsoft Windows, Security Center und dem SV Control Panel geliefert. Sie bietet außerdem RAID 5 für kritischen Videospeicher.

**SV-4000E**

SV-4000E ist eine Sicherheits-Appliance für die Rackmontage, die höchste Leistung und Zuverlässigkeit für Unternehmen bieten. Die zertifizierten Hardwarekonfigurationen und gebrauchsfertige Härtung gegen Cyber-Gefahren vereinfachen das Entwerfen und die Bereitstellung eines neuen Sicherheitssystems. SV-4000E wird mit vorinstalliertem Security Center und SV Control Panel geliefert.

**SV-7000E**

SV-7000E ist eine Sicherheits-Appliance für die Rackmontage, die für Anwendungen entworfen wurde, die eine hohe Anzahl von hochauflösenden Kameras, Benutzern und Ereignissen kombiniert. SV-7000E wird mit vorinstalliertem Security Center und SV Control Panel geliefert.

**SVA-100E**

SVA-100E ist eine kompakte Appliance, die Sie einsetzen können, um Ihr Sicherheitssystem auf einfache Weise mit KiwiVision™-Videoanalyse aufzuwerten. Das Design ist optimiert, damit Sie mehr Analysestreams auf Ihr Videoüberwachungssystem anwenden können, ob es sich um einen einzelnen oder mehrere Analysestreams pro Kamera handelt.

**SV Appliance**

Streamvault™ ist eine einsatzbereite Appliance mit einem eingebetteten Betriebssystem und vorinstalliertem Security Center. Mit Streamvault™ können Sie schnell ein einheitliches oder autonomes System für Videoüberwachung und Zutrittskontrolle einrichten.

**SV Control Panel**

SV Control Panel ist eine Oberflächenanwendung, mit der Sie die Streamvault™-Appliance für die Zusammenarbeit mit Zutrittskontrolle und Videoüberwachung in Security Center konfigurieren können.

**SVW-300E**

Die SVW-300E-Workstation ist eine schlüsselfertige Lösung, die für das Überwachen von kleinen bis mittleren Sicherheitssystemen mit mehreren Bildschirmen entworfen wurde. SVW-300E wird mit vorinstalliertem Security Center geliefert.

**SVW-500E**

Die SVW-500E-Workstation ist eine Hochleistungslösung, die für Benutzer entworfen wurde, die die Möglichkeit benötigen, Kameras mit einer sehr hohen Auflösung auf 4K-Monitoren und Videowänden anzuzeigen. SVW-500E wird mit vorinstalliertem Security Center geliefert.

**Wiederherstellungs-Image**

Ein Wiederherstellungs-Image wird für das Re-Imaging von Streamvault™-Appliances verwendet. Es handelt sich um ein festes Image, auf dem bestimmte Software-Versionen vorinstalliert sind.

# Wo finde ich Produktinformationen?

Unsere Produktdokumentation steht in folgenden Bereichen zur Verfügung:

- **Genetec™ TechDoc Hub:** Die aktuelle Dokumentation ist im [TechDoc Hub](#) verfügbar.  
Sie finden die gesuchte Information nicht? Nehmen Sie Kontakt mit [documentation@genetec.com](mailto:documentation@genetec.com) auf.
- **Installationspaket:** Das Installationshandbuch und die Versionshinweise stehen im Ordner Dokumentation zur Verfügung, der sich im Installationspaket befindet. Einige Dokumente beinhalten auch einen direkten Link zum Herunterladen der aktuellen Version des Dokuments.
- **Hilfe:** Security Center-Clientanwendungen und webbasierte Anwendungen beinhalten eine Hilfe, in der die Funktionsweise des Produkts und die Nutzung der Produktfunktionen erläutert werden. Um auf die Hilfe zuzugreifen, klicken Sie auf **Hilfe**, drücken Sie F1, oder tippen Sie auf das ? (Fragezeichen) in den jeweiligen Client-Anwendungen.