Streamvault™ Appliance – Benutzerhandbuch

Klicken Sie hier für die neueste Version dieses Dokuments.

Dokument zuletzt aktualisiert: 10. November 2023

Genetec™

Rechtliche Hinweise

Dokumentinformationen

Dokumenttitel: Streamvault™ Appliance – Benutzerhandbuch

Dokumentnummer original: EN.803.003

Dokumentnummer: DE.803.003

Aktualisierungsdatum des Dokuments: 10. November 2023

Sie können Kommentare, Korrekturen und Anregungen zu diesem Handbuch an 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

Kapitel 4: SV Control Panel – Referenz

Kapitel 5: Zusätzliche Ressourcen

Kapitel 6: Problembehebung

Kapitel 7: Technischer Support

1

Einführung zu Ihrer Streamvault Appliance

Dieser Abschnitt enthält die folgenden Themen:

Erste Schritte mit Ihrer Streamvault Appliance

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

Bereitstellung – Übersicht

Schri	Task	Wo finde ich weitere Informationen?
Machen Sie sich vor der Bereitstellung mit Voraussetzungen und zentralen Themen vertraut		
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.	• Von Streamvault verwendete Standardports auf Seite 4. • Komponenten der Streamvault-Appliance anschließen auf Seite 8. • Analoge Genetec-Encoder-Karte auf Seite 8. • Kameraeingaben auf Encoder-Karten auf einer Streamvault-Appliance deaktivieren auf Seite 9. • Alarmeingaben und -Ausgaben einer Streamvault-Appliance auf Seite 10.
2	Bevor Sie Ihre Appliance bereitstellen, lesen Sie die Versionshinweise, um sich über die neuen Funktionen, bekannten Probleme und Einschränkungen zu informieren.	In den *Streamvault – Versionshinweisen* finden Sie für die auf Ihrer Appliance installierte Image-Version Folgendes: • Was ist neu • Bekannte Probleme • Einschränkungen
3	Melden Sie sich bei Windows als Admin mit dem Passwort an, das auf Ihrer Appliance gedruckt ist, und ändern Sie dann das Passwort.	• Bei einer Streamvault-Appliance anmelden auf Seite 12.
Einrichtungs-Assistent abschließen		
4	Schließen Sie den Assistenten *Einrichtung von Streamvault Control Panel* ab. **BEMERKUNG:** Der Remotedesktop ist standardmäßig deaktiviert. Um Remotedesktop zu aktivieren, deaktivieren Sie die Einstellung **Remotedesktop blockieren** auf der Seite *SIcherheit* dieses Assistenten.	• Ihre Appliance im SV Control Panel einrichten auf Seite 15. • Remotedesktop-Verbindungen auf einer Streamvault™-Appliance erlauben auf Seite 72.
5	Aktivieren Sie Security-Center-Lizenz. • Wenn die Appliance mit dem Internet verbunden ist, aktivieren Sie Ihre Lizenz mithilfe des Assistenten *Aktivierung von Streamvault Control Panel*. • Wenn die Appliance nicht mit dem Internet verbunden ist, aktivieren Sie Ihre Lizenz manuell über Server Admin.	• Ihre Security-Center-Lizenz auf einer Appliance aktivieren auf Seite 19. • Eine Lizenz manuell über Server Admin ändern auf Seite 21.

Schritt	Task	Wo finde ich weitere Informationen?
6	Aktivieren Sie den System Availability Monitor.	• Den System Availability Monitor aktivieren auf Seite 23.
7	Konfigurieren Sie den Genetec™ Update Service, sodass Sie die neueste Version von Security Center und SV Control Panel erhalten können. Wenn Updates vorhanden sind, installieren Sie diese.	• Weitere Informationen finden Sie im *Genetec™ Update Service – Benutzerhandbuch* unter „Genetec Update Service konfigurieren“.
8	Wenn das SV Control Panel angibt, dass weitere Updates verfügbar sind, installieren Sie diese jetzt.	• Informationen über das Aktualisieren der SV-Software auf Seite 7.
9	Erstellen Sie die Anzahl von Archiver-Rollen, die Sie zum Unterstützen der Kameraanzahl und der gesamten Netzwerkbanbreite benötigen, die Sie für Ihre Bereitstellung planen.	• Für die Serien SV-1000E, SV-2000E, SV-4000E: Archiver-Rollen im SV Control Panel hinzufügen auf Seite 36. • Für SV-7000E und für All-in-One: Partitionen und Archiver-Rollen manuell hinzufügen auf Seite 38.
10	Melden Sie sich bei Config Tool an und konfigurieren Sie Ihre Security-Center-Video- und Zutrittskontrollfunktionen.	• Security-Center-Video- und Zutrittskontrollfunktionen aktivieren auf Seite 24. • Konfigurieren von Geräteerkennungseinstellungen auf Seite 27.
11	Sichern Sie die Security-Center-Konfiguration.	• Ihre Directory-Datenbank sichern auf Seite 34.

Von Streamvault verwendete Standardports

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

Erforderliche Ports für Streamvault™ Maintenance-Plugin

In der folgenden Tabelle werden die Ports aufgelistet, die für eingehenden Datenverkehr geöffnet sein müssen, damit das Streamvault™ Maintenance-Plugin mit der Streamvault™-Hardware kommunizieren kann.

Modul	Eingehender Port	Portverwendung
Streamvault-Hardwareüberwachung	65115	Dient der Kommunikation zwischen Security Center und dem iDRAC-Baseboard-Management-Controller der Streamvault™-Hardware über das Netzwerk.

Erforderliche Ports für Streamvault™-Systemsteuerung

In der folgenden Tabelle werden die Ports aufgelistet, die für ausgehenden Datenverkehr geöffnet sein müssen, damit die Komponenten der Streamvault™-Systemsteuerung eine Verbindung zu den Genetec™ Cloud Services herstellen können.

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

Erforderliche Ports für CylancePROTECT

In der folgenden Tabelle werden die Ports aufgelistet, die für ausgehenden Datenverkehr geöffnet sein müssen, damit der Desktop-Agent CylancePROTECT mit der Genetec™-Managementkonsole kommunizieren und Agentenaktualisierungen empfangen kann.

Ausgehender Port	Portverwendung	Ziel-URL
TCP 443	HTTPS-Kommunikation in Nordamerika	cement.cylance.com data.cylance.com protect.cylance.com update.cylance.com api.cylance.com download.cylance.com venueapi.cylance.com

Ausgehender Port	Portverwendung	Ziel-URL
TCP 443	HTTPS-Kommunikation in der Region Asien-Pazifik (Nordosten)	cement-apne1.cylance.com data-apne1.cylance.com protect-apne1.cylance.com update-apne1.cylance.com api.cylance.com download.cylance.com venueapi-apne1.cylance.com
TCP 443	HTTPS-Kommunikation in der Region Asien-Pazifik (Südosten)	cement-au.cylance.com cement-apse2.cylance.com data-au.cylance.com protect-au.cylance.com update-au.cylance.com api.cylance.com download.cylance.com venueapi-au.cylance.com
TCP 443	HTTPS-Kommunikation in Mitteleuropa	cement-euc1.cylance.com data-euc1.cylance.com protect-euc1.cylance.com update-euc1.cylance.com api.cylance.com download.cylance.com venueapi-euc1.cylance.com

Ausgehender Port	Portverwendung	Ziel-URL
TCP 443	HTTPS-Kommunikation in Südamerika	cement-sae1.cylance.com data-sae1.cylance.com protect-sae1.cylance.com update-sae1.cylance.com api.cylance.com download.cylance.com venueapi-sae1.cylance.com
TCP 443	HTTPS-Kommunikation in GovCloud	cement.us.cylance.com data.us.cylance.com protect.us.cylance.com update.us.cylance.com api.us.cylance.com download.cylance.com download.us.cylance.com venueapi.us.cylance.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).

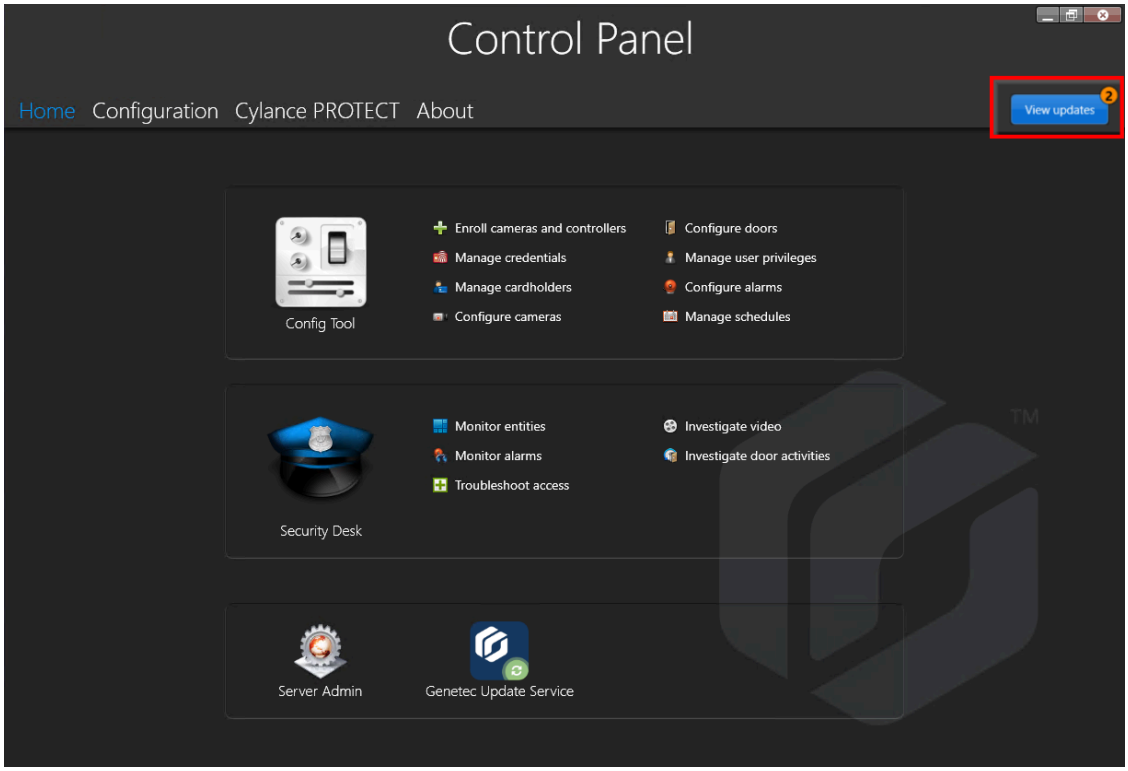
Weitere Informationen zu den Modi, in denen die Streamvault™-Appliance mit Genetec™-Verwaltungsservices kommuniziert, finden Sie unter CylancePROTECT-Seite im SV Control Panel auf Seite 62.

Informationen über das Aktualisieren der SV-Software

Das Genetec™ Update Service (GUS) ist in 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.



GUS 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*.

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.

So schließen Sie Peripheriegeräte und Strom an die Appliance an:

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
- Alarmeingaben und -ausgaben

5 Schließen Sie ein Ethernetkabel an den Ethernetanschluss der Appliance an und schließen Sie das andere Ende des Kabels an einen IP-Netzwerk-RJ-45-Anschluss an.

6 Stecken Sie bei SV-100E-Appliances den DC-Stecker in die 19,5V-Eingangsbuchse auf der Appliance an und das andere Ende in das Netzteil, schließen Sie dann 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

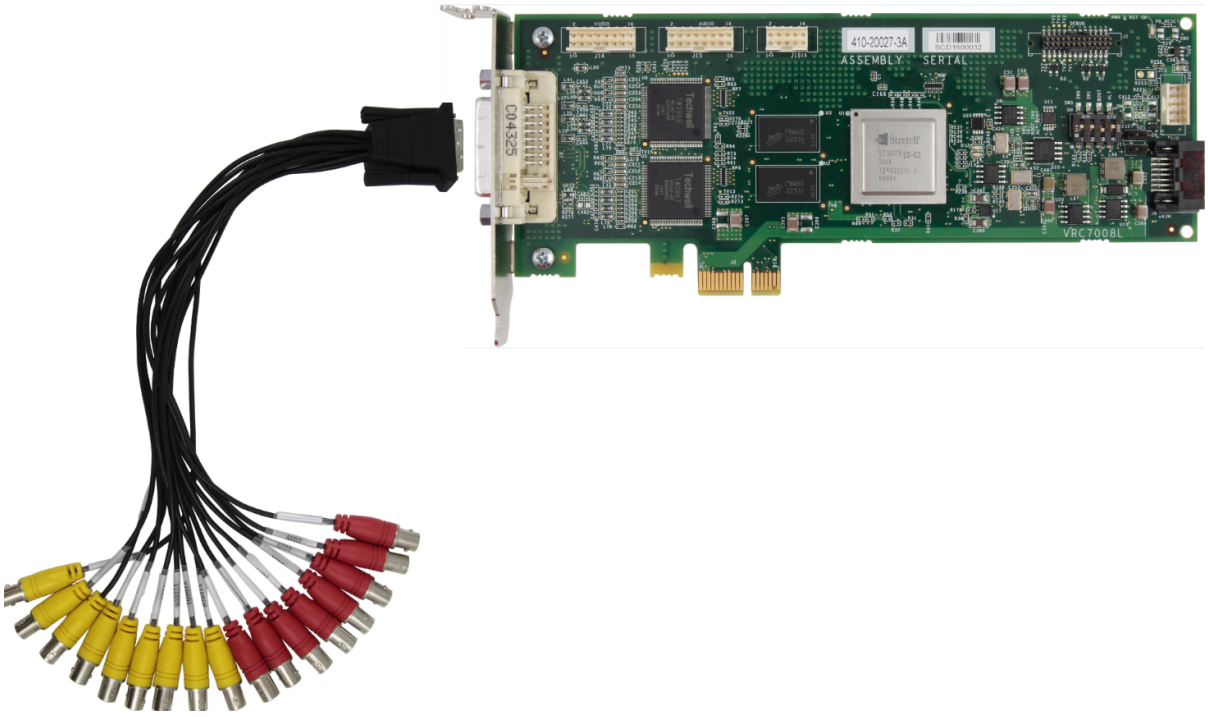
Wenn Sie eine Streamvault-Appliance verwenden, um ein Videoüberwachungssystem mit analogen Kameras zu implementieren, müssen Sie die Kameras mit der analogen Genetec™-Encoder-Karte auf der Appliance verbinden.

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, damit Sie die analogen Kameras direkt an die integrierte Encoder-Karte anschließen können.

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 über die das Geräteregistrierungs-Tool finden Sie im *Security Center – Administratorhandbuch*.

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

- Sie können analoge Kameras nicht in Security Center mithilfe der Methode *Manuell hinzufügen* hinzufügen. Sie müssen das Geräteregistrierungs-Tool verwenden.
- 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, werden alle analogen Kameras unter dem Hersteller *Genetec-Encoder-Karte* aufgelistet.

Kameraeingaben auf Encoder-Karten auf einer Streamvault-Appliance deaktivieren

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

So deaktivieren Sie Kameraeingaben auf Encoder-Karten:

1 Klicken Sie auf der 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 List 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 und Sie können Video von dieser Kamera wiedergeben.

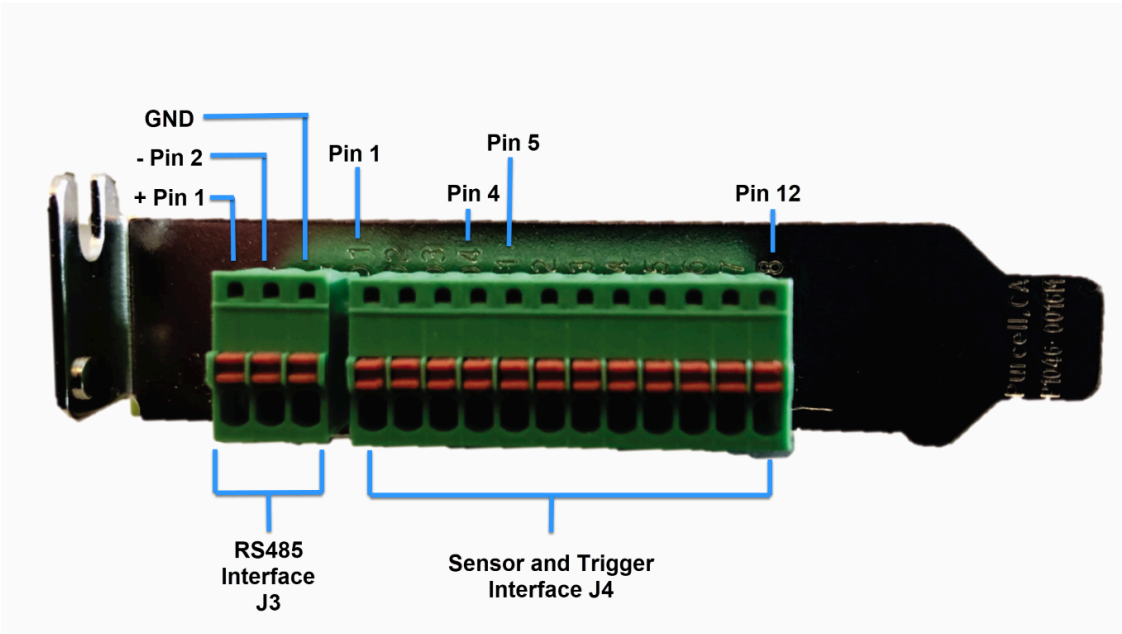
Alarmeingaben und -Ausgaben einer Streamvault-Appliance

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

Wenn Sie eine Streamvault-Appliance mit der E/A-Karte bestellen, können Sie die Eingangs- und Ausgangskabel von Hardwaregeräten direkt an die E/A-Karten auf der Rückseite der Appliance anschließen.

Die Drähte sollten mit einem kleinen Schlitzschraubendreher eingeführt werden, um die Spannklammern am Steckverbinder einzudrücken.

Informationen über das Erstellen von Event-to-Actions

Weitere Informationen über das Erstellen von Event-to-Action für Streamvault-Appliance-Eingaben und -Ausgaben finden Sie im *Security Center – Administratorhandbuch*.

Bei einer Streamvault-Appliance anmelden

Beim ersten Starten Ihrer Streamvault™-Appliance, werden Sie dazu aufgefordert, das Standard-Admin-Passwort zu ändern. Sie sollten auch das Standard-Bedienerpasswort ändern. 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

Sie müssen als Admin-Benutzer angemeldet sein, um Ihre Appliance im SV Control Panel zu konfigurieren.

WICHTIG: Passwörter müssen die folgenden Anforderungen erfüllen:

- Mindestens 10 Zeichen
- Mindestens drei Zeichen aus den folgenden vier Kategorien:
  - Großbuchstaben
  - Kleinbuchstaben
  - Basisziffern (0-9)
  - Nicht-alphanumerische Zeichen (wie $, %, !)

So melden Sie sich das erste Mal bei Ihrer Streamvault-Appliance an:

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.

Standardbenutzerkonten auf einer Streamvault-Appliance

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: • Windows: alle System- und administrativen Funktionen • Security Center • SV Control Panel	Nicht zutreffend
Operator	Bediener	• Papierkorb • Bibliotheken • Mein Computer • C: Laufwerk • SV Control Panel Startseite, Konfigurationsseite, nur regionale Einstellungen, Informationsseite • Server Admin: Admin-Password für volle Rechte erforderlich	• Windows: herunterfahren und neu starten • Systemeinstellungen • Videopartition
Nicht zutreffend	genetecfactory	Server Admin	Nicht anwendbar, bis das SV Control Panel abgeschlossen ist. **BEMERKUNG:** 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. Sie können alle Ihre Passwörter auf der Seite *Konfiguration* im Abschnitt *Benutzerkontoeinstellungen* 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 Verknüpfung **Server Admin** auf Ihrem Desktop.
- Damit Sie sich bei Server Admin von einem Remote-Computer 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.

2

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

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 auf dem SV Control Panel erfolgen, überschreiben Konfigurationsänderungen, 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.
- Die Option zum Aktivieren und Deaktivieren von Genetec™ Mobile und Synergis™ Softwire über den Abschnitt *Funktionen* der Seite *Konfiguration*, wenn diese auf der Appliance installiert sind.
- Links zu GTAP und der Produktdokumentation.
- Die CylancePROTECT-Kommunikationskonfigurationsseite zum Auswählen des Modus, in dem Ihre Streamvault™-Appliance mit der Cloud-Console kommuniziert.
- Die Möglichkeit, zusätzliche Archiver-Rollen und Partitionen für Einrichtungen auf Erweiterungsservern zu erstellen.

BEMERKUNG: Handbuch für Streamvault Control Panel 2.8 und älter.

Ihre Appliance im SV Control Panel einrichten

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.

So richten Sie Ihre Appliance ein:

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) Wählen Sie bei einer Appliance mit zwei Netzwerkschnittstellenkarten die Karte, die Sie konfigurieren möchten, aus der Liste **Netzwerkschnittstelle** aus.

Die Liste **Netzwerkschnittstelle** wird ausgeblendet, wenn nur eine Netzwerkschnittstellenkarte angeschlossen ist.

b) 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, und kicken Sie auf **Erneut versuchen**.

c) Wenn Sie die IP-Einstellungen angeben möchten, klicken Sie auf **Statische Konfiguration verwenden**, und geben Sie eine eindeutige IP-Adresse für diese Appliance ein.

d) Wenn das Feld **Status** etwas anderes als „Mit dem Internet verbunden“ anzeigt, klicken Sie auf **Erneut versuchen**.

e) 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 der Seite *Computereinrichtung* auf **Weiter**.

6 Ändern Sie auf der Seite *Sicherheit* das Password, das der Admin-Benutzer eingibt, um sich bei Windows anzumelden.

Standardmäßig wird dieses Passwort auch für die Anmeldung bei allen Genetec™-Anwendungen verwendet. Sie werden auf einer Appliance, bei der es sich nicht um einen Security-Center-Erweiterungsserver handelt, nicht dazu aufgefordert, Passwörter zu ändern.

7 Konfigurieren Sie Passwörter im Abschnitt **Sicherheit**, indem Sie auf **Passwort ändern** für die folgenden Anwendungen klicken:

- **Windows-Admin:** Das Passwort des Admin-Benutzers für Windows.
- **Client-Anwendungen:** Das Passwort des Admin-Benutzers für Security Desk, Config Tool und Genetec™ Update Service.
- **Server Admin:** Das Passwort für die Genetec™-Server-Admin-Anwendung.

8 Konfigurieren Sie die folgenden Sicherheitseinstellungen und klicken Sie dann auf **Weiter**:

- **Automatische Abmeldung:** Aktivieren Sie diese Option, wenn Sie Windows so konfigurieren möchten, dass ein Benutzer nach 15 Minuten Inaktivität abgemeldet wird.
- **Komplexität des Passworts:** Aktivieren Sie diese Option, um ein komplexes Passwort mit einer Länge von mindestens 10 Zeichen für Windows-Benutzer zu erfordern.
- **Servermanagementfunktionen:** Aktivieren Sie diese Option, um Funktionen zuzulassen, wie Rollen und andere Tasks hinzufügen mithilfe von Anwendungen wie *Windows Admin Center*, *Server Manager* oder *Windows PowerShell*.
- **Zugriff auf Wechselmedien:** Aktivieren Sie diese Option, um 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.

- **Support für Speicherkarten aktivieren:** Aktivieren Sie diese Option, um ein Speicherkartenlesegerät mithilfe der Security-Desk-Anwendung zu erstellen oder zu verwenden. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Eingehende Remote-Verbindungen:** Aktivieren Sie diese Option, um den Zugriff auf *Remotedesktop*-Verbindungen und Dateifreigabe auf der Appliance über Ihr Computernetzwerk zu erlauben. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Remotedesktop:** Aktivieren Sie diese Option, um Personen in Ihrem Netzwerk zu erlauben, sich bei der Appliance mithilfe der Anwendung *Remotedesktop* anzumelden. Die Option **Eingehende Remote-Verbindungen** muss aktiviert sein, um den Zugriff auf *Remotedesktop* zu ermöglichen. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Dateifreigabe:** Aktivieren Sie diese Option, um Dateien und Ordner, die sich auf der Appliance befinden, mit Personen in Ihrem Netzwerk zu teilen. Die Option **Eingehende Remote-Verbindungen** muss aktiviert sein, um die Dateifreigabe zu ermöglichen. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.

9 Lesen Sie die Informationen auf der Seite *Informationen über CylancePROTECT* und klicken Sie auf **Weiter**.

10 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.

WICHTIG: Wenn CylancePROTECT ausgeschaltet ist, können Sie nicht zwischen **Getrennt** und **Online** wechseln. Um diese Einstellungen zu ändern, müssen Sie das Software-Image auf Ihrer Appliance zurücksetzen.

11 Um auf Protokolle und erweiterte Funktionen für Ihr System zuzugreifen, wählen Sie **CylancePROTECT im erweiterten Schnittstellenmodus ausführen** aus.

12 Klicken Sie auf **Weiter**.

13 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.

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

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

Die Option **Aktivierungsassistent nach der Einrichtung starten** ist standardmäßig ausgewählt. Wenn Sie die Option deaktivieren, werden Sie später an die Produktaktivierung erinnert.

BEMERKUNG: Ihre Appliance muss vor der Verwendung aktiviert werden.

Nach Durchführen dieser Schritte

Aktivieren Sie Ihre Appliance.

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.

So aktivieren Sie Ihre Security-Center-Lizenz mithilfe einer System-ID:

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 zu dieser Zeit nicht bereit war, schlägt die Update-Überprüfung möglicherweise mit dieser Meldung fehl: *Es kann derzeit nicht nach Updates gesucht werden. Wir versuchen es später erneut.*

7 Aktivieren oder deaktivieren Sie Synergis™ Softwire 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

Eine Lizenz manuell über Server Admin ändern auf Seite 21
Informationsseite des SV Control Panel auf Seite 63
Lizenzoptionen auf Seite 63

Eine Lizenz manuell über Server Admin ändern

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

So aktivieren Sie eine Lizenz manuell über Server Admin:

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**.

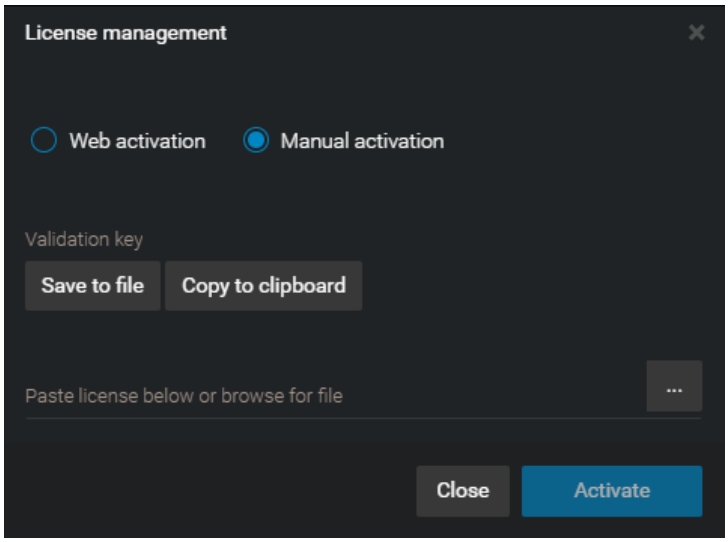
c) Melden Sie sich im Server Admin an.

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 Holen Sie die Lizenz vom GTAP:
   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* im Abschnitt *Lizenzinformationen* auf **Lizenz aktivieren**.
   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 19

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, wie im *System Availability Monitor – Benutzerhandbuch* beschrieben.

So aktivieren Sie den System Availability Monitor Agent:

1 Öffnen Sie SV Control Panel.

2 Klicken Sie auf der Seite *Konfiguration* unter dem 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 Videoüberwachung 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.

So aktivieren Sie Security-Center-Video- und Zutrittskontrollfunktionen:

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, ist sie in der Liste nicht verfügbar.

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 Zutrittskontrolleinheiten an und klicken Sie auf **Weiter**.

9 Wählen Sie auf der Seite *Karteninhaber* aus, wie Sie Berechtigungsnachweise (Karten) und Karteninhaber hinzufügen möchten.

a) Wählen Sie aus, ob Sie Karteninhaber (wenn der Security-Center-Installationsassistent geschlossen wird) über den Task *Karteninhaberverwaltung* 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.
- **Bericht:** 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. Zusätzlich kann ein Supervisor auch die Wartungstasks verwenden, Karteninhaber 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 Systemeinrichter.
- **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 Administrator-Handbuch* .

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 30
Benutzerdefinierte Aufzeichnungszeitpläne erstellen auf Seite 32
Startseite des SV Control Panel auf Seite 54

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 (Erkennungsport, 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*.

Verwandte Themen

Config-Tool-Kürzel im SV Control Panel auf Seite 54

Das Geräteregistrierungs-Tool öffnen

Es gibt drei Möglichkeiten, um das Geräteregistrierungs-Tool zu öffnen.

So öffnen Sie das Geräteregistrierungs-Tool:

- Führen Sie eine der folgenden Aktionen aus:
  - Klicken Sie auf der Seite *Start* 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** > **Geräteregistrierung**.
  - Klicken Sie auf der *Startseite* des SV Control Panel auf das **Config-Tool**-Symbol und dann auf das Symbol **Einheitenstatus hinzufügen** 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.

So konfigurieren Sie Erkennungseinstellungen:

1 Klicken Sie auf der Homepage auf **Tools** > **Geräteerkennung**.

2 Klicken Sie im Dialogfeld *Geräteerkennung* auf **Einstellungen und Hersteller** ( ).

3 Stellen Sie folgende Optionen ein:

- **Immer umfangreiche Suche ausführen**. Schalten Sie diese Option ein, wenn alle Geräte auf dem System erkannt werden sollen.

  BEMERKUNG: Es können dabei auch Geräte anderer Hersteller erkannt werden, das UPnP und *Zero config* bei der Suche verwendet werden.
- **Standardauthentifizierung ablehnen** (nur Videogeräte). Verwenden Sie diesen Schalter, um eine Basic-Authentifizierung zuzulassen oder zu deaktivieren. 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 Basic-

Authentifizierung unterstützt. Um die Basic-Authentifizierung wieder anzuschalten, müssen Sie **Basic-Authentifizierung ablehnen** auf **Aus** stellen.

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

4 Klicken Sie auf **Hersteller hinzufügen** (), um einen Hersteller in die Liste der zu erkennenden Geräte hinzuzufügen.

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 ignorierter Geräte (siehe Entfernen von Einheiten aus der Liste ignorierter Geräte auf Seite 29).

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.

So fügen Sie ein Gerät hinzu:

1 Klicken Sie auf der Homepage auf **Tools** > **Geräteerkennung**.

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 ein einzelnes Gerät 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.

So löschen Sie hinzugefügte Einheiten:

1 Fügen Sie die erkannten Einheiten zu Ihrem System hinzu, siehe Hinzufügen von Geräten auf Seite 28.

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.

So ignorieren Sie ein Gerät:

1 Klicken Sie auf der Homepage auf **Tools** > **Geräteerkennung**.

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 ignorierter Geräte, siehe Entfernen von Einheiten aus der Liste ignorierter Geräte auf Seite 29.

Entfernen von Einheiten aus der Liste ignorierter Geräte

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

So entfernen Sie eine Einheit aus der Liste der ignorierten Geräte:

1 Klicken Sie auf der Homepage auf **Tools** > **Geräteerkennung**.

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.

So konfigurieren Sie die Standardkameraeinstellungen:

1 Öffnen Sie die Aufgabe *Video* über die Config Tool-Homepage.

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.

Die verfügbaren Zeitpläne umfassen Zeitpläne, die über die Ansicht **Zeitpläne** im Task *System* erstellt wurden oder den benutzerdefinierten Zeitplan, wenn einer im Security-Center-Installationsassistent 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 **Anwenden**.

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 24

Benutzerdefinierte Aufzeichnungszeitpläne erstellen

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

So richten Sie einen Zeitplan ein:

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.

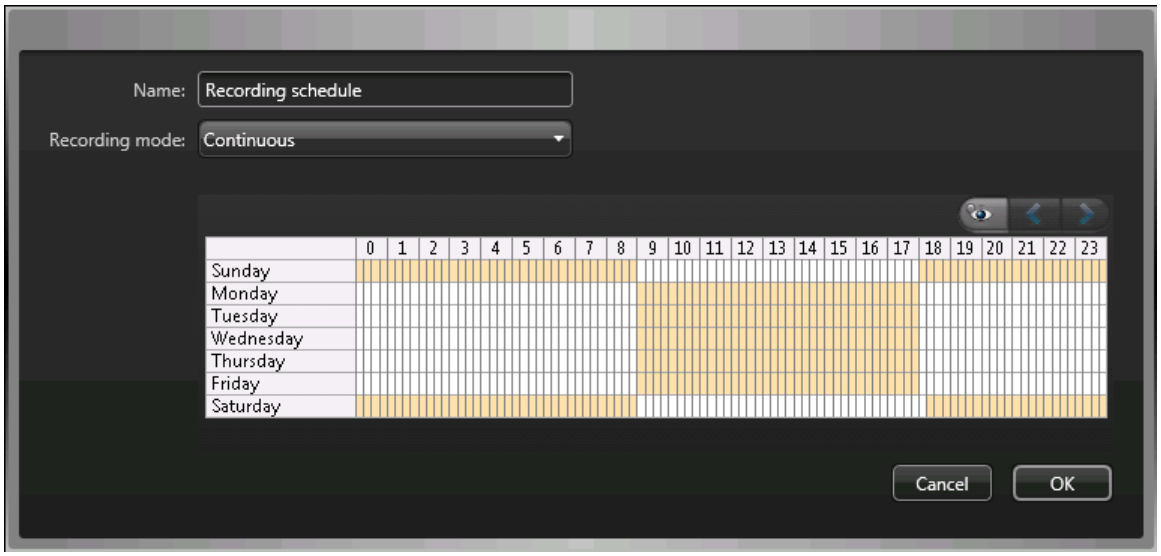
  BEMERKUNG: Wenn die Einstellung **Manuell** verwendet wird, dann löst Bewegung keine Aufzeichnung aus.
- **Benutzerdefiniert:** Sie können einen Zeitplan für die Aufzeichnung festlegen.

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

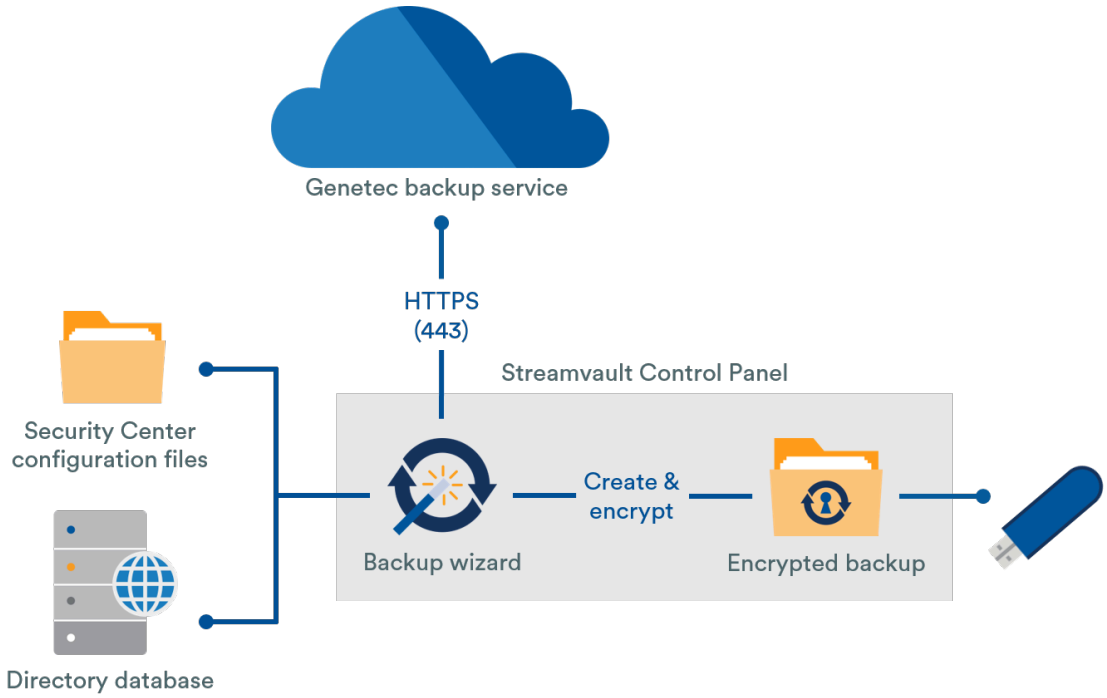
Security-Center-Video- und Zutrittskontrollfunktionen aktivieren auf Seite 24

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

- Sie können Ihre Dateien einfach in der Cloud oder lokal mithilfe des *Sicherungsassistenten* sichern. Wenn Sie Dateien in der Cloud sichern, werden die neuesten fünf Sicherungen aufbewahrt.
- 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-5.6-System auf einem Security-Center-5.5-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-5.5-Systems auf einem Security-Center-5.6-System wiederherstellen.

Verwandte Themen

Ihre Directory-Datenbank sichern auf Seite 34
Ihre Directory-Datenbank wiederherstellen auf Seite 35

Ihre Directory-Datenbank sichern

Um die Konfiguration Ihres Systems nach einem Hardware-Upgrade zu vereinfachen oder Ihre Konfigurationen nach einem Systemausfall wiederherzustellen, können Sie Ihre Directory-Datenbank und Konfigurationsdateien mithilfe von „Sichern und Wiederherstellen“ sichern.

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

- Security Center 5.5 oder neuer ist installiert.
- Genetec™ Server wird ausgeführt
- Sie haben eine gültige und aktive Lizenz.

Was Sie noch wissen sollten

- Sie können Ihre Dateien einfach in der Cloud oder lokal mithilfe des *Sicherungsassistenten* sichern. Wenn Sie Dateien in der Cloud sichern, werden die neuesten fünf Sicherungen aufbewahrt.
- Nur Administratoren können eine Sicherung durchführen und alle Sicherungen in der Cloud müssen authentifiziert werden.

So sichern Sie die Directory-Datenbank und die Konfigurationsdateien:

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**.

- **Cloud**. 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:** Sie müssen Ihr eigenes Passwort erstellen und es sich merken, um es später für die Verschlüsselung Ihrer Sicherungsdateien zu verwenden.
    WICHTIG: Wenn Sie Ihr Passwort verlieren oder vergessen, kann Genetec Inc. das Passwort nicht wiederherstellen.
- **Lokal**. 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 dir restlichen Schritte im Assistenten, um Ihre Sicherung abzuschließen.

Verwandte Themen

Informationen über Sichern und Wiederherstellen auf Seite 33
Ihre Directory-Datenbank wiederherstellen auf Seite 35

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 in Fällen wie einem Systemausfall oder Hardware-Upgrade zur gleichen System-ID wiederherstellen.

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

- Security Center 5.5 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.

So stellen Sie die Directory-Datenbank und die Konfigurationsdateien wieder her:

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 dir restlichen Schritte im Assistenten, um den Wiederherstellungsvorgang abzuschließen.

Verwandte Themen

Ihre Directory-Datenbank sichern auf Seite 34
Informationen über Sichern und Wiederherstellen auf Seite 33

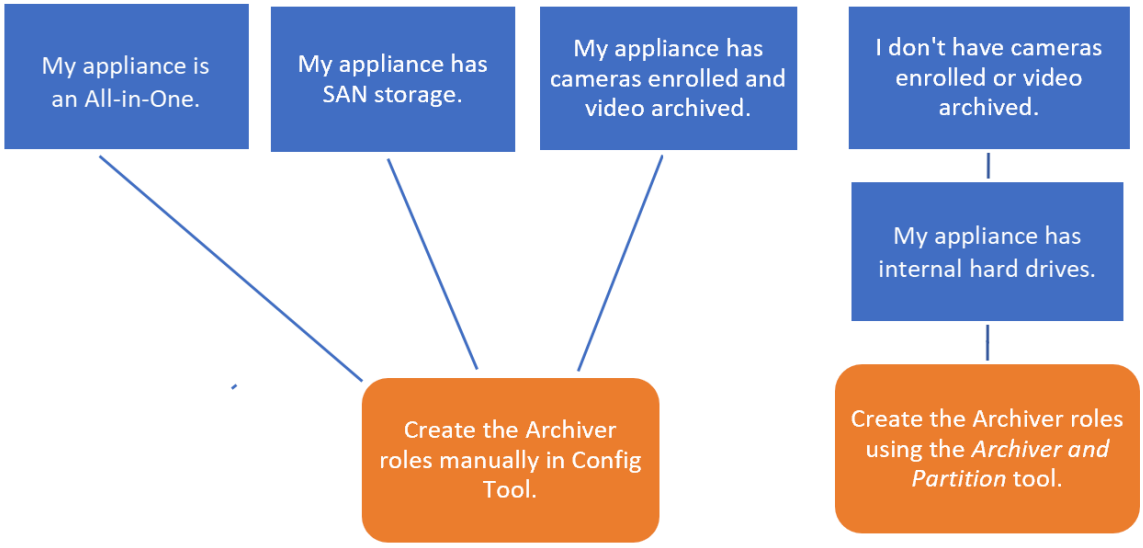
Die Methode für das Erstellen von Archiver-Rollen und Partitionen auswählen

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 *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 tool im SV Control Panel

Das Tool für Archiver-Rollen und Partitionen 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 SV-7000E-Appliance einrichten, befolgen Sie die Schritte unter Partitionen und Archiver-Rollen manuell hinzufügen auf Seite 38.

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

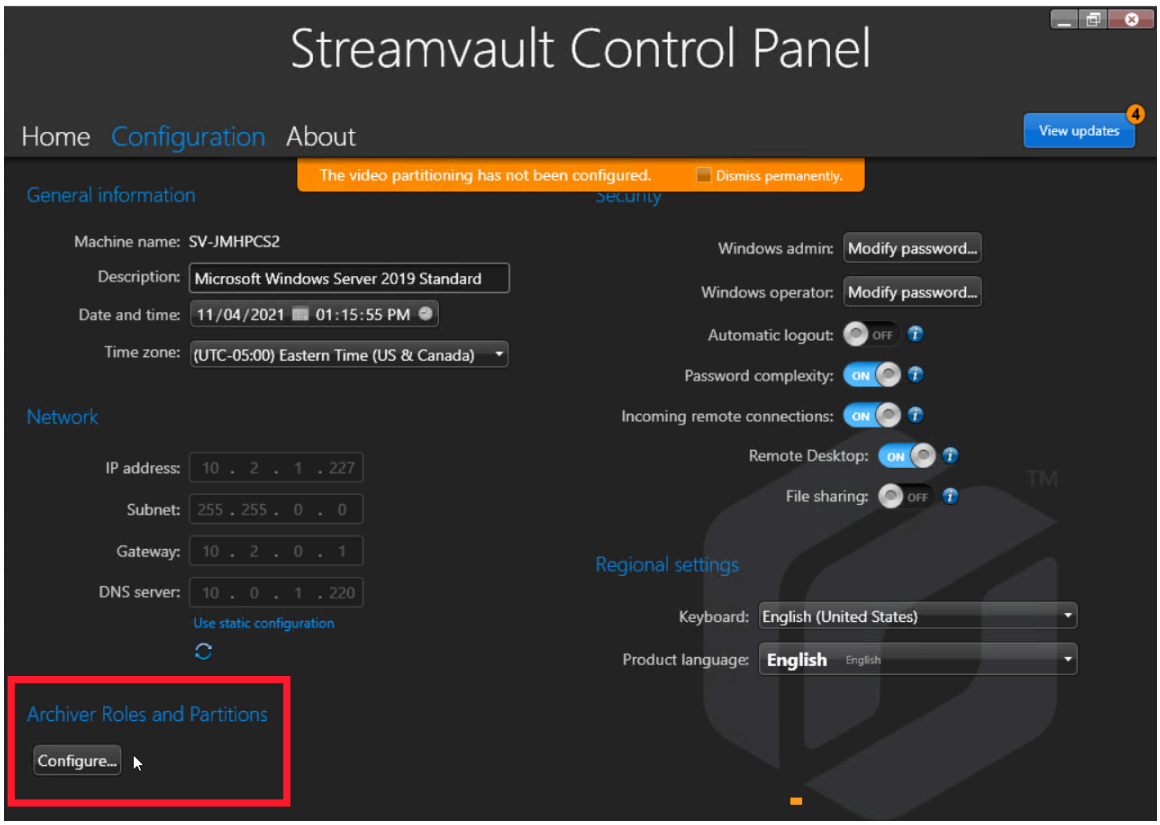
- Wählen Sie die entsprechende Methode für das Erstellen von Archiver-Rollen und Partitionen aus.
- Sichern Sie die wichtigen Daten auf der Festplatte, auf der Sie eine Partition erstellen möchten.

  ACHTUNG: Das Tool für Archiver-Rollen und Partitionen kann bestehende Daten löschen, einschließlich der Archiver-Rollenkonfiguration und aller Dateien auf dem D:-Laufwerk.

So erstellen Sie zusätzliche Archiver-Rollen und Laufwerkpartitionen:

1 Klicken Sie im SV Control Panel auf die Registerkarte **Konfiguration**.

2 Klicke Sie unter *Archiver-Rollen und Partitionen* auf **Konfigurieren**.



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

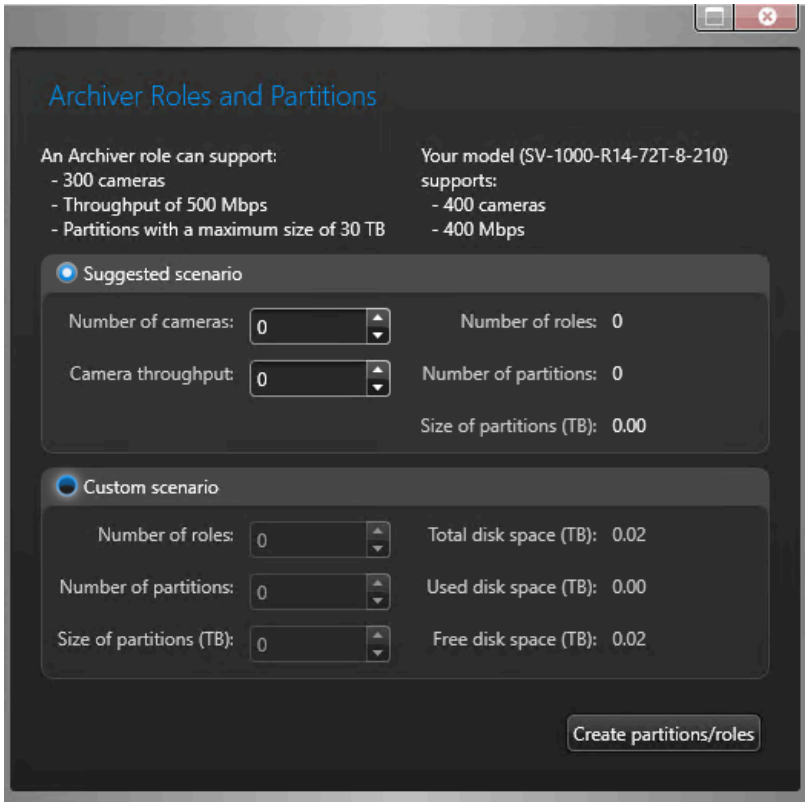
3 Wählen Sie eine der folgenden Optionen aus, um die Anzahl der Archiver-Rollen und Partitionen zu konfiguriere:

- 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 zu erstellenden Archiver-Roller und Partitionen anzugeben, wählen Sie **Benutzerdefiniertes Szenario** aus und geben Sie die Anzahl der Archiver-Rollen, die Anzahl von Partitionen und die Partitionsgröße ein.

  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**.



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 Laufwerkbuchstabe zugewiesen.

Partitionen und Archiver-Rollen manuell hinzufügen

Um Ihre SV-7000E- oder SV-300E-All-in-One-Appliance zum ersten Mal einzurichten, müssen Sie manuell Partitionen erstellen. Sie können Archiver-Rollen auch manuell zu einer Appliance hinzufüge, 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.

So verteilen Sie Kameras auf mehrere Archiver-Rollen:

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. Sehen Sie unter „Kameraeinstellungen anzeigen“ im *Security Center – Benutzerhandbuch* nach.

2 Erstellen Sie die Laufwerke, die Sie für die Archiver-Rollen benötigen, die Sie auf der Appliance erstellen möchten.

- Erstellen Sie auf Appliances, die SAN-Speicher haben, wie SV-7000E, 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:

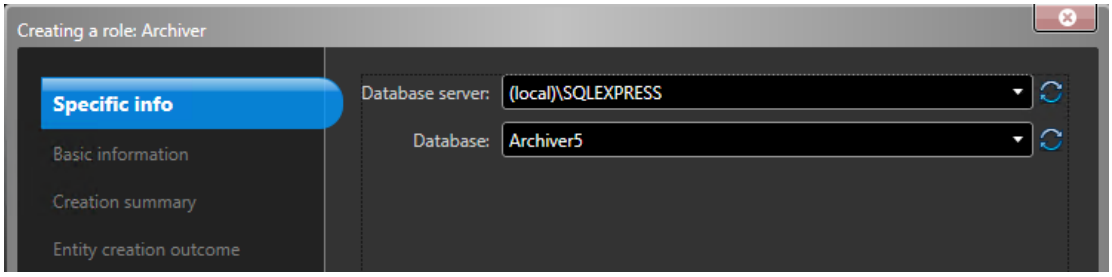
a) Öffnen Sie auf der Config-Tool-Startseite den Task *System* und klicken Sie auf die Ansicht **Rollen**.

b) Klicken Sie auf **Eine Entität hinzufügen** und wählen Sie **Archiver** aus.

Der Assistent für die Archiver-Rollenkonfiguration wird geöffnet.

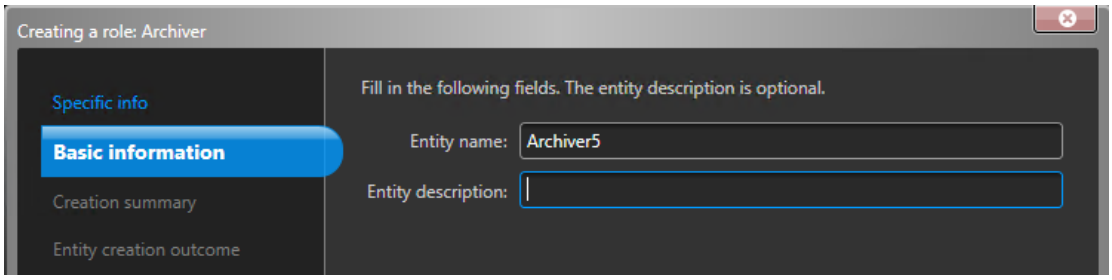
c) Geben Sie auf der Seite *Spezifische Informationen* einen Namen für die Archiver-Rollen**datenbank** ein und klicken Sie auf **Weiter**.

Jede Archiver-Rolle muss eine dedizierte Datenbank haben.



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.



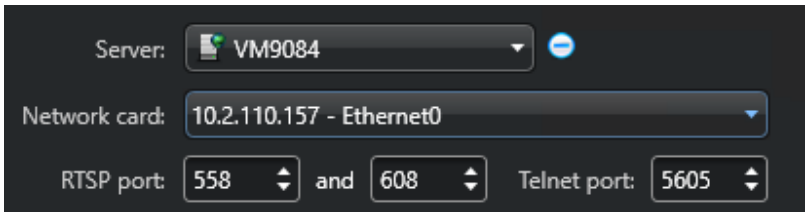
e) Vergewissern Sie sich, dass die Informationen, die auf der Seite *Zusammenfassung des Anlegens* gezeigt werden, korrekt sind und klicken Sie dann auf **Erstellen**.

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 ⊕, um den Abschnitt *Server* zu erweitern und wählen Sie eine NIC aus der Liste **Netzwerkkarte** aus.

Alle Archiver-Rollen müssen die gleiche NIC verwenden.



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 **Anwenden**.

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 **Anwenden**.

3

Erste Schritte mit dem Streamvault – Wartung-Plugin

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

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

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 Alarme 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.
- **iDRAC-Integration**: haben Sie eine präzisere Kontrolle über die Verwaltung von Berechtigungsnachweisen. Diese Funktion befindet sich auf der Registerkarte **Management** des Plugins.

  WICHTIG:

  - Die iDRAC-Firmware muss Version 6.0 oder neuer haben.
  - Das Streamvault – Wartung-Plugin greift auf Integritätsdaten mithilfe von Out-of-Band-Kommunikation mit iDRAC zu. Das bedeutet, dass es eine Netzwerkverbindung zwischen dem dedizierten iDRAC-Port und mindestens einem LAN-Port geben muss, 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-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip.
  - Eine Konfiguration mithilfe von iDRAC ist für die meisten Benutzer nicht relevant. Kontaktieren Sie das Streamvault-Produktteam, um weitere Informationen zu erhalten.
  - Handbuch für das Streamvault-Maintenance-Plugin 1.0.

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 Folgendes sicher:

- Eine kompatible Version von Security Center ist installiert.

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.

So installieren Sie das Plugin:

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 den Genetec™ Server jedoch 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 – Härtungsleitfaden*.

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 Rechte für	Aktionen, die ausgeführt werden können
Hardwareüberwachung	Hardwareüberwachung bearbeiten	• Alarmkonfigurationen bearbeiten • E-Mail-Empfänger bearbeiten • Remote-Management-Benachrichtigungsnachweise bearbeiten • Porteinstellungen ändern
	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	• Alarmkonfigurationen stapelweise bearbeiten • E-Mail-Empfänger stapelweise bearbeiten

Unterkategorie von Berechtigungen	Umfasst Rechte 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™-Hardwareüberwachungsentitäten 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, müssen Sie eine Rolle für diese Server nur dann erstellen, wenn Sie die Managerentität verwenden möchten.

So erstellen Sie eine Plugin-Rolle:

1 Öffnen Sie auf der Config-Tool-Startseite die 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.

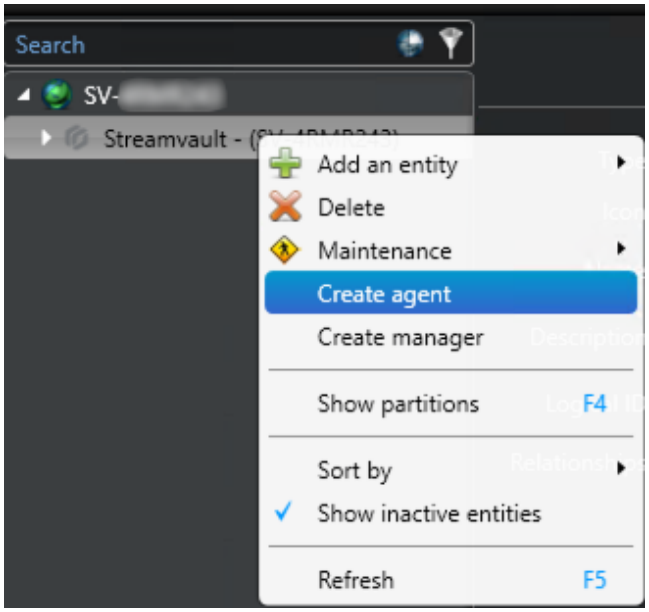
Bevor Sie beginnen

- Registrieren Sie Ihre Streamvault-Appliances.
- Erstellen Sie die Streamvault-Plugin-Rolle.
- **WICHTIG:** Ein Agent wird automatisch auf jedem Streamvault-Server erstellt, der eine Streamvault-Rolle hostet. Wenn der Agent nicht in Ihrem System vorhanden ist, nachdem Sie die Rolle erstellt haben, müssen Sie den Agenten manuell erstellen.

So konfigurieren Sie eine Streamvault-Hardwareüberwachungsentität:

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**.

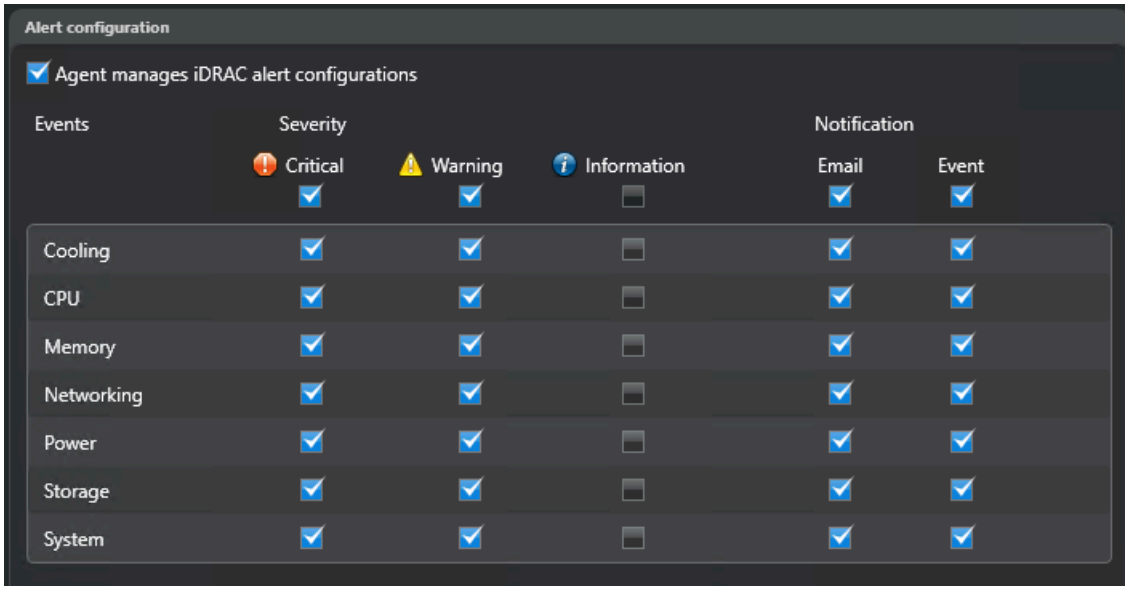


3 Geben Sie auf der Registerkarte **Identität** einen Namen für die Streamvault-Hardwareüberwachung im Feld **Name** ein.

4 Konfigurieren Sie auf der Registerkarte **Allgemein** Folgendes:

a) Um Alarmkonfigurationen über die Streamvault-Hardwareüberwachungsrolle zu verwalten, aktivieren Sie das Kontrollkästchen **Agent verwaltet iDRAC-Alarmkonfigurationen**.

b) Aktivieren Sie im Bereich **Alarmbenachrichtigung** die Kontrollkästchen, die den Typen von **Ereignissen**, dem **Schweregrad** und den **Benachrichtigungstypen** entsprechen, die Sie für diese Streamvault-Hardwareüberwachung einschließen möchten.



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

6 (Optional) Aktivieren Sie im Abschnitt **Berechtigungsnachweise für Remote-Management** das Kontrollkästchen **Agent verwaltet iDRAC-Konto**, um Berechtigungsnachweise direkt über das Plugin zu steuern.

7 (Optional) Deaktivieren Sie im Abschnitt **Berechtigungsnachweise für Remote-Management** das Kontrollkästchen **Agent verwaltet iDRAC-Konto**, um iDRAC zum Steuern der Benutzer- und Passworterstellung zu verwenden.

8 (Optional) Wenn Sie das Kontrollkästchen **Agent verwaltet das iDRAC-Konto** deaktiviert haben, navigieren Sie zur Registerkarte **Management** und konfigurieren Sie die Anmeldedaten direkt in iDRAC.

9 (Optional) Sie können im Abschnitt **eingehender Port** den Standardport von 65115 zu einem Port Ihrer Wahl ändern. Weitere Informationen dazu finden Sie unter Von Streamvault verwendete Standardports auf Seite 4.

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 und Benachrichtigungen einzurichten, die über auftretende Probleme informieren. Die Streamvault-Managerentität wird nur dafür verwendet und ist optional.

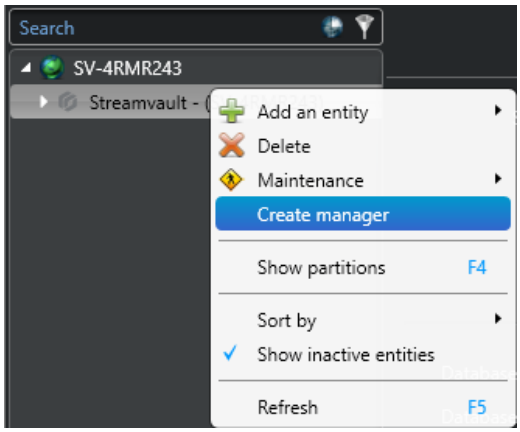
Bevor Sie beginnen

- Registrieren Sie Ihre Streamvault-Geräte.
- Erstellen Sie die Streamvault-Plugin-Rolle.

So konfigurieren Sie eine Streamvault-Managerentität:

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**.

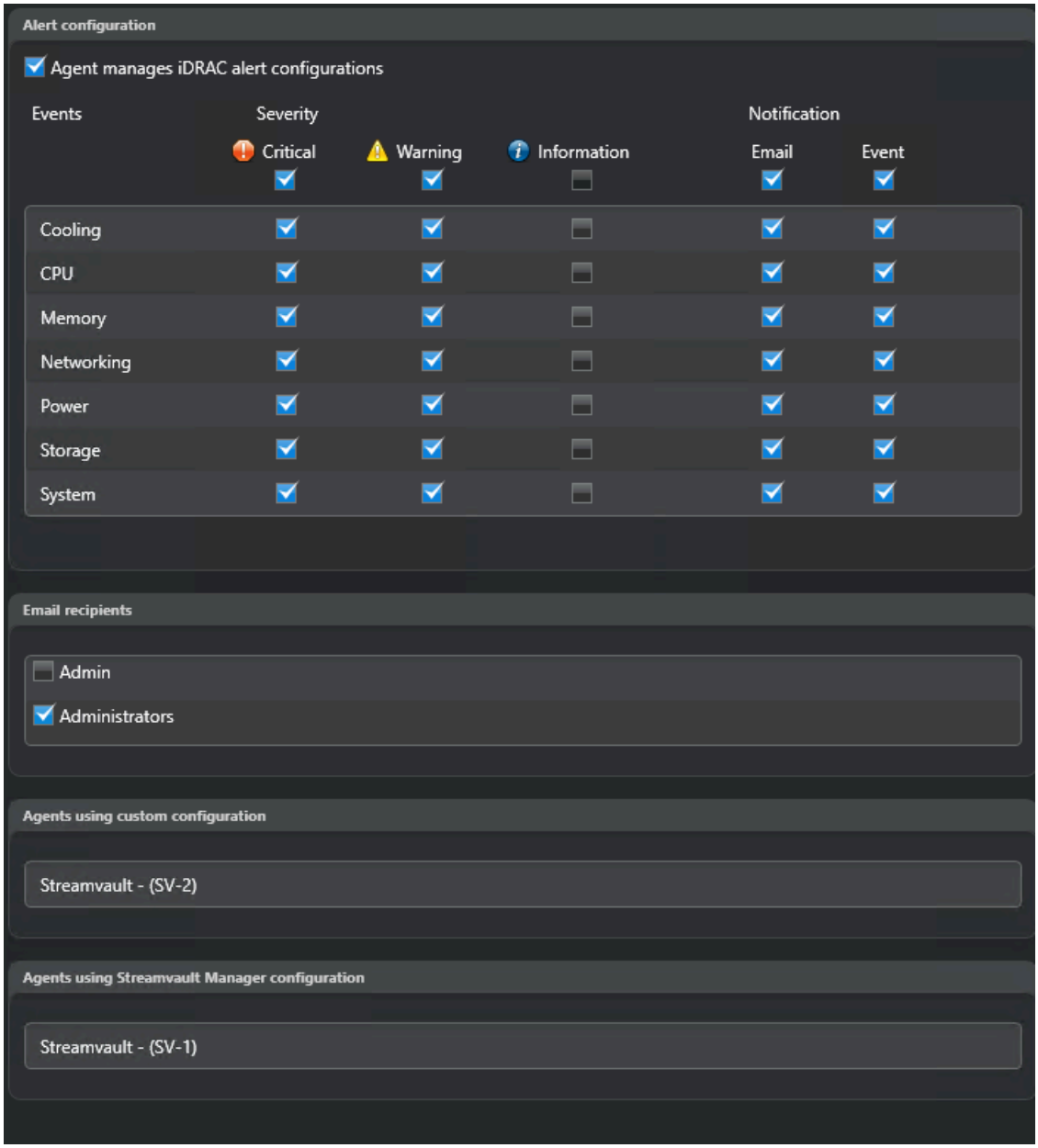


3 Konfigurieren Sie auf der Registerkarte **Allgemein** Folgendes:

a) Um Warnungskonfigurationen über die Streamvault-Managerkonfigurationen zu verwalten, aktivieren Sie das Kontrollkästchen **Agent verwaltet iDRAC-Alarmkonfigurationen**.

b) Aktivieren Sie im Bereich **Alarmbenachrichtigung** die Kontrollkästchen, die den Typen von **Ereignissen**, dem **Schweregrad** und den **Benachrichtigungstypen** entsprechen, die Sie in

Streamvault – Wartung-Plugininstanzen einschließen möchten, die von diesem Streamvault-Manager gesteuert werden.



BEMERKUNG: Streamvault-Instanzen, deren Konfigurationen über den Streamvault-Manager festgelegt werden, werden im Abschnitt **Agenten, die die Streamvault-Managerkonfiguration verwenden** angezeigt.

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

5 (Optional) Aktivieren Sie im Abschnitt **Berechtigungsnachweise für Remote-Management** das Kontrollkästchen **Agent verwaltet iDRAC-Konto**, um Berechtigungsnachweise direkt über das Plugin zu steuern.

6 (Optional) Deaktivieren Sie im Abschnitt **Berechtigungsnachweise für Remote-Management** das Kontrollkästchen **Agent verwaltet iDRAC-Konto**, um iDRAC zum Steuern der Benutzer- und Passworterstellung zu verwenden.

7 (Optional) Wenn Sie das Kontrollkästchen **Agent verwaltet das iDRAC-Konto** deaktiviert haben, navigieren Sie zur Registerkarte **Management** und konfigurieren Sie die Anmeldedaten direkt in iDRAC.

Die Integrität der Streamvault-Appliance überprüfen

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

So können Sie den Integritätsstatus Ihrer Streamvault-Appliances anzeigen:

1 Öffnen Sie auf der Startseite den Task *Streamvault-Hardware*.

2 **Time range** query filter, define the time period you want the report to include.

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.

4

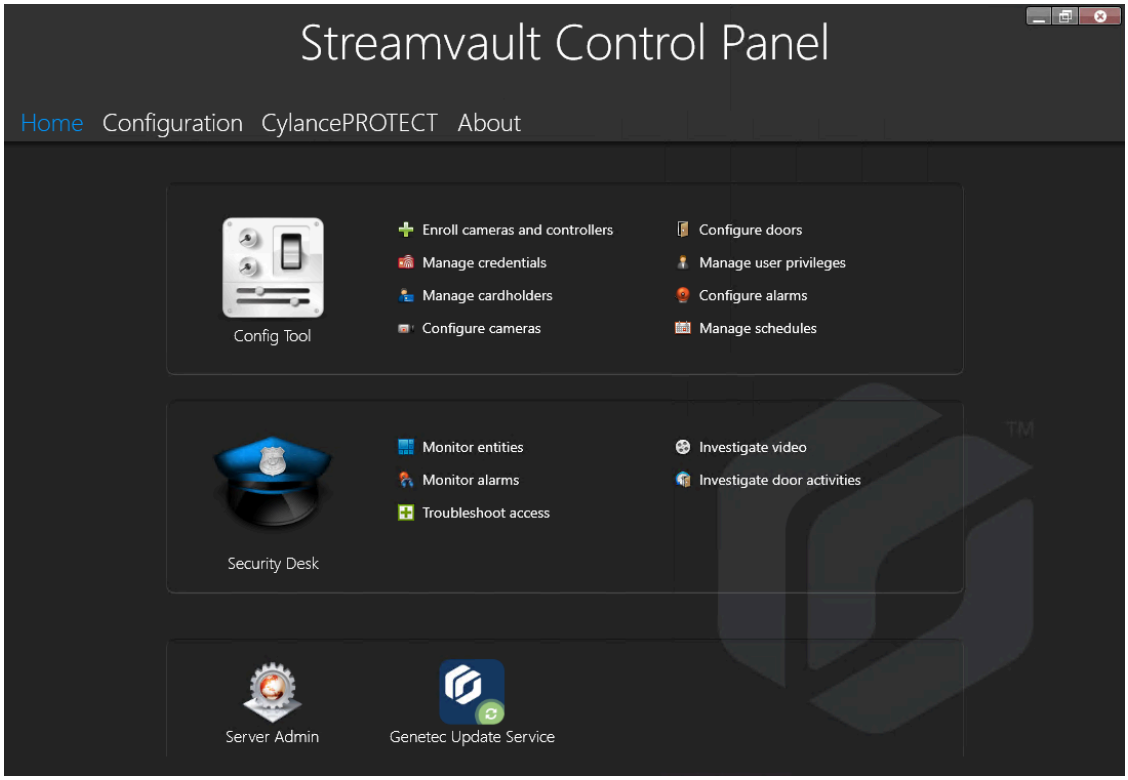
SV Control Panel – Referenz

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

Dieser Abschnitt enthält die folgenden Themen:

Startseite des SV Control Panel

Verwenden Sie die *Startseite*, 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-Verknüpfungen klicken, um die entsprechenden Tasks zu öffnen.

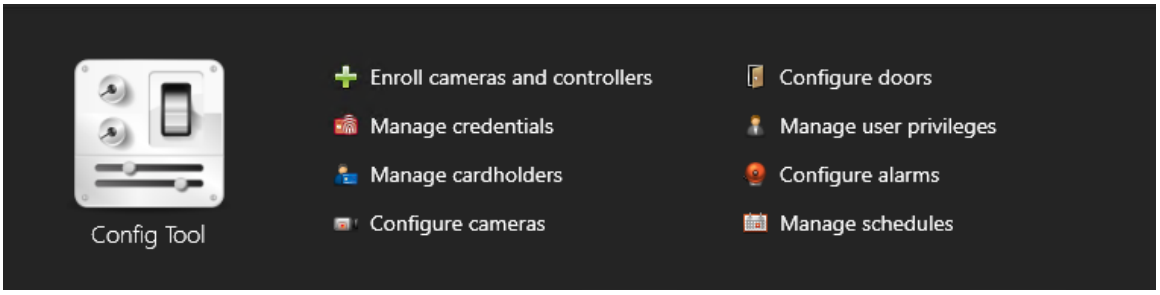
Bei Systemen, die im Client-Modus ausgeführt werden, ist das Server-Admin-Kürzel nicht verfügbar. Ebenso sind die Kürzel für Config Tool und Security Desk eingeschränkt.

BEMERKUNG: Wenn Ihr System nicht aktiviert ist, werden Sie durch ein rotes Banner benachrichtigt. Klicken Sie auf **Das System ist nicht aktiviert. Klicken Sie hier** , um den Assistenten *Aktivierung des Streamvault Control Panel* zu öffnen.

Config-Tool-Kürzel im SV Control Panel

Verwenden Sie die Tastaturkürzel zum Öffnen der Haupttasks in Config Tool.

Die verfügbaren Kürzel hängen von Ihren Lizenzoptionen ab.



- **Config Tool:** Klicken Sie auf das Symbol, um Config Tool zu öffnen.

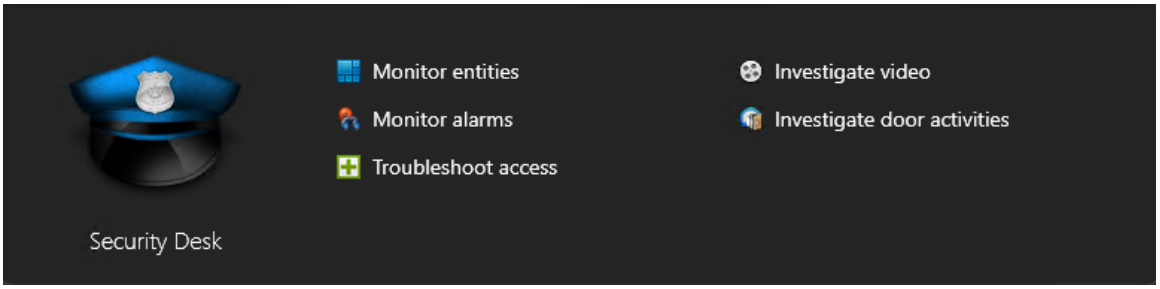
Verwandte Themen

Über das Geräteregistrierungs-Tool auf Seite 27

Security-Desk-Kürzel im SV Control Panel

Verwenden Sie die Verknüpfungen, um die Haupttasks in der Security-Desk-Anwendung zu öffnen.

Die verfügbaren Kürzel hängen von Ihren Lizenzoptionen ab.



- **Security Desk:** Klicken Sie auf das Symbol, um Security Desk zu öffnen.
- **Entitäten überwachen:** Klicken Sie, um den Task *Überwachung* zu öffnen und Systemereignisse in Echtzeit zu überwachen.
- **Alarme überwachen:** Klicken Sie, um den Task *Alarmüberwachung* zu öffnen und aktive Alarme zu überwachen und darauf zu reagieren sowie vergangene Alarme anzuzeigen.
- **Zutrittsfehlerbehebung:** Klicken Sie, um das Zutrittsfehlerbehebungs-Tool zu öffnen, um Konfigurationsprobleme zu diagnostizieren und darauf zuzugreifen.

  BEMERKUNG: Dieses Kürzel ist nicht für Systeme verfügbar, die im Client-Modus ausgeführt werden.
- **Video untersuchen:** Klicken Sie, um den Task *Archive* zu öffnen und nach Videoarchiven zu suchen.

  BEMERKUNG: Dieses Kürzel ist nicht für Systeme verfügbar, die im Client-Modus ausgeführt werden.
- **Türaktivitäten untersuchen:** Klicken Sie, um den Task *Türaktivitäten* zu öffnen, um Ereignisse bei ausgewählten Türen zu untersuchen.

  BEMERKUNG: Dieses Kürzel ist nicht für Systeme verfügbar, die im Client-Modus ausgeführt werden.

Server Admin im SV Control Panel

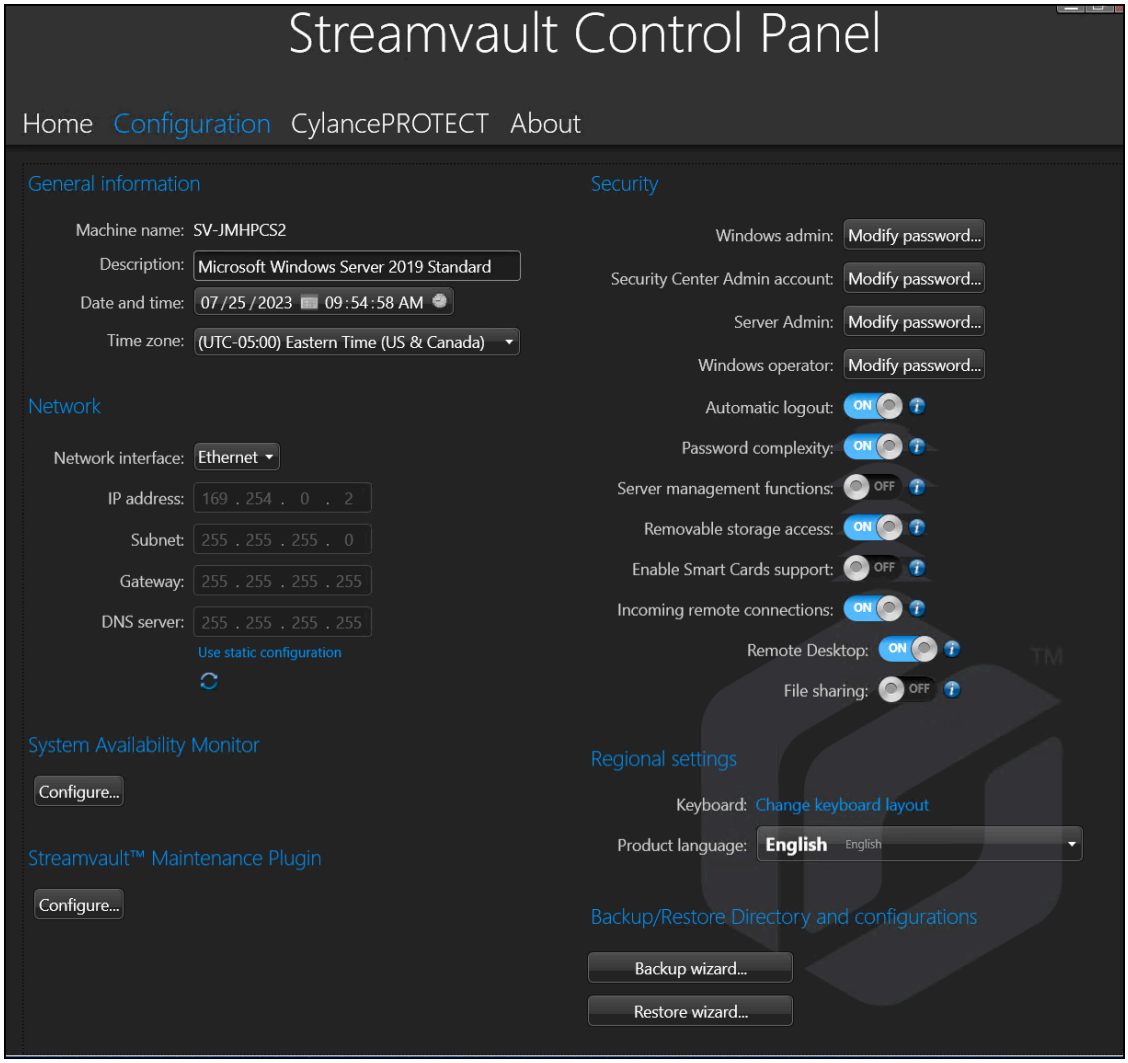
Verwenden Sie die Server-Admin-Anwendung, um eine Lizenz manuell anzuwenden oder die Konfiguration des Servers anzuzeigen und zu ändern.

Genetec Update Service im SV Control Panel

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

Konfigurationsseite des SV Control Panel

Verwenden Sie die Seite *Konfiguration* des SV Control Panel, um allgemeine Einstellungen wie *Netzwerkeinstellungen*, *Einstellungen für den System Availability Monitor*, *Benutzerkonten* und *regionale Einstellungen* anzupassen.



In Systemen, die auf einem Erweiterungsserver oder im Client-Modus ausgeführt werden, sind die Abschnitte *System Availability Monitor*, *Funktionen* und *Directory und Konfigurationen sichern/wiederherstellen* nicht verfügbar. Ebenso können im Abschnitt *Sicherheit* nur die Passwörter für **Windows-Admin** und **Windows-Bediener** geädert werden.

Einstellunfen für allgemeine Informationen

Verwenden Sie den Abschnitt *Allgemeine Informationen* der Seite *Konfiguration*, um allgemeine Einstellungen zu ändern, wie den Namen Ihrer Streamvault™-Appliance.

- **Computername.:** Zeigt den Namen des SV-Computers an.
- **Beschreibung:** Geben Sie

- **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 Uhrsymbol im Feld klicken, um die Einstellungen. zu konfigurieren.
- **Zeitzone:** Wählen Sie eine Zeitzone aus der Drop-down-Liste aus.

Netzwerkeinstellungen

Verwenden Sie den Abschnitt *Netzwerk* der Seite *Konfiguration*, um Netzwerkeinstellungen wie die IP-Adresse Ihrer Streamvault™-Appliance zu ändern.

- **Netzwerkschnittstelle:** Wählen Sie die Netzwerkkarte aus, die Sie konfigurieren möchten.
  BEMERKUNG: Diese Option ist nicht verfügbar, wenn nur eine Netzwerkkarte angeschlossen ist.
- **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.
- **Statische Konfiguration verwenden:** Wählen Sie diese Option, wenn die IP-Adresse von Ihrem DHCP (Dynamic Host Configuration Protocol)-Server nicht dynamisch zugewiesen werden soll. Das Dynamic Host Configuration Protocol (DHCP) wird verwendet, um die IP-Adresse, das Subnetz, Gateway und den DNS-Server automatisch zuzuweisen.
- **aktualisieren (nur DHCP):** Klicken Sie, um Ihre DHCP-Einstellungen zu aktualisieren und eine neue IP-Adresse zu erhalten.

Einstellungen im System Availability Monitor

Verwenden Sie den Abschnitt *System Availability Monitor* der Seite *Konfiguration*, um Einstellugen 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.

Funktionsinformationen

Verwenden Sie den Abschnitt *Funktionen* der Seite *Konfiguration*, um die zusätzlichen Funktionen, die Sie erworben haben, anzuzeigen und zu aktivieren.

Die folgenden Funktionen können aktiviert werden:

- Security Center Mobile
- Synergis™ Softwire

BEMERKUNG: Wenn Security Center Mobile oder Synergis Softwire nicht installiert sind, werden die entsprechenden Optionen nicht im Abschnitt *Funktionen* angezeigt. Security Center Mobile ist nur für Security Center 5.7 und älter verfügbar. In Systemen, die Security Center 5.8 GA und neuer ausführen, wird Security Center Mobile in Config Tool aktiviert.

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

Sicherheit

Verwenden Sie den Abschnitt *Sicherheit* der Seite *Konfiguration*, um die Benutzerkonto- und Systemsicherheitseinstellungen 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 für Security-Center-Anwendungen ändern.

Legen Sie ein Passwort für jedes Produkt fest:

- **Windows-Admin:** Das Passwort des Admin-Benutzers für Windows.
- **Client-Anwendungen:** 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.
- **Automatische Abmeldung:** Aktivieren Sie diese Option, wenn Sie Windows so konfigurieren möchten, dass ein Benutzer nach 15 Minuten Inaktivität abgemeldet wird.
- **Komplexität des Passworts:** Aktivieren Sie diese Option, um ein komplexes Passwort mit einer Länge von mindestens 10 Zeichen für Windows-Benutzer zu erfordern.
- **Servermanagementfunktionen:** Aktivieren Sie diese Option, um Funktionen zuzulassen, wie Rollen und andere Tasks hinzufügen mithilfe von Anwendungen wie *Windows Admin Center*, *Server Manager* oder *Windows PowerShell*.
- **Zugriff auf Wechselmedien:** Aktivieren Sie diese Option, um 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.
- **Support für Speicherkarten aktivieren:** Aktivieren Sie diese Option, um ein Speicherkartenlesegerät mithilfe der Security-Desk-Anwendung zu erstellen oder zu verwenden. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Eingehende Remote-Verbindungen:** Aktivieren Sie diese Option, um den Zugriff auf *Remotedesktop*-Verbindungen und Dateifreigabe auf der Appliance über Ihr Computernetzwerk zu erlauben. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Remotedesktop:** Aktivieren Sie diese Option, um Personen in Ihrem Netzwerk zu erlauben, sich bei der Appliance mithilfe der Anwendung *Remotedesktop* anzumelden. Die Option **Eingehende Remote-Verbindungen** muss aktiviert sein, um den Zugriff auf *Remotedesktop* zu ermöglichen. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.
- **Dateifreigabe:** Aktivieren Sie diese Option, um Dateien und Ordner, die sich auf der Appliance befinden, mit Personen in Ihrem Netzwerk zu teilen. Die Option **Eingehende Remote-Verbindungen** muss aktiviert sein, um die Dateifreigabe zu ermöglichen. Um das Gerät vor Malware zu schützen, wurde diese Option standardmäßig deaktiviert.

Regionale Einstellungen

Verwenden Sie den Abschnitt *Regionale Einstellungen* der Seite *Konfiguration*, um die Spracheinstellungen Ihres Systemtastaturlayouts zu ändern.

- **Das Tastaturlayout ändern:** Klicken Sie, um die *Windows-Systemsteuerung* zu öffnen und das Layout Ihrer Tastatur zu ändern.

  WICHTIG: Damit die Änderungen übernommen werden, müssen Sie Ihren Computer neu starten.
- **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.

BEMERKUNG: Das SV Control Panel ist nur auf Englisch verfügbar.

Sichern und Wiederherstellen

Verwenden Sie den Abschnitt *Directory und Konfigurationen* der Seite *Konfiguration*, um auf den Assistenten *Sichern* und *Wiederherstellen* zuzugreifen.

Sichern und Wiederherstellen ist eine Funktion im SV Control Panel, die Sie verwenden können, um Ihre Directory-Datenbank und Konfigurationsdateien zu sichern und später in Fällen wie einem Systemausfall oder Hardware-Upgrade zur gleichen System-ID wiederherzustellen. 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.

Verwandte Themen

Informationen über Sichern und Wiederherstellen auf Seite 33

Ihre Directory-Datenbank sichern auf Seite 34

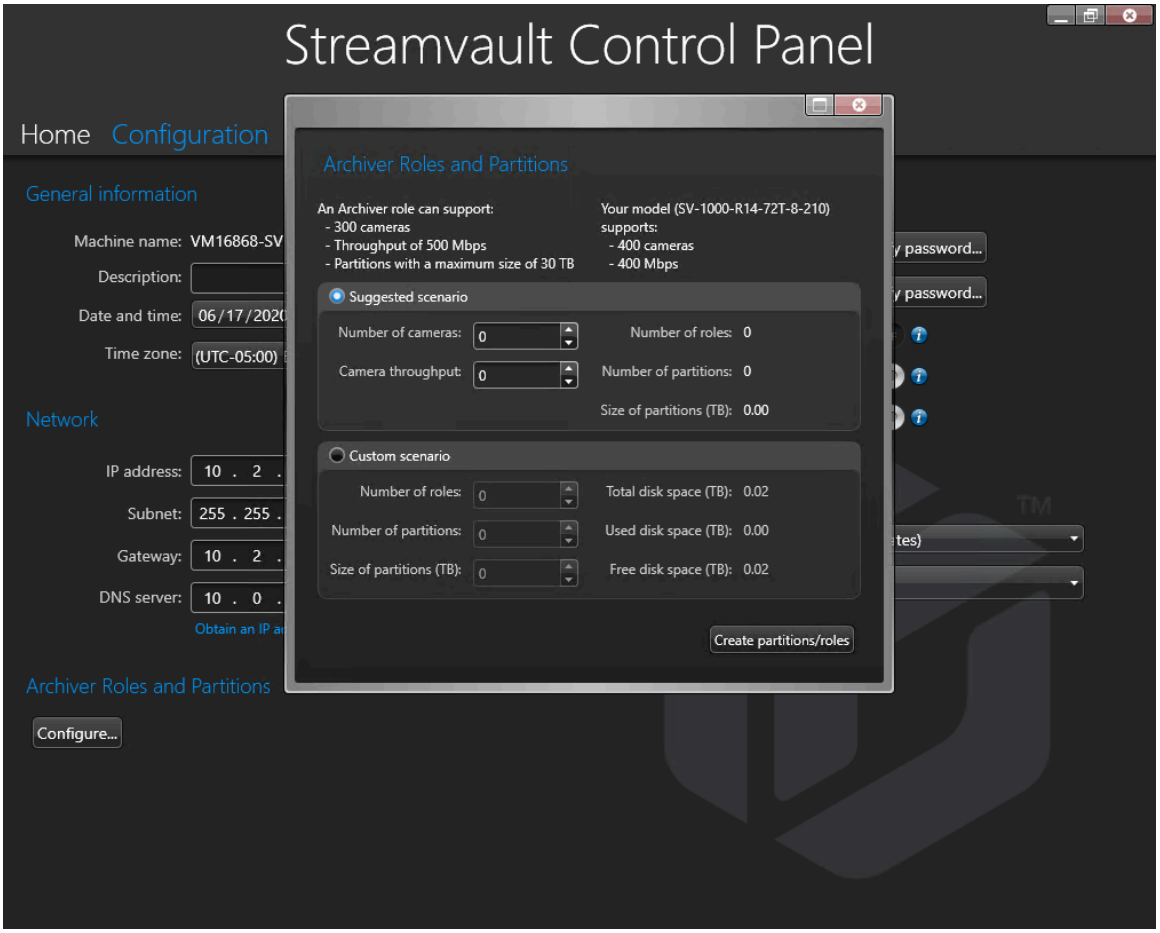
Ihre Directory-Datenbank wiederherstellen auf Seite 35

Archiver-Rollen und Partitionen

Verwenden Sie den Abschnitt *Archiver-Rollen und Partitionen* auf der Seite *Konfiguration*, um die maximale Anzahl der in Ihrem System unterstützten Kameras zu erweitern.

Archiver-Rollen und Partitions ist eine Funktion im SV Control Panel, mit der Sie Systeme konfigurieren können, die mehr Kameras und Durchsatz erfordern als ein einzelner Archiver maximal unterstützen kann.

Dieser Abschnitt ist nur für Systeme verfügbar, die auf einem Erweiterungsserver mit Security Center 5.8 und neuer ausgeführt werden.



- **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 36.

CylancePROTECT-Seite im SV Control Panel

Verwenden Sie die CylancePROTECT-Seite, um Informationen über Cylance anzuzeigen und den Modus auszuwählen, in dem die Streamvault™-Appliance mit der Cylance Console in der Cloud kommuniziert.

Sie können eine der folgenden Optionen auswählen:

- **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.

WICHTIG: Wenn CylancePROTECT ausgeschaltet ist, können Sie nicht zwischen **Getrennt** und **Online** wechseln. Um diese Einstellungen zu ändern, müssen Sie das Software-Image auf Ihrer Appliance zurücksetzen.

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

Um auf Protokolle und erweiterte Funktionen für Ihr System zuzugreifen, wählen Sie **CylancePROTECT im erweiterten Schnittstellenmodus ausführen** aus.

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 Lizenzinformationen, Informationen zur Softwarewartungsvereinbarung, Links zum Genetec™ Technical Assistance Portal (GTAP) sowie Links zur Produktdokumentation.

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

Lizenzoptionen

Im Abschnitt *Lizenz* auf der Seite *Informationen* können Sie Informationen über die Lizenz anzeigen. Die angezeigte Informationen hängen von Ihren Lizenzoptionen ab.

- **Ablaufdatum:** Zeigt an, wann Ihre Security-Center-Lizenz abläuft.
- **Zutrittskontroll-:** 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 zusätzliche Lizenzinformationen anzuzeigen.

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

Verwandte Themen

Ihre Security-Center-Lizenz auf einer Appliance aktivieren auf Seite 19

Informationen zur Softwarewartungsvereinbarung

Verwenden Sie den Abschnitt *Softwarewartungsvereinbarung* der Seite *Informationen*, um Informationen über die Softwarewartungsvereinbarung anzuzeigen.

- **Ablaufdatum:** Zeigt das Ablaufdatum der Softwarewartungsvereinbarung (Software Maintenance Agreement, SMA).
- **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.

Systeminformationen

Im Abschnitt *System* auf der Seite *Informationen* können Sie Informationen über das System anzeigen.

- **Hersteller:** Zeigt den Hersteller der Hardware an.
- **Hardware-Modell:** Zeigt das Hardware-Modell an.
- **Software-Revision:** Zeigt die Version oder das Image der Software 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.

Hilfsinformation

Verwenden Sie den Abschnitt *Hilfe* der Seite *Informationen*, um auf nützliche Links zum Genetec™ Technical Assistance Portal (GTAP) und zur Produktdokumentation zuzugreifen.

- **GTAP:** Klicken Sie auf den Link, um GTAP und Support-Foren zu öffnen.
  BEMERKUNG: Sie benötigen für das Anmelden im GTAP einen Benutzernamen und ein Passwort.
- **TechDoc Hub:** Klicken Sie auf den Link, um den Genetec TechDoc Hub zu öffnen.
- **Control Panel:** Klicken Sie, um das *SV Control Panel – Benutzerhandbuch* zu öffnen, das auch die Versionshinweise für SV Control Panel enthält.
- **Security Desk:** Klicken Sie hier, um das *Security Center – Benutzerhandbuch* zu öffnen.

5

Zusätzliche Ressourcen

Dieser Abschnitt enthält die folgenden Themen:

Einen USB-Schlüssel für eine Zurücksetzung auf die Werkseinstellungen erstellen

Um das Image auf einer Streamvault™ Appliance des Typs SV-100E, SV-300E oder SV-350E oder auf einer Streamvault™-Server- oder Workstation-Appliance zurückzusetzen, müssen Sie einen bootfähigen USB-Schlüssel vorbereiten, der das erforderliche Streamvault™-Software-Image enthält.

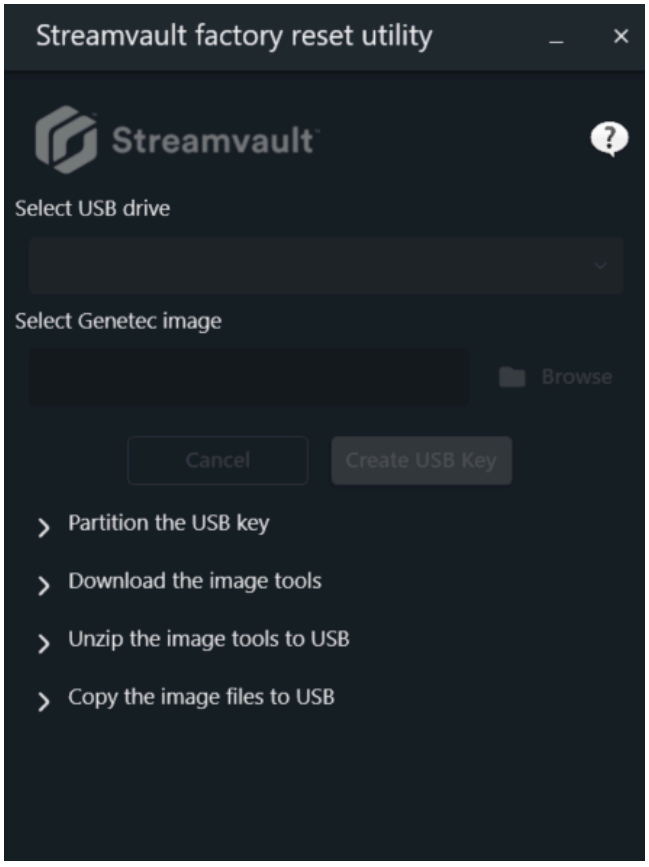
Bevor Sie beginnen

- Laden Sie das *Streamvault™-Hilfsprogramm für Werksreset* aus dem Abschnitt Downloads im *Benutzerhandbuch für die Streamvault™ Appliance* im TechDoc Hub herunter.
- Bevor Sie das *Streamvault™-Hilfsprogramm für Werksreset* öffnen, entpacken Sie die Sicherungs-Images in ein Windows-Directory
- Vergewissern Sie sich, dass Sie einen USB-Schlüssel mit mindestens 32 GB an Speicher haben.

Sehen Sie sich dieses Video an, um zu erfahren, wie Sie einen USB-Schlüssel für eine Zurücksetzung auf die Werkseinstellungen erstellen.

So erstellen Sie einen bootfähigen USB-Schlüssel mit dem erforderlichen Software-Image im *Streamvault™-Hilfsprogramm für Werksreset*:

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



2 Klicken Sie im Abschnitt *Genetec-Image auswählen* auf **Suchen** und wählen Sie die erforderliche *.swm*-Datei aus.

   - Wählen Sie für All-in-One-Appliances eine der entpackten Dateien aus dem *wim*-Ordner aus.
   - Wählen Sie für Workstations und Server das erforderliche Image im Ordner <*Servicekennzeichnummer*> aus.

3 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 Ihnen im *Streamvault™-Hilfsprogramm für Werksreset* eine Meldung angezeigt, die Sie darüber informiert, dass der USB-Schlüssel erfolgreich erstellt wurde.

Nach Durchführen dieser Schritte

- Bei den Appliances SV-100E, SV-300E oder SV-350E setzen Sie Software auf der Appliance zurück.
- Bei einer Workstation oder Server-Appliance setzen Sie das Image der Streamvault-Appliance mithilfe des bootfähigen USB-Schlüssels zurück.

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.

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-Kennzeichen mit Windows-Edition und Zertifikatsinformationen für Produkte, in denen Microsoft-Softwareversionen eingebettet sind.

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 Härtungsebene 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 die Softwarerevisionsnummer einer Streamvault-Appliance finden

Wenn Sie den Genetec™ Technical Support kontaktieren, benötigen Sie die System-ID und die Software-Revisionsnummer (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 Softwarerevisionsnummer fordert der Genetec Technical Support möglicherweise auch die Zertifizierungsnummer und die Seriennummer an. Diese Informationen finden Sie auf einem Etikett auf der Streamvault-Appliance.

So finden Sie die System-ID und die Image-Version Ihrer Appliance:

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 **Softwarerevisions**nummer.

Verwandte Themen

Die Appliances SV-100E, SV-300E oder SV-350E auf die Werkseinstellungen zurücksetzen auf Seite 74

Eine Zurücksetzung auf die Werkseinstellungen auf einer Streamvault-Workstation oder Server-Appliance durchführen auf Seite 77

Dateifreigabe auf einer Streamvault-Appliance erlauben

Um Dateien und Ordner mit Menschen in Ihrem Netzwerk zu teilen, müssen Sie die Dateifreigabe in 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.

So aktivieren Sie die Dateifreigabe auf Ihrer Appliance:

1 Auf der Seite *Konfiguration* von SV Control Panel:
   - Aktivieren Sie die Option **Eingehende Remote-Verbindungen**.
   - Aktivieren Sie die Option **Dateifreigabe**.

2 Klicken Sie auf **Anwenden**.

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.

So erlauben Sie Remotedesktop-Verbindungen auf Ihrer Streamvault™-Appliance:

1 Auf der Seite *Konfiguration* von SV Control Panel:
   - Aktivieren Sie die Option **Eingehende Remote-Verbindungen**.
   - Aktivieren Sie die Option **Remotedesktop**.

2 Klicken Sie auf **Anwenden**.

Verwandte Themen

Remotedesktop kann sich nicht mit einer Streamvault-Appliance verbinden auf Seite 82

6

Problembehebung

Dieser Abschnitt enthält die folgenden Themen:

Die Appliances SV-100E, SV-300E oder SV-350E auf die Werkseinstellungen zurücksetzen

Wenn die Software einer SV-100E-, SV-300E- oder SV-350E-Appliance 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 34.
- 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.
- (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

- Bei Appliances mit Modellnummern außer SV-100E, SV-300E und SV-350E sehen Sie unter Eine Zurücksetzung auf die Werkseinstellungen auf einer Streamvault-Workstation oder Server-Appliance durchführen auf Seite 77 nach.
- Eine Zurücksetzung auf die Werkseinstellungen löscht und überschreibt alle Daten, die sich aktuell auf dem Windows-Laufwerk (C:) befinden, einschließlich Datenbanken und Protokolle.

So setzen Sie Appliances der Serien SV-100E, SV-300E oder SV-350E auf die Werkseinstellungen zurück:

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

Richten Sie Ihre Appliance ein.

Verwandte Themen

Die System-ID und die Softwarerevisionsnummer einer Streamvault-Appliance finden auf Seite 70

Das Software-Image auf einer SV-100E-, SV-300E- oder SV-350E-Appliance mithilfe eines bootfähigen USB-Schlüssels zurücksetzen

Sie können das Software-Image mithilfe eines USB-Wiederherstellungslaufwerks wiederherstellen.

Bevor Sie beginnen

- Halten Sie den USB-Schlüssel bereit, der das Wiederherstellungssoftware-Image für Ihre Appliance enthält.
- 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

- Eine Zurücksetzung auf die Werkseinstellungen löscht und überschreibt alle Daten, die sich aktuell auf dem Windows-Laufwerk (C:) befinden, einschließlich Datenbanken und Protokolle.

  ACHTUNG: Es werden nur Dateien auf dem C:-Laufwerk gelöscht, aber wir empfehlen, die Videodateien auf allen Ihren Laufwerken zu sichern.
- Das Zurücksetzen dauert ungefähr 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.

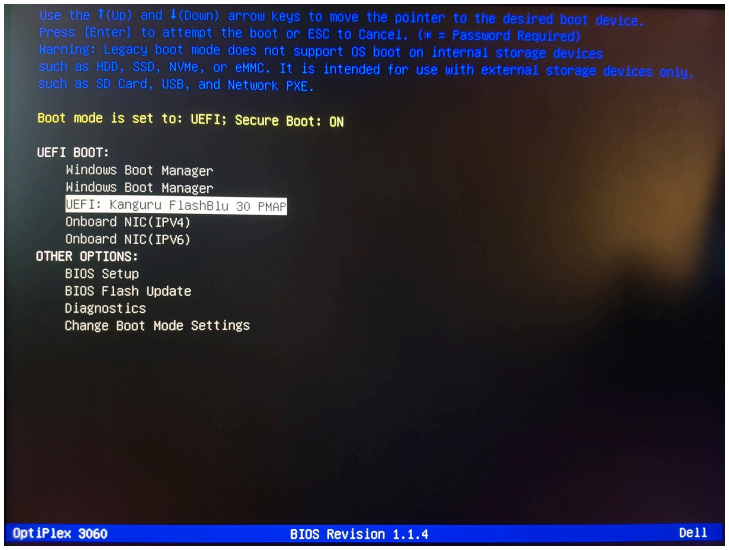
Sehen Sie sich dieses Video an, um zu erfahren, wie Sie das Software-Image auf einer SV-100E-, SV-300E- oder SV-350E-Appliance mithilfe eines bootfähigen USB-Schlüssels zurücksetzen.

So setzen Sie das Image der Appliances SV-100E, SV-300E oder SV-350E zurück:

1 Schalten Sie die Appliance aus.

2 Schließen Sie den von Ihnen erstellten USB-Schlüssel an einen USB-Anschluss an.

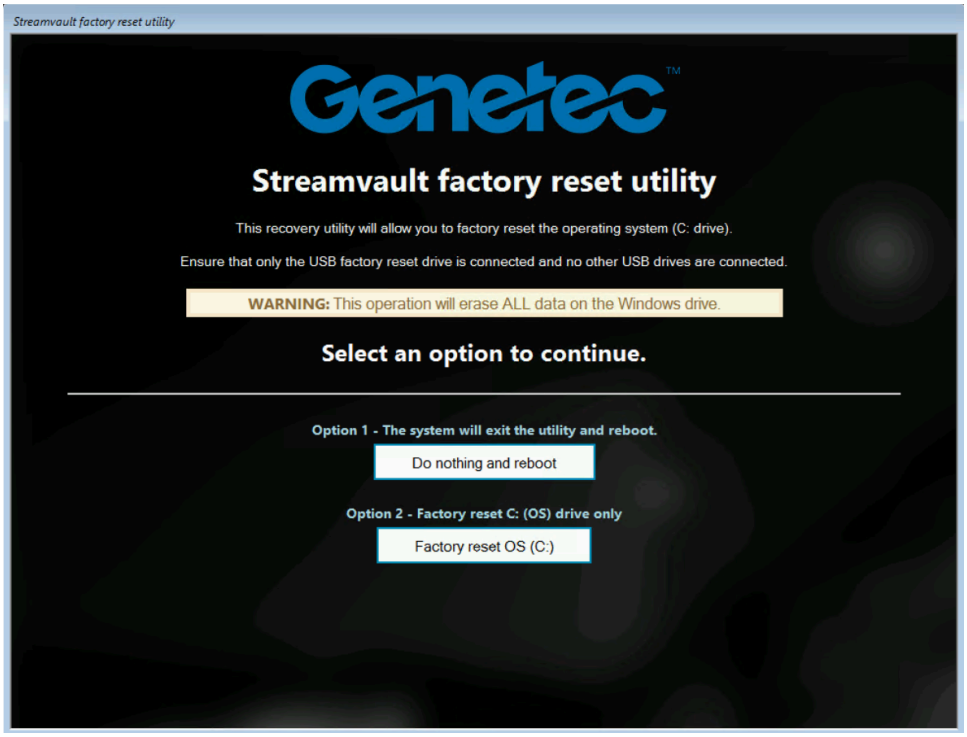
3 Wählen Sie das USB-Laufwerk aus und drücken Sie die Eingabetaste.



4 Wenn der USB-Schlüssel im Wiederherstellungsmodus startet, wählen Sie eine der folgenden Optionen aus:

- **Nichts tun und neu starten:** Wählen Sie diese Option aus, um das Wiederherstellungsprogramm zu schließen und starten Sie die Appliance neu.
- **Betriebssystem (C:) auf die Werkseinstellungen zurücksetzen:** Wählen Sie diese Option aus, um das Systemlaufwerk der Appliance zu formatieren und erneut zu installieren und die Videodateien

auf den anderen Videofestplatte aufzubewahren. Alle Dateien auf dem C:-Laufwerk werden gelöscht: Datenbankprotokolle usw.



5 Wenn Sie dazu aufgefordert werden, tippen Sie Yes und drücken Sie die Eingabetaste, um mit dem Zurücksetzen auf die Werkseinstellungen fortzufahren, und warten Sie darauf, dass der Vorgang abgeschlossen ist.

6 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.

7 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

8 Klicken Sie auf **Start**.

Eine der folgenden Statusmeldungen wird angezeigt:

- **BESTANDEN:** Der Vorgang wurde als erfolgreich validiert. Fahren Sie mit dem nächsten Schritt fort.
- **FEHLGESCHLAGEN – Keine Übertragung:** Der Vorgang wurde als erfolgreich validiert; zu diesem Zeitpunkt war jedoch keine Internetverbindung verfügbar. Fahren Sie mit dem nächsten Schritt fort.
- **FEHLGESCHLAGEN:** Der Vorgang wurde als nicht erfolgreich validiert. Wenden Sie sich Genetec Technical Assistance.

9 Wenn Sie eine Meldung BESTANDEN oder BESTANDEN – Keine Übertragung erhalten, schließen Sie das Fenster *Genetec™ Product Validator*.

10 Warten Sie darauf, dass das Hintergrundskript geschlossen wird, und starten Sie die Appliance neu.

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 Lizenz.
- Wenn Sie die Security-Center-Konfiguration vor dem Zurücksetzen auf die Werkseinstellungen gesichert haben, stellen Sie die Konfiguration mithilfe des SV Control Panel wieder her.

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 34.
- 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 Die Appliances SV-100E, SV-300E oder SV-350E auf die Werkseinstellungen zurücksetzen auf Seite 74 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. Wenn dies der Fall ist, kontaktieren Sie das Genetec™ Technical Assistance Center (GTAC).

So führen Sie eine Zurücksetzung auf die Werkseinstellungen auf einer Streamvault-Workstation oder Server-Appliances durch:

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 die Softwarerevisionsnummer einer Streamvault-Appliance finden auf Seite 70

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

Sie können das Software-Image Ihrer Streamvault-Appliance zum Standardstatus mithilfe eines USB-Wiederherstellungslaufwerk zurücksetzen.

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

- Beim Zurücksetzen werden alle Daten gelöscht, die sich auf dem Systemlaufwerk befinden.
- Das Zurücksetzen beeinträchtigt die Standard-Werkseinstellungen des RAID-Laufwerks nicht.
- Das Zurücksetzen schlägt möglicherweise fehl, wenn die Standardwerkseinstellungen von Festplatten, RAID-Laufwerken oder Partitionen auf der Appliance geändert wurden. Wenn dies der Fall ist, kontaktieren Sie das Genetec™ Technical Assistance Center (GTAC).

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

So setzen Sie das Image auf der Streamvault-Appliance zurück:

1 Schalten Sie die Appliance aus.

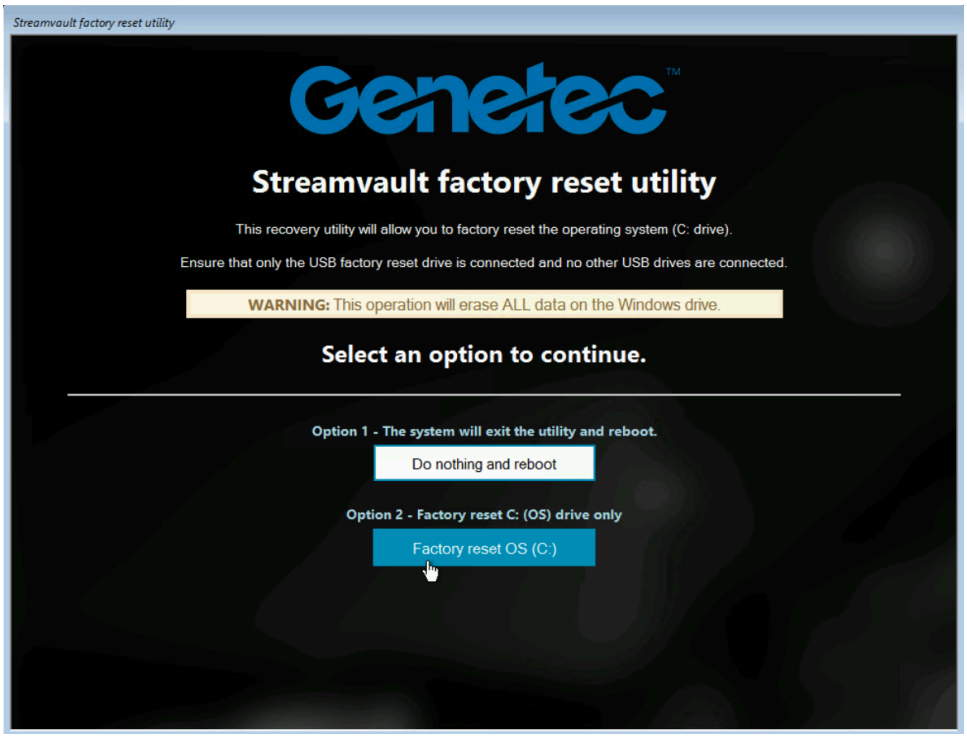
2 Schließen Sie den von Ihnen erstellten bootfähigen USB-Schlüssel an einen USB-Anschluss an.

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.

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 Lizenz.
- Wenn Sie die Security-Center-Konfiguration vor dem Zurücksetzen auf die Werkseinstellungen gesichert haben, stellen Sie die Konfiguration mithilfe des SV Control Panel wieder her.

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:

- SV-100E 16.3 und neuer
- SV-300E 16.3 und neuer
- 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 im Windows Registrierungseditor.

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 von ihrem Gerät erfordert wird.
- Sie müssen TLS auf den Server- (eingehend) und Clientknoten (ausgehen) aktivieren.
- Aus Sicherheitsgründen sind die Optionen für Interneteigenschaften auf Appliances deaktiviert. Aus diesem Grund können Sie TLS nur über den Windows Registrierungseditor aktivieren.

So aktivieren Sie TLS auf einer Appliance:

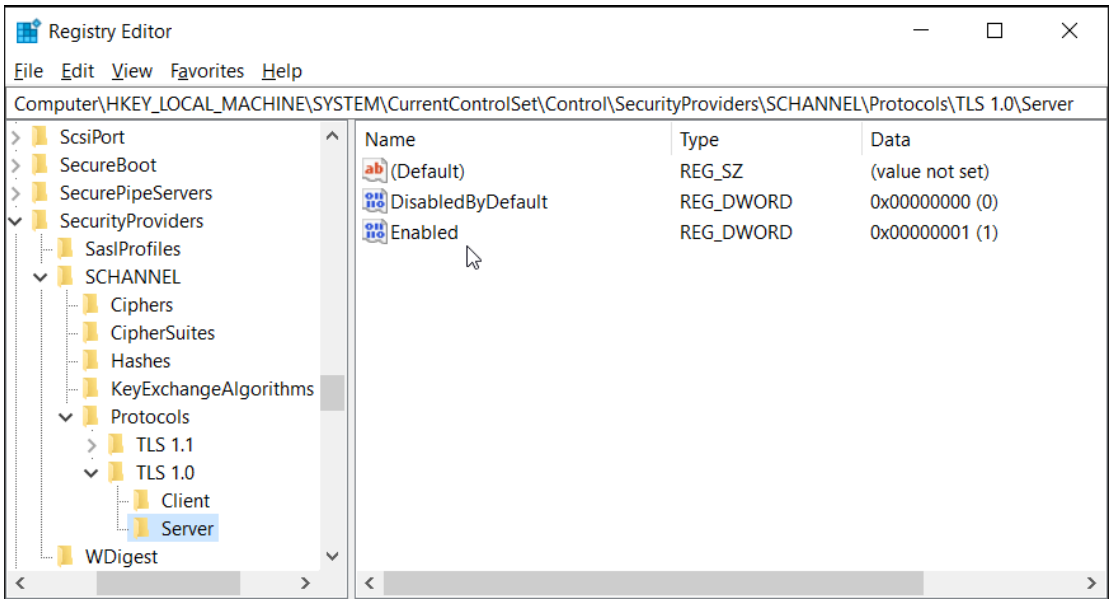
1 Öffnen Sie den Windows Registrierungseditor.

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.

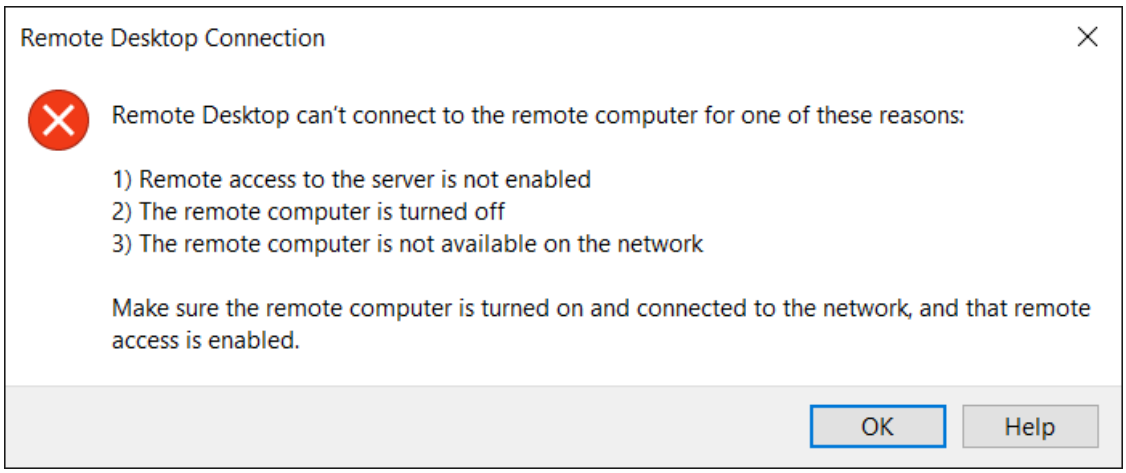
c) Wählen Sie den Knoten **Client** aus, legen Sie **DisabledByDefault** auf 0 und **Aktiviert** auf 1 fest.



3 Starten Sie Windows neu.

Remotedesktop kann sich nicht mit einer Streamvault-Appliance verbinden

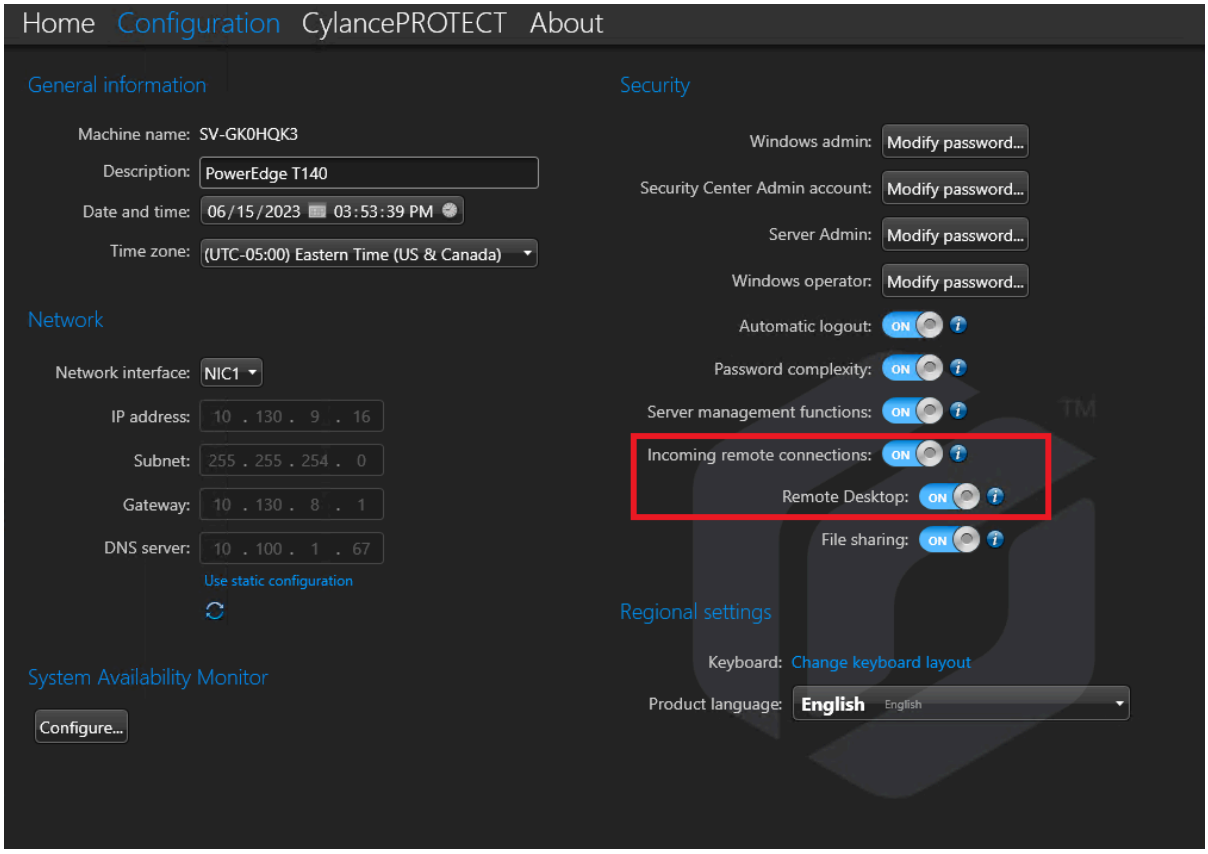
Wenn Sie versuchen, mithilfe von Remotedesktop auf eine SV-Appliance zuzugreifen, erhalten Sie eine Meldung, dass sich Remotedesktop nicht mit dem Remote-Computer verbinden kann.



Remote-Verbindungen und Remotedesktop sind in 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. Aktivieren Sie auf der Seite *Konfiguration* des SV Control Panel die Optionen **Eingehende Remote-Verbindungen** und **Remotedesktop**.



Remote-Verbindungen oder Remotedesktop sind in Windows nicht erlaubt

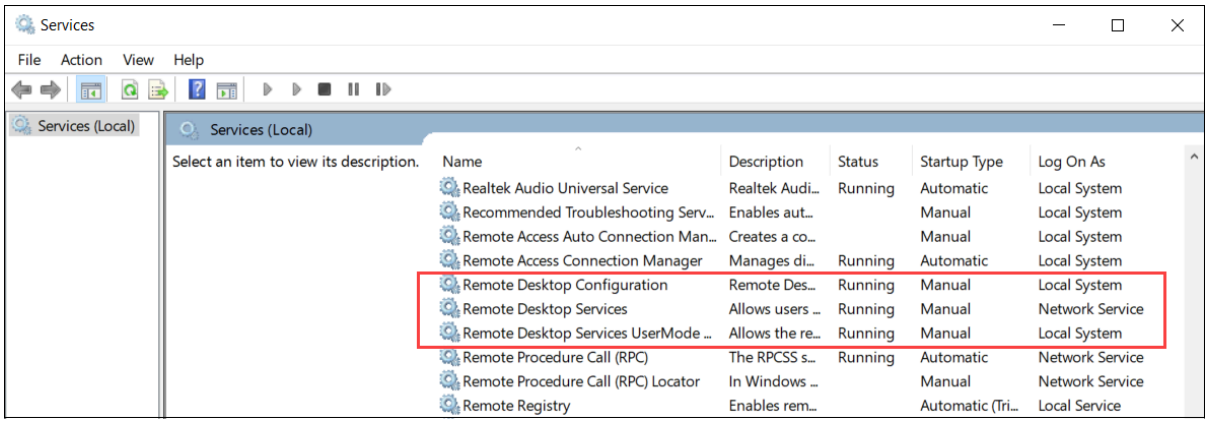
Beschreibung: Obwohl sowohl **Eingehende Remote-Verbindungen** als auch **Remotedesktop** im SV Control Panel aktiviert sind, sind diese Einstellungen aktuell nicht in Windows erlaubt.

Lösung: Überschreiben Sie die Windows-Einstellungen, indem Sie die Optionen **eingehende Remote-Verbindungen** und **Remotedesktop** in SV Control Panel deaktivieren und wieder aktivieren.

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.

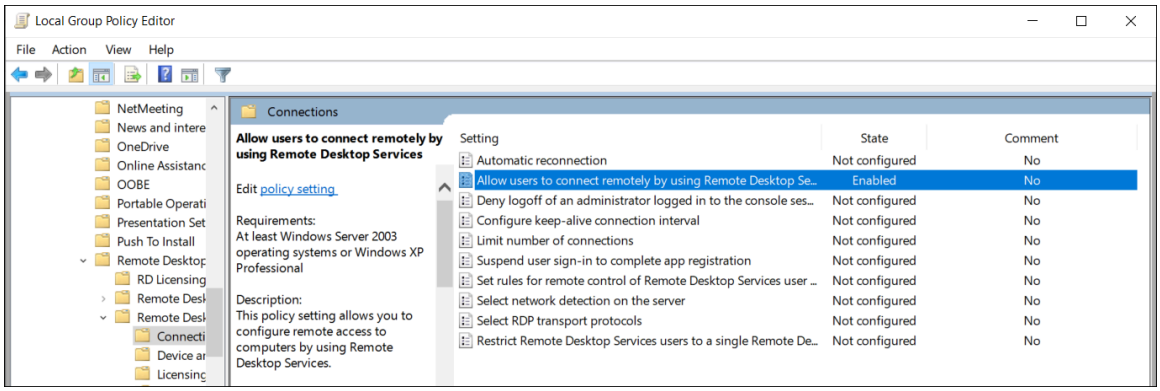


Remote Desktop Services werden verweigert

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

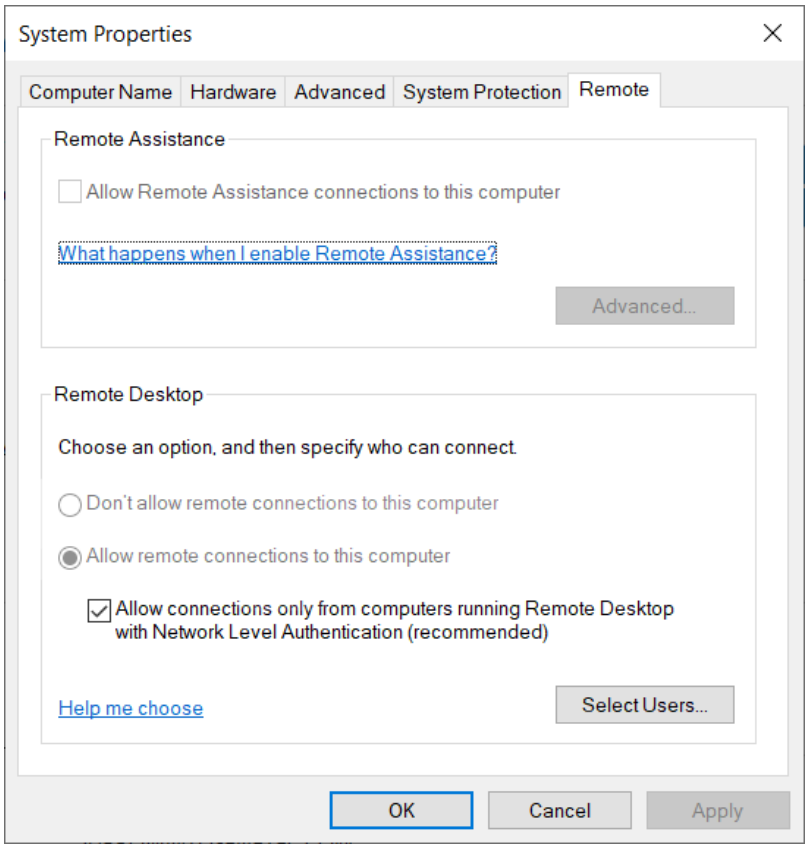
Lösung: Erlauben Sie Remote-Benutzern Zugriff zur Appliance mithilfe von Remotedesktopdiensten:

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** > **Remote-Einstellungen**. Das Fenster *Systemeigenschaften* wird geöffnet.

6. Stelle Sie auf der Registerkarte *Remote* im Abschnitt *Remotedesktop* sicher, dass die Option **Remote-Verbindungen auf diesem Computer erlauben** 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 Remote Desktop Connection weiterhin keine Verbindung herstellen kann, kontaktieren Sie den technischen Support.

Verwandte Themen

Remotedesktop-Verbindungen auf einer Streamvault™-Appliance erlauben auf Seite 72

CylancePROTECT kann für einige Streamvault-Appliances nicht von SV Control Panel deinstalliert werden

Sie haben die Option **CylancePROTECT** von SV Control Panel deaktiviert, aber CylancePROTECT wird nicht von Ihrer Streamvault™-Appliance deinstalliert.

Betroffene Versionen

Die folgenden Streamvault-Image-Versionen sind von diesem Problem betroffen:

- 0011.2.X.27.G (veröffentlicht am 18. Januar 2021) und höher
- 16.8.0 (veröffentlicht am 10. März 2021) und höher
- 2019.1.C.14.G (veröffentlicht am 14. Januar 2021) und höher
- 2016.1.C.19.G (veröffentlicht am 8. Februar 2021) und höher

Ursache

Ein Codierungsproblem.

Workaround

1. Öffnen Sie die Windows-Konsole *Dienste*.
2. Klicken Sie mit der rechten Maustaste auf den **Server**-Service und klicken Sie auf **Eigenschaften**.
3. Ändern Sie die Option **Starttyp** in **Manuell** und starten Sie den Service dann.
4. Öffnen Sie SV Control Panel, klicken Sie auf die Registerkarte **CylancePROTECT** und wählen Sie die Option **Ausschalten** aus.

   Warten Sie 2 Minuten, bis der Prozess abgeschlossen ist.
5. Ändern Sie in der Windows-Konsole *Dienste* den **Starttyp** des **Server**-Service in **Deaktiviert**.
6. Starten Sie die Streamvault-Appliance neu.

7

Technischer Support

Dieser Abschnitt enthält die folgenden Themen:

Den Genetec-Support kontaktieren

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).

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 *Kontaktieren Sie uns*.
2. Rufen Sie das Genetec Technical Assistance Center an und wählen Sie die Option 2 aus.

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

Den Genetec-Support über GTAP kontaktieren

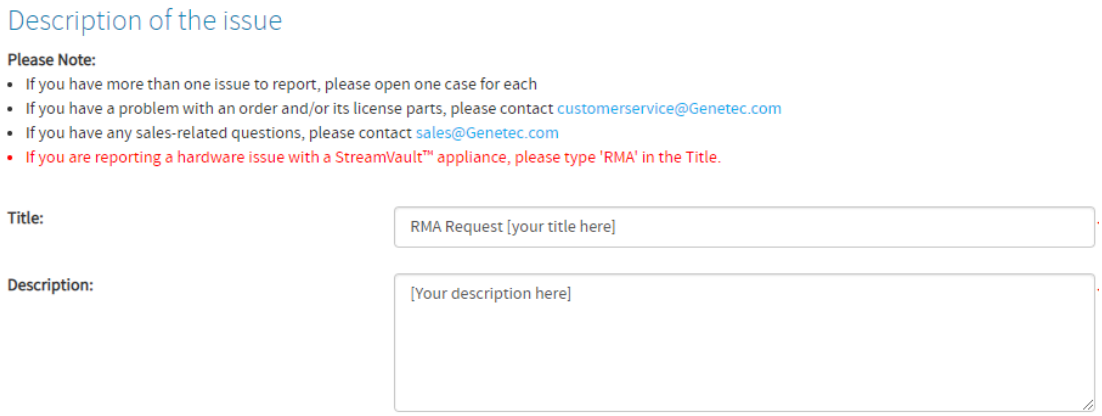
Alle Kunden erhalten während der Geschäftszeiten in Ihrer Region Unterstützung über Online-Support-Fälle im Genetec™ Technical Assistance Portal (GTAP).

Bei Kunden ohne 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.

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.



6. Fügen Sie die Seriennumer 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.

Den Genetec-Support über den Live-Chat kontaktieren

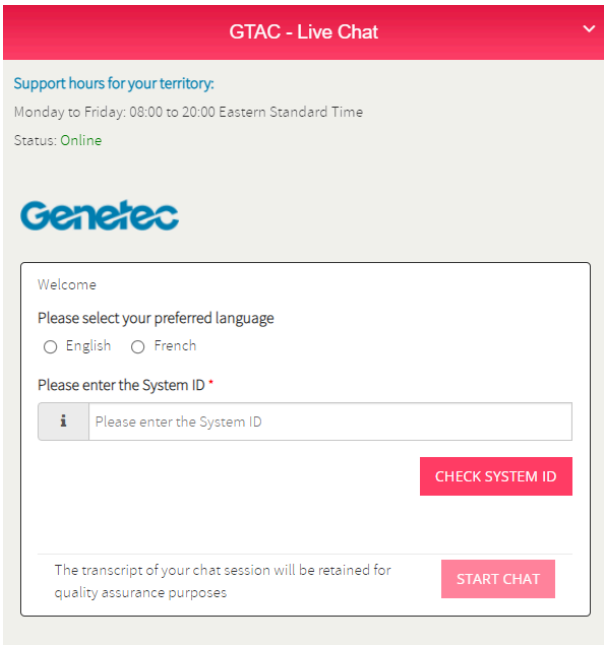
Kunden mit Genetec Advantage erhalten Live-Support während der Geschäftszeiten in Ihrer Region über Live-Chat im Genetec Technical Assistance Portal (GTAP).

Bei Kunden ohne 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.

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 Seriennumer 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 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 Genetec-Lifecycle-Management (GLM)-Dokumenten beschriebenen Supportverfahren abgedeckt: Genetec Advantage – Beschreibung und Genetec Assurance – 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 DellProSupport.

Produktfamilie	Garantielänge[1]		Erweiterter Ersatz oder Reparatur vor Ort	In der Garantie enthaltene Rückgabe und Reparatur[2]
	Standard	Erweitert		
SV-100E SV-300E SV-350E	3 Jahre	2 Jahre	1 Jahr erweiterter Ersatz	Enthalten
SVW-300 SVW-500 SV-1000	3 Jahre	Nicht zutreffend	HP-Garantie für Reparatur vor Ort[3]	Enthalten
SV-2000E SV-4000E SV-7000E	5 Jahre	2 Jahre	Dell ProSupport Reparaturgarantie am nächsten Werktag[4] vor Ort mit Behalten der eigenen Festplatte[3]	Enthalten
SVW-300E SVW-500E SV-1000E	5 Jahre	Nicht zutreffend	Dell ProSupport Reparaturgarantie am nächsten Werktag[4] vor Ort mit Behalten der eigenen Festplatte[3]	Enthalten
SV-2000 SV-4000 SV-7000	5 Jahre	2 Jahre	HP-Garantie für Reparatur vor Ort[3]	Enthalten
Speicherbereich Netzwerk (SAN)	5 Jahre	Eine Erweiterung ist auf Anfrage und auf Einzelfallbasis möglich	Dell ProSupport Reparaturgarantie am nächsten Werktag[4] vor Ort mit Behalten der eigenen Festplatte[3]	Enthalten

[1]Sie können eine zusätzliche Garantieerweiterung für 2 Jahre erwerben (für eine gesamte Garantielaufzeit von 7 Jahren). Die Erweiterung muss gekauft werden, bevor 5 Jahre verstrichen sind.

[2]Sie können zwischen Rücksendung des Geräts zur Reparatur oder Reparatur vor Ort wählen.

[3]Weitere Informationen über die von diesen Anbietern festgelegten Bedingungen finden Sie in der Dokumentation von Dell ProSupport und HP Support.

[4]Die Reparatur vor Ort am nächsten Werktag beginnt, wenn die Fehlerbehebung abgeschlossen wurde, das Hardwareproblem identifiziert wurde, der Fall bei Dell gemeldet wurde und Dell festgestellt hat, dass es sich

um einen Hardwarefehler handelt. Der nächste Werktag ist nicht dann, wenn der Support-Fall bei Genetec Inc. eröffnet wird.

Technische Daten für Streamvault™

Beachten Sie diese technischen, mechanischen und umweltbezogenen Daten beim Planen und Bereitstellen der Streamvault™-Appliance.

Technische, mechanische und umweltbezogene Daten

All-in-One-Appliances:

- SV-100E-Datenblatt
- SV-300E-Datenblatt
- SV-350E-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
- Datenblatt der SVS-7000E NAS-Serie
- Datenblatt der SVS-7000E SAN-Serie

Workstations:

- Datenblatt der SVW-300E-Serie
- Datenblatt der SVW-500E-Serie

Analysefähige Appliances:

- Datenblatt der SVA-100E-Serie
- Datenblatt der SVA-1000E-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 Hardwaregarantie werden von den folgenden Bedingungen hinsichtlich Reparaturen, Ersatzteilen und -geräten, Rechtsmitteln oder Garantieausschlüssen bestimmt.

Hardwaregarantiebedingungen

Garantie bei Reparatur und Ersatzteilen

Alle Genetec™-Produkte, die von Genetec Inc. repariert oder mit Ersatzteilen versehen wurden, stehen im Fall von Bearbeitungs- und Materialfehlern unter Garantie – entweder für eine Dauer von 90 Tagen oder die verbleibende Dauer der originalen Garantie, je nachdem, welche länger ist. Es können zusätzliche Kosten verrechnet werden, wenn Schäden am Produkt durch unsachgemäße Benutzung entstanden sind.

Im Falle von Streamvault™ werden alle ersetzten Geräte (oder Teile davon) das Eigentum von Genetec Inc., sobald der Kunde den entsprechenden Ersatz erhält. Der Kunde muss ersetzte Geräte (oder Teile davon) bei Forderung von Genetec Inc. umgehend zurückgeben. Wenn ersetzte Geräte bzw. Teile nicht innerhalb von 30 Tagen nach Erhalt der neuen Teile zurückgesendet werden, muss der Kunde den Wert des ersetzten Teils an Genetec Inc. bezahlen. Dies gilt nicht für den Service **Behalten Sie Ihre Festplatte**.

Exklusiver Gewährleistungsbehelf

Während der gültigen Garantiedauer und im Fall, dass Genetec Inc. feststellt, dass es sich beim Produkt um Material- oder Montagefehler handelt, wird Genetec Inc. nach eigenem Ermessen eine der folgenden Optionen durchführen:

- Dem Kunden den bezahlten Preis für das defekte Produkt gutschreiben.
- Reparatur des defekten Produkts.
- Das defekte Produkt mit einem neuen oder generalüberholten Produkt ersetzen.
- Das defekte Produkt mit einem anderen Produkt ersetzen, welches identische oder bessere Spezifikationen aufweist.

Garantieausschlüsse

Die folgenden Punkte sind von der Genetec-Standard-Hardwaregarantie ausgenommen:

- Geräte, die nicht von Genetec Inc. bezogen wurden.
- Produkte, die mit nicht unterstützten zusätzlichen Geräten oder Software verwendet wurden.
- Fehler oder Schäden durch missbräuchliche Verwendung (einschließlich, aber nicht begrenzt auf, Verwendung, die der beiliegenden Dokumentation und den Anweisungen entspricht), unsachgemäße Änderung, Unfälle oder Nachlässigkeit.
- Mängel oder Schäden, die durch das Bohren von Löchern, Anbringen von Aufklebern und Klebern oder Bemalen des Produkts verursacht wurden.
- Mängel oder Schäden, die durch Wasser, Blitze, Explosionen und andere elektrische Entladungen verursacht wurden.
- Produkte, die zerlegt oder repariert wurden, um die Leistung nachteilig zu beeinflussen oder um entsprechende Begutachtung und Testen, die der Überprüfung des Garantieanspruchs dienen, zu verhindern.
- Modifikation, unsachgemäßer Gebrauch und Manipulation des Produkts.
- Höhere Gewalt (Flut, Erdbeben, Blitzeinschlag, Feuer, Gasaustritt etc.).
- Normale Abnutzungserscheinungen.

Bedingungen der Genetec-Warenrücksendegenehmigung

Warenrücksendegenehmigung

Vor der Rückgabe eines Artikels muss der Kunde ein Formular zur Warenrücksendungsgenehmigung von Genetec Inc. beziehen. Die Warenrücksendegenehmigungsnummer muss sichtbar auf der Außenseite jedes retournierten Pakets angegeben sein und das Formular muss sich im Paket befinden. Der Kunde muss die Rückgabe des exakten Materials in richtiger Anzahl und mit den entsprechenden Seriennummern (wenn zutreffend), die von Genetec Inc. bewilligt wurden, und gemäß des registrierten Formulars zur Warenrücksendegenehmigung sicherstellen. Jegliches nicht genehmigte, falsch gekennzeichnete oder überflüssige Inventar, das an Genetec Inc. gesendet wird, wird abgelehnt und an den Absender retourniert.

Verpackung

Der Kunde ist für die entsprechende Verpackung von retournierten Waren verantwortlich. Jegliche Schäden, die durch mangelhafte Verpackung entstehen, werden nicht von der Genetec Hardwaregarantie abgedeckt. Der Kunde ist für alle Schäden verantwortlich, die während des Transports entstehen. Wenn der Kunde dem nicht nachkommt, erklärt Genetec Inc. die Warenrücksendungsgenehmigung für ungültig und die Reparaturkosten oder die vollständigen Ersatzkosten können in Rechnung gestellt werden.

Fracht

Der Kunde trägt alle Kosten, die für die Rückgabe des Geräts anfallen. Wenn die Warenrücksendungsgenehmigung nicht für ungültig erklärt wird, trägt Genetec Inc. alle anfallenden Kosten für die Rücksendung der reparierten Geräte oder der Ersatzgeräte an den Kunden.

Wenn Genetec Inc. fälschlicherweise nicht erworbene oder überflüssige Produkte an den Kunden sendet, übernimmt Genetec Inc. die Versandkosten für die Rücksendung der Produkte und wird dem Kunden, falls erforderlich, Rücksendeetiketten und Exportdokumente bereitstellen. Andernfalls werden die Waren dem Kunden in Rechnung gestellt.

Unter bestimmten Umständen akzeptiert Genetec Inc. die Rückgabe von nicht beschädigten Artikeln und stellt eine Gutschrift aus. Um eine Rückgabe gegen Gutschrift beantragen zu können, darf das Produkt nicht verwendet worden sein und muss sich im gleichen Zustand befinden, in dem es erhalten wurde. Es muss außerdem originalverpackt sein. Der Artikel muss innerhalb von 30 Tagen zurückgegeben werden, nachdem der Artikel an den Kunden gesendet wurde, oder innerhalb der vom Genetec-Inc.-Verkäufer zugelassenen Frist – je nachdem, was kürzer ist.

Bei allen Rückgaben gegen Gutschrift stellt Genetec Inc. eine Gutschrift aus, wenn die Produkte erhalten und überprüft wurden und sich in gutem Zustand befinden. Die Gutschrift wird für den Originalpreis abzüglich der Rücknahmegebühr laut Zeitplan A ausgestellt. Genetec Inc. behält sich das Recht vor, eine Rückgabe gegen Gutschrift abzulehnen. Außerdem behält sich Genetec Inc. das Recht vor, die Wiedereinlagerungsgebühr nach eigenem Ermessen unter außergewöhnlichen Umständen zu ändern.

Kundenspezifische Artikel, die als nicht stornierbar und nicht retournierbar verkauft wurden, können nicht gegen eine Gutschrift zurückgegeben werden.

Bei Transport beschädigt

Die Produkte werden nach Erhalt begutachtet. Jegliche Schäden, die beim Transport entstanden sind, müssen Genetec Inc. innerhalb von 14 Tagen nach Erhalt des Produkts gemeldet werden. Wenn Schäden nicht innerhalb von 14 Tagen nach Erhalt des Produkts gemeldet werden, behält sich Genetec Inc. das Recht vor, Rückgaben gegen Gutschrift oder den Ersatz der beschädigten Produkte zu verweigern. Bei Produkten, die beim Transport beschädigt wurden, senden Sie umgehend eine E-Mail an customerservice@genetec.com. Eine Beschreibung des Schadens ist erforderlich – wenn möglich, mit Fotos.

Zuständigkeiten und Erwartungen

- Eine Warenrücksendegenehmigung ist 30 Tage lang gültig. Die Artikel müssen innerhalb dieses Zeitraums zurückgegeben werden und müssen über die entsprechende RMA-Nummer identifiziert werden.
- Bei Retouren, bei denen der Kunde sich dazu entschließt, das Genetec Technical Assistance Center (GTAC) zu umgehen, wird eine Servicegebühr gemäß Zeitplan A erhoben, wenn kein Defekt am retournierten Gerät gefunden wird.
- Die Geräte, die dem Kunden im Rahmen der „Erweiterter Ersatz"-Garantie gesendet werden, werden dem Kunden sofort in Rechnung gestellt und werden gutgeschrieben, wenn das beschädigte Gerät innerhalb von 30 Tagen nach Erstellung der Warenrücksendungsgenehmigung zurückgegeben wird.

- Der Kunde ist dafür verantwortlich, Geräte in ordnungsgemäßem Zustand und gemäß der Anweisungen in diesem Dokument zu retournieren. Wenn der Kunde dem nicht nachkommt, können zusätzliche Gebühren in Rechnung gestellt werden oder Genetec Inc. kann den Antrag auf eine Warenrücksendegenehmigung für ungültig erklären.
- Wenn ein Gerät, das unter erweiterten Ersatz fällt, falsch gehandhabt oder unsachgemäß gebraucht wurde, kann dem Kunden der volle Preis des erweiterten Ersatzgerätes der „Erweiterter Ersatz“-Garantie in Rechnung gestellt werden.
- Gebühren für Rückgaben und Reparaturen außerhalb der Garantie werden laut Plan A berechnet.

Hinweise zur Rückgabe

1. Tragen Sie die folgenden Details zusammen, bevor Sie Genetec Inc. bezüglich einer Warenrücksendegenehmigung kontaktieren.
   - Name des Unternehmens (Integrators), das/der die Bestellung aufgegeben hat.
   - Die Bestellnummer des Kunden von jenem Gerät, das eine Warenrücksendegenehmigung erfordert.
   - Gültige Kontaktinformation (Name, E-Mail, Adresse, Telefonnummer) für zukünftige Korrespondenz.
   - Die Teilenummer des Geräts, für das eine Reparatur, Ersatz oder Gutschrift gefordert wird.
   - Die Seriennummer des Geräts, das eine Warenrücksendegenehmigung erfordert, falls zutreffend.
   - Die System-ID, falls vorhanden.
   - Grund für die Rückgabe.
   - So viele Details wie möglich zum Hardwareproblem, falls zutreffend.
2. Kontaktieren Sie Genetec Inc., um eine Warenrücksendegenehmigung zu beantragen.

Warenrücksendegenehmigungen für Rückgabe und Reparatur

1. Kontaktieren Sie das Genetec Technical Assistance Center (GTAC), um uns über das Problem zu informieren und eine Warenrücksendungsgenehmigung zu beantragen.

   Für Kunden mit Genetec Advantage ist Live-Support über das Telefon und Online-Chat zu Geschäftszeiten im Genetec™ Technical Assistance Portal (GTAP) verfügbar. Bei Kunden ohne Advantage-Garantie muss ein Fall über das GTAP geöffnet werden. Fügen Sie beim Erstellen des Falls **Antrag auf Warenrücksendegenehmigung** in den Titel ein, damit unser Team diese Anfragen einfach erkennen kann. Sie finden die GTAC-Telefonnummer und Geschäftszeiten für Ihre Region auf der Seite Genetec Technical Assistance Center *Kontaktieren Sie uns*.
2. Der Genetec-Kundenservice stellt dem Kunden ein Warenrücksendegenehmigungsformular bereit.

   Dieses Formular ist erforderlich, um das Gerät zu retournieren. Der Kunde erhält das Formular innerhalb von 24 Stunden per E-Mail, nachdem der GTAC kontaktiert wurde und die Anfrage vom Kundenservice verarbeitet wurde. Dieses Warenrücksendegenehmigungsformular stellt dem Kunden die Rücksendeadresse von Genetec Inc. oder dem Verkäufer sowie die Warenrücksendegenehmigungsnummer von Genetec Inc. oder dem Verkäufer bereit.

Warenrücksendegenehmigungen für Rückgaben gegen Gutschrift

1. Kontaktieren Sie den Genetec-Kundenservice, um uns über den Rückgabegrund zu informieren. Die Anfrage kann per E-Mail an customerservice@genetec.com oder per Telefon übermittelt werden. Die Telefonnummern und Geschäftszeiten des Kundenservice in Ihrer Region finden Sie unter *Kontaktieren Sie uns* auf der Genetec-Inc.-Website.
2. Der Genetec-Kundenservice stellt dem Kunden ein Warenrücksendegenehmigungsformular bereit.

   Dieses Formular ist erforderlich, um das Gerät zu retournieren. Der Kunde erhält das Formular innerhalb von 24 Stunden per E-Mail, nachdem der Genetec-Kundenservice kontaktiert wurde. Dieses Warenrücksendegenehmigungsformular stellt dem Kunden die Rücksendeadresse sowie die Warenrücksendegenehmigungsnummer von Genetec Inc. oder dem Verkäufer bereit.

3. Der Kunde retourniert das Gerät an Genetec oder den Verkäufer.
   a. Der Kunde übernimmt jegliche Versandkosten, die anfallen, um das Produkt an Genetec Inc. oder den entsprechenden Verkäufer zu retournieren.
   b. Der Kunde muss das Warenrücksendegenehmigungsformular (von Genetec Inc. an den Kunden per E-Mail gesendet) ausdrucken und der Sendung beifügen, zusammen mit dem Gerät, sodass Genetec Inc. oder die Verkäufer das Paket identifizieren können.
   c. Die Warenrücksendegenehmigungsnummer muss sichtbar an der Außenseite des Pakets angebracht sein. Genetec Inc. stellt dem Kunden diese Nummer auf dem Warenrücksendegenehmigungsformular bereit.
   d. Der Kunde darf nur jene Produkte versenden, für welche die Warenrücksendegenehmigung beantragt wurde. Versenden Sie die Produkte an die komplette Adresse, die auf dem Warenrücksendegenehmigungsformular angegeben wurde.
   e. Genetec Inc. oder der Verkäufer muss das retournierte Gerät innerhalb von 30 Tagen nach Ausstellung der Warenrücksendegenehmigung erhalten. Nach dieser 30-tägigen Frist wird jede Warenrücksendegenehmigung für „Rückgabe gegen Gutschrift" oder „Rückgabe und Reparatur" annulliert.
   f. Beim „erweiterten Ersatz" versendet Genetec Inc. das Ersatzgerät, sobald die Warenrücksendegenehmigung erstellt wurde oder sobald das Teil verfügbar ist.

      BEMERKUNG: Wenn das beschädigte Gerät innerhalb von 30 Tagen nach Erstellung der Warenrücksendungsgenehmigung zurückgegeben wird, werden die Geräte, die dem Kunden im Rahmen der „Erweiterter Ersatz"-Garantie gesendet werden, dem Kunden sofort in Rechnung gestellt und gutgeschrieben.
   g. Genetec Inc. fordert eine Sendungsverfolgungsnummer vom Kunden an, die an den Kundenservice gesendet wird.
4. Genetec Inc. erhält und begutachtet die retournierten Gegenstände.
   a. Die Teile- und Seriennummern (falls zutreffend) der retournierten Geräte müssen jenen entsprechen, die der Kunde Genetec Inc. bei der Erstellung der Warenrücksendegenehmigung mitgeteilt hat. Falls es Unstimmigkeiten gibt, wird sich der Genetec-Kundenservice mit dem Kunden in Verbindung setzen. Die Warenrücksendegenehmigung wird nicht bearbeitet, bevor der Kunde kontaktiert wurde, da die Garantie je nach Serien- und Teilenummer variieren kann.
   b. **Rückgabe gegen Gutschrift**: Wenn unbeschädigt, wird das Gerät als „Rückgabe gegen Gutschrift" bearbeitet. Eine Gutschrift erfolgt erst, sobald das Gerät erhalten und begutachtet wurde. Wenn die Verpackung beschädigt oder auf irgendeine Weise geändert wurde, hat Genetec Inc. das Recht, die Gutschrift zu verweigern. Für „Rückgabe gegen Gutschrift“ wird laut Zeitplan A eine Rücknahmegebühr in Rechnung gestellt.
   c. **Rückgabe für Reparatur**: Wenn das retournierte Gerät unter Garantie steht und der Schaden am Gerät nicht durch unsachgemäßen Gebrauch oder falsche Handhabung durch den Kunden verursacht wurde, wird Genetec Inc. oder der Verkäufer die Reparatur durchführen. Das reparierte Gerät wird dann an den Kunden zurückgesendet. In Fällen, in denen keine Reparatur möglich ist, können die Produkte mit voll funktionsfähigen Produkten ersetzt werden – repariert oder neu, je nach Verfügbarkeit. Reparaturzeiten hängen von Produktlinie, Produkttyp, Anzahl und Hersteller ab. Wenn das Gerät nicht von der Garantie gedeckt ist oder wenn die Warenrücksendegenehmigung ungültig ist, bestimmt Genetec, ob der Artikel repariert werden kann. In solchen Fällen fallen Reparaturkosten laut Zeitplan A an.
   d. Erweiterter Ersatz: Wenn das retournierte Gerät als „erweiterter Ersatz" unter Garantie steht und der Schaden am Gerät nicht durch unsachgemäßen Gebrauch oder falsche Handhabung durch den Kunden verursacht wurde, so wird dem Kunden das von Genetec Inc. bereitgestellte Ersatzgerät nicht in Rechnung gestellt.
5. Genetec Inc. verarbeitet die Warenrücksendegenehmigung und retourniert das Gerät, wenn zutreffend.

   Genetec Inc. ist für alle Versandkosten und Zollabfertigung (falls zutreffend) des an den Kunden zu retournierenden Geräts zuständig.

   Die Sendungsverfolgungsnummer wird dem Kunden nach Versand des Artikels per E-Mail mitgeteilt.

Zeitplan A

Produktfamilie	Rücknahmegebühren	Reparaturgebühren[3]	Begutachtungsgebühren
Streamvault	Gebühren werden auf Fallbasis berechnet und dem Kunden mitgeteilt.	Gebühren werden auf Fallbasis berechnet und dem Kunden mitgeteilt.	Nicht zutreffend

[3]Wenn das Gerät nicht repariert werden kann, muss der Kunde entscheiden, ob er stattdessen einen Ersatz des Geräts wünscht.

Glossar

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™-Hardwareüberwachungsentitäten verwendet. Nur ein Streamvault™-Manager ist pro System erlaubt.

SV-1000E

SV-1000E ist eine kosteneffiziente Rackmontage-Sicherheits-Appliance für mittlere Sicherheitssysteme. Sie hilft Ihnen beim Umstieg auf ein einheitlichen 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 einheitlichen 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, Einbruchserkennung 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-700E 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 im einen einzelnen oder mehre 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.

Wo finde ich Produktinformationen?

Unsere Produktdokumentation steht in folgenden Bereichen zur Verfügung:

- **Genetec™ TechDoc Hub:** Die aktuelle Dokumentation ist im TechDoc Hub verfügbar. Melden Sie sich im Genetec Portal an, und klicken Sie auf TechDoc Hub, um auf den TechDoc Hub zuzugreifen. Sie finden die gesuchte Information nicht? Wenden Sie sich an documentation@genetec.com.
- **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.