

Podręcznik Użytkownika Narzędzia Streamvault™

Kliknij Tutaj najnowszej wersji tego dokumentu.

Dokument ostatnio zaktualizowany: 30 Kwiecień, 2025



Informacje prawne

©2025 Genetec Inc. Wszelkie prawa zastrzeżone.

Genetec Inc rozpowszechnia ten dokument wraz z oprogramowaniem zawierającym umowę licencyjną użytkownika końcowego i jest udostępniany na podstawie licencji i może być używany tylko zgodnie z warunkami umowy licencyjnej. Treść tego dokumentu jest chroniona prawem autorskim.

Treść tego dokumentu ma wyłącznie charakter informacyjny i może ulec zmianie bez wcześniejszego powiadomienia. Genetec Inc. nie ponosi żadnej odpowiedzialności za jakiekolwiek błędy lub nieścisłości, które mogą pojawić się w treści informacyjnej zawartej w tym dokumencie.

Niniejsza publikacja nie może być kopiowana, zmieniana ani powielana w żadnej formie ani w żadnym celu, ani nie można tworzyć z niej żadnych treści pochodnych bez uprzedniej pisemnej zgody Genetec Inc.

Genetec Inc zastrzega sobie prawo do poprawiania i ulepszania swoich produktów według własnego uznania. Ten dokument opisuje stan produktu w czasie ostatniej aktualizacji dokumentu i może nie odzwierciedlać produktu przez cały czas w przyszłości.

W żadnym wypadku Genetec Inc nie będzie ponosić odpowiedzialności wobec jakiejkolwiek osoby lub podmiotu w związku z jakimikolwiek stratami lub szkodami, które są przypadkowe lub wynikają z instrukcji zawartych w niniejszym dokumencie lub oprogramowania komputerowego i opisanych tutaj produktów sprzętowych.

Genetec[™], AutoVu[™], AutoVu MLC[™], Citywise[™], Cloud Link Roadrunner[™], Community Connect[™], Curb Sense[™], Federation[™], Flexreader[™], Genetec Airport Sense[™], Genetec Citigraf[™], Genetec Clearance[™], Genetec ClearID[™], Genetec Cloudlink[™], Genetec Mission Control[™], Genetec Motoscan[™], Genetec Patroller[™], Genetec Retail Sense[™], Genetec Traffic Sense[™], KiwiVision[™], KiwiSecurity[™], Omnicast[™], Privacy Protector[™], Sipelia[™], Stratocast[™], Streamvault[™], Streamvault Edge[™], Synergis[™], Valcri[™], ich loga, jak również logo Mobius Strip są znakami towarowymi Genetec Inc. i mogą być zarejestrowane lub mogą oczekiwać na rejestrację w kilku jurysdykcjach.

Inne znaki towarowe użyte w tym dokumencie mogą być znakami towarowymi producentów lub sprzedawców odpowiednich produktów.

Patent zgłoszony. Genetec[™] Security Center, Omnicast[™], AutoVu[™], Stratocast[™], Genetec Citigraf[™], Genetec Clearance[™], i inne produkty Genetec[™] są przedmiotem zgłoszonych wniosków patentowych i mogą być przedmiotem już wydanych patentów w Stanach Zjednoczonych i innych jurysdykcjach na całym świecie.

Wszystkie specyfikacje mogą ulec zmianie bez powiadomienia.

Informacje o dokumencie

Tytuł dokumentu: Podręcznik Użytkownika Narzędzia Streamvault™

Numer oryginalnego dokumentu: EN.803.003

Numer dokumentu: PL.803.003

Data aktualizacji dokumentu: 30 Kwiecień, 2025

Możesz przesłać swoje uwagi, poprawki i sugestie dotyczące tych wytycznych adres documentation@genetec.com.

O tym przewodniku

W tym przewodniku wyjaśniono, jak skonfigurować urządzenie Streamvault aby współpracowało z kontrolą dostępu i nadzorem wideo Security Center przy pomocy aktualnej wersji Panelu sterowania SV. Ten przewodnik stanowi uzupełnienie Podręcznika Administratora Security Center i Podręcznika Konfiguracji Narzędzia Synergis[™].

Ten przewodnik jest napisany dla integratora, który przeprowadza wstępną konfigurację urządzenia SV. Zakłada się, że znasz terminologię i koncepcje stosowane w Security Center.

Notatki i uwagi

W tym przewodniku mogą pojawić się następujące notki i uwagi:

- Wskazówki: Sugestie, jak zastosować informacje dotyczące danego tematu lub kroku.
- Uwagi: Wyjaśnienia dotyczące wyjątkowych przypadków lub więcej informacji na ważny temat.
- Ważne: Wskazuje najważniejsze informacje dotyczące danego tematu lub kroku.
- **Przestroga:** Wskazuje, że podjęte działanie lub krok może spowodować utratę danych, problemy z bezpieczeństwem lub problemy z wydajnością.
- **Ostrzeżenie:** Wskazuje, że podjęte działanie lub krok może spowodować obrażenia fizyczne lub uszkodzenie sprzętu.

Ważne: Treść tych wytycznych, która odwołuje się do informacji ze stron internetowych firm zewnętrznych, jest poprawna w momencie publikacji, jednak informacje te mogą ulec zmianie bez uprzedniego powiadomienia ze strony Genetec Inc.

Spis treści

Wstęp: Preface
Informacje prawne
O tym przewodniku
Rozdział 1: Wprowadzenie do narzedzia Streamvault
Wprowadzenie do Narzedzia Streamvault [™]
Domyślne porty używane przez Streamyault
Informacie o aktualizacii oprogramowania SV w Panelu Sterowania SV
Podłaczanie komponentów urządzenia Streamyault
Wyłaczanie wejść dla kamery na kartach kodera w Streamyault urządzeniu
Wojączanie wejse ula kaniejy na kanach kodera w Streanwadić urządzeniu
Informacio na tomat kont ujutkowników Streamyault
Informacje na temat kont uzytkowników Streanwaut
Informacje dotyczące logowania do domysinych kont uzytkowników na urządzeniu Streamvault
O wzmacnianiu bezpieczenstwa Streamvault
Urządzenia z możliwością zarządzania wzmacnianiem bezpieczeństwa 1.
Rozdział 2: Pierwsze kroki z Panelem sterowania SV
Informacje o Panelu Sterowania SV
Konfigurowanie urządzenia w Panelu sterowania SV
Aktywacja licencji Security Center na urządzeniu
Ręczna aktywacja licencji z Server Admin
Aktywacja Monitora dostępności systemu
Włączanie funkcji kontroli dostępu i wideo w Security Center
Informacje o narzędziu rejestracji Jednostek
Otwarcie narzędzia rejestracji jednostek
Konfigurowanie ustawień dla rejestracji jednostek
Dodawanie jednostek
Usuwanie dodanych jednostek
Ignorowanie jednostek
Usuwanie jednostek z listy ignorowanych jednostek
Konfigurowanie domyślnych ustawień kamery
Tworzenienie niestandardowych harmonogramów nagrywania
Informacie o tworzeniu kopii zapasowych i przywracaniu danych
Tworzenie kopii zapasowej bazy danych Directory
Przywracanie bazy danych Diectory
Wybór metody tworzenia ról i partycii Archivera
Dodanie roli Archiver w Panelu Sterowania SV
Dodawanie partycji i ról Archiver recznie.
Rozdział 3: Pierwsze kroki z wtyczką Streamvault Maintenance
O Kancanyagia Straamyaulta utugtaa

O Konserwacja Streamvaulta wtyczce	•	•	•	•	•	•	•	•	•	•		•	•	46
Pobieranie i instalowanie wtyczki .				•		•	•							47

	Uprawnienia Genetec Streamvault	8
	Tworzenie roli wtyczki)
	Configurowanie Streamvault hardware monitor 5	1
	Konfigurowanie podmiotu managera Streamvault 5	5
	Informacje o karcie Zarządzanie	3
	Sprawdzanie stanu urządzenia przez Streamvault	9
	Kolumny panelu raportu dla zadania sprzętowego Streamvault 6	0
	Tworzenie reguł dla "od zdarzenia do działania" dla problemów technicznych Streamvault 6	1
Roz	dział 4: Informacje o Panelu Sterowania SV	
	Strona Główna Panelu Sterowania SV	4
	Strona Konfiguracujna Panelu Sterowania SV	6
	Strona Bezpieczeństwo w Panelu Sterowania SV	9
	Informacie o Panelu Sterowania SV	2
D		
KOZ	dział 5: Dodatkowe zasoby	
	Gwarancja na produkt dla Twojego urządzenia Streamvault	5
	Ponowne tworzenie obrazu urządzenia Streamvault	6
	Znajdowanie identyfikatora systemu i wersji obrazu dla urządzenia Streamvault 7	7
	Zezwalanie na udostępnianie plików na urządzeniu Streamvault	8
	Zezwalanie na połączenia Pulpitu Zdalnego z urządzeniem Streamvault 7	9
Roz	dział 6: Rozwiązywanie problemów	
	81 Wykonywanie resetu fabrycznego w urządzeniu typu All-in-one Streamvault (wszystko w jednym)	1
	Tworzenie klucza USB do resetowania ustawień fabrycznych dla urządzenia Streamvault All-in-one	
	(wszystko w jednym)	1
	Resetowanie obrazu oprogramowania na urządzeniu typu All-in-one (wszystko w jednym) 83	3
	Przywracanie ustawień fabrycznych naStreamvault stacji roboczej lub urządzeniu serwerowym 9	0
	Tworzenie klucza USB dla przywracania ustawień fabrycznych dla stacji roboczej Streamvault lub urządzenia serwerowego	0
	Przywracania obrazu fabrycznego oprogramowania na Streamvault stacji roboczej lub urządzeniu serwerowym	3
	Kontrolery Mercury EP pozostają w trybie offline, gdy protokół TLS 1.1 jest wyłączony 9	5
	Włączenie Harmonogramu Świtu i Zmroku (TLS)	6
	Pulpit zdalny nie chce się połączyć się z urządzeniem Streamvault	9
	Usuwanie ograniczeń z kont użytkowników niebędących administratorami	3
	Konta lokalne nie mają dostępu do Pulpitu Zdalnego, usługi udostępniania plików ani zdalnego	
	zarządzania	4
	Włączenie usług związanych ze Smart Card	5
	Włączanie obsługi oprogramowania układowego kontrolerów Mercury EP i LP w wersji 1.x.x 10	6
	Włączanie wsparcia integracji Synergis IX	8
Roz	dział 7: Pomoc techniczna	
	Kontakt z Centrum pomocy technicznej Genetec)
	Kontakt telefoniczny z GTAC	0
	Kontaktowanie się z GTAC poprzez GTAP	1
	Kontaktowanie się z GTAC za pośrednictwem czatu na żywo	1
	Wsparcie dotyczące oprogramowania	3
	Wsparcie sprzętowe	4
	Specyfikacje Streamvault	5
	Ogólne warunki wsparcia dotyczące Streamvault	6

Glosariusz	•	•	•	 •	•	•	•	•	•	•	•	•	117
Gdzie znaleźć informacje o produkc	ie .	•		•		•	•	•	•				119

1

Wprowadzenie do narzędzia Streamvault

Ta sekcja zawiera następujące tematy:

- "Wprowadzenie do Narzędzia Streamvault[™]", 2
- "Domyślne porty używane przez Streamvault", 4
- "Informacje o aktualizacji oprogramowania SV w Panelu Sterowania SV ", 7
- "Podłączanie komponentów urządzenia Streamvault", 8
- "Informacje na temat kont użytkowników Streamvault", 12
- "Logowanie do Streamvault urządzenia", 14
- "O usłudze Streamvault", 15
- "O wzmacnianiu bezpieczeństwa Streamvault", 16

Wprowadzenie do Narzędzia Streamvault™

Możesz wdrożyć urządzenie Streamvault[™] w Security Center, wykonując sekwencję kroków.

Przegląd procesu wdrożenia

Krok	Zadanie	Gd	zie znaleźć więcej informacji
Przec	l wdrożeniem zapoznaj się z wymaganiami	wst	ępnymi i kluczowymi problemami
1	Otwórz wymagane porty sieciowe, aby połączyć podstawowe systemy w Security Center i moduły Streamvault. Podłącz urządzenia peryferyjne, takie jak monitor, klawiatura, karta enkodera analogowego i urządzenia do wejść i wyjść. Podłącz urządzenie do swojej sieci.	•	Domyślne porty używane przez Streamvault, 4. Podłączanie komponentów urządzenia Streamvault, 8. Karty enkoderów analogowych Genetec, 8. Wyłączanie wejść dla kamery na kartach kodera w Streamvault urządzeniu, 9. Wejścia i wyjścia alarmowe Streamvault urządzenia, 10.
2	Przed wdrożeniem urządzenia zapoznaj się z zawartością wersji obrazu.	•	Zawartość każdego wydania obrazu Streamvault.
3	Zaloguj się do systemu Windows jako administrator, używając hasła wydrukowanego na urządzeniu, a następnie zmień hasło.	•	Logowanie do Streamvault urządzenia, 14.
Ukoń	cz kreatory konfiguracjujne		
4	Ukończ kreator <i>Konfiguracji Panelu</i> Sterowania Streamvault . Uwaga: Pulpit zdalny jest domyślnie wyłączony. Aby włączyć pulpit zdalny, włącz usługę Pulpit zdalny na stronie <i>Bezpieczeństwo</i> w Panelu sterowania SV.	•	Konfigurowanie urządzenia w Panelu sterowania SV , 19. Zezwalanie na połączenia Pulpitu Zdalnego z urządzeniem Streamvault, 79.
5	 Aktywuj licencję Security Center. Jeśli urządzenie jest podłączone do Internetu, aktywuj licencję za pomocą kreatora Aktywacji Panelu Sterowania Streamvault . Jeśli urządzenie nie jest podłączone do Internetu, aktywuj licencję ręcznie z poziomu Administratora Serwera. 	•	Aktywacja licencji Security Center na urządzeniu , 22. Ręczna aktywacja licencji z Server Admin , 24.
6	Aktywuj Monitor Dostępności Systemu.	•	Aktywacja Monitora dostępności systemu , 26.
7	Skonfiguruj Usługę dotyczącą Aktualizacji Genetec [™] , aby mieć zawsze najnowszą wersję Security Center i Panelu Sterowania SV Jeśli są aktualizacje, zainstaluj je.	•	Konfigurowanie Usługi Aktualizacji Genetec.

Krok	Zadanie	G	dzie znaleźć więcej informacji
8	Jeśli Panel Sterowania SV wskazuje, że dostępnych jest więcej aktualizacji, zainstaluj je teraz.	•	Informacje o aktualizacji oprogramowania SV w Panelu Sterowania SV , 7.
9	W przypadku urządzenia Archiver utwórz wymaganą ilość ról Archiver potrzebną do obsługi danej ilości kamer i całkowitej przepustowości sieci zaplanowanej do wdrożenia.	•	Dla serii SV-1000E, SV-2000E, SV-4000E : Dodanie roli Archiver w Panelu Sterowania SV, 40. Dla SV-7000EX i All-in-one: Dodawanie partycji i ról Archiver ręcznie., 42.
10	Zaloguj się do Narzędzia Konfiguracyjnego Config Tool i skonfiguruj funkcje Wideo i Kontroli Dostępu w Centrum zabezpieczeń.	•	Włączanie funkcji kontroli dostępu i wideo w Security Center , 27. Konfigurowanie ustawień dla rejestracji jednostek, 30.
11	Utwórz kopię zapasową konfiguracji Security Center.	•	Tworzenie kopii zapasowej bazy danych Directory , 38.

Domyślne porty używane przez Streamvault

Wymagane porty sieciowe muszą być otwarte, aby umożliwić prawidłowe działanie następujących komponentów Streamvault[™].

Wymagane porty dla wtyczki Streamvault Maintenance

Na zewnętrznej zaporze sieciowej musi być otwarty następujący port dla ruchu przychodzącego, aby wtyczka Streamvault[™] Maintenance mogła komunikować się ze sprzętem Streamvault. Wymaganie to ma zastosowanie wyłącznie w przypadku spełnienia następujących trzech warunków:

- Wewnętrzne połączenie systemu operacyjnego z kontrolerem iDRAC Pass-through jest wyłączone
- iDRAC korzysta z dedykowanego portu LAN
- Między siecią iDRAC a siecią hosta znajduje się zapora sieciowa firewall

W każdej innej sytuacji, wymóg ten można zignorować.

Moduł	Port wejściowy	Wykorzystanie portu
monitor sprzętu Streamvault	65116	Służy do komunikacji HTTPS między Security Center i kontrolerem zarządzania płytą główną iDRAC sprzętu Streamvault za pośrednictwem sieci.

Panel Sterowania SV wymaga portów

Wymienione poniżej porty wyjściowe muszą być otwarte, aby umożliwić komponentom Panelu sterowania Streamvault połączenie się z usługami w chmurze Genetec[™].

Port wyjściowy	Wykorzystanie portu	Docelowy adres URL	
TCP 443	Komunikacja HTTPS z usługami	svbackupservices.genetec.com	
	tworzenia kopil zapasowych Genetec	genetecbackupservice.blob.core.win	idows.net

Wymagane porty dla CylancePROTECT

Wymienione poniżej porty ruchu wychodzącego muszą być otwarte, aby agent CylancePROTECT mógł komunikować się z konsolą zarządzania Genetec i otrzymywać aktualizacje dla agenta.

Port wyjściowy	Wykorzystanie portu	Docelowy adres URL
ТСР 443 К Р	Komunikacja HTTPS w Ameryce	cement.cylance.com
	Połnocnej	data.cylance.com
		protect.cylance.com
		update.cylance.com
		api.cylance.com
		download.cylance.com
		venueapi.cylance.com

Port wyjściowy	Wykorzystanie portu	Docelowy adres URL
TCP 443	Komunikacja HTTPS w północno- wschodniej części Azji i Pacyfiku	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	Komunikacja HTTPS w południowo-wschodniej części Azji i Pacyfiku	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	Komunikacja HTTPS w Europie Środkowej	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
TCP 443	Komunikacja HTTPS w Ameryce Południowej	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

Port wyjściowy	Wykorzystanie portu	Docelowy adres URL					
TCP 443	Komunikacja HTTPS w 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					
TCP 443	Komunikacja HTTPS w celu aktywacji Cylance po ponownej instalacji	svservices.genetec.com					

Uwaga: Jeśli nie chcesz otwierać powyższych połączeń wychodzących, CylancePROTECT można przełączyć w tryb rozłączony. W trybie rozłączonym CylancePROTECT otrzymuje aktualizacje z narzędzi podprocesu poprzez Usługi Aktualizacji Genetec[™] (GUS).

Aby uzyskać więcej informacji na temat trybów, w których urządzenie Streamvault komunikuje się z usługami zarządzania Genetec, zobacz Strona Bezpieczeństwo w Panelu Sterowania SV, 69.

Informacje o aktualizacji oprogramowania SV w Panelu Sterowania SV

Usługa Aktualizacji Genetec[™] (GUS) jest zintegrowana z Panelem Sterowania SV, aby zapewnić aktualizacje komponentów oprogramowania urządzenia.

Gdy aktualizacje będą dostępne, wyświetlony zostanie przycisk **Wyświetl aktualizacje** z etykietą wskazującą liczbę dostępnych aktualizacji. Kliknięcie przycisku **Wyświetl aktualizacje** powoduje uruchomienie GUS w przeglądarce.

Uwaga: Kolor etykiety różni się w zależności od tego jak ważna jest aktualizacja. Pomarańczowa etykieta oznacza zalecane aktualizacje, a czerwona etykieta oznacza aktualizacje krytyczne.



Główne cechy GUS są następujące:

- Zaktualizuj swoje produkty Genetec[™], gdy pojawi się nowa wersja.
- Sprawdzaj dostępność aktualizacji w regularnych odstępach czasu.
- Skonfiguruj aktualizacje, które mogą być pobierane w tle, ale nadal musisz je zainstalować ręcznie.
- · Zobacz, kiedy miało miejsce ostatnie sprawdzenie dostępności aktualizacji.
- Automatycznie odświeża licencję w tle, aby upewnić się, że jest ważna, a data jej wygaśnięcia jest aktualizowana.
- Włącz różne funkcje, takie jak Genetec Improvement Program.
- Sprawdza oprogramowanie sprzętowe i zaleca aktualizacje lub powiadamia o lukach w zabezpieczeniach.

Więcej informacji na temat korzystania z GUS można znaleźć w zakładce Genetec[™] Update Service User Guide w TechDoc Hub

Podłączanie komponentów urządzenia Streamvault

Aby przygotować urządzenie Streamvault[™] do użycia, należy podłączyć wymagane urządzenia peryferyjne (monitor, klawiatura i mysz), opcjonalne urządzenia peryferyjne, sieć i źródło zasilania.

Zanim rozpoczniesz

Oczyść przestrzeń wokół przycisku zasilania. Aby zapobiec przypadkowemu wyłączeniu urządzenia, upewnij się, że nic nie dotyka przycisku zasilania ani nie znajduje się zbyt blisko niego.

Procedura

- 1 Podłącz kabel monitora do obsługiwanego wejścia wideo: złącza VGA, HDMI lub DisplayPort. Do urządzenia musi być podłączony co najmniej jeden monitor. Do tego samego urządzenia można podłączyć maksymalnie trzy monitory.
- 2 Podłącz monitor do gniazdka elektrycznego i włącz monitor.
- 3 Podłącz klawiaturę i mysz do wolnego portu USB.
- 4 (Opcjonalnie) Podłącz opcjonalne urządzenia peryferyjne:
 - Głośniki
 - Kamery analogowe
 - Wejścia i wyjścia alarmowe
- 5 Podłącz kabel Ethernet do portu Ethernet w urządzeniu. Podłącz drugi koniec kabla do gniazda RJ-45 sieci IP.
- 6 W przypadku urządzeń Streamvault[™] SV-100E włóż wtyczkę prądu stałego do gniazda wejściowego 19.5V urządzenia, a drugi koniec do zasilacza. Podłącz przewód z cegły do gniazdka elektrycznego.
- 7 Aby włączyć urządzenie Streamvault, naciśnij przycisk zasilania.

Po zakończeniu

Zaloguj się do swojego urządzenia Streamvault.

Karty enkoderów analogowych Genetec

Jeśli używasz urządzenia Streamvault do wdrożenia systemu zarządzania wideo z kamerami analogowymi, musisz podłączyć kamery do karty enkodera analogowego Genetec[™] w urządzeniu.

Specyfikacje karty enkodera analogowego

Poniższe specyfikacje mają zastosowanie dla Streamvault urządzeń wyposażonych w analogową kartę graficzną

- 8 lub 16 analogowych wejść wideo w zależności od zainstalowanej karty
- Maksymalna rozdzielczość wideo 4CIF
- Maksymalna liczba klatek na sekundę: 30 kl./s
- Obsługuje format kompresji H.264

Ograniczenie: Aby karta enkodera analogowego mogła nagrywać, urządzenie Streamvault musi mieć połączenie sieciowe. Jeśli połączenie sieciowe jest niedostępne, należy skonfigurować interfejs pętli zwrotnej, aby karta kodera mogła działać prawidłowo.



O podłączaniu kamer analogowych

Jeśli urządzenie Streamvault zawiera kartę enkodera analogowego Genetec, jest ono dostarczane z kablem ze złączami BNC. Złącza BNC służą do podłączenia kamer analogowych bezpośrednio do wbudowanej karty enkodera.

Informacje o dodawaniu kamer analogowych w Security Center

Aby dodać kamery analogowe w Security Center musisz skorzystać z narzędzia rejestracji jednostek. Aby uzyskać więcej informacji zobacz Informacje o narzędziu rejestracji jednostek.

Podczas dodawania kamer analogowych należy wziąć pod uwagę następujące kwestie:

- Nie można dodawać kamer analogowych w Security Center przy użyciu metody *Dodawania Ręcznego* . Skorzystaj z Narzędzia rejestracji Jednostek.
- Aby odkryć nowe jednostki i skorzystać z Narzędzia do rejestracji jednostek, musisz lokalnie połączyć się z narzędziem konfiguracyjnym (Config Tool)
- Po wybraniu producenta kamery w narzędziu rejestracji jednostek, wszystkie kamery analogowe zostaną wyświetlone według nazwy producenta *Karty enkodera Genetec*.

Wyłączanie wejść dla kamery na kartach kodera w Streamvault urządzeniu

Aby uaktualnić licencję na połączenie kamery z analogowej na IP, należy wyłączyć wejścia dla kamery na karcie kodera.

Procedura

- 1 Na stronie głównej narzędzia konfiguracyjnego Config Tool kliknij kartę Informacje .
- 2 Kliknij kartę **Omnicast**[™] i sprawdź liczbę kamer wyświetloną przy opcji *Liczba kamer i monitorów analogowych*.

Na przykład 16 / 16.

- 3 Otwórz zadanie Wideo.
- 4 W drzewie podmiotów, kliknij jednostkę wideo odpowiadającą karcie kodera.
- 5 Kliknij kartę **Urządzenia Peryferyjne** i wybierz kamery, które chcesz wyłączyć. Można wybrać wiele kamer, naciskając klawisz Ctrl i klikając poszczególne kamery.
- ⁶ Na dole strony *Urządzenia peryferyjne* kliknij czerwone kółko (), aby wyłączyć kamery, a następnie kliknij **Zastosuj**.

Wyłączone kamery są wyszarzone, a po lewej stronie każdej wyłączonej kamery na liście wyświetlana zostanie czerwona kropka.

7 Na stronie *Informacje* sprawdź, czy liczba kamer jest zgodna. Może być konieczne ponowne uruchomienie narzędzia konfiguracyjnego w celu odświeżenia poprawnej ilości kamer.

Uwaga: Jeśli kamera którą wyłączyłeś nagrała wideo, zostanie wyświetlona w drzewie podmiotów w zadaniu Security Desk *Monitoring* Będziesz mógł odtworzyć wideo z tej kamery.

Wejścia i wyjścia alarmowe Streamvault urządzenia

Jeśli używasz Streamvault urządzenia do wdrożenia systemu kontroli dostępu, możesz użyć karty wejścia/ wyjścia, aby podłączyć sprzętowe wejścia alarmowe bezpośrednio do urządzenia, aby następnie móc sterować jego wyjściami za pomocą funkcji zdarzenie-działanie (event-to-action) w Security Center.

Specyfikacje karty wejścia/wyjścia

Poniższe specyfikacje dotyczą Streamvault modeli wyposażonych w kartę wejścia/wyjścia

- 4 wyjścia wyzwalające
- 8 wejść alarmowych
- Port komunikacyjny RS-485



Informacje na temat podłączania kart wejść/wyjścia

Można podłączyć przewody wejściowe i wyjściowe urządzeń sprzętowych bezpośrednio do karty we/wy z tyłu Streamvault urządzenia. Przewody należy włożyć za pomocą małego płaskiego śrubokręta wciskając zaciski napinające na złączu.

Jak utworzyć funkcje zdarzenie-działanie

Aby uzyskać informacje na temat funkcji zdarzenie-działanie dla Streamvault zobacz Tworzenie funkcji zdarzenie-działanie w TechDoc Hub.

Informacje na temat kont użytkowników Streamvault

Istnieją dwa typy kont użytkowników Streamvault[™]: konta administratora lokalnego i konta użytkownika lokalnego innego niż administrator. W zależności od tego, jakiego typu konta użytkownika używasz do logowania się w Panelu sterowania SV, zobaczysz tylko te funkcje, które mają zastosowanie dla Twojego typu konta.

Administrator lokalny

Konto użytkownika administratora lokalnego (Admin) jest tworzone domyślnie. Osoba zalogowana jako Administrator posiada pełne uprawnienia administracyjne do Panelu Sterowania SV. Administrator może konfigurować wszystkie ustawienia systemowe oraz te związane z bezpieczeństwem poprzez Panel Sterowania SV, a także tworzyć konta użytkowników które nie mają uprawnień administratora.

Konto użytkownika lokalnego (bez uprawnień administratora)

Domyślnym kontem użytkownika lokalnego (bez uprawnień administratora) dla urządzeń All-in-one i stacji roboczych jest konto Operatora. Osoba zalogowana jako Operator posiada ograniczony dostęp do funkcji Panelu Sterowania SV. Operator może uruchomić narzędzie Config Tool i Security Desk, przeglądać informacje o systemie i licencjach oraz uzyskiwać dostęp do dokumentacji produktu.

Osoba zalogowana jako Administrator może tworzyć konta (bez uprawnień administratora), które również będą miały ograniczony dostęp do Panelu Sterowania SV.

Uwaga: Możliwe jest usunięcie domyślnych ograniczeń dostępu, nałożonych na wszystkie konta użytkowników bez uprawnień administratora. Aby uzyskać informacje na temat tego jak to zrobić, zobacz Usuwanie ograniczeń z kont użytkowników niebędących administratorami, 103.

Tematy pokrewne

Informacje dotyczące logowania do domyślnych kont użytkowników na urządzeniu Streamvault, 12

Informacje dotyczące logowania do domyślnych kont użytkowników na urządzeniu Streamvault

Przy pierwszym uruchomieniu urządzenia Streamvault tworzone są konta Administratora i Operatora systemu Windows. Konta te mają różne prawa dostępu i ustawione domyślne hasła. Administrator Serwera również ma ustawione domyślne hasło.

Poniższe hasła domyślne służą do pierwszego logowania. Podczas konfiguracji, możesz utworzyć własne hasło do Narzędzia Konfiguracyjnego Config Tool i Security Desk.

Nazwa użytkownika	Domyślne hasło	Przyznano dostęp do	Odmowa dostępu do
Administrator	admin	Pełny dostęp do systemu:	Nie dotyczy
		 Windows: wszystkie funkcje systemowe i administracyjne 	
		Security Center	
		Panelu Sterowania SV	

Nazwa użytkownika	Domyślne hasło	Przyznano dostęp do	Odmowa dostępu do
Operator	Operator	 Kosza Biblioteki Mojego Komputera dysku C: Strony głównej Panelu Sterowania SV, Strony Konfiguracyjnej- tylko ustawienia regionalne, strony Informacyjnej Administrator serwera: wymaga hasła Administratora, aby uzyskać pełne uprawnienia 	 Windowsa: zamknij i uruchom ponownie Ustawień systemowych Partycji wideo
Nie dotyczy	genetecfactory	Server Admin	Uwaga: Ta opcja jest niedostępna dla urządzeń Stacji Roboczej.

Aby zmienić konto użytkownika systemu Windows, aplikację kliencką lub hasło dla Administratora Serwera, zaloguj się do Panelu Sterowania SV przy użyciu konta użytkownika Administratora Systemu Windows Na stronie *Bezpieczeństwo, w* sekcji Dane uwierzytelniające możesz zarządzać wszystkimi swoimi hasłami.

Uwaga: Konta Operatora nie tworzy się przy użyciu szablonu. Jeśli utworzysz nowe konto użytkownika, domyślnie nie będą one miały takich samych ograniczeń.

Administrator Serwera w Security Center

- Tylko użytkownicy administracyjni mogą się logować do Server Admin.
- Aby zalogować się z komputera lokalnego, kliknij skrót **Server Admin** na pulpicie.
- Aby zdalnie zalogować się do Administratora Serwera, potrzebujesz nazwy DNS lub adresu IP serwera, portu serwera WWW i hasła serwera. Po wprowadzeniu domyślnego hasła zostanie wyświetlona prośba o jego zmianę.

Ważne: Aby zapewnić bezpieczeństwo systemu, natychmiast zmień wszystkie domyślne hasła. Stosuj najlepsze praktyki branżowe do tworzenia silnych haseł.

Tematy pokrewne

Informacje na temat kont użytkowników Streamvault, 12

Logowanie do Streamvault urządzenia

Przy pierwszym uruchomieniu urządzenia Streamvault[™] zostanie wyświetlony monit o zmianę domyślnego hasła administratora. Zmień także domyślne hasło Operatora. Następnie możesz zalogować się jako użytkownik w trybie Operatora lub Administratora.

Zanim rozpoczniesz

Dowiedz się, jakie uprawnienia dostępu mają konta Operatora i Administratora.

Co powinieneś wiedzieć

Aby skonfigurować urządzenie w Panelu Sterowania SV, zaloguj się jako Administrator. Ważne: Hasła muszą spełniać następujące wymagania:

Minimum 14 znaków

Minimalna długość znaków wynosi 10, w przypadku urządzeń z wersjami obrazu, które nie posiadają usługi Streamvault. Aby uzyskać informacje na temat tego, które urządzenia obsługują usługę Streamvault, a które nie, zobacz Urządzenia z możliwością zarządzania wzmacnianiem bezpieczeństwa, 17.

- Co najmniej trzy symbole z następujących czterech kategorii:
 - Wielkie litery
 - Małe litery
 - Cyfry od 0-9
 - Znaki inne niż alfanumeryczne (takie jak \$,%,!)

Procedura

- 1 Włącz urządzenie.
- 2 Zaloguj się, używając konta administratora i domyślnego hasła wydrukowego na urządzeniu
- Wprowadź nowe hasło dla Administratora.
 Jesteś zalogowany jako Administrator.
 Uwaga: Niektóre modele mają domyślnie dostępne tylko konto administratora.
- 4 Wyloguj się, a następnie zaloguj, używając konta Operatora i domyślnego hasła wydrukowanego na urządzeniu.
- 5 Wprowadź nowe hasło dla Operatora. Jesteś zalogowany jako Operator.
- 6 Kontynuuj operacje na koncie Operatora lub wyloguj się i zaloguj ponownie jako użytkownik Admin.

Po zakończeniu

Rozpocznij wstępną konfigurację urządzenia.

O usłudze Streamvault

Usługa Streamvault to usługa systemu Windows umożliwiająca użytkownikom konfigurowanie urządzenia Streamvault[™], np. poprzez stosowanie profili wzmacniających bezpieczeństwo.

Usługa Streamvault może wdrożyć na urządzeniach następujące profile wzmacniania zabezpieczeń:

- Podstawowe zasady bezpieczeństwa firmy Microsoft
- Podstawowe zasady bezpieczeństwa firmy Microsoft z profilem Centrum Bezpieczeństwa Internetowego (CIS) Poziom 1
- Podstawowe zasady bezpieczeństwa firmy Microsoft z profilem CIS poziom 2
- Podstawowe linie zabezpieczeń firmy Microsoft z profilem Wdrożenie Techniczne Zabezpieczeń (STIG)

Więcej informacji o profilach wzmacniania bezpieczeństwa znajdziesz tutaj O wzmacnianiu bezpieczeństwa Streamvault, 16

Gdy użytkownik będący administratorem wybierze profil wzmacniania bezpieczeństwa w Panelu Sterowania SV, usługa Streamvault wdroży określony profil dla urządzenia.

Aktualizacje Streamvault są okresowo udostępniane i można je zainstalować za pośrednictwem usługi Aktualizacja Genetec[™](GUS) lub Portalu Pomocy Technicznej (GTAP). Gdy aktualizacja będzie dostępna, w Panelu Sterowania SV pojawi się powiadomienie. Stosowanie aktualizacji jest opcjonalne, ale zalecane w celu uzyskania dostępu do aktualnych wersji dla profili wzmacniania bezpieczeństwa.

O wzmacnianiu bezpieczeństwa Streamvault

Wzmacnianie bezpieczeństwa zwiększa bezpieczeństwo urządzenia Streamvault[™] poprzez zastosowanie określonych ustawień zabezpieczeń.

Gdy wzmacniasz zabezpieczenia swojego urządzenia, optymalizujesz je pod kątem większego bezpieczeństwa, ale może się to odbywać kosztem użyteczności i wydajności tego urządzenia. Stopień wzmocnienia zabezpieczenia urządzenia zależy od modelu zagrożenia i wrażliwości informacji.

Wzmacnianie zabezpieczenia urządzenia odbywa się na stronie *Bezpieczeństwo* w Panelu Sterowania SV. Można wybierać spośród czterech predefiniowanych profili wzmacniania.

Domyślnie, wszystkie urządzenia są dostarczane z zastosowanym profilem wzmacniającym Microsoft CIS na poziomie 2.

Profil wzmacniający zabezpieczenia	Opis	
Microsoft (tylko)	Ten profil wzmacniania zabezpieczeń stosuje w Twoim systemie podstawowe zasady bezpieczeństwa firmy Microsoft. Podstawowe linie zabezpieczeń firmy Microsoft to grupa zalecanych przez firmę Microsoft konfiguracji ustawień, które zostały opracowane na podstawie opinii zespołów inżynierów ds. zabezpieczeń, grup produktów, partnerów i klientów firmy Microsoft.	
	W urządzeniach Streamvault wdrożono następujące wersje bazowe oprogramowania Microsoft: wersję bazową systemu Windows i wersję bazową przeglądarki Microsoft Edge.	
Microsoft z CIS Poziom 1	Ten profil wzmacniania zabezpieczeń stosuje w systemie podstawowe zasady bezpieczeństwa firmy Microsoft oraz profil Centrum Bezpieczeństwa Internetowego (CIS) Poziom 1 (CIS L1). Certyfikat CIS L1 zapewnia podstawowe wymagania bezpieczeństwa, które można wdrożyć w dowolnym systemie przy niewielkim lub żadnym wpływie na wydajność lub ograniczenie funkcjonalności.	
Microsoft z CIS Poziom 2	Ten profil wzmacniania zabezpieczeń stosuje w systemie podstawowe zabezpieczenia firmy Microsoft oraz profile CIS L1 i Poziom 2 (L2). Profil CIS L2 oferuje najwyższy poziom bezpieczeństwa i jest przeznaczony dla organizacji, dla których bezpieczeństwo jest priorytetem.	
	Bezwzględne zabezpieczenia, jakie wprowadza ten profil wzmacniający bezpieczeństwo mogą ograniczyć funkcjonalność systemu i utrudnić zdalne zarządzanie serwerem.	
Microsoft z STIG	Ten profil wzmacniania zabezpieczeń stosuje dla systemu podstawowe zasady bezpieczeństwa firmy Microsoft oraz opiera dane na wytycznych Wdrażania Rozwiązań Technicznych w Zakresie Bezpieczeństwa (STIG) Agencji ds. Systemów Informacyjnych Departamentu Obrony (DISA). DISA STIG opierają się na standardach Narodowego Instytutu Norm i Technologii (NIST) i zapewniają zaawansowaną ochronę bezpieczeństwa systemów Windows dla Departamentu Obrony Stanów Zjednoczonych.	

Uwaga: Profile wzmacniające bezpieczeństwo są dostępne tylko w urządzeniach, które mają*Usługa Streamvault*. Aby uzyskać więcej informacji, zobacz O usłudze Streamvault, 15.

Urządzenia z możliwością zarządzania wzmacnianiem bezpieczeństwa

Możliwości zarządzania wzmacnianiem zabezpieczeń są dostępne tylko w urządzeniach z usługą Streamvault™. Typ urządzenia i obraz decydują o dostępności usługi Streamvault.

Typ urządzenia	Wersje obrazów z usługą Streamvault	Wersje obrazów bez usługi Streamvault
All-in-one (Wszystko w jedym)	• 11.2024.2	 16 17 18 19
SVW	• 11.2024.2	 0010.4 0011.2 0012.2 0013.2
SVA	• 11.2024.2	 0010.4 0011.2 0012.2 0013.2
SVR	10.2021.211.2024.2	• 0012.2.X
Inne urządzenia Streamvault.	• WS.2022.1	 2016.1.B 2016.1.C 2019.1 2019.4.C 2022.1.C

Poniższa tabela przedstawia, które urządzenia oferują usługę Streamvault, a które nie.

Uwaga: Aby znaleźć informacje na temat wersji obrazu swojego urządzenia, zobacz tutaj Znajdowanie identyfikatora systemu i wersji obrazu dla urządzenia Streamvault, 77

Pierwsze kroki z Panelem sterowania SV

Dokument Pierwsze Kroki zawiera wprowadzenie do Panelu Sterowania SV oraz informacje na temat konfigurowania urządzenia Streamvault.

Ta sekcja zawiera następujące tematy:

- "Informacje o Panelu Sterowania SV", 19
- "Aktywacja licencji Security Center na urządzeniu", 22
- "Ręczna aktywacja licencji z Server Admin", 24
- "Aktywacja Monitora dostępności systemu ", 26
- "Włączanie funkcji kontroli dostępu i wideo w Security Center ", 27
- "Informacje o narzędziu rejestracji Jednostek", 30
- "Konfigurowanie domyślnych ustawień kamery", 33
- "Tworzenienie niestandardowych harmonogramów nagrywania", 35
- "Informacje o tworzeniu kopii zapasowych i przywracaniu danych ", 37
- "Wybór metody tworzenia ról i partycji Archivera", 40

Informacje o Panelu Sterowania SV

Panel Sterowania SV to aplikacja interfejsu użytkownika, której można użyć do skonfigurowania urządzenia Streamvault[™] do współpracy z kontrolą dostępu i nadzorem wideo w Security Center. Ostrożnie: Zmiany konfiguracji wprowadzone w Panelu Sterowania SV spowoduja nadpisanie zmian

konfiguracji dokonanych poza Panelem sterowania SV, w tym niestandardowych ustawień systemu Windows.

Panel Sterowania SV można uruchomić w następujących trybach:

- Tryb rozszerzony dla konfiguracji działających na serwerze dodatkowym.
- Tryb klienta dla konfiguracji działających na urządzeniach stacji roboczej.
- Tryb Directory dla konfiguracji uruchomionych na serwerze Primary.

Panel Sterowania SV obsługuje następujące funkcje:

- Kreator konfiguracji Panelu Sterowania Streamvault, który pomoże Ci szybko skonfigurować urządzenie.
- Kreator aktywacji Panelu Sterowania Streamvault, który pomoże Ci aktywować urządzenie.
- Asystent Instalatora Security Center, którego można użyć do skonfigurowania Security Center.
- *Kreatory Kopii Zapasowych Panelu Sterowania Streamvault* i *Kreatory Przywracania danych Panelu Sterowania Streamvault* pomagają w tworzeniu kopii zapasowych bazy danych i konfiguracji Directory oraz przywracaniu tych plików dla potrzeb systemu, jeśli to konieczne.
- Usługę Aktualizacji Genetec[™] (GUS), która regularnie sprawdza dostępność aktualizacji oprogramowania
- Skróty do często używanych zadań w Config Tool i Security Desk.
- Linki do Portalu Pomocy Technicznej Genetec (GTAP) i dokumentacji produktu.
- Możliwość wyboru trybu działania oprogramowania antywirusowego Cylance dostarczonego z urządzeniem Streamvault[™]. Opcje są wymienione na stronie konfiguracji dla *Zabezpieczeń*.
- Możliwość tworzenia kolejnych ról i partycji Archiver dla konfiguracji na serwerach dodatkowych.

Uwaga: Niniejszy przewodnik dotyczy SV Control Panel w wersji 3.0, którą można pobrać ze strony GTAP.

Panel Sterowania SV w wersji 3.0 jest kompatybilny z urządzeniami, które nie obsługują usługi Streamvault. Jednakże urządzenia te nie będą miały dostępu do profili o wzmocnionym zabezpieczeniu.

Konfigurowanie urządzenia w Panelu sterowania SV

Gdy po raz pierwszy logujesz się do urządzenia Streamvault[™], Panel sterowania SV otworzy kreator *Konfiguracji Panelu Sterowania Streamvault*, który poprowadzi Cię przez wstępną konfigurację.

Zanim rozpoczniesz

Podłącz urządzenie do Internetu.

Co powinieneś wiedzieć

- Ustawienia zastosowane w kreatorze można później zmienić na stronie Konfiguracja Panelu Sterowania SV.
- W przypadku Archivera, Analytics, Workstation lub innego urządzenia będącego serwerem rozszerzeń Security Center nie pojawia się monit o zmianę haseł użytkowników.

Procedura

1 Uruchom urządzenie.

Panel Sterowania SV uruchamia się oknem *Konfiguracji Panelu Sterowania Streamvault* **Uwaga:** Panel Sterowania SV otwiera się automatycznie dopiero przy pierwszym uruchomieniu urządzenia. Przy kolejnych uruchomieniach użytkownicy muszą zalogować się przy użyciu danych administratora i uruchomić Panel Sterowania SV.

- 2 Na stronie Wprowadzenie kliknij przycisk Dalej.
- 3 Na stronie Sieć skonfiguruj ustawienia dla połączenia IP:
 - a) Jeśli używasz protokołu DHCP do automatycznego przydzielenia adresu IP (domyślnie) ale tego adresu IP nie ma na liście, kliknij Odśwież (), aby uzyskać nowy adres IP. Następnie kliknij Spróbuj ponownie.
 - b) Jeśli w polu **Status** wyświetlona zostanie informacja inna niż "Połączono z Internetem", kliknij opcję **Spróbuj Ponownie**.
 - c) Gdy w polu Status wyświetlony zostanie komunikat "Połączono z Internetem", kliknij Dalej.
- 4 Na stronie Konfiguracja komputera wypełnij pola w sekcjach Informacje Ogólne i Ustawienia Regionalne .
- 5 Aby zmienić interfejs użytkownika na inny język:
 - a) Z listy Język Produktuwybierz swój język.
 - b) Uruchom ponownie Panel Sterowania SV.
 - c) Gdy ponownie otworzy się kreator *Konfiguracji Panelu sterowania Streamvault*na stronie **Konfiguracji komputera** kliknij *Dalej.*
- 6 Na stronie Konfiguruj CylancePROTECT wybierz tryb komunikacji:
 - **Online (zalecane):** W trybie online Agent CylancePROTECT komunikuje się z firmą Genetec w celu zgłaszania nowych zagrożeń, aktualizacji narzędzia podprocesu i wysyłania danych w celu udoskonalenia modeli matematycznych. Ta opcja zapewnia najwyższy poziom ochrony.
 - Tryb Rozłączony: Tryb rozłączony dotyczy urządzenia bez połączenia z Internetem. W tym trybie CylancePROTECT nie może łączyć się, ani wysyłać informacji do usług zarządzania Genetec w chmurze. Twoje urządzenie jest chronione przed większością zagrożeń. Przeglądy techniczne i aktualizacje są dostępne za pośrednictwem Usługi Aktualizacji Genetec[™] (GUS).
 - **Tryb Wyłączony:** Wybierz ten tryb, aby trwale odinstalować CylancePROTECT ze swojego urządzenia. Twoje urządzenie będzie używać usługi Microsoft Defender do ochrony i wykrywania zagrożeń. Nie zalecamy wyłączania CylancePROTECT, jeśli urządzenie nie może otrzymywać aktualizacji dotyczących sygnatur wirusów w Microsoft Defender.
- 7 Kliknij opcję **Włącz zarządzanie kwarantanną**, aby dodać dodatkowe funkcje do ikony Cylance na pasku zadań, w tym opcję **Usuń poddane kwarantannie**, umożliwiającą usuwanie plików poddanych kwarantannie przez Cylance.
- 8 Na stronie *Poświadczenia* kliknij opcję **Zmień hasło** aby skonfigurować hasła dla następujących aplikacji:
 - Security Center (Administrator): Hasło administratora dla Security Desk, Config Tool, and Genetec[™] Update Service.
 - Server Admin : Hasło dla Genetec[™] Server Admin application.

Jeśli Twoje urządzenie Security Center posiada dodatkowy serwer, nie zostaniesz poproszony o zmianę hasła. Wybierz opcję **Pomiń ten krok**, jeśli nie chcesz ustawiać nowych haseł.

- 9 Na stronie Wzmocnione zabezpieczenia wybierz jeden z następujących profili wzmocnienia:
 - Microsoft (tylko): Ten profil wzmacniania zabezpieczeń stosuje w Twoim systemie podstawowe zasady bezpieczeństwa firmy Microsoft. Podstawowe linie zabezpieczeń firmy Microsoft to grupa zalecanych przez firmę Microsoft konfiguracji ustawień, które zostały opracowane na podstawie opinii zespołów inżynierów ds. zabezpieczeń, grup produktów, partnerów i klientów firmy Microsoft.
 - Microsoft z CIS Poziom 1: Ten profil wzmacniania zabezpieczeń stosuje w systemie podstawowe zasady bezpieczeństwa firmy Microsoft oraz profil Centrum Bezpieczeństwa Internetowego (CIS) Poziom 1 (CIS L1). Certyfikat CIS L1 zapewnia podstawowe wymagania bezpieczeństwa, które można wdrożyć w dowolnym systemie przy niewielkim lub żadnym wpływie na wydajność lub ograniczenie funkcjonalności.
 - Microsoft z CIS Poziom 2: Ten profil wzmacniania zabezpieczeń stosuje w systemie podstawowe zabezpieczenia firmy Microsoft oraz profile CIS L1 i Poziom 2 (L2). Profil CIS L2 oferuje najwyższy

poziom bezpieczeństwa i jest przeznaczony dla organizacji, dla których bezpieczeństwo jest priorytetem.

Uwaga: Surowe zabezpieczenia, jakie wprowadza ten profil wzmacniający, mogą ograniczyć funkcjonalność systemu i utrudnić zdalne zarządzanie serwerem.

 Microsoft z STIG: Ten profil wzmacniania zabezpieczeń stosuje dla systemu podstawowe zasady bezpieczeństwa firmy Microsoft oraz opiera dane na wytycznych Wdrażania Rozwiązań Technicznych w Zakresie Bezpieczeństwa (STIG) Agencji ds. Systemów Informacyjnych Departamentu Obrony (DISA). DISA STIG opierają się na standardach Narodowego Instytutu Norm i Technologii (NIST) i zapewniają zaawansowaną ochronę bezpieczeństwa systemów Windows dla Departamentu Obrony Stanów Zjednoczonych.

Uwaga: Strona Wzmocnione zabezpieczenia jest dostępna tylko dla urządzeń z usługą Streamvault.

- 10 Na stronie *Monitor Dostępności Systemu* wybierz metodę przetrzymywania danych:
 - **Nie zbieraj danych:** Agent Monitorowania Dostępności Systemu jest zainstalowany, ale nie zbiera żadnych danych.
 - **Dane będą zbierane anonimowo:** Nie jest wymagany żaden kod aktywacyjny. Dane dotyczące stanu technicznego są wysyłane do dedykowanej Usługi Monitorowania Stanu Technicznego, gdzie nazwy podmiotów są ukryte i niemożliwe do wyśledzenia. Dane te są wykorzystywane wyłącznie przez firmę Genetec Inc. do celów statystycznych i nie można uzyskać do nich dostępu poprzez GTAP.
 - **Dane będą zbierane i powiązane z systemem:** Wymagany jest kod aktywacyjny. Gromadzone dane dotyczące stanu technicznego są powiązane z systemem stowarzyszonym z aktywną Umową Serwisową Systemu (SMA).
- 11 Przeczytaj umowę o zachowaniu poufności, zaznacz pole **Akceptuję warunki umowy o zachowaniu poufności i** kliknij **Zastosuj**.
- 12 Na stronie *Wnioski* kliknij przycisk **Zamknij**.

Opcja **Uruchom kreator aktywacji po instalacji** jest domyślnie zaznaczona. Jeśli ją usuniesz, pojawi się przypomnienie o konieczności aktywowania produktu.

Po zakończeniu

Urządzenie należy aktywować przed użyciem.

Aktywacja licencji Security Center na urządzeniu

Kreator aktywacji Panelu sterowania Streamvault pomaga aktywować licencję Security Center na urządzeniu Streamvault[™].

Zanim rozpoczniesz

- Podłącz swoje urządzenie do Internetu.
- Upewnij się, że masz identyfikator systemu i hasło, które zostały przesłane do Ciebie po zakupie licencji.

Co powinieneś wiedzieć

- To zadanie dotyczy tylko urządzeń z połączeniem internetowym. W przypadku urządzenia bez podłączenia do Internetu ręcznie aktywuj licencję Security Center poprzez kontakt z Administratorem Serwera.
- Wystarczy aktywować licencję Security Center na urządzeniu obsługującym rolę Katalogu, a nie na serwerze zapasowym lub stacjach roboczych.

Procedura

1 W Panelu sterowania SV kliknij opcję **System nie został aktywowany. Kliknij tutaj, aby aktywować** Otworzy się *Kreator Aktywacji Panelu Sterowania Streamvault*.

Uwaga: Jeśli zobaczysz komunikat Do aktywacji wymagany jest dostęp do Internetu, oznacza to, że Twoje urządzenie nie jest aktualnie połączone z Internetem. Podłącz teraz swoje urządzenie lub ręcznie aktywuj licencję u Administratora Serwera.

- 2 Na stronie Aktywacja kliknij Identyfikator systemu i kliknij Dalej.
- 3 Na stronie Identyfikator Systemu wprowadź identyfikator systemu i hasło, a następniekliknij Dalej.
- 4 Na stronie *Podsumowanie* sprawdź, czy identyfikator systemu jest poprawny i kliknij **Aktywuj**. Zostanie otwarta strona *Rezultat* , która będzie wskazywała, że aktywacja przebiegła pomyślnie.
- 5 Kliknij Dalej.
- 6 (Opcjonalnie) Na stronie Aktualizacje wykonaj jedną z następujących czynności:
 - Jeśli nie są dostępne żadne aktualizacje, kliknij Otwórz asystenta instalacji Security Center.
 - Jeśli aktualizacje są dostępne, kliknij Wyświetl aktualizacje, aby otworzyć usługę aktualizacji Genetec[™] i zainstalować aktualizacje.
 - Jeśli sprawdzenie aktualizacji nie powiodło się, ponieważ Directory nie odpowiada, kliknij opcję Otwórz Administratora Serwera i upewnij się, że Directory jest gotowy.

Uwaga: Jeśli Usługa Aktualizacji Genetec nie była gotowa, sprawdzanie aktualizacji może zakończyć się niepowodzeniem. Zostanie wyświetlony komunikat Nie można w tej chwili sprawdzić dostępności aktualizacji. Spróbujemy ponownie później.

- 7 Na stronie Dodatkowe funkcje włącz lub wyłącz Synergis[™] Software i Genetec[™] Mobile. Funkcje te zostaną wyświetlane tylko wtedy, gdy będą zainstalowane na twoim urządzeniu. Funkcja Genetec Mobile jest dostępna tylko w Security Center 5.8 i wcześniejszych wersjach.
- 8 Zamknij Kreator Aktywacji Panelu Sterowania Streamvault.

Po zakończeniu

- (Opcjonalnie) Aktywuj Agenta Monitora Dostępności Systemu.
- Skonfiguruj ustawienia Security Center za pomocą Asystenta Instalacji Security Center

Tematy pokrewne

Ręczna aktywacja licencji z Server Admin, 24 Informacje o Panelu Sterowania SV, 72

Ręczna aktywacja licencji z Server Admin

Jeśli Twoje urządzenie Streamvault[™] nie ma dostępu do Internetu, musisz ręcznie aktywować licencję Security Center przez Administratora Serwera.

Procedura

- 1 Zapisz klucz weryfikacyjny:
 - a) W urządzeniu otwórz Panel sterowania SV.
 - b) Na Stronie Głównej kliknij ikonę Administrator serwera .
 - c) Zaloguj się do Administratora Serwera.

Jeśli hasło Administratora Serwera różni się od hasła administratora systemu Windows, zaloguj się do Administratora Serwera przy użyciu poświadczeń określonych w kreatorze *konfiguracji Panelu sterowania Streamvault* .

- d) Na stronie *Licencja* kliknij **Modyfikuj**.
- e) W oknie dialogowym Zarządzanie licencjami wybierz opcję Aktywacja ręczna > Zapisz do pliku . Domyślna nazwa pliku to validation.vk.

License ma	×					
Web activation OManual activation						
Save to file	Copy to clipboard					
Paste license below or browse for file						
		•				
	Close	Activate				

- f) Skopiuj plik validation.vk na klucz USB.
- g) Wyjmij klucz USB z komputera.
- 2 Zdobądź licencję z GTAP:
 - a) Na innym komputerze, który ma dostęp do Internetu, podłącz klucz USB.
 - b) Zaloguj się do GTAP.
 - c) Na stronie *logowania GTAP* wprowadź identyfikator systemu i hasło przypisane Ci podczas zakupu licencji, a następnie kliknij **Zaloguj**się.
 - d) Na stronie Informacje o systemie kliknij opcję Aktywuj licencję w sekcji Informacje o licencji.
 - e) W otwartym oknie dialogowym wklej klucz weryfikacyjny lub wyszukaj plik.
 - f) W oknie dialogowym *Aktywacja* przejdź do pliku *validation.vk* na kluczu USB, a następnie kliknij przycisk **Prześlij**.

Wyświetlony zostanie komunikat że Twoja licencja została pomyślnie aktywowana .

- g) Kliknij opcję Pobierz licencję, a następnie zapisz klucz licencyjny.
 Domyślna nazwa pliku to identyfikator systemu (ID), po którym następuje _Directory_License.lic.
- h) Skopiuj plik_Directory_License.lic na klucz USB.
- i) Wyjmij klucz USB z komputera.

- 3 Dokonaj aktywacji swojej licencji.
 - a) W urządzeniu podłącz klucz USB.
 - b) Wróć do Administratora Serwera.
 - c) Na stronie *Licencja* kliknij **Modyfikuj**.
 - d) W oknie dialogowym *Zarządzanie licencjami* wybierz opcję **Aktywacja ręczna**.
 - e) Wklej informacje o licencji z pliku *License.lic* (otwórz w edytorze tekstu) lub wyszukaj plik *License.lic* , a następnie kliknij **Otwórz**.
 - f) Kliknij, aby **Aktywować**

Tematy pokrewne

Aktywacja licencji Security Center na urządzeniu, 22

Aktywacja Monitora dostępności systemu

Aby monitorować dostępność systemu i problemy ze stanem systemu w GTAP, możesz ustawić Monitor dostępności systemu tak, aby zbierał dane o urządzeniu i wysyłał je do usługi Health Monitoring.

Zanim rozpoczniesz

Aby móc gromadzić i zgłaszać informacje o stanie swojego urządzenia, musisz wygenerować kod aktywacyjny w GTAP Aby uzyskać informacje, jak to zrobić, zobacz Generowanie kodów aktywacyjnych dla agenta monitorowania dostępności systemu w Centrum TechDoc.

Procedura

- 1 Uruchom Panel Sterowania SV.
- 2 Na stronie Konfiguracja kliknij opcję Konfiguruj w Monitorze Dostępności Systemu.
- 3 W oknie Agenta Monitorowania Dostępności Systemu Genetec kliknij Modyfikuj.
- 4 Sprawdź, czy pole Dane zostaną zebrane i powiązane z moim systemem jest zaznaczone
- 5 W polu Kod aktywacyjny wpisz kod swojego urządzenia.
- 6 Kliknij **OK**.

Włączanie funkcji kontroli dostępu i wideo w Security Center

Asystent *instalacji Security Center przeprowadzi* Cię przez konfigurację głównych funkcji zarządzania plikami wideo i kontroli dostępu.

Co powinieneś wiedzieć

Ustawienia, które zastosujesz w asystencie, możesz później zmienić w narzędziu konfiguracyjnym.

Dotyczy: urządzeń obsługujących rolę Directory, takich jak urządzenia all-in-one

Procedura

1 Zaloguj się jako Administrator.

Wskazówka: Jeśli hasło do Security Center różni się od hasła administratora systemu Windows, zaloguj się do Security Center przy użyciu haseł ustawionych w *kreatorze konfiguracji Panelu sterowania Streamvault.*

Zostanie otwarty asystent instalatora Security Center.

- 2 Po przeczytaniu Wprowadzenia kliknij Dalej.
- 3 Na stronie *Dostępne funkcje* wybierz żądane funkcje i kliknij **Dalej**. Podstawowe funkcje są włączone domyślnie . Możesz później włączać i wyłączać funkcje na stronie *Funkcje* w widoku **Ustawienia ogólne** zadania *System* . **Uwaga:** Jeśli Twoja licencja nie obsługuje danej funkcji, nie pojawi się ona na liście.

4 Na stronie *Zabezpieczenia kamery* określ domyślną nazwę użytkownika i hasło używane dla wszystkich kamer, a następnie kliknij **Dalej**.

Wskazówka: Aby zwiększyć bezpieczeństwo, wybierz opcję Użyj protokołu HTTPS.

- 5 Na stronie *Ustawienia jakości kamery* skonfiguruj następujące opcje:
 - Rozdzielczość:
 - Wysoka: 1280x720 i wyższa
 - Standardowa: Większa niż 320 x 240 i mniej niż 1280 x 720
 - Niska: 320x240 i niższa
 - Domyślna: Domyślne ustawienia producenta

Kamera zawsze wykorzystuje najwyższą rozdzielczość, jaką może obsłużyć z wybranej kategorii. Jeśli kamera nie obsługuje żadnej rozdzielczości z wybranej kategorii, użyje najwyższej rozdzielczości, jaką może obsłużyć z następnej kategorii. Na przykład, jeśli kamera nie obsługuje wysokiej rozdzielczości, użyje najwyższej możliwej rozdzielczości z grupy Standard.

Ustawienia na tej stronie można później zmodyfikować w *ustawieniach domyślnych Kamery* w roli Archiwizator.

- 6 Na stronie *Ustawienia nagrywania* wybierz domyślne ustawienia nagrywania, które mają zostać zastosowane do wszystkich kamer:
 - Wyłączone: Nagrywanie jest wyłączone
 - Ciągłe: Kamery nagrywają w sposób ciągły. Jest to ustawienie domyślne.
 - W ruchu/Ręczne: Kamery zaczynają nagrywać wyzwalane działaniem (np. Rozpocznij nagrywanie, Dodaj zakładkę lub Wyzwól alarm), po wykryciu ruchu lub ręcznie przez użytkownika.
 - **Ręczne:** Kamery zaczynają nagrywać wyzwalane działaniem (np. Rozpocznij nagrywanie, Dodaj zakładkę lub Wyzwól alarm), lub ręcznie przez użytkownika.

Uwaga: Gdy włączony jest tryb**Ręczny**, wykrycie ruchu nie wyzwala nagrywania.

- **Niestandardowe:** Można ustawić harmonogram nagrywania.
- 7 Kliknij Dalej.
- 8 Na stronie *Zabezpieczenia jednostki kontroli dostępu* podaj domyślną nazwę użytkownika i hasło dla wszystkich jednostek kontroli Dostępu, a **następnie** kliknij Dalej.
- 9 Na stronie Posiadacze kart wybierz sposób dodawania poświadczeń (kart) i posiadaczy kart.
 - a) Wybierz, czy chcesz dodać posiadaczy kart (po zamknięciu asystenta instalatora Security Center) poprzez zadanie *Zarządzanie posiadaczami kart*, czy za pomocą narzędzia Importuj.
 - b) Kliknij Dalej.
- 10 Na stronie Użytkownicy dodaj więcej użytkowników do swojego systemu:
 - a) Wpisz nazwę użytkownika.
 - b) Wybierz Rodzaj Użytkownika:
 - Operator: Operator może korzystać z zadania *Monitorowanie*, przeglądać wideo i zarządzać gośćmi w Security Desk
 - Użytkownik Raportujący : Użytkownik raportujący może korzystać z aplikacji Security Desk i wykonywać najbardziej podstawowe funkcje raportowania, z wyłączeniem zadań dla AutoVu[™] ALPR. Użytkownik posiadający uprawnienia jedynie do raportowania nie może przeglądać żadnego z plików wideo, sterować urządzeniami fizycznymi ani zgłaszać incydentów.
 - Referent: Referent może korzystać z zadania Monitorowanie, przeglądać wideo, sterować kamerami PTZ, nagrywać i eksportować wideo, dodawać zakładki i zdarzenia, korzystać z zadań dochodzeniowych, zarządzać alarmami i gośćmi, zmieniać harmonogramy otwierania drzwi, zapisywać zadania itd.
 - Supervisor: Nadzorca może korzystać z zadania Monitorowanie, przeglądać wideo, sterować kamerami PTZ, nagrywać i eksportować wideo, dodawać zakładki i zdarzenia, korzystać z zadań dochodzeniowych, zarządzać alarmami i gośćmi, zmieniać harmonogramy otwierania drzwi, zapisywać zadania itd. Supervisor może również wykonywać zadania z zakresu dozoru technicznego, zarządzać posiadaczami kart i danymi uwierzytelniającymi, modyfikować pola niestandardowe, ustawiać poziomy zagrożeń, blokować kamery i zliczać osoby.
 - Konfigurator: Użytkownik ma większość uprawnień konfiguracyjnych, z wyjątkiem następujących: zarządzanie rolami, makrami, użytkownikami, grupami użytkowników, zdarzeniami niestandardowymi, ścieżkami aktywności, poziomami zagrożeń i plikami audio. Użytkownikiem konfiguracyjnym jest zazwyczaj instalator systemu.
 - **Podstawowy operator AutoVu**[™]: Ten typ użytkownika jest przeznaczony dla operatorów korzystających z AutoVu ALPR. Podstawowy użytkownik AutoVu może korzystać z zadań ALPR, konfigurować obiekty ALPR, tworzyć reguły ALPR, monitorować zdarzenia ALPR i tak dalej.
 - Użytkownik Patroller'a: Ten typ użytkownika jest przeznaczony dla użytkowników Genetec Patroller™, którzy korzystają z AutoVu ALPR. Użytkownik Patroller'a może korzystać z zadań ALPR, konfigurować obiekty ALPR, tworzyć reguły ALPR, monitorować zdarzenia ALPR i tak dalej. Użytkownik Patrollera nie ma dostępu do innych aplikacji Security Center, na przykład Narzędzia Konfiguracyjnego i Security Desk. Użytkownik Patrollera nie może modyfikować raportów ani zmieniać hasła Patrollera.
- 11 Wprowadź i potwierdź Hasło, a następnie kliknij Dodaj.

Nowy użytkownik zostanie dodany do listy użytkowników po prawej stronie okna dialogowego. Aby usunąć użytkownika, wybierz go z listy i kliknij 💢.

Profile użytkowników zmienisz w **Użytkownicy** zadania *Zarządzanie użytkownikami*. Aby uzyskać informację, skorzystaj z Przewodnika Administratora Security Center znajdującego się w TechDoc Hub

- 12 Kliknij Dalej.
- 13 Potwierdź, że informacje na stronie *Podsumowanie* są prawidłowe, a następnie kliknij **Zastosuj**lub kliknij **Wstecz**, aby naprawić błędy.

14 Na stronie *Wnioski* kliknij opcję **Uruchom Ponownie**.

Narzędzie konfiguracyjne uruchomi się ponownie, aby zastosować nowe ustawienia.

Uwaga: Opcja **Otwórz narzędzie rejestracji jednostek po zamknięciu kreatora** jest wybrana domyślnie. Możesz odznaczyć tę opcję i otworzyć Narzędzie Rejestracji Jednostek później, klikając skrót **Zarejestruj kamery i kontrolery** na *Stronie Głównej* w Panelu sterowania SV.

Po zakończeniu

Dodaj jednostki do swojego systemukorzystając z Narzędzia do Rejestracji Jednostek.

Tematy pokrewne

Konfigurowanie domyślnych ustawień kamery, 33 Tworzenienie niestandardowych harmonogramów nagrywania, 35 Strona Główna Panelu Sterowania SV, 64

Informacje o narzędziu rejestracji Jednostek

Rejestracja jednostek to narzędzie, którego można używać do wykrywania jednostek IP (wideo i kontroli dostępu) podłączonych do sieci na podstawie nazwy producenta i właściwości sieci (port wykrywania, zakres adresów IP, hasło itd.). Po wykryciu jednostki możesz ją dodać do swojego systemu.

- Narzędzie rejestracji jednostek otwiera się automatycznie po wyświetleniu Asystenta instalatora Security Center, chyba że opcja Otwórz narzędzie rejestracji jednostek zaraz po kreatorze została wyczyszczona.
- Podczas dodawania jednostek kontroli dostępu za pomocą narzędzia do rejestracji jednostek można zarejestrować wyłącznie jednostki HID i Synergis[™]. Szczegółowe informacje na temat rejestrowania jednostek Synergis można znaleźć w *Przewodniku Konfiguracji urządzenia Synergis*[™].

Otwarcie narzędzia rejestracji jednostek

Istnieją trzy sposoby otwarcia narzędzia rejestracji Jednostek.

Procedura

- Wykonaj jedną z następujących czynności:
 - Na stronie Głównej Panelu sterowania SV kliknij opcję 4 Zarejestruj kamery i kontrolery .
 - Na stronie głównej Panelu Sterowania SV kliknij ikonę Narzędzie konfiguracji, a następnie kliknij Zadania > Rejestracja jednostki.
 - Na stronie głównej Panelu Sterowania SV kliknij ikonę **Narzędzia konfiguracji**, a następnie kliknij ikonę **Dodaj status jednostki** na pasku powiadomień Narzędzia Konfiguracji.

📷 🕪 🌏 🔲 Tue 11:21 AM 📃 🗖 💌

Konfigurowanie ustawień dla rejestracji jednostek

Możesz użyć przycisku **Ustawienia i producenci** w narzędziu Rejestracja jednostek, aby określić, których producentów uwzględnić podczas wyszukiwania nowych jednostek. Można także skonfigurować ustawienia wykrywania jednostek oraz określić nazwę użytkownika i hasło dla jednostek, aby można było je łatwo zarejestrować.

Procedura

- 1 Na stronie głównej kliknij Narzędzia > Rejestracja jednostki.
- 2 W oknie dialogowym Rejestracja jednostki kliknij Ustawienia i Producenci (
- 3 Użyj opcji Odrzuć uwierzytelnianie podstawowe, aby włączyć lub wyłączyć uwierzytelnianie podstawowe (tylko w przypadku jednostek wideo). Jest to przydatne, jeśli wyłączyłeś uwierzytelnianie podstawowe w Security Center InstallShield, ale musisz je włączyć ponownie, aby przeprowadzić aktualizację oprogramowania sprzętowego lub aby zarejestrować kamerę obsługującą tylko uwierzytelnianie podstawowe. Aby ponownie włączyć uwierzytelnianie podstawowe, należy przestawić opcję Odrzuć uwierzytelnianie podstawowe na Wyłączone.

Uwaga: Ta opcja jest dostępna tylko dla użytkowników z uprawnieniami Administratora.

4 Kliknij Dodaj Producenta (-), aby dodać producenta do listy jednostek, które mają zostać wykryte.
 Aby usunąć producenta z listy należy go zaznaczyć i kliknąć X.
5 Skonfiguruj indywidualne ustawienia dla każdego z dodanych producentów. W tym celu wybierz producenta i kliknij *2*.

Ważne: Aby urządzenie zostało prawidłowo zarejestrowane, należy wprowadzić poprawną nazwę użytkownika i hasło.

- 6 (Opcjonalnie) Usuń jednostki z listy ignorowanych jednostek (patrz Usuwanie jednostek z listy ignorowanych jednostek, 32).
- 7 Kliknij Zapisz.

Dodawanie jednostek

Po wykryciu nowych jednostek możesz użyć narzędzia rejestracji jednostek, aby dodać je do swojego systemu.

Procedura

- 1 Na stronie głównej kliknij **Narzędzia** > **Rejestracja jednostki**.
- 2 Nowo odkryte jednostki można dodawać na trzy sposoby:
 - Dodaj wszystkie nowo odkryte jednostki jednocześnie, klikając przycisk **Dodaj wszystkie** (+) w prawym dolnym rogu okna dialogowego.
 - Kliknij pojedynczą jednostkę na liście, a następnie kliknij opcję Dodaj w kolumnie Status
 - Kliknij prawym przyciskiem myszy pojedynczą jednostkę na liście i kliknij opcję Dodaj lub Dodaj jednostkę.

Jeśli jednostka wideo nie ma prawidłowej nazwy użytkownika i hasła, **Status** urządzenia zostanie wyświetlony jako **Nieprawidłowe logowanie**, a podczas dodawania urządzenia zostanie wyświetlony monit o wprowadzenie prawidłowych informacji. Jeśli chcesz użyć tej samej nazwy użytkownika i hasła dla wszystkich kamer w systemie, wybierz opcję **Zapisz jako domyślne uwierzytelnienie dla wszystkich producentów**.

Jednostkę można także dodać ręcznie, klikając przycisk **Dodaj ręcznie** u dołu okna dialogowego *Narzędzia rejestracji jednostek* .

Uwaga:

- W przypadku jednostek wideo, jeśli dodana kamera jest koderem z wieloma dostępnymi strumieniami, każdy strumień jest dodawany z ciągiem *Camera n* dołączonym do nazwy kamery, *n* oznacza numer strumienia. W przypadku kamery IP tylko z jednym dostępnym strumieniem, nazwa kamery nie jest modyfikowana.
- Jeśli dodajesz urządzenie SharpV, kamery domyślnie uwzględniają certyfikat z podpisem własnym, który wykorzystuje wspólną nazwę urządzenia SharpV (na przykład SharpV12345). Aby dodać SharpV do Archivera, musisz wygenerować nowy certyfikat (podpisany lub z podpisem własnym), który będzie korzystał z adresu IP kamery zamiast nazwy zwyczajowej.

Usuwanie dodanych jednostek

Możesz usunąć jednostki, które zostały już dodane do systemu, aby nie były wyświetlane za każdym razem, gdy używasz narzędzia Rejestracji Jednostek do wykrywania jednostek w systemie.

Co powinieneś wiedzieć

Opcja Usuwanie zakończone w narzędziu Rejestracji Jednostek jest trwała i nie można jej cofnąć.

Procedura

1 Dodaj potrzebne odkryte jednostki do swojego systemu, zobaczDodawanie jednostek, 31.

2 Po dodaniu jednostek kliknij opcję Usuwanie zakończone. Każda jednostka, która ma opcję Dodano wyświetloną w kolumnie Status, zostanie usunięta z listy odkrytych jednostek.

Ignorowanie jednostek

Możesz zignorować jednostki, aby nie pojawiały się one na liście odkrytych jednostek w narzędziu rejestracji jednostek.

Procedura

- Na stronie głównej kliknij Narzędzia > Rejestracja jednostki.
 The narzędzie do rejestracji Jednostki IP otwiera się z listą jednostek wykrytych w systemie.
- 2 Kliknij prawym przyciskiem myszy jednostkę, którą chcesz zignorować, i wybierz **Ignoruj**. Jednostka zostanie usunięta z listy i będzie ignorowana, gdy narzędzie rejestracji jednostek wykryje nowe jednostki. Informacje o usuwaniu jednostki z listy ignorowanych jednostek znajdziesz w Usuwanie jednostek z listy ignorowanych jednostek, 32.

Usuwanie jednostek z listy ignorowanych jednostek

Możesz usunąć jednostkę z listy ignorowanych jednostek, aby nie była ona ignorowana w przypadku wykrycia przez narzędzie do rejestracji jednostek.

Procedura

- 1 Na stronie głównej kliknij Narzędzia > Rejestracja jednostki.
- 2 W prawym górnym rogu okna dialogowego Rejestracja jednostki kliknij Ustawienia i producenci (()).
- 3 Kliknij opcję **Ignorowane jednostki** , a następnie opcję **Usuń wszystkie ignorowane jednostki**. Można też wybrać pojedynczą jednostkę i kliknąć przycisk **Usuń zignorowaną jednostkę** (**X**).

Konfigurowanie domyślnych ustawień kamery

W *domyślnych ustawieniach Kamery*możesz modyfikować domyślne ustawienia nagrywania i jakości wideo stosowane dla wszystkich kamer kontrolowanych przez Archiver. Początkowo, ustawienia te konfiguruje się na stronie *Ustawienia jakości Kamery*przy pomocy asystenta instalatora Security Center.

Co powinieneś wiedzieć

Możesz także zastosować ustawienia wideo i nagrywania dla kamery w narzędziu konfiguracyjnym Config Tool, korzystając z karty **Wideo i Nagrywanie**. Ustawienia wprowadzone dla pojedynczej kamery mają pierwszeństwo przed ustawieniami zastosowanymi przy pomocy asystenta instalatora Security Center lub na stronie *Ustawień domyślnych Kamery*.

Procedura

- 1 Na stronie głównej Narzędzia konfiguracyjnego otwórz zadanie Wideo .
- 2 Wybierz rolę Archiver, a następnie kliknij zakładkę Ustawienia domyślne Kamery .
- 3 W obszarze Jakość wideo (taka sama we wszystkich rolach archiver) skonfiguruj następujące opcje:
 - Rozdzielczość:
 - Wysoka: 1280x720 i wyższa
 - Standardowa: Większa niż 320 x 240 i mniej niż 1280 x 720
 - Niska: 320x240 i niższa
 - Domyślna: Domyślne ustawienia producenta

Kamera zawsze wykorzystuje najwyższą rozdzielczość, jaką może obsłużyć z wybranej kategorii. Jeśli kamera nie obsługuje żadnej rozdzielczości z wybranej kategorii, użyje najwyższej rozdzielczości, jaką może obsłużyć z następnej kategorii. Na przykład, jeśli kamera nie obsługuje wysokiej rozdzielczości, użyje najwyższej możliwej rozdzielczości z grupy Standard.

4 W obszarze **Nagrywanie**kliknij 🛖, aby dodać harmonogram.

Dostępne harmonogramy obejmują:

- Harmonogramy utworzone przy użyciu widoku Harmonogramy w zadaniu Systemowym.
- Harmonogram niestandardowy, jeśli został utworzony przy pomocy asystenta instalatora w Security Center.
- 5 Z listy rozwijanej **Tryb** wybierz tryb harmonogramu nagrywania:
 - Wyłączone: Nagrywanie jest wyłączone
 - **Ciągłe:** Kamery nagrywają w sposób ciągły. Jest to ustawienie domyślne.
 - W ruchu/Ręczne: Kamery zaczynają nagrywać wyzwalane działaniem (np. Rozpocznij nagrywanie, Dodaj zakładkę lub Wyzwól alarm), po wykryciu ruchu lub ręcznie przez użytkownika.
 - **Ręczne:** Kamery zaczynają nagrywać wyzwalane działaniem (np. Rozpocznij nagrywanie, Dodaj zakładkę lub Wyzwól alarm), lub ręcznie przez użytkownika.
 - **Uwaga:** Gdy włączony jest tryb**Ręczny**, wykrycie ruchu nie wyzwala nagrywania.
 - Niestandardowe: Można ustawić harmonogram nagrywania.

- 6 Skonfiguruj następujące opcje:
 - **Nagrywaj dźwięk:** Włącz tę opcję, jeśli chcesz nagrywać dźwięk wraz z obrazem wideo. Aby ta opcja działała, do kamer musi być podłączony mikrofon.
 - **Zapasowa archiwizacja:** Włącz tę opcję, jeśli chcesz, aby zarówno serwer główny, jak i pomocniczy archiwizowały wideo w tym samym czasie. To ustawienie obowiązuje tylko wtedy, gdy skonfigurowane jest przełączanie awaryjne.
 - **Automatyczne czyszczenie:** Włącz tę opcję, jeśli chcesz aby wideo zostało usunięte po określonej liczbie dni. Wideo jest usuwane niezależnie od tego, czy pamięć Archivera jest pełna, czy nie.
 - **Czas nagrywania przed zdarzeniem:** Użyj suwaka, aby ustawić liczbę sekund, które chcesz nagrać przed zdarzeniem. Bufor ten jest zapisywany za każdym razem, gdy rozpoczyna się nagrywanie, gwarantując, że cokolwiek wywołało nagrywanie, zostanie również zarejestrowane na wideo.
 - **Czas nagrywania po wykryciu ruchu:** Ustaw liczbę sekund, przez którą nagrywanie ma być kontynuowane po wykryciu ruchu. W tym czasie, użytkownik nie może zatrzymać nagrywania.
 - **Domyślna długość nagrywania ręcznego :** Ustaw liczbę minut, które chcesz nagrać, gdy użytkownik rozpocznie nagrywanie. Użytkownik może zatrzymać nagrywanie w dowolnym momencie przed upływem czasu jego trwania. Wartość ta jest także wykorzystywana przy akcji Rozpocznij nagrywanie, gdy wybrana jest domyślna długość nagrywania.
- 7 Kliknij Zastosuj.
- 8 Jeśli chcesz zastosować nowe ustawienia dla wszystkich istniejących kamer, kliknij Tak.

Tematy pokrewne

Włączanie funkcji kontroli dostępu i wideo w Security Center, 27

Tworzenienie niestandardowych harmonogramów nagrywania

Stwórz niestandardowe harmonogramy nagrywania za pomocą asystenta instalatora Security Center, aby kamery nagrywały w różnych trybach nagrywania przez określony zakres czasu.

Procedura

- 1 Na stronie *Ustawienia Nagrywania* kliknij 🛖 opcję **Harmonogram nagrywania**.
- 2 Wprowadź nazwę nowego harmonogramu.
- 3 Z listy Tryb nagrywania wybierz jedną z następujących opcji:
 - Wyłączone: Nagrywanie jest wyłączone
 - **Ciągłe:** Kamery nagrywają w sposób ciągły. Jest to ustawienie domyślne.
 - **W ruchu/Ręczne:** Kamery zaczynają nagrywać wyzwalane działaniem (np. Rozpocznij nagrywanie, Dodaj zakładkę lub Wyzwól alarm), po wykryciu ruchu lub ręcznie przez użytkownika.
 - Ręczne: Kamery zaczynają nagrywać wyzwalane działaniem (np. Rozpocznij nagrywanie, Dodaj zakładkę lub Wyzwól alarm), lub ręcznie przez użytkownika.
 - **Uwaga:** Gdy włączony jest tryb**Ręczny**, wykrycie ruchu nie wyzwala nagrywania.
 - Niestandardowe: Można ustawić harmonogram nagrywania.
- 4 Dla każdego dnia tygodnia określ zakres czasowy rejestracji wideo:
 - Kliknij i przeciągnij, aby wybrać blok zakresu czasu.
 - Kliknij prawym przyciskiem myszy i przeciągnij, aby wyczyścić ustawienia zakresu czasu.
 - Użyjklawiszy kursora, aby przewinąć 24-godzinną oś czasu.

Wskazówka: Aby przejść do trybu wysokiej rozdzielczości, gdzie każdy blok czasowy reprezentuje 1 minutę, kliknija.

Przykład

Poniższy przykład przedstawia harmonogram, w którym nagrywanie odbywa się w sposób ciągły od 18:00 do 9:00 w weekendy i od 9:00 do 17:00 w dni powszednie.



Tematy pokrewne

Włączanie funkcji kontroli dostępu i wideo w Security Center, 27

Informacje o tworzeniu kopii zapasowych i przywracaniu danych

Korzystając z Panelu Sterowania SV, możesz bezpiecznie wykonać kopię zapasową bazy danych Directory i plików konfiguracyjnych. Następnie, możesz przywrócić pliki do poziomu danych dla tego samego identyfikatora systemowego w przypadku awarii systemu lub aktualizacji sprzętu.

Jak działa proces tworzenia kopii zapasowych i przywracania danych w Panelu Sterowania SV

Tworzysz kopie zapasowe bazy danych Directory oraz plików konfiguracyjnych i przechowujesz je w chmurze lub lokalnie. Poniższy diagram architektury pokazuje, jak działa kopia zapasowa w Panelu Sterowania SV:



Directory database

Korzyści z tworzenia kopii zapasowych i przywracania danych

- •
- Z łatwością przywróć dowolną z pięciu kopii zapasowych ulokowanych w chmurze lub dowolne lokalne kopie zapasowe dla tego samego identyfikatora systemu, korzystając z kreatora *Przywracania*.
- Wszystkie pliki kopii zapasowych można szyfrować.
- System blokuje się po pięciu nieudanych próbach logowania.
- Aby korzystać z tej funkcji, nie trzeba być zarejestrowanym w programie Genetec Advantage.

Ograniczenia dotyczące tworzenia kopii zapasowych i przywracania danych

- Kopia zapasowa nie obejmuje plików licencyjnych, archiwów wideo ani innych baz danych.
- Nie można przywrócić kopii zapasowej we wcześniejszej wersji Security Center. Na przykład nie można przywrócić kopii zapasowej z wersji systemu Security Center 5.10 do systemu Security Center 5.9.
- Nie można przywrócić plików konfiguracyjnych, jeśli przywracasz dane dla głównych wersji Security Center. Na przykład nie można przywrócić plików konfiguracyjnych z kopii zapasowej systemu Security Center 5.9 do systemu Security Center 5.10.

Tematy pokrewne

Tworzenie kopii zapasowej bazy danych Directory, 38 Przywracanie bazy danych Diectory, 39

Tworzenie kopii zapasowej bazy danych Directory

Za pomocą funkcji tworzenia kopii zapasowych i przywracania można bezpiecznie utworzyć kopię zapasową bazy danych katalogu i plików konfiguracyjnych. Tworzenie kopii zapasowych i przywracanie ułatwia konfigurację systemu po modernizacji sprzętu i umożliwia przywrócenie konfiguracji po awarii systemu.

Zanim rozpoczniesz

Upewnij się, że:

- Zainstalowano Security Center w wersji 5.9 lub nowszej.
- Serwer Genetec[™] działa.
- Masz ważną i aktywną licencję.

Co powinieneś wiedzieć

- •
- Tylko administratorzy mogą wykonać kopię zapasową, a wszystkie kopie zapasowe w chmurze muszą zostać uwierzytelnione.

Procedura

- 1 W Panelu sterowania SV kliknij zakładkę Konfiguracja.
- 2 W obszarze *Directory i konfiguracji kopii zapasowej/przywracania* kliknij opcję **Kreator kopii zapasowej** > **Dalej**.
- 3 Na stronie *Metoda tworzenia kopii zapasowej* wybierz opcję **Chmura** lub **Lokalna**, a następnie kliknij **Dalej**.
 - Jeśli wybrałeś Chmurę, wykonaj następujące czynności:

tworzenie kopii zapasowych w przyszłości.

- a. Na stronie *Uwierzytelnianie* wprowadź identyfikator systemu lub poświadczenia GTAP, aby uwierzytelnić kopię zapasową.
 Uwaga: Po pierwszym wprowadzeniu danych uwierzytelniających nie będziesz już pytany o
- b. Na stronie *Bezpieczeństwo* wybierz jedną z dwóch następujących opcji:
 - **Pozwól firmie Genetec zarządzać moim bezpieczeństwem:** Nie musisz podawać hasła. Usługa tworzenia kopii zapasowych w chmurze firmy Genetec Inc. szyfruje Twoje dane.
 - Użyj mojego własnego hasła: Utwórz i zapamiętaj hasło, którego będziesz mógł użyć później do szyfrowania plików kopii zapasowych.
 Ważne: Jeśli zgubisz lub zapomnisz hasła, Genetec Inc. nie będzie w stanie odzyskać utraconego hasła.
- Jeśli wybrałeś **Lokalne**, wykonaj następujące czynności:
 - a. Na stronie *Folder docelowy* wprowadź nazwę kopii zapasowej i przejdź do folderu, w którym chcesz przechowywać kopię zapasową.
 - b. Na stronie *Bezpieczeństwo* utwórz hasło, aby zaszyfrować plik kopii zapasowej. Możesz także wybrać opcję **Nie szyfruj mojej kopii zapasowej**, chociaż nie jest to zalecane.
- 4 Wykonaj pozostałe kroki kreatora, aby ukończyć tworzenie kopii zapasowej.

Tematy pokrewne

Informacje o tworzeniu kopii zapasowych i przywracaniu danych, 37 Przywracanie bazy danych Diectory, 39

Przywracanie bazy danych Diectory

Jeśli wykonałeś kopię zapasową bazy danych Directory i plików konfiguracyjnych za pomocą funkcji tworzenia kopii zapasowych i przywracania w Panelu Sterowania SV, możesz przywrócić pliki kopii zapasowej dla tego samego identyfikatora systemowego. Pliki kopii zapasowych można przywrócić w przypadku awarii systemu lub aktualizacji sprzętu.

Zanim rozpoczniesz

Upewnij się, że:

- Zainstalowano Security Center w wersji 5.9 lub nowszej.
- Serwer Genetec[™] działa.
- Masz ważną i aktywną licencję.

Co powinieneś wiedzieć

- Jeśli utworzyłeś kopię zapasową plików w chmurze, możesz przywrócić dowolną z pięciu ostatnich kopii zapasowych do poziomu tego samego identyfikatora systemu.
- Jeśli kopię zapasową plików utworzyłeś lokalnie, możesz przywrócić dowolną kopię zapasową do poziomu tego samego identyfikatora systemowego.
- Jeśli podczas tworzenia kopii zapasowej utworzyłeś własne hasło do zaszyfrowanych plików kopii zapasowej, będzie potrzebne do przywrócenia plików.

Procedura

- 1 W Panelu sterowania SV kliknij zakładkę Konfiguracja.
- 2 W obszarze *Directory i konfiguracji kopii zapasowej/przywracania* kliknij opcję **Przywroć kopie zapasowe** > **Dalej**.
- 3 Na stronie Metoda przywracania wybierz opcję Chmura lub Lokalnie. Jeśli wybrałeś Chmurę, na stronie Uwierzytelnianiewprowadź identyfikator systemu lub poświadczenia GTAP, w zależności od tego, które z nich zostało użyte do uwierzytelnienia kopii zapasowej. Jeśli korzystasz z danych uwierzytelniających GTAP, na Twój adres e-mail zostanie wysłany kod aktywacyjny.
- 4 Na stronie Wybór kopii zapasowej wybierz plik, który chcesz przywrócić do systemu.
- 5 Jeśli na stronie *Przywracanie danych* zdecydowałeś się utworzyć hasło podczas procesu tworzenia kopii zapasowej, musisz wprowadzić je tutaj.
- 6 Wykonaj pozostałe kroki kreatora, aby ukończyć proces przywracania.

Tematy pokrewne

Tworzenie kopii zapasowej bazy danych Directory, 38 Informacje o tworzeniu kopii zapasowych i przywracaniu danych, 37

Wybór metody tworzenia ról i partycji Archivera

Aby skonfigurować urządzenie pod kątem oczekiwanej liczby kamer i wykorzystania przepustowości, musisz utworzyć odpowiednią ilość ról Archiver. W zależności od typu i stanu urządzenia możesz wybrać jedną z dwóch metod.

- Korzystanie z narzędzi Role Archiver'a i Partycje.
- Ręczne tworzenie partycji i roli Archiver.

Wybór metody dla twoich potrzeb

Skorzystaj z poniższego drzewa decyzyjnego, które pomoże Ci zdecydować, której metody użyć:



Informacje na temat narzędzi Role Archiver'a i Partycji.

Dostęp do narzędzi Roli Archiver i Partycji archiwizatora można uzyskać w Panelu Sterowania SV. Narzędzie oblicza liczbę potrzebnych ról Archivera na podstawie liczby kamer które planujesz wdrożyć oraz ich oczekiwanej przepustowości.

To narzędzie jest dostępne tylko w modelach Streamvault[™] wyposażonych w wewnętrzny dysk twardy. Jeśli konfigurujesz zewnętrzne urządzenie pamięci masowej, takie jak SAN w urządzeniu serii Streamvault[™] SV-7000EX, wykonaj czynności opisane w Dodawanie partycji i ról Archiver ręcznie., 42.

Gdy narzędzie tworzy partycje, wszystkie woluminy lokalne z wyjątkiem C: są usuwane, a istniejące role Archiver i zarejestrowane kamery są usuwane z Security Center. Jeśli więc Twoje urządzenie ma kamery i nagrania wideo, które chcesz zachować, ręcznie dodaj partycje i role Archiver.

Dodanie roli Archiver w Panelu Sterowania SV

Użyj narzędzia Role i Partycje Archiver, aby dodać wystarczającą liczbę roli Archiver, aby obsłużyć zakładany ruch wideo. To narzędzie jest dostępne w urządzeniach Archiver z serii Streamvault[™] 1000, 2000 i 4000.

Zanim rozpoczniesz

• Wybierz odpowiednią metodę tworzenia ról i partycji Archiver.

Utwórz kopię zapasową ważnych danych na dysku, który chcesz podzielić na partycje.
 Ostrożnie: Narzędzie Role i Partycje Archivera może usunąć istniejące dane, w tym konfigurację roli archiver i wszystkie pliki na dysku D:.

Procedura

- 1 W Panelu sterowania SV kliknij zakładkę Konfiguracja.
- 2 W obszarze *role i partycje Archivera*kliknij opcję **Konfiguruj**.

Zostanie otwarte okno dialogowe Role i Partycje Archivera .

- 3 Aby skonfigurować ilość ról i partycji dla Archivera, wybierz jedną z poniższych opcji:
 - Aby narzędzie mogło obliczyć liczbę ról, liczbę partycji i wymagany rozmiar partycji, wybierz opcję Sugerowany scenariusz. Wprowadź liczbę kamer, które chcesz wdrożyć, oraz oczekiwaną przepustowość każdej kamery.
 - Aby określić liczbę ról Archivera i partycji do utworzenia, wybierz **Scenariusz niestandardowy**. Wprowadź ilość ról Archivera, liczbę partycji i rozmiar partycji.

Liczba partycji musi być wielokrotnością liczby ról archivera.

Ostrożnie: Pliki na dysku, na którym dokonujesz partycji zostaną usunięte.

4 Kliknij opcję **Utwórz partycje i role**.

Archiver Roles an	d Partitions		
An Archiver role can supp - 300 cameras - Throughput of 500 Mb - Partitions with a maxim	oort: ops num size of 30 TB	Your model (SV-1000- supports: - 400 cameras - 400 Mbps	R14-72T-8-210)
Suggested scenario			
Number of cameras:	0	Number of roles:	0
Camera throughput:	0	Number of partitions:	0
		Size of partitions (TB):	0.00
Custom scenario			
Number of roles:	0	Total disk space (TB):	0.02
Number of partitions:	0	Used disk space (TB):	0.00
Size of partitions (TB):	0	Free disk space (TB):	0.02
		Cre	ate partitions/roles

- 5 W oknie Ostrzeżenie zaznacz wymagane pole , abypotwierdzić, że chcesz kontynuować.
- 6 Kliknij **OK**.

Zostanie otwarte okno *Wynik*, w którym zostaną wyświetlone nazwy i lokalizacje ról i partycji archivera. Do każdej roli archivera automatycznie przypisana jest litera dysku.

Dodawanie partycji i ról Archiver ręcznie.

Aby po raz pierwszy skonfigurować urządzenie wielofunkcyjne Streamvault[™] SV-7000EX lub SV-300E, należy ręcznie utworzyć partycje. Możesz także ręcznie dodać role Archiver do urządzenia, na którym znajdują się już dane, aby dane nie zostały utracone.

Zanim rozpoczniesz

Wybierz metodę tworzenia partycji na swoim urządzeniu.

Co powinieneś wiedzieć

Formatowanie woluminu usuwa dane znajdujące się na partycji. Aby zachować dane, zmniejsz wolumin, a następnie utwórz nowe woluminy.

Procedura

- 1 Jeśli na urządzeniu są już zarejestrowane kamery, zarchiwizowane wideo lub dane kontroli dostępu, wykonaj następujące czynności:
 - a) Utwórz kopię zapasową dla bazy danych Directory za pomocą Panelu sterowania SV.
 - b) Wygeneruj raport *Konfiguracji kamery*, aby zrobić migawkę bieżącej konfiguracji kamery. Aby uzyskać informacje, zobacz ustawień wyświetleń z kamery w Centrum TechDoc.
- 2 Utwórz woluminy potrzebne dla ról Archiver, które planujesz utworzyć na urządzeniu.
 - W przypadku urządzeń łączących się z pamięcią masową SAN, takich jak urządzenia serii SV-7000EX, utwórz numer jednostki logicznej (LUN) dla każdej roli archiwizatora.
 - Na urządzeniach wyposażonych w wewnętrzne dyski pamięci, takich jak SV-1000E, SV-2000E i SV-4000E, użyj narzędzia *Zarządzanie dyskami systemu Windows*, aby skonfigurować woluminy.

- 3 W Security Center utwórz rolę Archiver:
 - a) Na stronie głównej Narzędzia konfiguracyjnego Config Tool otwórz zadanie System i kliknij widok Role .
 - b) Kliknij Dodaj podmiot i wybierz Archiver.
 Otworzy się Kreator konfiguracji dla roli Archiver.
 - c) Na stronie *Informacje szczegółowe* wprowadź nazwę bazy danych roli **Archiver** i kliknij **Dalej**. Każda rola Archiver musi mieć dedykowaną bazę danych.

Cr	eating a role: Archiver			
L	Specific info	Database server:	(local)\SQLEXPRESS	
L	Basic information	Database:	Archiver5	• 0
L	Creation summary			
	Entity creation outcome			

d) W sekcji Informacje podstawowe wpisz Nazwę podmiotu i kliknij Dalej.

Najlepszą praktyką jest to, aby nazwa bazy danych roli Archiver była zgodna z nazwą jednostki.

Creating a role: Archiver		8
Specific info	Fill in the following fields. The entity description is optional.	
Basic information	Entity name: Archiver5	
Creation summary	Entity description:	
Entity creation outcome		

- e) Sprawdź, czy informacje na stronie *Podsumowanie Utworzenia* są poprawne i kliknij **Utwórz**.
- 4 Skonfiguruj rolę Archiver.
 - a) W przeglądarce dotyczącej podmiotu wybierz nową rolę Archiver i kliknij Zasoby.
 - b) Kliknij,
 aby rozwinąć sekcję Serwer i wybierz kartę sieciową (NIC) z listy Karta sieciowa .
 Wszystkie role Archiver muszą korzystać z tej samej karty sieciowej.



- c) W obszarze *Nagrywanie*wybierz lub utwórz **grupę Dysków** lub **Lokalizację Sieciową** dla roli Archiver. Każda rola Archiver wymaga dedykowanej lokalizacji nagrywania. Jeśli Archiver A zapisuje dane na dyskach A, B i C, Archiver B powinien zapisywać dane na dyskach D, E i F. Rola może posiadać wiele partycji, ale dwie role nigdy nie powinny korzystać z tej samej partycji.
- d) Kliknij Zastosuj.
- 5 Powtórz kroki 3 i 4, aby utworzyć każdą rolę Archiver.

- 6 Dodaj swoje kamery do wyznaczonej roli Archiver:
 - a) Na stronie głównej Narzędzia konfiguracyjnego otwórz zadanie Wideo .
 - b) Za pomocą przeglądarki podmiotu wybierz rolę Archiver, do której chcesz przypisać kamerę i kliknij **Jednostka Wideo** (
 - c) W oknie dialogowym, które się otworzy wprowadź wymagane informacje dotyczące kamery i kliknij **OK**.

Uwaga: Dodanie kamer zajmuje kilka sekund. Jeżeli rola nie będzie mogła dodać kamery w określonym czasie, zasygnalizowany zostanie status niepowodzenia i kamera zostanie usunięta.

d) Kliknij Zastosuj.

Pierwsze kroki z wtyczką Streamvault Maintenance

Przewodnik zawiera wprowadzenie do Konserwacja Streamvaultawtyczki i podaje informacje jak ją skonfigurować.

Ta sekcja zawiera następujące tematy:

- "O Konserwacja Streamvaulta wtyczce", 46
- "Pobieranie i instalowanie wtyczki", 47
- "Uprawnienia Genetec Streamvault", 48
- "Tworzenie roli wtyczki ", 50
- "Configurowanie Streamvault hardware monitor", 51
- "Konfigurowanie podmiotu managera Streamvault", 55
- "Informacje o karcie Zarządzanie", 58
- "Sprawdzanie stanu urządzenia przez Streamvault", 59
- "Kolumny panelu raportu dla zadania sprzętowego Streamvault", 60
- "Tworzenie reguł dla "od zdarzenia do działania" dla problemów technicznych Streamvault", 61

O Konserwacja Streamvaulta wtyczce

Wtyczka Streamvault Maintenance służy do monitorowania stanu urządzeń Streamvault i wysyła powiadomienia w przypadku wystąpienia problemów.

Uwaga: Przewodnik dotyczy Wtyczki Streamvault Maintenance 2.0.

Wtyczka Konserwacja Streamvaultazawiera następujące komponenty:

- Rola Streamvault: rola wtyczki jest używana do uruchamiania Hardware Monitor lub managera podmiotów. Dla każdego urządzenia Streamvault, które chcesz monitorować, wymagana jest jedna rola.
- *Streamvault*[™] *hardware monitor*: Jednostka używana do definiowania konfiguracji alertów dla każdego urządzenia Streamvault.
- *Streamvault*[™] *manager*: Jednostka używana do zbiorczego kontrolowania konfiguracji grupy urządzeń Streamvault. Można utworzyć tylko jedną instancję Streamvault manager.
- *Streamvault*[™] *hardware*: Zadanie raportowania w Security Center używane do przeglądania listy problemów technicznych wpływających na urządzenia Streamvault.

Konfiguracje jednostki wtyczki składają się z następujących ustawień:

- Konfiguracje alertów: używane do definiowania typów Zdarzeń, Stopni Intensywności zdarzenia i Powiadomień wpływających na alerty dotyczące stanów serwerów Streamvault.
- Odbiorcy e-maili: którzy użytkownicy i grupy użytkowników będą otrzymywać powiadomienia e-mail.
- Zdalne Zarządzanie Poświadczeniami : używane do kontrolowania i tworzenia profili użytkowników w kontrolerze iDRAC.
- Zintegrowana Integracja Kontrolera Dostępu Zdalnego Dell (iDRAC) (w przypadku modeli Streamvault obsługujących iDRAC): umożliwia bardziej precyzyjną kontrolę nad zarządzaniem poświadczeniami. Funkcję tę można znaleźć w zakładce dot. wtyczki Zarządzanie

Aby uzyskać więcej informacji, zobacz https://www.dell.com/en-us/lp/dt/open-manage-idrac

Ważne:

- W przypadku systemów z serwerami obsługującymi iDRAC oprogramowanie sprzętowe iDRAC musi być w wersji 6.0 lub nowszej.
- W przypadku urządzeń obsługiwanych przez kontroler iDRAC Konserwacja Streamvaulta wtyczka uzyskuje dostęp do danych dotyczących stanu urządzenia za pomocą połączenia wewnętrznego, o ile jest zainstalowane oprogramowanie modułu serwisowego iDRAC firmy Dell (iSM). iSM jest instalowany domyślnie w modelach obsługujących kontroler iDRAC.

Jeśli moduł iSM nie jest dostępny, wtyczka korzysta z komunikacji pozapasmowej z kontrolerem iDRAC. W takim przypadku musi istnieć połączenie sieciowe między dedykowanym portem kontrolera iDRAC a co najmniej jednym portem LAN, jeśli nie jest używane udostępnianie portów. Dedykowany port iDRAC jest domyślnie wyłączony. Aby dowiedzieć się więcej, zapoznaj się z poniższymi informacjami: https://www.dell.com/support/kbdoc/en-ca/000177212/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip.

Pobieranie i instalowanie wtyczki

Aby zintegrować wtyczkę Streamvault[™] Maintenance z Security Center, musisz zainstalować wtyczkę na serwerze Directory, serwerach Streamvault[™], które chcesz monitorować, oraz na wszystkich klienckich stacjach roboczych, na których chcesz skonfigurować wtyczkę.

Zanim rozpoczniesz

Upewnij się że zainstalowana jest kompatybilna wersja Security Center. Aby uzyskać informacje, zobacz Obsługiwane wtyczki w Security Center w TechDoc Hub.

Co powinieneś wiedzieć

- NAJLEPSZE PRAKTYKI: Zainstaluj rolę Streamvault na każdym serwerze, który chcesz monitorować.
- Ważne: Upewnij się, że moduł iDRAC każdego serwera jest podłączony do sieci i może komunikować się z systemem hosta. Domyślnie, moduł iDRAC korzysta z tego samego portu LAN co system hosta i jest skonfigurowany do uzyskiwania adresu IP przy użyciu protokołu DHCP.
- Ważne: Przed kontynuowaniem, upewnij się, że moduł iDRAC został zaktualizowany do oprogramowania sprzętowego 6.00 lub nowszego oraz że BIOS serwera został zaktualizowany do najnowszej wersji.
- Wtyczka jest obsługiwana wyłącznie na serwerach, na których działa oprogramowanie serwerowe Security Center.
- **Uwaga:** Konserwacja Streamvaulta Wtyczka jest preinstalowana na wszystkich kompatybilnych serwerach Streamvault. Z tego powodu, większość użytkowników musi jedynie utworzyć role i podmioty w Security Center. Jeśli Twój serwer został dostarczony przed udostępnieniem wtyczki lub jeśli została odinstalowana, wykonaj poniższe kroki, aby ją zainstalować.

Procedura

- 1 Otwórz stronę Pobierania Produktu GTAP.
- 2 W obszarze **Pobierz Finder**wybierz wersję Security Center.
- 3 Z sekcji Wtyczki Genetec pobierz pakiet dla swojego produktu.
- 4 Uruchom plik .exe, a następnie rozpakuj plik. Domyślnie plik jest rozpakowywany do *C*:*Genetec*.
- 5 Otwórz wyodrębniony folder, kliknij prawym przyciskiem myszy plik *setup.exe* i kliknij opcję **Uruchom jako** administrator.
- 6 Postępuj zgodnie z instrukcjami instalacji.
- 7 Na stronie *Kreator instalacji ukończony* kliknij przycisk **Zakończ**.
 - Ważne: Domyślnie ustawiona jest opcja **Uruchom ponownie Serwer Genetec**[™] . Możesz odznaczyć tę opcję, jeśli nie chcesz natychmiast restartować serwera Genetec[™]. Aby zakończyć instalację, należy ponownie uruchomić serwer Genetec.
- 8 Zamknij, a następnie otwórz wszystkie okna narzędzia Config Tool i Security Desk.

Uprawnienia Genetec Streamvault

Aby móc korzystać z zadań *Hardware monitor* i *Manager* powiązanych z urządzeniem Streamvault[™], należy przypisać wymagane uprawnienia dla kont użytkowników.

Konfigurowanie uprawnień użytkownika dla Streamvault

Domyślnie uprawnienia są przypisane niektórym grupom użytkowników, np. administratorom.

W zadaniu *Zarządzanie użytkownikami* w Config Tool możesz skonfigurować lub zmodyfikować uprawnienia użytkownika lub grupy użytkowników na stronie *Uprawnienia* użytkownika lub grupy użytkowników.

Aby dowiedzieć się więcej na temat hierarchii uprawnień, dziedziczenia uprawnień i przypisywania uprawnień, sprawdź Podręcznik Administratora Security Center i Przewodnik Wzmacniania zabezpieczeń Security Centerw TechDoc Hub

Uwaga: Listę wszystkich dostępnych uprawnień Security Center znajdziesz w arkuszu uprawnień Security Center . W razie potrzeby możesz sortować i filtrować tę listę.

Uprawnienia roli wtyczki Streamvault

Uprawnienia roli wtyczki Streamvault zapewniają dostęp do zadań związanych z *Hardware monitor* i *Managerem* Streamvault.

Domyślnie, administratorzy mają wszystkie uprawnienia. Jeśli utworzysz konto użytkownika na podstawie jednego z pozostałych szablonów uprawnień, konto użytkownika wymaga następujących uprawnień roli dotyczącej wtyczki Streamvault dla narzędzia konfiguracyjnego w Streamvault.

Podkategoria uprawnień	Zawiera uprawnienia do	Działania które można wykonać
Monitor sprzętowy hardware monitor	Modyfikowania hardware monitor	 Zmodyfikować konfiguracje alertów Zmodyfikować odbiorców wiadomości e-mail Zmodyfikować poświadczenia dotyczące zdalnego zarządzania Zmienić ustawienia portu
	Dodawania hardware monitor	Utworzyć nową jednostkę hardware monitor i przypisać ją do serwera Streamvault
	Usuwania hardware monitor	Usunąć istniejącą jednostkę hardware monitor
	Przeglądania hardware monitor	Wyświetlić konfigurację hardware monitor
Manager	Wprowadzania zmian dotyczących managera	 Zbiorczo modyfikować konfiguracje alertów Zbiorczo modyfikować odbiorców wiadomości e-mail

Podkategoria uprawnień	Zawiera uprawnienia do	Działania które można wykonać
	Dodawania managera	Utworzyć podmiot managera i przypisać go do serwera Streamvault
	Usuwania managera	Usuwać encję menedżera
	Przeglądania managera	Wyświetlać konfigurację managera

Tworzenie roli wtyczki

Zanim będziesz mógł skonfigurować wtyczkę i używać jej, musisz utworzyć rolę wtyczki Streamvault[™] Maintenance w narzędziu konfiguracyjnym.

Zanim rozpoczniesz

Pobierz i zainstaluj wtyczkę.

Co powinieneś wiedzieć

Konserwacja Streamvaulta Wtyczka zawiera dwie role:

- Streamvault[™] hardware monitor Jednostka monitorująca sprzęt hardware monitor Streamvault[™] służy do monitorowania stanu urządzeń Streamvault[™] i zapewnia otrzymywanie powiadomień w przypadku wystąpienia problemów. Wymagany jest jeden hardware monitor Streamvault[™] na każde urządzenie Streamvault[™].
- manager Streamvault[™] Jednostka Streamvault[™] manager służy do kontrolowania konfiguracji alertów dla grupy podmiotów w Streamvault[™] Agent. W każdym systemie dozwolony jest tylko jeden Streamvault[™] manager.
- **Uwaga:** Jeśli serwery Directory są urządzeniami wirtualnymi lub serwerami innymi niż Streamvault, utwórz rolę dla tych serwerów tylko wtedy, gdy chcesz korzystać z podmiotu managera.

Procedura

- 1 Na stronie głównej Narzędzia konfiguracyjnego otwórz zadanie Wtyczki.
- 2 W zadaniu *Wtyczki* kliknij **Dodaj podmiot** (+) i wybierz **Wtyczka**.

Otworzy się kreator tworzenia wtyczki.

3 Na stronie *Informacje szczegółowe* wybierz serwer, na którym hostowana jest rola wtyczki oraz typ wtyczki, a następnie kliknij **Dalej**.

Jeżeli w systemie nie używasz serwera dodatkowego, opcja Serwer nie zostanie wyświetlona.

- 4 Na stronie Informacje podstawowe określ informacje na temat roli:
 - a) Wprowadź nazwę podmiotu.
 - b) Wprowadź opis podmiotu.
 - c) Wybierz Partycję dla roli wtyczki.

Jeśli w systemie nie używasz partycji, opcja **Partycja** nie zostanie wyświetlona. Partycje to logiczne grupy używane do kontrolowania widoczności podmiotów. Tylko użytkownicy będący członkami tej partycji mogą wyświetlać i modyfikować tę rolę.

- d) Kliknij Dalej.
- 5 Na stronie *Podsumowanie utworzenia* przejrzyj informacje, a następnie kliknij **Utwórz**lub **Wstecz**, aby wprowadzić zmiany.

Po utworzeniu roli wtyczki wyświetli się komunikat: Operacja zakończyła się pomyślnie.

6 Kliknij Zamknij

Po zakończeniu

- Skonfiguruj podmiot Streamvault hardware monitoring.
- Skonfiguruj podmiot Streamvault manager.

Configurowanie Streamvault hardware monitor

Możesz skonfigurować Streamvault[™] hardware monitor do monitorowania stanu urządzenia Streamvault[™] i konfigurowania powiadomień wysyłanych w przypadku wystąpienia problemów.

Zanim rozpoczniesz

- Zarejestruj swoje urządzenia Streamvault.
- Utwórz rolę wtyczki Streamvault.

Ważne: Monitor sprzętu Streamvault jest tworzony automatycznie na każdym serwerze Streamvault obsługującym rolę Streamvault. Jeśli podmiot monitora sprzętu nie jest obecny w systemie po utworzeniu roli, należy ręcznie utworzyć monitor sprzętu.

Co powinieneś wiedzieć

Opcje konfiguracji różnią się w zależności od tego, czy posiadasz serwery z obsługą kontrolera iDRAC, czy inne serwery bez kontrolera iDRAC.

- Konfigurowanie serwera obsługującego kontroler iDRAC.
- Konfigurowanie serwera innego niż iDRAC.

Procedura

Aby skonfigurować serwer obsługujący kontroler iDRAC:

- 1 W narzędziu konfiguracyjnym przejdź do zadania Wtyczki i wybierz rolę wtyczki Streamvault.
- 2 Kliknij prawym przyciskiem myszy rolę wtyczki Streamvault i kliknij opcję **Utwórz hardware monitor**.



- 3 Na karcie Tożsamość wprowadź nazwę dla hardware monitor Streamvault w polu Nazwa .
- 4 Wybierz kartę Ogólne .
- 5 (Opcjonalnie) Jeśli dla swojego systemu utworzyłeś podmiot managera Streamvault[™], zaznacz pole wyboru **Użyj ustawień managera** , aby użyć ustawień profilu konfiguracji alertów dla managera Streamvault.
- 6 W sekcji *Profil konfiguracji alertów* zaznacz pole wyboru **Monitor sprzętu zarządza konfiguracjami alertów iDRAC**, aby zarządzać konfiguracjami alertów za pośrednictwem monitora sprzętu Streamvault.

7 Zaznacz pola wyboru powiązane ze **Zdarzeniami**, **poziomami ważności** i typami **Powiadomień**, które chcesz uwzględnić dla tego monitora sprzętu Streamvault.

Use manager settings						
Alert configuration profile	e					
Hardware monitor	manages iDRAC ale	rt configurations				
Events	Severity			Notification		
	🕕 Critical 🗹	Å Warning ▼	Information	Email	Event	
Cooling				<	Z	
СРИ		✓		$\mathbf{\overline{\checkmark}}$	✓	
Memory				<	Z	
Networking		<		<	✓	
Power		<		<	Z	
Storage		✓		<	✓	
System		V			₹	

8 W sekcji *Odbiorcy e-maili* wybierz, którzy użytkownicy i grupy użytkowników otrzymają powiadomienia email, gdy spełniony zostanie warunek w sekcji *Profil konfiguracji alertu*

Email recipients	
Admin	
Administrators	No email configured for this group
AutoVu	
AutoVu operators	
Patroller	
Patroller users	

- 9 W sekcji Poświadczenia zdalnego zarządzania wykonaj jedną z następujących czynności:
 - Zaznacz pole wyboru **Monitor sprzętu zarządza kontami iDRAC**, aby zarządzać poświadczeniami bezpośrednio za pomocą wtyczki.
 - Wyczyść pole wyboru **Monitor sprzętu zarządza kontami iDRAC**, aby używać kontrolera iDRAC do kontrolowania i tworzenia użytkowników i haseł.
- 10 (Opcjonalnie) Jeśli pole wyboru **Monitor sprzętu zarządza kontami iDRAC** zostało wyczyszczone, przejdź do karty **Zarządzanie** i skonfiguruj poświadczenia bezpośrednio w kontrolerze iDRAC.

11 (Opcjonalnie) W sekcji *Ustawienia* możesz zmienić **port domyślny** z 65115 na własny, preferowany. Aby uzyskać więcej informacji, zobacz Domyślne porty używane przez Streamvault, 4.

Remote management credentials	
Hardware monitor manages iDRAC accounts	
Username:	
Password:	
Settings	
Inbound port: 65116	

12 Kliknij Zastosuj.

Aby skonfigurować serwer inny niż iDRAC:

- 1 W narzędziu konfiguracyjnym przejdź do zadania Wtyczki i wybierz rolę wtyczki Streamvault.
- 2 Kliknij prawym przyciskiem myszy rolę wtyczki Streamvault i kliknij opcję **Utwórz hardware monitor**.



- 3 W karcie Tożsamość wprowadź nazwę dla hardware monitor Streamvault w polu Nazwa .
- 4 Wybierz kartę Ogólne .
- 5 (Opcjonalnie) Jeśli dla swojego systemu utworzyłeś podmiot managera Streamvault, zaznacz pole wyboru **Użyj ustawień managera** , aby użyć ustawień profilu konfiguracji alertów dla managera Streamvault.
- 6 W sekcji *Profil konfiguracji alertów* zaznacz pola wyboru odpowiadające typom **Zdarzeń** i **Powiadomień** , które chcesz zastosować do instancji Konserwacja Streamvaulta wtyczek kontrolowanych przez menedżera Streamvault.
- 7 W obszarze **Konfiguracja**ustaw **Próg zużycia dysku** półprzewodnikowego (SSD), przy który chcesz otrzymać powiadomienie informujące o konieczności wymiany dysku SSD.

8 W sekcji *Odbiorcy e-maili* wybierz, którzy użytkownicy i grupy użytkowników otrzymają powiadomienia email, gdy spełniony zostanie warunek w sekcji *Profil konfiguracji alertu*

Use manager settings				
Alert configuration profile				
Events	Notification		Status	Configuration
	Email	Event		
				
Predictive drive failure			Normal	
SSD wear			Normal	Threshold % 90
Offline drive	✓			
Email recipients				
Admin				
Administrature				
	No emai	I configured for this	group	
AutoVu				
AutoVu operators				
Patroller				
Patroller users				

9 Kliknij Zastosuj.

Tematy pokrewne

Informacje o karcie Zarządzanie, 58

Konfigurowanie podmiotu managera Streamvault

Możesz skonfigurować podmiot managera Streamvault[™] do kontrolowania konfiguracji alertów grupy monitorów sprzętowych Streamvault z jednej lokalizacji. Możesz także skonfigurować powiadomienia wysyłane w przypadku wystąpienia problemów. Korzystanie z podmiotu managera Streamvault jest opcjonalne.

Zanim rozpoczniesz

- Zarejestruj swoje urządzenia Streamvault[™].
- Utwórz rolę wtyczki Streamvault.

Uwaga: Podmiot managera Streamvault może działać na dowolnym serwerze Streamvault lub serwerze innym niż Streamvault w systemie Security Center. Do systemu można dodać tylko jeden podmiot managera Streamvault.

Procedura

- 1 W narzędziu konfiguracyjnym przejdź do zadania *Wtyczki* i wybierz rolę wtyczki Streamvault.
- 2 Kliknij prawym przyciskiem myszy rolę wtyczki Streamvault i kliknij **Utwórz managera**.



- 3 Wybierz podmiot managera Streamvault i kliknij kartę **Ogólne** .
 - Wyświetlone zostaną następujące sekcje:
 - Sekcja *profilu konfiguracji alertów kontrolera iDRAC* zarządza serwerami obsługującymi kontroler iDRAC w systemie.
 - Sekcja *profilu konfiguracji alertów innych niż iDRAC* służy do zarządzania w systemie serwerami innymi niż iDRAC .

Obie sekcje są zawsze wyświetlane, niezależnie od tego, czy masz system iDRAC, czy inny niż iDRAC.

- 4 (Jeśli dotyczy) W sekcji *profilu konfiguracji alertów kontrolera iDRAC* skonfiguruj następujące elementy:
 - a) Aby zarządzać konfiguracjami alertów iDRAC za pośrednictwem monitora sprzętu Streamvault wybranego serwera, zaznacz pole wyboru Monitor sprzętu zarządza konfiguracjami alertów iDRAC
 - b) Zaznacz pola wyboru powiązane ze Zdarzeniami, Poziomami ważności i rodzajami Powiadomień, które chcesz zastosować do ustawień dla Konserwacja Streamvaulta wtyczek kontrolowanych przez menedżera Streamvault.

iDRAC alert configuration profile						
🗹 Hardware monitor m	anages iDRAC ale	rt configurations				
Events	Severity			Notification		
	🚯 Critical 🗹	🛕 Warning 🗹	Information	Email	Event	
Cooling						
CPU		V		<		
Memory	✓			✓	✓	
Networking					✓	
Power					✓	
Storage					\checkmark	
System	<	✓		✓	≤	
Hardware monitors using Streamvault™ manager configuration						
Streamvault (SV-C5SH	1V3) - Streamvaul	t™ hardware moni	itor			

Uwaga: Monitory sprzętowe, których konfiguracje są ustawione przez managera Streamvault, są wymienione w sekcji **Monitory sprzętowe korzystające z konfiguracji managera Streamvault**[™]. Monitory sprzętowe korzystające z własnych konfiguracji są wymienione w sekcji **Monitory sprzętowe korzystające z konfiguracji niestandardowej**.

- 5 (Jeśli dotyczy) W sekcji Profil konfiguracji alertów innych niż iDRAC skonfiguruj następujące elementy:
 - a) Zaznacz pola wyboru odpowiadające typom **Zdarzeń** i **Powiadomień**, które chcesz zastosować dla instancji Konserwacja Streamvaulta wtyczek kontrolowanych przez managera Streamvault.
 - b) W obszarze **Konfiguracja**ustaw **Próg zużycia dysku** półprzewodnikowego (SSD), przy który chcesz otrzymać powiadomienie informujące o konieczności wymiany dysku SSD.

Non-iDRAC alert configuration profil	e			
Events	Notification		Configuration	
	Email	Event		
Predictive drive failure		V		
SSD wear			Threshold % 90	
Offline drive	✓			
Hardware monitors using Streamvault [™] manager configuration Streamvault (SVFR426S3) - Streamvault [™] hardware monitor				

Uwaga: Monitory sprzętowe, których konfiguracje są ustawione przez managera Streamvault, są wymienione w sekcji **Monitory sprzętowe korzystające z konfiguracji managera Streamvault**[™]. Monitory sprzętowe korzystające z własnych konfiguracji są wymienione w sekcji **Monitory sprzętowe korzystające z konfiguracji niestandardowej**.

6 W sekcji Odbiorcy wiadomości e-mail wybierz, którzy użytkownicy i grupy użytkowników będą otrzymywać powiadomienia e -mail, gdy spełniony zostanie warunek w profilu konfiguracji alertów kontrolera iDRAC lub w sekcji profilu konfiguracji alertów innych niż iDRAC.

Email recipients	
Admin	
Administrators	No email configured for this group
AutoVu	
AutoVu operators	
Patroller	
Patroller users	

7 Kliknij Zastosuj.

Informacje o karcie Zarządzanie

Karta **Zarządzanie** wyświetla stronę internetową iDRAC, za pomocą której można konfigurować poświadczenia serwera iDRAC i zarządzać nimi. Możesz tam także znaleźć więcej informacji o serwerze iDRAC i skonfigurować inne opcje, które nie są dostępne za pośrednictwem interfejsu użytkownika wtyczki Streamvault[™].

Dostęp do karty **Zarządzanie** można uzyskać za pośrednictwem monitora sprzętu Streamvault[™] dowolnego serwera obsługującego iDRAC lub za pośrednictwem menedżera Streamvault[™].

Jeśli uzyskasz dostęp do karty **Zarządzanie** za pośrednictwem menedżera Streamvault, u góry strony zostanie wyświetlone rozwijane menu . Możesz z niego skorzystać aby przełączyć się z jednego serwera iDRAC na inny, zamiast konieczności ręcznego przełączania z jednego monitora sprzętowego na drugi. Każdy serwer iDRAC ma własną stronę iDRAC.

Search	e se					
Streamvault (SV-C5SH1V3)						
Streamvault** hardware monitor	Streamvault (SV-CSSHTV3) - Streamvault = hardware =					
 Streamvault (SVFR426S3) 	Currently displaying web page at https://					
Streamvault** hardware monitor						
Streamvault ^{en} manager						
	Integrated Remote Access Controller 9					
	idrac-ms06657 Streamvault Enterprise					
	Type the User Name and Password and click Log in.					
	Usename: Password 🔍					
	Domán This IDRAC V					
	O Security Notice: By accessing this computer, you confirm that such access compiles with your organization's security policy.					
	Ligh .					
	🗭 Streamvault					
	Here I Succest					

Aby uzyskać informacje dotyczące logowania, kliknij opcję **Pomoc** u dołu strony internetowej.

Uwaga: Aby uzyskać dostęp do strony internetowej kontrolera iDRAC, potrzebne jest połączenie sieciowe między systemem klienckim, na którym działa narzędzie konfiguracyjne Config Tool, a adresem IP serwera iDRAC. Jeśli połączenie sieciowe jest niedostępne, użyj strony Narzędzia konfiguracyjnego Config Tool bezpośrednio z urządzenia Streamvault poprzez sesję z pulpitu zdalnego lub konsoli lokalnej.

Jeśli w systemie nie ma żadnych serwerów iDRAC, karta **Zarządzanie** pozostanie pusta. Wyświetli się informacja, że nie ma dostępnych monitorów sprzętowych Streamvault z funkcjami zarządzania iDRAC.

Uwaga: Jeśli strona internetowa kontrolera iDRAC nie załąduje się, kliknij inną kartę, a następnie wróć do karty **Zarządzanie** .

Tematy pokrewne

Configurowanie Streamvault hardware monitor, 51 Konfigurowanie podmiotu managera Streamvault, 55

Sprawdzanie stanu urządzenia przez Streamvault

Użyj zadania Sprzęt Streamvault[™], aby wyświetlić listę problemów sprzętowych wpływających na urządzenia Streamvault.

Procedura

- 1 Na stronie głównej otwórz zadanie urządzenia Streamvault.
- 2 Poprzez filter Zakres Czasu zdefiniuj okres, który ma obejmować raport.
- 3 Kliknij Generuj raport.Właściwości jednostki są wymienione w panelu raportu.

Kolumny panelu raportu dla zadania sprzętowego Streamvault

Po wygenerowaniu raportu wyniki zapytania zostaną wyświetlone w panelu raportowym. W tej sekcji wymieniono kolumny dostępne dla zadania sprzętowego Streamvault™.

- **Obraz:** Ikona przedstawiająca typ problemu.
- Powaga: Poziom ważności powiązany z problemem.
- Znacznik czasu: Data i godzina kiedy wystąpiło zdarzenie.
- Źródło: Urządzenie Streamvault, którego dotyczy problem.
- MessageID: Identyfikacja sekwencji alfanumerycznej powiązanej ze zgłoszonym problemem.
- Wiadomość: Opis problemu.
- **Opis:** Opis przyczyny problemu.

Uwaga: Aby uzyskać więcej informacji na temat tworzenia raportów, zobacz Omówienie obszaru roboczego zadań dotyczących raportowaniaw TechDoc Hub.

Tworzenie reguł dla "od zdarzenia do działania" dla problemów technicznych Streamvault

Korzystając z "od zdarzenia do działania" możesz wyzwolić działania, które będą uruchamiane w przypadku wykrycia problemu sprzętowego Streamvault™.

Zanim rozpoczniesz

- Utwórz rolę Wtyczki Streamvault Maintenance.
- Konfigurowanie podmiotu Streamvault hardware monitor.

Procedura

- 1 Na stronie głównej Narzędzia konfiguracyjnego Config Tool kliknij zadanie *Automatyzacja* i kliknij widok **Działania** .

- 3 Skonfiguruj "od zdarzenia do działania":
 - a) Z listy rozwijanej Kiedy wybierz opcję Wykryto problem sprzętowy Streamvault.
 - b) Kliknij opcję Określ warunek błędu i wprowadź błąd kodu iDRAC. Możesz także wprowadzić pełen identyfikator, aby zapobiec fałszywym wyzwalaniom działania.

Na przykład na poniższym zrzucie ekranu kod błędu to TMP0103, a pełny identyfikator to IDRAC.2.8.TMP0103.

Event-to-action	
When:	IDRAC.2.8.TMP0103 ▼ occurs
From:	Any entity
Action:	
Effective	Always
Enabled:	
	Cancel Save

c) (Opcjonalnie) W opcjach **Od** wybierz swoją wtyczkę Streamvault lub monitor sprzętowy.
 Uwaga: Ponieważ wtyczka Streamvault korzysta z niestandardowych zdarzeń, które mają znaczenie tylko dla niej samej, nie ma potrzeby przypisywania jej źródła.

Jeśli wybierzesz wtyczkę Streamvault jako podmiot źródłowy, to w przypadku usunięcia roli wtyczki, wszystkie powiązane reguły automatyzacji zostaną usunięte. Jeśli nie określono żadnego podmiotu źródłowego i rola została usunięta, reguły automatyzacji pozostają niezmienione.

- d) Z listy rozwijanej Działania wybierz rodzaj działania i skonfiguruj jego parametry.
- e) (Opcjonalnie) W opcji **Efektywne** kliknij **Zawsze** i wybierz harmonogram, w którym "od zdarzenia do działania" będzie aktywne.

Jeśli zdarzenie nastąpi poza zdefiniowanym harmonogramem, działanie nie zostanie wyzwolone.

- 4 Upewnij się że wariant "od zdarzenia do działania" jest włączony.
- 5 Kliknij Zapisz.

Uwaga: Aby zapoznać się z pełną listą kodów błędów kontrolera iDRAC, zobacz tu https:// developer.dell.com/apis/2978/versions/5.xx/docs/Error%20Codes/EEMIRegistry.md.

4

Informacje o Panelu Sterowania SV

Te informacje pomogą Ci zrozumieć Panel Sterowania SV.

Ta sekcja zawiera następujące tematy:

- "Strona Główna Panelu Sterowania SV", 64
- "Strona Konfiguracujna Panelu Sterowania SV", 66
- "Strona Bezpieczeństwo w Panelu Sterowania SV", 69
- "Informacje o Panelu Sterowania SV", 72

Strona Główna Panelu Sterowania SV

Użyj Strony Głównej w Panelu Sterowania SV aby uzyskać dostęp do podstawowych zadań wymaganych do konfiguracji i korzystania z systemu. Kliknij ikony interfejsu, aby uzyskać dostęp do aplikacji Config Tool, Security Desk, Server Admin lub Genetec[™] Update Service.



Alternatywnie możesz kliknąć skróty Narzędzia Konfiguracyjnego (Config Tool) lub skróty Security Desk, aby otworzyć powiązane zadania.

W przypadku systemów działających w trybie Klient, skrót Server Admin jest niedostępny. Również skróty do Narzędzi Konfiguracyjnych (Config Tool) i Security Desk są ograniczone.

Uwaga: Informacja: Jeśli Twój system nie został aktywowany, pojawi się czerwony baner z tym powiadomieniem. Kliknij **System nie jest aktywowany. Kliknij tutaj, aby go aktywować.**, aby otworzyć kreator Aktywacji Panelu Sterowania Streamvault.

Skróty dla Narzędzia Konfiguracyjnego

Użyj skrótów, aby otworzyć główne zadania w aplikacji Config Tool. Dostępne skróty zależą od rodzaju posiadanej licencji.

Skrót	Działanie		
Config Tool	Otwiera narzędzie konfiguracyjne.		
Zarejestruj kamery i	Otwiera narzędzie do rejestracji jednostek, w którym możesz zarejestrować swoje		
kontrolery	kamery i kontrolery.		
Zarządzaj	Otwiera zadanie <i>Zarządzanie Poświadczeniami</i> , w którym można zarządzać		
poświadczeniami	poświadczeniami użytkowników.		

Skrót	Działanie		
Zarządzaj posiadaczami kart	Otwiera zadanie <i>Zarządzanie posiadaczami kart</i> , w którym można zarządzać posiadaczami kart.		
Konfiguruj kamery	Otwiera zadanie <i>Wideo</i> , w którym można dodawać kamery i nimi zarządzać.		
Konfiguruj drzwi	Otwiera zadanie <i>Widoku Obszaru</i> , w którym można dodawać drzwi i zarządzać nimi.		
Zarządzaj uprawnieniami użytkownika	Otwiera zadanie <i>Zarządzanie użytkownikami</i> , w którym można dodawać i zarządzać uprawnieniami użytkowników.		
Konfiguruj alarmy	Otwiera zadanie <i>Alarmy</i> , w którym można konfigurować alarmy.		
Zarządzaj harmonogramami	Otwiera <i>Zadanie systemowe</i> , w którym można tworzyć i zarządzać harmonogramami.		

Skróty w Security Desk

Skorzystaj ze skrótów, aby otworzyć główne zadania w aplikacji Security Desk. Dostępne skróty zależą od rodzaju posiadanej licencji.

Skrót	Działanie			
Security Desk	Otwiera Security Desk.			
Monitoruj obiekty	Otwiera zadanie <i>Monitorowanie</i> , w którym można monitorować zdarzenia systemowe w czasie rzeczywistym.			
Monitoruj alarmy	Otwiera zadanie <i>Monitorowanie</i> , w którym można monitorować zdarzenia systemowe w czasie rzeczywistym.			
Rozwiązywanie problemów z dostępem	Otwiera narzędzie do rozwiązywania problemów z Dostępem, które umożliwia diagnozowanie i rozwiązywanie problemów z konfiguracją. Uwaga: Skrót ten jest niedostępny w systemach działających w trybie Klienta.			
Zbadaj wideo	Otwiera zadanie <i>Archiwa</i> , w którym można wyszukiwać archiwa wideo. Uwaga: Skrót ten jest niedostępny w systemach działających w trybie Klienta.			
Zbadaj aktywność drzwi	Otwiera zadanie <i>Zdarzenia dot. drzwi</i> gdzie możesz sprawdzić zdarzenia dotyczące wybranych drzwi. Uwaga: Skrót ten jest niedostępny w systemach działających w trybie Klienta.			

Skrót do Usługi Aktualizacji Genetec

Skorzystaj z Usługi Aktualizacji Genetec, aby mieć pewność, że komponenty oprogramowania twojego urządzenia są aktualne.

Skrót do Server Admin

Użyj aplikacji Server Admin, aby ręcznie wprowadzić licencję lub wyświetlić i zmienić konfigurację serwera.

Strona Konfiguracujna Panelu Sterowania SV

Na stronie *Konfiguracja* Panelu Sterowania Streamvault[™] możesz modyfikować ustawienia ogólne, takie jak *ustawienia regionalne, ustawienia sieciowe*i ustawienia *Monitora Dostępności Systemu*.

Streamvault Control Panel								
Home		ation Security About						
	Machine name: SVFR426S3			Automatic (DHCP) 📿				
	Description:	Microsoft Windows 11 IoT Enterprise LTSC	IP address:	10 . 122 . 0 . 125				
			Subnet:	255.255.0.0				
	Date and time:	11/27/2024 🔳 02:03:25 PM 🏶	Gateway:	10 . 122 . 0 . 1				
	Time zone:	(UTC-05:00) Eastern Time (US & Canada) 🔻	DNS server:	10 . 0 . 1 . 220				
	Regional settings Product language: English English			d partitions				
			Configure					
	Change keyboard layout in Windows System Availability Monitor							
		Configure	Configure					
	Backup wizard Restore wizard			intenance plugin				
		Configure						

W przypadku systemów działających na serwerze dodatkowym lub w trybie Klienta sekcje *Monitor Dostępności Systemu* oraz *Directory i konfiguracji kopii zapasowej/przywracania* są niedostępne.

Ustawienia informacji ogólnych

Skorzystaj z sekcji *Informacje ogólne*, aby zmienić ustawienia ogólne, takie jak nazwa urządzenia Streamvault[™].

- Nazwa urządzenia: Wyświetla nazwę urządzenia SV.
- Opis: Wprowadź zrozumiały opis, który pomoże zidentyfikować urządzenie.
- **Data i godzina:** Kliknij pole, aby skonfigurować wartości daty i godziny wyświetlane na komputerze. Alternatywnie możesz kliknąć ikonę kalendarza lub zegara w polu, aby skonfigurować ustawienia.
- Strefa czasowa: Wybierz strefę czasową z rozwijanej listy.

Ustawienia regionalne

Aby zmienić ustawienia językowe układu klawiatury systemowej, skorzystaj z sekcji Ustawienia regionalne .

- Język produktu: Wybierz język z listy, aby zmienić język w Config Tool i Security Desk.
 Ważne: Aby zmiany zaczęły obowiązywać, należy ponownie uruchomić aplikacje Security Center.
- Zmień układ klawiatury w systemie Windows: Kliknij tę opcję, aby otworzyć stronę ustawień dla *Języka i regionu* systemu Windows i zmienić układ klawiatury.

Ważne: Aby zmiany odniosły skutek, należy ponownie uruchomić komputer.

Uwaga: Panel Sterowania SV jest dostępny w języku angielskim, francuskim i hiszpańskim.
Kopia zapasowa i przywracanie

Skorzystaj z sekcji Directory i konfiguracje kopii Zapasowej/Przywracania aby uzyskać dostęp do Kreatora kopii zapasowej i Kreatora przywracania.

Tworzenie kopii zapasowych i przywracanie danych to funkcja Panelu Sterowania SV. Umożliwia bezpieczne tworzenie kopii zapasowych bazy danych katalogu i plików konfiguracyjnych, a następnie przywracanie ich z tym samym identyfikatorem systemowym. Kopie zapasowe i przywracanie można wykorzystać w przypadku awarii systemu lub aktualizacji sprzętu. Ta funkcja nie tworzy kopii zapasowej pliku licencji, archiwów wideo ani innych baz danych.

Ta sekcja jest niedostępna w przypadku systemów działających na serwerze powiększonym lub działających w trybie Klient.

- Kreator kopii zapasowych: Kliknij opcję Kreator kopii zapasowej, aby utworzyć kopię zapasową bazy danych katalogu i plików konfiguracyjnych.
- Kreator przywracania danych: Kliknij opcję Kreator przywracania danych, aby przywrócić w systemie kopię zapasową bazy danych katalogu i plików konfiguracyjnych.

Ważne: Musisz otworzyć wymagany port, aby mieć pewność, że funkcja *Directory kopii zapasowych/ przywracania i konfiguracji* będzie mogła skomunikować się z Panelem Sterowania SV. Aby uzyskać więcej informacji, zobacz Domyślne porty używane przez Streamvault, 4.

Ustawienia sieci

Użyj sekcji Sieć, aby zmienić ustawienia sieciowe, takie jak adres IP na urządzeniu Streamvault.

• Automatycznie (DHCP): Domyślnie, protokół dynamicznej konfiguracji hosta (DHCP) jest używany do automatycznego przypisywania adresu IP, podsieci, bramy i serwera DNS. Wyłącz tę opcję, jeśli nie chcesz, aby adres IP był przydzielany dynamicznie przez serwer DHCP.

Kliknij Odśwież () aby odświeżyć ustawienia DHCP i uzyskać nowy adres IP.

- Adres IP: Adres IP urządzenia.
- Podsieć: Maska podsieci urządzenia.
- Brama: Adres bramy IP .
- **serwer DNS:** Adres IP serwera DNS.

Role Archivera i Partycje

Użyj sekcji *Role Archivera i Partycje*, aby skonfigurować systemy wymagające większej liczby kamer i przepustowości niż maksymalna liczba obsługiwana przez pojedynczy archiwizator.

Ta sekcja jest dostępna dla systemów, w których działa Security Center w wersji 5.9 i nowszej na serwerze dodatkowym.

Streamvault Control Panel							
Home							
	General informatio Machine name: Description: Micro	Archiver Roles and Partitions An Archiver role can support: Your model (SV-1000-R14-72T-8-210) - 300 cameras supports: - Throughput of 500 Mbps - 400 cameras - Partitions with a maximum size of 30 TB - 400 Mbps	-1CP) 💭				
		Suggested scenario	. 122 . 0 . 125				
	Data and times.	Number of cameras: 0 Number of roles: 0	5.255.0.0				
	Date and time: 1	Camera throughput: 0 Number of partitions: 0	.122.0.1				
	Time zone: (UTC-	05 Size of partitions (TB): 0.00	. 0 . 1 . 220				
		O Custom scenario					
	Product language:	Number of roles: 0 Total disk space (TB): 0.02					
	Change keyboard layout	Number of partitions: 0 Used disk space (TB): 0.00					
		Size of partitions (TB): 0 Free disk space (TB): 0.02					
	Backup wizard	Create partitions/roles	ain				
		Configure					

- Rola Archiver może obsługiwać: Wyświetla maksymalną liczbę kamer, przepustowość i rozmiar partycji obsługiwaną przez pojedynczą rolę Archivera.
- **Twój model obsługuje:** Wyświetla maksymalną liczbę kamer i przepustowość obsługiwaną przez Twój model urządzenia Streamvault.
- **Sugerowany scenariusz:** Automatycznie oblicza ilość ról, partycji i rozmiar partycji potrzebnych dla żądanej ilości kamer i przepustowości.
- Scenariusz niestandardowy: Wybierz liczbę ról, partycji i rozmiar partycji potrzebnych do konfiguracji systemu.

Aby uzyskać więcej informacji na temat korzystania z tej funkcji, zobacz Dodanie roli Archiver w Panelu Sterowania SV, 40.

Ustawienia Monitora Dostępności Systemu

Użyj sekcji *Monitor Dostępności Systemu*, aby skonfigurować ustawienia Agenta Monitora Dostępności Systemu na urządzeniu Streamvault. Na przykład dotyczące ustawienie metody zbierania danych i aktywacji Agenta.

Możesz także sprawdzić następujące kwestie:

- Czy urządzenie komunikuje się z Security Center
- Kiedy nastąpił ostatni punkt kontrolny
- · Jakie błędy i ostrzeżenia zostały ostatnio zgłoszone w dziennikach dotyczących Aplikacji i Usług

Ta sekcja jest niedostępna w przypadku systemów działających na serwerze powiększonym lub działających w trybie Klient.

Ustawienia Wtyczki Serwisowej Streamvault™ Maintenance 2.0.0

Skorzystaj z *Wtyczki Serwisowej Streamvault*[™]aby zarejestrować wtyczkę w Security Center, jeśli jeszcze tego nie zrobiono.

Strona Bezpieczeństwo w Panelu Sterowania SV

Na stronie *Bezpieczeństwo* możesz modyfikować hasła użytkowników, wybrać tryb komunikacji między agentem CylancePROTECT a Genetec[™] oraz zastosować profile zwiększające bezpieczeństwo i dokonać ustawień zabezpieczeń systemu w urządzeniu Streamvault[™].

Streamvault Control Panel							
Home	Configuratior	n Security About					
	Credentials Security Center (Adm Al antivirus Operation mode:	in user) Modify password Online (recommended) Olisconnected	1 ANCE ect 7 7	Hardening Hardening profile: More information Some settings b hardening profil	Microsoft with CIS Level 2 elow might not align with t e.	the selected	
	Enable quarantine n	O Turn off (uninstall)	Ŧ	Remote Desktop servic Remote management: File sharing service: Never lock screen: Removable storage acc	ress:		

Ustawienia hasła

Aby zmienić hasła kont użytkowników dla urządzenia Streamvault, skorzystaj z sekcji *Dane uwierzytelniające* na stronie *Bezpieczeństwo*.

Uwaga: Dla bieżącego użytkownika zarówno na serwerze głównym i serwerze dodatkowym dostępne są różne opcje konfiguracji haseł. Na serwerze dodatkowym, administrator może zmieniać tylko hasła do systemu Windows, ale nie hasła dla Security Center.

Zdefiniuj hasło dla każdego typu użytkownika:

- Security Center (użytkownik administratora): Hasło administratora dla Security Desk, Config Tool, and Genetec[™] Update Service.
- Server Admin : Hasło dla Genetec[™] Server Admin application.
- Operator Windowsa: Kliknij Modyfikuj hasło, aby zmienić hasło operatora dla systemu Windows.

Ustawienia antywirusowe

Użyj sekcji AI Antivirus , aby wybrać tryb, w którym agent CylancePROTECT będzie komunikował się z Genetec.

CylancePROTECT to oprogramowanie antywirusowe oparte na sztucznej inteligencji, służące do ochrony przed zagrożeniami i ich wykrywania.

Można wybrać pomiędzy następującymi trybami pracy:

- **Online (zalecane):** W trybie online Agent CylancePROTECT komunikuje się z firmą Genetec w celu zgłaszania nowych zagrożeń, aktualizacji narzędzia podprocesu i wysyłania danych w celu udoskonalenia modeli matematycznych. Ta opcja zapewnia najwyższy poziom ochrony.
- Tryb Rozłączony: Tryb rozłączony dotyczy urządzenia bez połączenia z Internetem. W tym trybie CylancePROTECT nie może łączyć się, ani wysyłać informacji do usług zarządzania Genetec w chmurze. Twoje urządzenie jest chronione przed większością zagrożeń. Przeglądy techniczne i aktualizacje są dostępne za pośrednictwem Usługi Aktualizacji Genetec[™] (GUS).
- **Tryb Wyłączony:** Wybierz ten tryb, aby trwale odinstalować CylancePROTECT ze swojego urządzenia. Twoje urządzenie będzie używać usługi Microsoft Defender do ochrony i wykrywania zagrożeń. Nie zalecamy wyłączania CylancePROTECT, jeśli urządzenie nie może otrzymywać aktualizacji dotyczących sygnatur wirusów w Microsoft Defender.

Ostrożnie: Przełączanie pomiędzy opcjami może wymagać ponownego uruchomienia komputera, powodując przestoje systemu.

Kliknij opcję **Włącz zarządzanie kwarantanną**, aby dodać opcję **Zarządzanie zagrożeniami** do menu podręcznego ikony Cylance na pasku zadań systemu Windows. Ta opcja umożliwia usunięcie elementów poddanych kwarantannie. **Logowanie** i **Wykrywanie Ochrony Uruchamiania Run Protect** zostały również dodane do menu kontekstowego (menu po kliknięciu prawym przyciskiem myszy). Opcje te umożliwiają dostęp do logów i powodują uruchomienie skanowania.

Check for Updates Check for Policy Update About System Check		
Options	>	
Run Protect Detection	>	
Threat Management	>	Delete Quarantined
		✓ 日 印) 11:42 AM 12/11/2024

Ustawienia wzmacniające bezpieczeństwo

Użyj sekcji *Wzmacnianie bezpieczeństwa*, aby wybrać profil wzmocnienia i skonfigurować ustawienia zabezpieczeń systemu dla urządzenia Streamvault.

Uwaga: Profile wzmacniające bezpieczeństwo są dostępne tylko w urządzeniach, które mają*Usługa Streamvault*. Aby uzyskać więcej informacji, zobacz O usłudze Streamvault, 15.

Istnieją cztery predefiniowane profile wzmacniania bezpieczeństwa:

- **Microsoft (tylko):** Ten profil wzmacniania zabezpieczeń stosuje w Twoim systemie podstawowe zasady bezpieczeństwa firmy Microsoft. Podstawowe linie zabezpieczeń firmy Microsoft to grupa zalecanych przez firmę Microsoft konfiguracji ustawień, które zostały opracowane na podstawie opinii zespołów inżynierów ds. zabezpieczeń, grup produktów, partnerów i klientów firmy Microsoft.
- Microsoft z CIS Poziom 1: Ten profil wzmacniania zabezpieczeń stosuje w systemie podstawowe zasady bezpieczeństwa firmy Microsoft oraz profil Centrum Bezpieczeństwa Internetowego (CIS) Poziom 1 (CIS L1). Certyfikat CIS L1 zapewnia podstawowe wymagania bezpieczeństwa, które można wdrożyć w dowolnym systemie przy niewielkim lub żadnym wpływie na wydajność lub ograniczenie funkcjonalności.

- Microsoft z CIS Poziom 2: Ten profil wzmacniania zabezpieczeń stosuje w systemie podstawowe zabezpieczenia firmy Microsoft oraz profile CIS L1 i Poziom 2 (L2). Profil CIS L2 oferuje najwyższy poziom bezpieczeństwa i jest przeznaczony dla organizacji, dla których bezpieczeństwo jest priorytetem.
 Uwaga: Surowe zabezpieczenia, jakie wprowadza ten profil wzmacniający, mogą ograniczyć funkcjonalność systemu i utrudnić zdalne zarządzanie serwerem.
- Microsoft z STIG: Ten profil wzmacniania zabezpieczeń stosuje dla systemu podstawowe zasady bezpieczeństwa firmy Microsoft oraz opiera dane na wytycznych Wdrażania Rozwiązań Technicznych w Zakresie Bezpieczeństwa (STIG) Agencji ds. Systemów Informacyjnych Departamentu Obrony (DISA). DISA STIG opierają się na standardach Narodowego Instytutu Norm i Technologii (NIST) i zapewniają zaawansowaną ochronę bezpieczeństwa systemów Windows dla Departamentu Obrony Stanów Zjednoczonych.

Uwaga: Domyślnie wszystkie urządzenia są dostarczane z zastosowanym profilem wzmacniającym Microsoft CIS poziomu 2.

Gdy dostępna będzie nowa wersja wybranego profilu wzmacniającego bezpieczeństwo, pojawi się przycisk **Kliknij tutaj, aby zaktualizować**. Kliknij przycisk, aby zastosować aktualizację.

Hardening	
A new version o	of the Microsoft (only) profile is available.
Hardening profile:	Microsoft (only)

Oprócz profili wzmacniających bezpieczeństwo można skonfigurować również następujące ustawienia zabezpieczeń systemu:

- **Usługi Pulpitu Zdalnego:** Zezwól osobom w twojej sieci na logowanie się do urządzenia za pomocą aplikacji *Pulpit zdalny*. Aby zapobiec wpływowi złośliwego oprogramowania na urządzenie, opcja ta została domyślnie wyłączona.
- Zdalne Zarządzanie: Włącz zdalną pomoc techniczną dla narzędzi do zarządzania firmy Microsoft, takich jak Windows Admin Center, Microsoft Server Manager i Remote PowerShell.
- **Usługa udostępniania plików:** Zezwalaj osobom w twojej sieci na udostępnianie plików i folderów znajdujących się na urządzeniu. Aby zapobiec wpływowi złośliwego oprogramowania na urządzenie, opcja ta została domyślnie wyłączona.
- **Nigdy nie blokuj ekranu:** Jeżeli ta opcja jest włączona, system Windows będzie utrzymywał użytkownika zalogowanego nawet po 15 minutach braku aktywności.
- Wyjmowany dostęp do pamięci masowej: Włącz dostęp do podłączonego klucza USB lub dysku twardego USB z poziomu systemu Windows.

Uwaga: Użytkownicy z uprawnieniami administracyjnymi automatycznie uzyskują dostęp do pamięci wymiennej.

Informacje o Panelu Sterowania SV

Skorzystaj ze strony *Informacje*, aby wyświetlić przydatne informacje, jeśli potrzebujesz pomocy przy urządzeniu Streamvault[™]. Na stronie *Informacje* znajdują się dane o systemie, linki do Portalu Pomocy Technicznej Genetec[™] (GTAP) oraz dokumentacji produktu, informacje o licencji i informacje o Umowie Serwisowej Oprogramowania (SMA).

W przypadku systemów działających na serwerze rezerwowym lub znajdujących się w trybie Klienta dostępne są tylko sekcje *System* i *Pomoc*.

		Stream	ivault Co	ontrol Pa	nel	
Home	Configurat	ion Security Abo				
	System Manufacturer: Hardware model: Image version: System ID:	GENETEC Inc. SV-100E-1T-I3-TST 11.2024.2.000.00.G SV-1234ABC Show installed products		License Expiration date: Access control: Number of readers: Number of cardholders: Video:	11/3/2025 Supported 100 Unlimited Supported	
	Help GTAP: TechDoc Hub:			Number of cameras: Show full license Genetec Advantage	100	
	Control Panel: Security Desk:			Expiration date: SMA number: Type:	11/5/2025 SMA-0001-001 4	
			Genetec Inc. 2024, All rig	hts reserved.		

Informacje o Systemie

Aby wyświetlić informacje o systemie, skorzystaj z sekcji System.

- Producent: Wyświetla producenta sprzętu.
- Model sprzętu: Wyświetla model sprzętu.
- Wersja obrazu: Wyświetla wersję obrazu oprogramowania.
- System ID : Wyświetla numer identyfikacyjny systemu.
- **Pokaż zainstalowane produkty:** Kliknij, aby wyświetlić wersję oprogramowania komponentów Genetec zainstalowanych na urządzeniu.

Pomoc

W sekcji Pomoc znajdziesz przydatne linki do GTAP i dokumentacji produktu.

- GTAP: Kliknij link, aby otworzyć forum dotyczącego GTAP i pomocy technicznej.
 Uwaga: Aby zalogować się do GTAP, musisz znać prawidłową nazwę użytkownika i hasło.
- TechDoc Hub: Kliknij link, aby otworzyć Genetec TechDoc Hub.
- **Panel Sterowania:** Kliknij łącze, aby otworzyć *Podręcznik Użytkownika Urządzenia Streamvault*, który zawiera informacje z Panelu sterowania SV.

• Security Desk: Kliknij łącze, aby otworzyć Podręcznik Użytkownika Security Center.

Informacje na temat licencji

Aby wyświetlić informacje o *Licencji*, skorzystaj z sekcji Licencja. Wyświetlane informacje różnią się w zależności od opcji licencji.

- Data ważności: Wyświetl się, gdy wygaśnie licencja Security Center.
- Kontrola dostępu: Pokazuje czy funkcje kontroli dostępu są obsługiwane .
- Liczba czytników: Wyświetla liczbę czytników obsługiwanych przez system.
- Liczba posiadaczy kart: Wyświetla liczbę posiadaczy kart obsługiwanych przez system.
- Wideo: Pokazuje czy obsługiwane są funkcje wideo.
- Liczba kamer: Wyświetla liczbę kamer obsługiwanych przez system.
- Pokaż pełną licencję: Kliknij, aby wyświetlić więcej informacje dytyczących licencji.

Ta sekcja jest niedostępna w przypadku systemów działających na serwerze powiększonym lub działających w trybie Klient.

Informacje na temat usługi Genetec Advantage

Aby wyświetlić informacje na temat SMA, skorzystaj z sekcji Genetec Advantage .

- Data ważności: Wyświetla datę wygaśnięcia Umowy Serwisowej dotyczącej Oprogramowania.
- numer SMA: Wyświetl numer SMA.
- **Typ:** Wyświetla typ SMA.

Ta sekcja jest niedostępna w przypadku systemów działających na serwerze powiększonym lub działających w trybie Klient.

Dodatkowe zasoby

Ta sekcja zawiera następujące tematy:

- "Gwarancja na produkt dla Twojego urządzenia Streamvault", 75
- "Ponowne tworzenie obrazu urządzenia Streamvault", 76
- "Znajdowanie identyfikatora systemu i wersji obrazu dla urządzenia Streamvault", 77
- "Zezwalanie na udostępnianie plików na urządzeniu Streamvault", 78
- "Zezwalanie na połączenia Pulpitu Zdalnego z urządzeniem Streamvault", 79

Gwarancja na produkt dla Twojego urządzenia Streamvault

Twoje urządzenie Streamvault[™] jest objęte 3-letnią standardową gwarancją na sprzęt i oprogramowanie, z opcją przedłużenia o 2 lata.

Szczegółowy opis warunków gwarancji na produkt Genetec[™] znajduje się w Przeglądzie gwarancji na produkty Genetec[™].

Ponowne tworzenie obrazu urządzenia Streamvault

Aby ponownie utworzyć obraz urządzenia Streamvault[™], potrzebny jest Certyfikat autentyczności firmy Microsoft (COA), aby określić, jakiego obrazu można używać w urządzeniu. Każde urządzenie Streamvault posiada przyklejoną etykietę COA, która wskazuje jaka wersja systemu Windows jest uruchomiona na urządzeniu.

Listę obrazów zgodnych z Twoim urządzeniem w oparciu o wersję systemu Windows można znaleźć w Uwagach do wydania Streamvault . Nie używaj obrazu oprogramowania, jeśli na urządzeniu działa inna wersja systemu Windows niż ta wskazana w informacjach o jej wersji.

Poniżej znajduje się przykład typowej etykiety COA z wytłoczonymi informacjami dotyczącymi wersji systemu Windows i certyfikatu. Produkty zawierające wbudowane wersje oprogramowania firmy Microsoft mają etykietę COA.



Uwaga: Każdy obraz Streamvault jest zaprojektowany do współpracy z odpowiednią wersją Security Center, jak wskazano w Uwagach do wydania Streamvault. Zmiana wersji Security Center do wcześniejszej wersji może wymagać zmniejszenia poziomu zabezpieczeń urządzenia.

Przegląd dostępności produktów, pomocy technicznej i dostępnych usług można znaleźć na stronie Cykl życia Produktu w witrynie GTAP

Znajdowanie identyfikatora systemu i wersji obrazu dla urządzenia Streamvault

Kontaktując się z Centrum Pomocy Technicznej Genetec[™] (GTAC), potrzebny jest identyfikator systemu i wersja obrazu oprogramowania Genetec[™] zainstalowanego na urządzeniu.

Zanim rozpoczniesz

Zaloguj się do systemu Windows jako administrator.

Co powinieneś wiedzieć

Oprócz identyfikatora systemu i wersji obrazu, GTAC może poprosić o numer certyfikatu i numer seryjny. Aby znaleźć te informacje, poszukaj etykiety na urządzeniu Streamvault[™].

Procedura

- 1 Na pulpicie systemu Windows otwórz **Panel sterowania SV Genetec**[™] .
- 2 Jeśli zostanie wyświetlony monit, wprowadź hasło użytkownika Admin.
- 3 Kliknij Informacje.
- 4 W sekcji System zapisz numer identyfikators Systemu i Wersję obrazu.

Tematy pokrewne

Wykonywanie resetu fabrycznego w urządzeniu typu All-in-one Streamvault (wszystko w jednym), 81 Przywracanie ustawień fabrycznych naStreamvault stacji roboczej lub urządzeniu serwerowym, 90

Zezwalanie na udostępnianie plików na urządzeniu Streamvault

Aby udostępniać pliki i foldery na urządzeniu osobom w sieci, musisz włączyć udostępnianie plików w Panelu sterowania SV.

Zanim rozpoczniesz

Na urządzeniu, zaloguj się do systemu Windows jako Administrator.

Co powinieneś wiedzieć

- Aby zapewnić maksymalne bezpieczeństwo, udostępnianie plików jest domyślnie wyłączone.
- Komputery zdalne i twoje urządzenie muszą być podłączone do tej samej sieci IP.

Procedura

- 1 Na stronie *Bezpieczeństwo* w Panelu Sterowania SV włącz usługę **Udostępnianie plików**.
- 2 Kliknij **Zastosuj**.
- 3 Aby udostępnić folder lub plik innym osobom, kliknij na folder lub plik prawym przyciskiem myszy w Eksploratorze plików systemu Windows i kliknij opcję **Udostępnij**.

Zezwalanie na połączenia Pulpitu Zdalnego z urządzeniem Streamvault

Aby sterować urządzeniem z dowolnego komputera lub maszyny wirtualnej w sieci, należy najpierw włączyć w urządzeniu zdalny dostęp.

Zanim rozpoczniesz

Na urządzeniu, zaloguj się do systemu Windows jako Administrator.

Co powinieneś wiedzieć

- Aby zapewnić maksymalne bezpieczeństwo, dostęp zdalny jest domyślnie wyłączony.
- Urządzenie i komputer zdalny muszą być podłączone do tej samej sieci.

Procedura

- 1 Na stronie Bezpieczeństwo w Panelu Sterowania SV włącz opcję usługi Pulpit Zdalny.
- 2 Kliknij Zastosuj.

Tematy pokrewne

Pulpit zdalny nie chce się połączyć się z urządzeniem Streamvault, 99

Rozwiązywanie problemów

Ta sekcja zawiera następujące tematy:

- "Wykonywanie resetu fabrycznego w urządzeniu typu All-in-one Streamvault (wszystko w jednym) ", 81
- "Przywracanie ustawień fabrycznych naStreamvault stacji roboczej lub urządzeniu serwerowym", 90
- "Kontrolery Mercury EP pozostają w trybie offline, gdy protokół TLS 1.1 jest wyłączony", 95
- "Włączenie Harmonogramu Świtu i Zmroku (TLS)", 96
- "Pulpit zdalny nie chce się połączyć się z urządzeniem Streamvault", 99
- "Usuwanie ograniczeń z kont użytkowników niebędących administratorami", 103
- "Konta lokalne nie mają dostępu do Pulpitu Zdalnego, usługi udostępniania plików ani zdalnego zarządzania ", 104
- "Włączenie usług związanych ze Smart Card", 105
- "Włączanie obsługi oprogramowania układowego kontrolerów Mercury EP i LP w wersji 1.x.x", 106
- "Włączanie wsparcia integracji Synergis IX", 108

Wykonywanie resetu fabrycznego w urządzeniu typu Allin-one Streamvault (wszystko w jednym)

Jeśli oprogramowanie na urządzeniu Streamvault[™] All-in-one nie uruchamia się lub przestaje działać zgodnie z oczekiwaniami, możesz przywrócić ustawienia fabryczne za pomocą klucza USB.

Zanim rozpoczniesz

- Utwórz kopię zapasową swojej bazy danych Directly w Panelu sterowania SV
- Miej w pobliżu odpowiednią licencję wersji Security Center, którą chcesz przywrócić lub zainstalować.
- Przygotuj identyfikator systemu i hasło przesłane e-mailem po zakupie urządzenia. Zobacz Znajdowanie identyfikatora systemu i wersji obrazu dla urządzenia Streamvault, 77.
- (Zalecane) Podłącz urządzenie do Internetu za pomocą przewodowego połączenia Ethernet, aby system mógł sprawdzić łączność.

Uwaga: Weryfikacja skończy się niepowodzeniem, jeśli połączenie internetowe nie jest dostępne, ale możesz nadal korzystać z urządzenia.

Co powinieneś wiedzieć

Przywrócenie ustawień fabrycznych powoduje usunięcie i zastąpienie wszystkich danych znajdujących się aktualnie na dysku Windows (C :), w tym baz danych i dzienników Pliki wideo na innych dyskach nie są naruszone.

Procedura

- 1 Utwórz przywracany do ustawień fabrycznych klucz USB zawierający obraz oprogramowania.
- 2 Za pomocą klucza USB zresetuj obraz na urządzeniu.

Po zakończeniu

Ponowna konfiguracja urządzenia.

Tematy pokrewne

Znajdowanie identyfikatora systemu i wersji obrazu dla urządzenia Streamvault, 77

Tworzenie klucza USB do resetowania ustawień fabrycznych dla urządzenia Streamvault All-in-one (wszystko w jednym)

Zanim będzie można zresetować obraz urządzenia Streamvault[™] All-in-one (wszystko w jednym), należy przygotować rozruchowy nośnik USB zawierający wymagany obraz oprogramowania Streamvault.

Zanim rozpoczniesz

 Zdobądź klucz USB o pojemności co najmniej 32 GB. Niektóre klucze USB nie mogą uruchomić obrazu; jeśli tak się stanie, spróbuj użyć klucza innej marki lub modelu.
 Ostrożnie: Wszystkie dane na kluczu USB są usuwane podczas tworzenia dysku startowego.

Procedura

- 1 Skontaktuj się z Centrum Pomocy Technicznej Genetec[™](GTAC)aby uzyskać obraz odzyskiwania. Obraz odzyskiwania jest dostępny w jednym z trzech następujących formatów:
 - Plik .zip zawierający pliki .swm .
 - *Plik .iso zawierający pliki .swm* i interfejs użytkownika narzędzia do przywracania ustawień *fabrycznych Streamvault* , którego użyjesz do zresetowania obrazu oprogramowania.
 - *Plik .iso* zawierający kreator *instalacji systemu Windows* , którego możesz uzyć do zresetowania obrazu oprogramowania.
- 2 Jeśli obraz odzyskiwania jest *plikiem .zip* , rozpakuj jego zawartość do dowolnego folderu systemu Windows.
- 3 Ze strony Pobierania Produktów w GTAP pobierz kreator USB narzędzia Streamvault do przywracania ustawień fabrycznych.
 - a) W obszarze Pobierz Finderwybierz wersję Security Center.
 - b) Z listy Inne pobierz pakiet Streamvault Factory Reset Utility.

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

- 4 Włóż klucz USB do portu USB.
- 5 Otwórz kreator USB narzędzia do przywracania *ustawień fabrycznych Streamvault* , które pobrałeś z TechDoc Hub.
- 6 Z listy Wybierz dysk USB wybierz klucz USB o pojemności co najmniej 32 GB.

Streamvault factory reset utility	×
Streamvault	2
Select USB drive	
Select Genetec image	
	e
> Partition the USB key	
> Download the image tools	
> Unzip the image tools to USB	
> Copy the image files to USB	

- 7 W sekcji *Wybierz obraz Genetec* kliknij **Przeglądaj** i wybierz plik *.swm* lub *.iso*. Jeśli potrzebujesz plik *.swm*, wybierz wymagany obraz z folderu *wim* .
- 8 Kliknij opcję Utwórz klucz USB.

Narzędzie do przywracania *ustawień fabrycznych Streamvault* rozpoczyna partycjonowanie klucza USB, pobieranie narzędzi obrazu i kopiowanie plików obrazów.

Po zakończeniu pobierania zostanie wyświetlony następujący komunikat: Nośnik USB został pomyślnie utworzony.

Przykład

Poniższy film pokazuje, jak utworzyć pamięć USB umożliwiającą przywrócenie ustawień fabrycznych przy użyciu *plików .swm* .



Po zakończeniu

Wybierz z poniższych:

- Zresetuj obraz oprogramowania swojego urządzenia typu "Streamvault wszystko w jednym".
- Zresetuj obraz oprogramowania Streamvault stacji roboczej lub serwera.

Resetowanie obrazu oprogramowania na urządzeniu typu All-in-one (wszystko w jednym)

Po przygotowaniu rozruchowego nośnika USB zawierającego wymagany obraz oprogramowania Streamvault[™] możesz go użyć do zresetowania obrazu oprogramowania na urządzeniu Streamvault All-in-one (wszystko w jednym).

Zanim rozpoczniesz

• Upewnij się, że masz klucz USB zawierający oprogramowanie do odzyskiwania danych urządzenia.

Co powinieneś wiedzieć

- Resetowanie trwa około 20-30 minut, a podczas niego uruchamianych jest kilka skryptów, a urządzenie uruchamia się kilka razy.
- Nie przerywaj procesu resetowania. Ręczne zamknięcie lub wyłączenie urządzenia może spowodować uszkodzenie odzyskiwania.

Procedura

Aby zresetować obraz oprogramowania:

- 1 Wyłącz urządzenie.
- 2 Włóż utworzony klucz USB do portu USB.
- Włącz urządzenie i naciskaj kilkakrotnie klawisz F12, aż pojawi się menu rozruchu.
 W zależności od urządzenia, otworzy się menu rozruchu UEFI lub menu jednorazowego rozruchu Streamvault.

4 Wybierz dysk USB i naciśnij Enter. **Uwaga:** Wygląd menu startowego może się różnić.

Use the f(Up) and 4(0 Press [Enter] to atte Marning: Legacy boot such as HCO, SSO, NVM such as So Card, USB, Boot mode 1s set to: I UEF1 BOOT: Windows Boot Mana, <u>WIFIS Kangung Fla</u> Onboard NIC(IPW) Onbeard NIC(IPW) OTHER OPTIONS:	own) arrow keys to move the pointer to the desired / mpt the boot or ESO to Cancel. (* = Password Regult mode does not support OB boot on internal strange d e. or eHKC. It is intended for use with external str and Network PXE. UEFI: Secure Boot: ON gen gen shGlu 30 PHNE	soot device, ad svices prage devices only,	Genetec Inc. Streamvault One-Time Boot Settings Control the boot flow for the SupportAssist OS Recovery Tool. NOTE: Once a system and/or admin password is set, the system will always prompt for system and/or admin password during boot.	Pre-Boot Tasks Change important BIOS settings on your system, cor BIOS SETUP Configure BIOS options and control how your system functions.
Diss rash quarte Disgnostics Change Boot Hode 3 OptiPlex 3060	Settings BIDS Revision 1.1.4	Dell	UEFI Boot Devices Windows Boot Manager UEFI PC SN740 NVMe WD 256GB 22454K441619 1 Wefi UEFI USB Device UEFI Hard Drive	Device Configuration Configure device settings
	UEEI Boot menu		Streamvault One-t	ime Boot menu

W zależności od obrazu oprogramowania, zostanie otwarte narzędzie do *przywracania ustawień fabrycznych Streamvault* lub Kreator *instalacji systemu Windows*.

- 5 Zresetuj obraz oprogramowania przy użyciu narzędzia odpowiedniego dla Twojego urządzenia:
 - Narzędzie do przywracania ustawień fabrycznych Streamvault
 - Kreator instalacji systemu Windows

Aby zresetować obraz oprogramowania za pomocą narzędzia do przywracania ustawień fabrycznych Streamvault:

1 Gdy USB uruchomi się w trybie odzyskiwania, wybierz opcję **Przywróć ustawienia fabryczne systemu operacyjnego (C:)**, aby sformatować i ponownie zainstalować dysk systemowy urządzenia.



- 2 Gdy pojawi się monit, wpisz Tak i naciśnij Enter. Poczekaj, aż przywrócenie ustawień fabrycznych zostanie ukończone.
- 3 Po zakończeniu przywracania ustawień fabrycznych wyjmij klucz USB z urządzenia i naciśnij klawisz Enter, aby ponownie uruchomić urządzenie.

4 W oknie dialogowym *Genetec*[™] *Product Validator* wprowadź numer dla części urządzenia (nr produktu) i numer seryjny Genetec[™]

Numery te można znaleźć na etykiecie Genetec znajdującej się na górze urządzenia. Jeśli nie ma etykiety, możesz wpisać dowolny tekst, aby kontynuować.

Pojawi się przycisk Start .

5 Kliknij **Start**.

Wyświetli się jeden z następujących komunikatów dotyczących statusu:

- SUKCES: Proces zakończył się sukcesem. Przejdź do następnego kroku.
- **SUKCES- Brak transmisji:** Proces powiódł się, jednak w momencie uruchomienia urządzenia połączenie internetowe było niedostępne. Przejdź do następnego kroku.
- **PRÓBA NIEUDANA:** Proces nie powiódł się. Skontaktuj się z Centrum Pomocy Technicznej Genetec™(GTAC)
- 6 Jeśli otrzymasz komunikat SUKCES lub SUKCES- Brak transmisji , zamknij okno Genetec[™] Product Validator .
- 7 Poczekaj na zamknięcie skryptu działającego w tle, a następnie uruchom ponownie urządzenie.

Aby zresetować obraz oprogramowania za pomocą Kreatora instalacji systemu Windows:

- 1 Na ekranie *Wybierz ustawienia językowe* zaznacz preferowany język i ustawienia czasu, a następnie kliknij **Dalej**.
- 2 Na ekranie Wybierz ustawienia klawiatury wybierz preferowaną klawiaturę i kliknij Dalej.
- 3 Na ekranie *Wybierz opcję instalacji* wybierz **Zainstaluj system Windows X**, gdzie X oznacza wersję systemu Windows, którą instalujesz. Potwierdź, że Twoje pliki, aplikacje i ustawienia zostaną usunięte i kliknij **Dalej**.

Select setup Install the latest version of Windo and settings will be deleted. I would like to	Option ows 11, or repair your PC. If you're installing Install Windows 11 Repair my PC leted including files, apps, and settings	Windows <mark>11</mark> , please note your files, apps,
I would like to	 Install Windows 11 Repair my PC leted including files, apps, and settings 	
I agree everything will be del	 Repair my PC leted including files, apps, and settings 	
I agree everything will be del	leted including files, apps, and settings	
Previous Version of Setup		
Microsoft Support	Legal	Back Next

Uwaga: Archiwa wideo zapisane na dodatkowym dysku wideo nie ulegną zmianie. Usunięte zostaną tylko pliki znajdujące się na dysku systemu operacyjnego.

- 4 Na ekranie *Klucz produktu* wykonaj jedną z następujących czynności:
 - Jeśli urządzenie jest podłączone do Internetu, kliknij opcję **Nie mam klucza produktu** , aby kontynuować. Urządzenie automatycznie pobiera dane aktywacyjne z firmy Microsoft.
 - Jeśli urządzenie nie jest podłączone do Internetu, wprowadź klucz licencyjny znajdujący się na etykiecie Certyfikatu Autentyczności (COA) dołączonej do urządzenia i kliknij **Dalej**.

Product key should be with the box the DVD came in or on your email receipt. looks similar to this: XXXXX-XXXXX-XXXXX-XXXXX nter Product key Dashes will be added automatically	
Iooks similar to this: XXXXX-XXXXXX-XXXXXX-XXXXXX nter Product key Dashes will be added automatically	
nter Product key Dashes will be added automatically	
Dashes will be added automatically	
don't have a product key	
rivacy statement	
Microsoft Support Legal Back N	
	ext

5 Na ekranie Obowiązujące powiadomienia i warunki licencji przeczytaj warunki licencji i kliknij **Akceptuję**.



6 Na ekranie *Wybierz lokalizację instalacji systemu Windows X* wybierz *Partycję podstawową* na dysku z systemem operacyjnym. Rozmiar tej partycji jest zazwyczaj mniejszy niż 1 TB. Kliknij **Dalej**.

G Refresh	Load Driver	🗳 Bri	ing Disk Online	
X Delete Partition	Format Partition	+ Cr	eate Partition	Extend Partition
			Sec. P. Marcolast M. Ma	To the set of the
Name		Total Size	Free Space	Туре
Disk 0 Partition 1: New	Volume	5.5 TB	5.5 TB	Primary
Disk 0 Unallocated Space	e	600.0 KB	600.0 KB	Unallocated Space
Disk 1 Partition 1		16.0 MB	16.0 MB	MSR (Reserved)
Disk 1 Partition 2: New	Volume	5.5 TB	5.5 TB	Primary
Disk 1 Unallocated Space	e	600.0 KB	600.0 KB	Unallocated Space
Disk 2 Partition 1		100.0 MB	100.0 MB	System
Disk 2 Partition 2		238.4 GB	204.1 GB	Primary
Disk 2 Unallocated Space	e	344.0 KB	344.0 KB	Unallocated Space
Disk 3 Partition 1: AIO5	13	58.3 GB	58.5 GB	Primary

Ostrożnie: Nie wybieraj głównej partycji dysku do przechowywania plików wideo, ponieważ nadpiszesz całą przechowywaną na niej zawartość.

7 Na ekranie *Gotowy do instalacji* kliknij **Zainstaluj**.



8 Po zakończeniu instalacji, system Windows zostanie uruchomiony ponownie, a skrypt zostanie automatycznie uruchomiony w celu sfinalizowania instalacji. Po zakończeniu działania skryptu, ponownie uruchom urządzenie.

Przykład

Obejrzyj ten film, aby dowiedzieć się, jak zresetować obraz oprogramowania na urządzeniu typu All-in-one (wszystko w jednym) przy użyciu rozruchowego dysku USB zawierającego *pliki .swm* .



Po zakończeniu

- Zaloguj się do systemu Windows przy użyciu domyślnej nazwy użytkownika i hasła, które znajdują się na naklejce przyklejonej do urządzenia.
- Aktywuj licencję Security Center
- Jeśli wykonałeś kopię zapasową konfiguracji Security Center przed przywróceniem ustawień fabrycznych, przywróć konfigurację za pomocą Panelu sterowania SV.
- Ponowna konfiguracja urządzenia.

Przywracanie ustawień fabrycznych naStreamvault stacji roboczej lub urządzeniu serwerowym

Jeśli oprogramowanie na Streamvault serwerze lub stacji roboczej nie uruchamia się lub przestanie działać zgodnie z oczekiwaniami, możesz przywrócić ustawienia fabryczne za pomocą klucza USB.

Zanim rozpoczniesz

- Utwórz kopię zapasową całej konfiguracji Security Center za pomocą Panelu Sterowania SV. Aby uzyskać więcej informacji, zobacz Tworzenie kopii zapasowej bazy danych Directory , 38.
- Zdobądź klucz USB o pojemności co najmniej 32 GB. Niektóre klucze USB nie mogą uruchomić obrazu; jeśli tak się stanie, spróbuj użyć klucza innej marki lub modelu.
- Ostrożnie: Wszystkie dane na kluczu USB są usuwane podczas tworzenia dysku startowego.
- Miej w pobliżu odpowiednią licencję wersji Security Center, którą chcesz przywrócić lub zainstalować.
- Przygotuj identyfikator systemu i hasło przesłane e-mailem po zakupie urządzenia.

Co powinieneś wiedzieć

- **Dotyczy:** Wszystkich modeli rozpoczynających się od SVW, SVR i SVA oraz wszystkich serwerów o numerze modelu SV-1000E i wyższym.
- Aby zapoznać się z urządzeniami All-in-One, zobacz Wykonywanie resetu fabrycznego w urządzeniu typu All-in-one Streamvault (wszystko w jednym) , 81.
- Przywrócenie ustawień fabrycznych powoduje usunięcie wszystkich danych znajdujących się obecnie na dysku systemowym (OS), ale nie ma wpływu na domyślne ustawienia fabryczne dysku RAID.
- Resetowanie może się nie powieść, jeśli dyski twarde, dyski RAID lub partycje w urządzeniu zostały zmienione z domyślnych ustawień fabrycznych. W takim wypadku, skontaktuj się z Centrum Pomocy Technicznej (GTAC)

Procedura

- 1 Utwórz klucz USB przywracający ustawienia fabryczne.
- 2 Za pomocą klucza USB zresetuj obraz na urządzeniu.

Po zakończeniu

Skonfiguruj swoje urządzenie.

Tematy pokrewne

Znajdowanie identyfikatora systemu i wersji obrazu dla urządzenia Streamvault, 77

Tworzenie klucza USB dla przywracania ustawień fabrycznych dla stacji roboczej Streamvault lub urządzenia serwerowego

Zanim będzie można zresetować obraz stacji roboczej lub serwera Streamvault[™], należy przygotować rozruchowy nośnik USB zawierający wymagany obraz oprogramowania Streamvault.

Zanim rozpoczniesz

Zdobądź klucz USB o pojemności co najmniej 32 GB. Niektóre klucze USB nie mogą uruchomić obrazu; jeśli tak się stanie, spróbuj użyć klucza innej marki lub modelu.

Ostrożnie: Wszystkie dane na kluczu USB są usuwane podczas tworzenia dysku startowego.

Procedura

1 Skontaktuj się z Centrum Pomocy Technicznej Genetec[™](GTAC)aby uzyskać obraz odzyskiwania.

Obraz odzyskiwania jest dostępny w jednym z trzech następujących formatów:

- Plik .zip zawierający pliki .swm .
- *Plik .iso* zawierający *pliki .swm* i interfejs użytkownika narzędzia do przywracania ustawień fabrycznych *Streamvault* , którego możesz użyć do zresetowania obrazu oprogramowania.
- *Plik .iso* zawierający kreator *instalacji systemu Windows* , którego możesz uzyć do zresetowania obrazu oprogramowania.
- 2 Jeśli obraz odzyskiwania jest *plikiem .zip* , rozpakuj jego zawartość do dowolnego folderu w systemie Windows.
- 3 Ze strony Pobierania Produktów w GTAP pobierz kreator USB Streamvault do przywracania ustawień fabrycznych.
 - a) Z listy Pobierz Finderwybierz swoją wersję Security Center.
 - b) Z listy Inne pobierz pakiet Narzędzie do przywracania ustawień fabrycznych Streamvault .

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

- 4 Włóż klucz USB do portu USB.
- 5 Otwórz kreator USB dla Narzędzi do przywracania ustawień fabrycznych Streamvault

6 Z listy Wybierz dysk USB wybierz klucz USB o pojemności co najmniej 32 GB.

Streamvault factory reset utility	_	×
Streamvault		?
Select USB drive		
		~
Select Genetec image		
		se
> Partition the USB key		
> Download the image tools		
> Unzip the image tools to USB		
> Copy the image files to USB		

- 7 W sekcji *Wybierz obraz Genetec* kliknij **Przeglądaj** i wybierz plik *.swm* lub *<service tag number>*. Jeśli potrzebujesz plik *.swm*, wybierz wymagany obraz z folderu *wim* .
- 8 Kliknij opcję **Utwórz klucz USB**.

Narzędzie do przywracania *ustawień fabrycznych Streamvault* rozpoczyna partycjonowanie klucza USB, pobieranie narzędzi obrazu i kopiowanie plików obrazów.

Po zakończeniu pobierania zostanie wyświetlony następujący komunikat: Nośnik USB został pomyślnie utworzony.

Przykład

Poniższy film pokazuje, jak utworzyć pamięć USB umożliwiającą przywrócenie ustawień fabrycznych przy użyciu *plików .swm*.



Po zakończeniu

Wybierz z poniższych:

- Zresetuj obraz oprogramowania swojego urządzenia typu Streamvault "All-in-one (wszystko w jednym).
- Zresetuj obraz oprogramowania Streamvault stacji roboczej lub serwera.

Przywracania obrazu fabrycznego oprogramowania na Streamvault stacji roboczej lub urządzeniu serwerowym

Po przygotowaniu rozruchowego nośnika USB zawierającego wymagany obraz oprogramowania Streamvault [™] możesz go użyć do zresetowania obrazu oprogramowania na stacji roboczej lub na serwerze.

Zanim rozpoczniesz

• Upewnij się, że masz klucz USB zawierający oprogramowanie do odzyskiwania danych urządzenia.

Co powinieneś wiedzieć

- Resetowanie nie ma wpływu na domyślne ustawienia fabryczne dysku RAID.
- Resetowanie może się nie powieść, jeśli dyski twarde, dyski RAID lub partycje w urządzeniu zostały zmienione względem domyślnych ustawień fabrycznych. W takim wypadku, skontaktuj się z Centrum Pomocy Technicznej (GTAC)

Procedura

- 1 Wyłącz urządzenie.
- 2 Włóż utworzony wcześniej rozruchowy klucz USB do portu USB.
- 3 Włącz urządzenie Streamvault .
- 4 Po wyświetleniu monitu naciśnij klawisz F12. Zostanie otwarty *Menedżer Rozruchu*. Kliknij **Menu Jednorazowego Rozruchu UEFI**.
- 5 Wybierz dysk USB, a następnie naciśnij klawisz Enter. Otworzy się *Narzędzie do przywracania ustawień fabrycznych Streamvault*
- 6 Kliknij Przywróć ustawienia fabryczne systemu operacyjnego (C:).

itreamvault factory reset utility
Genetec
Streamvault factory reset utility
This recovery utility will allow you to factory reset the operating system (C: drive).
Ensure that only the USB factory reset drive is connected and no other USB drives are connected.
WARNING: This operation will erase ALL data on the Windows drive.
Select an option to continue.
Option 1 - The system will exit the utility and reboot.
Do nothing and reboot
Option 2 - Factory reset C: (OS) drive only
Factory reset OS (C:)

Zostanie otwarty wiersz poleceń, a narzędzie do przywracania *ustawień fabrycznych Streamvault* przeanalizuje system w celu wykrycia dysku systemowego (OS).

- W wierszu poleceń wpisz Tak , aby potwierdzić, że wykryto właściwy twardy dysk, a następnie naciśnij klawisz Enter, aby rozpocząć przywracanie ustawień fabrycznych.
 Ważne: Nie przerywaj, nie wyłączaj ani nie uruchamiaj ponownie stacji roboczej podczas procesu
- ponownego tworzenia obrazu. Może to zająć do 20 minut, w zależności od szybkości klucza USB. 8 Po zakończeniu przywracania ustawień fabrycznych i pojawieniu się monitu o ponowne uruchomienie
- stacji roboczej naciśnij Enter. 9 Wyjmij klucz USB z portu USB.

Stacja robocza została teraz zresetowana do stanu domyślnego.

Przykład

Obejrzyj ten film, aby dowiedzieć się, jak przywrócić obraz fabryczny oprogramowania na stacji roboczej lub serwerze Streamvault.



Po zakończeniu

- Zaloguj się do systemu Windows przy użyciu domyślnej nazwy użytkownika i hasła, które znajdują się na naklejce przyklejonej do urządzenia.
- Aktywuj licencję Security Center
- Jeśli wykonałeś kopię zapasową konfiguracji Security Center przed przywróceniem ustawień fabrycznych, przywróć konfigurację za pomocą Panelu Sterowania SV.
- Ponowna konfiguracja urządzenia.

Kontrolery Mercury EP pozostają w trybie offline, gdy protokół TLS 1.1 jest wyłączony

Po zarejestrowaniu kontrolera Mercury EP w Security Center urządzenie nie łączy się z Internetem. Nie otrzymasz żadnych błędów ani ostrzeżeń dotyczących tego problemu.

Dotyczy:

- Streamvault[™] SV-100E 16.3 i nowsze
- Streamvault[™] SV-300E 16.3 i nowsze
- Streamvault[™] SV-350E 16.3 i nowsze

Przyczyna

Wszystkie kontrolery Mercury EP wymagają protokołu Transport Layer Security (TLS) 1.1 do komunikacji z Security Center. Jednakże protokół ten jest wyłączony we wszystkich urządzeniach Streamvault[™] All-in-One w wersji 16.3 i nowszych.

Rozwiązanie

Włącz TLS 1.1.

Włączenie Harmonogramu Świtu i Zmroku (TLS)

Protokoły Transport Layer Security (TLS) 1.0 i 1.1 mają kilka poważnych luk w zabezpieczeniach, dlatego są wyłączone w urządzeniach Streamvault[™]. Jeśli urządzenie zarejestrowane w Security Center wymaga do komunikacji jednego z tych protokołów, należy włączyć ten protokół na swoim urządzeniu.

Co powinieneś wiedzieć

- TLS 1.1 jest wyłączony w oprogramowaniu Streamvault w wersji 16.3 i nowszych.
- TLS 1.0 jest wyłączony w oprogramowaniu Streamvault w wersji 16.0 i nowszych.
- Włącz tylko tę wersję protokołu TLS, której wymaga Twoje urządzenie.
- Włącz TLS na węzłach serwera (przychodzące) i klienta (wychodzące).
- Ze względów bezpieczeństwa, opcje Właściwości internetowych są wyłączone na urządzeniach. Jeśli Twoje urządzenie korzysta z usługi Streamvault, możesz włączyć protokół TLS w Edytorze Lokalnych Zasad dla Grupy. Jeśli Twoje urządzenie nie korzysta z usługi Streamvault, możesz włączyć protokół TLS tylko w Edytorze Rejestru Systemu Windows.

Procedura

Aby włączyć protokół TLS na urządzeniu z usługą Streamvault:

- 1 Otwórz Wiersz Poleceń jako administrator i uruchom gpedit.msc. Otworzy się Edytor Lokalnych Zasad dla Grupy.
- 2 Przejdź do Konfiguracja Komputera > Szablony Administracyjne > Streamvault > Genetec > Szablony dodatkowe.
- 3 Włącz protokół TLS 1.*n* przy kliencie, gdzie *n* oznacza numer wersji pomocniczej:
 - a) Kliknij prawym przyciskiem myszy \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL \Protocols\TLS 1.n\Client\Enabled i kliknij **Edycja**.
 - b) Przełącz**Włączone** na 1 i kliknij **Zastosuj > OK**.
 - c) Kliknij prawym przyciskiem myszy\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL \Protocols\TLS 1.n\Client\DisabledByDefault i kliknij **Edycja**.
 - d) Ustaw **DisabledByDefault** na 0 i kliknij **Zastosuj** > **OK**.

- 4 Włącz TLS 1.*n* na serwerze:
 - a) Kliknij prawym przyciskiem myszy \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL \Protocols\TLS 1.n\Server\Enabled i kliknij Edycja.
 - b) Ustaw Włączone na 1 i kliknij Zastosuj > OK.
 - c) Kliknij prawym przyciskiem myszy \SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL \Protocols\TLS 1.n\Server\DisabledByDefault i kliknij **Edycja**.
 - d) Ustaw **DisabledByDefault** na 0 i kliknij **Zastosuj > OK**.

Local Group Policy Editor			C	- Normation Content (Section NUCL) Protocols TIC 100 Clines (Content Section 2010)	, – – – – – – – – – – – – – – – – – – –
File Action View Help		Se (Statewi(curren	controiset(contro	DisecurityHonders(SchAnniel(Hotocols(TES 1.0(client/ena	
		SYSTEM\Current	tControlSet\Contro	ol/SecurityProviders/SCHANNEL/Protocols/TLS 1.0/Client/Enabled	
Local Computer Policy Local Computer Configuration	Setting Software\Policies\Mi	Previous Setting	Next Setting		ment lo
Software Settings	Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi	Enabled Disabled	Supported on:	Ak landt Windows Viden	lo lo lo lo
Microsoft Edge Microsoft Edge - Default Settings Microsoft Edge Update Microsoft Edge WebView2	Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi Software\Policies\Mi	Options:		At least windows vista Help:	lo lo
MS Security Guide MSS (Legacy) > Network Printers	Software\Policies\Mi SYSTEM\CurrentCon SYSTEM\CurrentCon	Enabled 1	A V	This Policy configures the Value [Enabled] located under the [SYSTEM/CurrentControlSet/ControlSetwithyProviders \SCHANNELIProtocols\TLS 1.0/Client\Key. Streamyault default value is defined as (0) and Type (DWORD).	lo lo
 Sterver Start Menu and Taskbar Streamvault Streamvault CIS Benchmark Level 1 	SYSTEM\CurrentCon SYSTEM\CurrentCon SYSTEM\CurrentCon SYSTEM\CurrentCon			The order of precedence for default values is as follows: 1. Microsoft security baselines; 2. CIS or STIG: 3. Genetec. The last applied setting takes precedence. A site/Domain/OU GPO will ownersite this 'default' value.	lo lo lo
 Genetec Additional Templates Microsoft Security Baseline System Windows Components 	SYSTEM\CurrentCon SYSTEM\CurrentCon SYSTEM\CurrentCon SYSTEM\CurrentCon			overwrite trib uelaur, value.	lo lo lo
All Settings User Configuration Software Settings Windows Settings	SYSTEM\CurrentCon SYSTEM\CurrentCon SYSTEM\CurrentCon SYSTEM\CurrentCon				lo lo w lo
Administrative Templates	SYSTEM\CurrentCon			OK Cancel Apply	

5 Uruchom ponownie system Windows.

Aby włączyć protokół TLS na urządzeniu bez usługi Streamvault:

1 Otwórz Edytor Rejestru Systemu Windows.

- 2 Włącz TLS 1.*n*, gdzie *n* oznacza pomocniczy numer wersji:
 - a) Nawiguj do HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL \Protocols\TLS 1.n.
 - b) Wybierz węzeł Serwera, ustaw DisabledByDefault na 0 i ustaw Enabled na 1
 - c) Wybierz węzeł Klient, ustaw DisabledByDefault na 0 i ustaw Enabled na 1.

📑 Registry Editor				-		×
<u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>H</u> elp						
Computer\HKEY_LOCAL_MACHINE\	SYS	EM\CurrentControlSet\Control\	SecurityProviders\SCHAN	NEL\Protoco	Is\TLS 1.0\S	Server
 ScsiPort SecureBoot SecurePipeServers SecurityProviders SaslProfiles SCHANNEL Ciphers CipherSuites Hashes 	^	Name (Default) DisabledByDefault Enabled S	Type REG_SZ REG_DWORD REG_DWORD	Data (value n 0x00000 0x00000	ot set) 0000 (0) 0001 (1)	
Protocols Protocols In TLS 1.1 In TLS 1.0 In Client Server WDigest	~	<		_		>

3 Uruchom ponownie system Windows.

Pulpit zdalny nie chce się połączyć się z urządzeniem Streamvault

Podczas próby uzyskania dostępu do urządzenia Streamvault[™] za pomocą Pulpitu zdalnego pojawia się komunikat, że Pulpit zdalny nie może połączyć się z komputerem zdalnym.

Remote	e Desktop Connection	×
$\boldsymbol{\times}$	Remote Desktop can't connect to the remote computer for one of these reasons:	
	 Remote access to the server is not enabled The remote computer is turned off The remote computer is not available on the network 	
	Make sure the remote computer is turned on and connected to the network, and that remo access is enabled.	te
	ОК Неір	

Usługa pulpitu zdalnego jest niedostępna w Panelu Sterowania SV

Opis: Aby zapewnić maksymalne bezpieczeństwo, dostęp zdalny jest domyślnie wyłączony na urządzeniu.

Rozwiązanie: Włącz zdalny dostęp do urządzenia. Na stronie *Bezpieczeństwo* w Panelu Sterowania SV włącz usługę Pulpit Zdalny.

		Streamvault	t Control Panel	
Home	Configuration	n Security About		
	Security Center (Adm	in user) Modify password	Hardening profile: Microsoft with CIS Level 2	
	Operation mode:	Online (recommended) T Disconnected T	Some settings below might not align with the selected hardening profile.	
		O Turn off (uninstall)	Remote Desktop service: 🛛 🔐 🙆 🗛	
	Eachie augustics		Remote management: 💿 OFF 😗	
		management	File sharing service: 🛛 🔐 🙆 🛕	
			Never lock screen:	
			Removable storage access: OFF 😚	

Pulpit zdalny nie jest dozwolony w systemie Windows

Opis: Mimo że **usługa Pulpit Zdalny** jest włączona w Panelu Sterowania SV, to ustawienie jest obecnie niedozwolone w systemie Windows.

Rozwiązanie: Nadpisz ustawienia systemu Windows, wyłączając i włączając ponownie opcję **usługi Pulpit Zdalny**.

Usługi Pulpitu Zdalnego nie uruchomiły się

Opis: Usługi pulpitu zdalnego zostały zatrzymane przez system Windows.

Rozwiązanie: Otwórz konsolę Usług systemu Windows, upewnij się, że **Usługi Pulpitu Zdalnego** są zalogowane w trybie użytkownika **Usługi Sieciowej** i upewnij się, że inne usługi Pulpitu Zdalnego są uruchomione.

🤹 Services						- 🗆	\times
File Action View	Help						
🗢 🄿 📅 🖬 🖬							
Services (Local)	Services (Local)						
	Select an item to view its description.	Name	Description	Status	Startup Type	Log On As	^
		🎑 Realtek Audio Universal Service	Realtek Audi	Running	Automatic	Local System	
		🌼 Recommended Troubleshooting Serv	Enables aut		Manual	Local System	
		虊 Remote Access Auto Connection Man	Creates a co		Manual	Local System	
		🧛 Remote Access Connection Manager	Manages di	Running	Automatic	Local System	_
		🧟 Remote Desktop Configuration	Remote Des	Running	Manual	Local System	
		🎑 Remote Desktop Services	Allows users	Running	Manual	Network Service	
		🎑 Remote Desktop Services UserMode	Allows the re	Running	Manual	Local System	
	-	🥋 Remote Procedure Call (RPC)	The RPCSS s	Running	Automatic	Network Service	_
		🎑 Remote Procedure Call (RPC) Locator	In Windows		Manual	Network Service	
		🌼 Remote Registry	Enables rem		Automatic (Tri	Local Service	

Usługi Pulpitu Zdalnego zostały zablokowane

Opis: System Windows jest skonfigurowany tak, aby blokować użytkownikom zdalnym dostęp do Usług Pulpitu Zdalnego.

Rozwiązanie: Zezwól użytkownikowi zdalnemu na dostęp do urządzenia za pomocą usług Pulpitu Zdalnego:

- 1. Otwórz Wiersz Poleceń jako administrator i uruchom gpedit.msc.
- 2. Przejdź do Konfiguracji Komputera > Szablony Administracyjne > Komponenty systemu Windows > Usługi Pulpitu Zdalnego > Host sesji Pulpitu Zdalnego > Połączenia
- 3. Włącz opcję Zezwalaj użytkownikom na zdalne łączenie się przy użyciu usług Pulpitu Zdalnego.

Local Group Policy Editor				-	×
File Action View Help					
🗢 🄿 🙍 🔂 🔂 🖬 🦷	7				
NetMeeting ^	Connections				
OneDrive	Allow users to connect remotely by using Remote Desktop Services	Setting	State Not configured	Comment No	
OOBE	Edit policy setting	Allow users to connect remotely by using Remote Desktop Se Deny logoff of an administrator logged in to the console ses	Enabled Not configured	No	
Presentation Set Push To Install C Remote Desktor	Requirements: At least Windows Server 2003 operating systems or Windows XP Professional	E Configure keep-alive connection interval E Limit number of connections E Suspend user sign-in to complete app registration	Not configured Not configured Not configured	No No No	
RD Licensing Remote Desi Remote Desi Remote Desi Connecti	Description: This policy setting allows you to configure remote access to	Set rules for remote control of Remote Desktop Services user _ Select network detection on the server Select RDP transport protocols Restrict Remote Desktop Services users to a single Remote De	Not configured Not configured Not configured Not configured	No No No	
Device ar	Desktop Services.	· · · · · · · · · · · · · · · · · · ·			

4. W wierszu poleceń uruchomgpupdate /force.

5. W Panelu Sterowania Systemu Windows przejdź do opcji **System i zabezpieczenia > Zezwalaj na dostęp** zdalny .

Okno Właściwości systemu zostanie otwarte na karcie Zdalne .

6. W sekcji *Pulpit zdalny* upewnij się, że jest zaznaczona opcja **Zezwalaj na połączenia tylko z komputerów, na których działa Pulpit zdalny z uwierzytelnianiem na poziomie sieci (zalecane)**.

Computer Name	Hardware	Advanced	System Protection	Remote	
Remote Assist	tance				
Allow Rem	ote Assistan	ice connectio	ons to this compute	r	
What happens	s when I ena	ble Remote	Assistance?		
				Advance	d
Remote Deskt	ор				
Remote Deskt Choose an op	tion, and the remote con	n specify wh nections to th	o can connect. nis computer		
Remote Deskt Choose an op Don't allow	tion, and the remote con	n specify wh nections to the to the total the total to the total total total to the total	o can connect. nis computer mputer		
Remote Deskt Choose an op Don't allow Allow remo	op tion, and the remote con te connections o twork Level /	n specify wh nections to th ons to this country from con Authenticatio	o can connect. his computer mputer nputers running Ren n (recommended)	note Desktop	•
Remote Deskt Choose an op Don't allow Allow remo With Net Help me choo	op tion, and the remote con te connections of twork Level /	n specify wh nections to th ons to this cou only from con Authenticatio	o can connect. his computer mputer nputers running Ren n (recommended)	note Desktop Select Use	ers

Zasady dla grupy lokalnej odmawiają dostępu zdalnego

Opis: Zasady dla grupy lokalnej systemu Windows są skonfigurowane tak, aby odmawiać zdalnego dostępu do urządzenia.

Rozwiązanie: Skonfiguruj zasady dla grupy na swoim urządzeniu, aby umożliwić zdalny dostęp:

- 1. Otwórz Wiersz Poleceń jako administrator i uruchom gpedit.msc.
- 2. Przejdź do Konfiguracja komputera > Ustawienia systemu Windows > Ustawienia Zabezpieczeń > Zasady lokalne > Przypisanie Praw Użytkownika .
- 3. Sprawdź następujące ustawienia zasad dla grupy:
 - Upewnij się że logowanie za pośrednictwem usług Pulpitu Zdalnego jest ustawione na Administratorzy.
 - · Odmowa dostępu do tego komputera z sieci jest ustawiona na Goście.
 - Opcja Odmowa logowania za pośrednictwem usług Pulpitu Zdalnego jest ustawiona na Goście.

Uwierzytelnianie NTLMv2 nie jest obsługiwane

Opis: Urządzenie lub komputer zdalny nie obsługują uwierzytelniania NTLMv2.

Uwaga: Jeśli wszystkie komputery klienckie obsługują protokół NTLMv2, firma Microsoft i kilka niezależnych organizacji zdecydowanie zalecają zasadę *Wysyłaj tylko odpowiedzi NTLMv2*. Przed zmianą ustawień zapoznaj się z Bezpieczeństwo sieci Microsoft: najlepsze praktyki dotyczące poziomu uwierzytelniania LAN Manager i zagadnienia dotyczące bezpieczeństwa.

Rozwiązanie: Aby mieć pewność, że Twoje środowisko umożliwia uwierzytelnianie NTLMv2:

- 1. Otwórz Wiersz Poleceń jako administrator i uruchom gpedit.msc.
- 2. Przejdź do Konfiguracja komputera > Ustawienia systemu Windows > Ustawienia zabezpieczeń > Zasady lokalne > Opcje zabezpieczeń > Bezpieczeństwo sieci: Poziom uwierzytelniania LAN Manager
- 3. Ustaw zasadę na Wyślij LM i NTLM użyj zabezpieczeń sesji NTLMv2, jeśli zostało to wynegocjowane.

Skontaktuj się z nami

Rozwiązanie: Jeśli w dalszym ciągu nie można nawiązać połączenia z usługą Podłączanie Pulpitu Zdalnego, skontaktuj się z Pomocą Techniczną (GTAC).

Tematy pokrewne

Zezwalanie na połączenia Pulpitu Zdalnego z urządzeniem Streamvault, 79
Usuwanie ograniczeń z kont użytkowników niebędących administratorami

Domyślnie, konta użytkowników bez uprawnień administratora, w tym Operator, mają ograniczony dostęp do funkcji Panelu Sterowania Streamvault[™]. Możesz usunąć ograniczenia z tych kont, aby dać im większy dostęp do różnych funkcji.

Zanim rozpoczniesz

- Tylko osoba zalogowana jako Administrator może usunąć ograniczenia z kont użytkowników niebędących administratorami.
- Ograniczenia można usunąć tylko w systemach z dostępną usługą Streamvault.

Procedura

- 1 Otwórz Eksplorator plików i przejdź do C:\Windows\System32\GroupPolicyUsers.
- 2 Usuń folder *S-1-5-32-545* z całą jego zawartością. Ten folder zawiera ograniczenia dla użytkowników niebędących administratorami.
- 3 Uruchom ponownie system Windows.

Konta lokalne nie mają dostępu do Pulpitu Zdalnego, usługi udostępniania plików ani zdalnego zarządzania

Po włączeniu usługi **Pulpit Zdalny**, **Zarządzanie Zdalne** lub **Udostępniania Plików** w Panelu Sterowania SV, konta lokalne nadal nie będą miały dostępu do tych funkcji.

Ta zasada dotyczy produktów Windows Server z Panelem sterowania SV w wersji 3.0 i nowszych:

- Streamvault[™] seria SV-1000E
- Streamvault[™] seria SV-2000E
- Streamvault[™] seria SV-4000EX
- Streamvault[™] seria SV-7000EX

Domyślnie, usługi Pulpit Zdalny, Zarządzanie Zdalne i Udostępnianie Plików są niedostępne dla administratora lokalnego i kont lokalnych, takich jak Operator. W poprzednich wersjach Panelu Sterowania SV dostęp do tych funkcji mieli lokalny administrator i konta lokalne po ich uruchomieniu. Począwszy od wersji SV Panelu Sterowania 3.0 dostęp do funkcji jest przyznawany tylko administratorowi lokalnemu.

To nowa zasada jest kontrolowana za pomocą zabezpieczeń sieciowych **Odmów dostępu do tego komputera** i jest zgodne z podstawowymi zasadami bezpieczeństwa firmy Microsoft dla systemu Windows Server.

Włączenie usług związanych ze Smart Card

Jeśli dokonałeś uaktualnienia ze starszej wersji do SV Control Panel 3.0 i chcesz włączyć usługi związane ze Smart Card, możesz to zrobić za pomocą aplikacji Usługi systemu Windows.

Co powinieneś wiedzieć

Opcja **Uruchom obsługę Karty Smart** nie jest dostępna w Panelu Sterowania SV 3.0, ponieważ usługi kart inteligentnych są domyślnie włączone.

Procedura

- 1 W systemie Windows uruchom services.msc , aby otworzyć aplikację Usługi.
- 2 Włącz usługę Karty Smart .
 - a) Kliknij prawym przyciskiem myszy usługę Karty Smart i wybierz Właściwości.
 Otworzy się okno dialogowe Właściwości .
 - b) Na karcie **Ogólne** znajdź pole **Rodzaj uruchomienia** i wybierz opcję **Automatyczne**.
 - c) Kliknij **Zastosuj** > **OK**.
- 3 Włącz Usługę Identyfikacji Urządzeń Kart Smart.
 - a) Kliknij prawym przyciskiem myszy **Usługę Identyfikacji Urządzeń Kart Smart** i wybierz **Właściwości**. Otworzy się okno dialogowe *Właściwości*.
 - b) Na karcie Ogólne znajdź pole Rodzaj uruchomienia i wybierz opcję Manualne.
 - c) Kliknij Zastosuj > OK.

4 Włącz Usługę Identyfikacji dla Urządzeń Kart Smart.

- a) Kliknij prawym przyciskiem myszy na usługę **Zasady Usuwania Kart Smart** i wybierz **Właściwości**. Otworzy się okno dialogowe *Właściwości*.
- b) Na karcie **Ogólne** znajdź pole **Rodzaj uruchomienia** i wybierz opcję **Manualne**.
- c) Kliknij **Zastosuj** > **OK**.



Włączanie obsługi oprogramowania układowego kontrolerów Mercury EP i LP w wersji 1.x.x

Aby móc zintegrować kontrolery Mercury EP lub LP z oprogramowaniem układowym w wersji 1.x.x na urządzeniu Streamvault™, należy włączyć starszy zestaw szyfrów SSL.

Co powinieneś wiedzieć

W zależności od integracji konieczne jest dodanie jednego z następujących zestawów szyfrów, aby umożliwić jednostkom komunikację z urządzeniem:

- Integracja sterownika Mercury LP z oprogramowaniem układowym w wersji 1.31 i starszych:
 - TLS_RSA_WITH_AES_256_GCM_SHA384
 - TLS_RSA_WITH_AES_128_GCM_SHA256
- Integracja sterownika Mercury EP z oprogramowaniem układowym w wersji 1.29.7 i starszych:
 - TLS_RSA_WITH_AES_256_CBC_SHA

Procedura

- 1 W systemie Windows uruchom gpedit.msc, aby otworzyć *Edytor lokalnych zasad grupy*.
- 2 Przejdź do Konfiguracja komputera > Szablony administracyjne > Sieci > Ustawienia konfiguracji SSL
- 3 Kliknij dwukrotnie opcję Zamów pakiet szyfrów SSL.
- 4 W okienku *Opcje* w polu **Zestawy szyfrów SSL** dodaj przecinek na końcu listy, a następnie zestaw szyfrów mający zastosowanie dla Twojej integracji. Nie dodawaj żadnych spacji.

5 Kliknij **OK**, aby zapisać obiekt zasad grupy (GPO).

Local Group Policy Editor			—				
File Action View Help							
🗢 🔿 🙍 📰 🔒 🚺 🗊 🍞							
	. SSL Cipher Suite Order						\times
x I Computer Configuration							
> Software Settings	SSL Cipher Suite Order		Previous S	etting Ne	ext Setting		
> 🛄 Windows Settings							
✓ ☐ Administrative Templates	O Not Configured Comment:						
> 🧮 Control Panel	A						
Desktop	Enabled						
> 🧮 Microsoft Edge	O Disabled						W
> Microsoft Edge - Default Settings (us	Supported on:	At least Window	vs Vista				
> Microsoft Edge Update							_
> Microsoft Edge WebView2	-						*
MS Security Guide	Options:		Help:				
NISS (Legacy)							
Background Intelligent Transfer S	SSL Cipher Suites		This policy setting deter	mines the ciph	er suites used l	by the	
BranchCache		. I	Secure Socket Layer (SSL).			
DirectAccess Client Experience Se	384,1LS_RSA_WITH_AES_256_GCM_SHA384	<u> 1</u>	If you anable this policy	cotting CCL sin	her suites are	oviovitized	lin
DNS Client			the order specified.	setting, SSL ap	oner suites are	prioritized	
📔 Fonts							
Hotspot Authentication			If you disable or do not	configure this	policy setting,	default	
🚞 Lanman Server			cipher suite order is use	d.			
📔 Lanman Workstation			Link for all the cipherSui	itor: http://go.g	aicrosoft.com/h	ulink /2	
Link-Layer Topology Discovery			Linkld=517265	tes. http://go.n	licrosoft.com/in	WIITIK/:	
Network Connections							
Network Connectivity Status Indi	(
Network Isolation							
Network Provider							
On Des Packet Scheduler							
SNMP							
SSL Configuration Settings							
	L						
				OK	Cancel	An	alv
2 setting(s)					Cancer		, y

6 Uruchom ponownie usługę Softwire lub uruchom ponownie urządzenie.

Włączanie wsparcia integracji Synergis IX

Zanim zarejestrujesz kontrolery Synergis[™] IX na urządzeniu Streamvault[™], musisz dodać dodatkowy zestaw szyfrów SSL.

Co powinieneś wiedzieć

Aby zarejestrować kontrolery Synergis IX na urządzeniu Streamvault, należy dodać jeden z następujących zestawów szyfrów:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Procedura

- 1 W systemie Windows uruchom gpedit.msc, aby otworzyć Edytor lokalnych zasad grupy.
- 2 Przejdź do **Konfiguracja komputera > Szablony administracyjne > Sieci > Ustawienia konfiguracji SSL**.
- 3 Kliknij dwukrotnie opcję Zamów pakiet szyfrów SSL.
- 4 W okienku Opcje w polu Zestawy szyfrów SSL dodaj przecinek na końcu listy, a następnie wstaw TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 lubTLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256. Nie dodawaj żadnych spacji.
- 5 Kliknij **OK**, aby zapisać obiekt zasad grupy (GPO).

Local Group Policy Editor			- 🗆 ×	
File Action View Help				
🗢 🔿 🙍 🔂 🖬 🦷				
🗐 Local Computer Policy	SSL Cipher Suite Order		— U X	
V 🛃 Computer Configuration	SSL Cipher Suite Order			
> Software Settings			Previous Setting Next Setting	
> Windows Settings	O Not Configured Comment:			
Control Panel	() Not configured			۴.
📔 Desktop	 Enabled 			
> 🧮 Microsoft Edge	 Disabled 		· · · · · · · · · · · · · · · · · · ·	1
> Microsoft Edge - Default Settings (u	Supported on:	At least Windov	vs Vista	
Microsoft Edge Update				,
MICrosoft Edge WebView2	-			
MSS (Legacy)	Options:		Help:	
✓ III Network		_		
Background Intelligent Transfer	SSL Cipher Suites		This policy setting determines the cipher suites used by the	۰.
BranchCache	_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ĩ –	Secure Socket Layer (SSL).	
DirectAccess Client Experience Se	t <u></u>	-	If you enable this policy setting, SSL cipher suites are prioritized in	
DNS Client		_	the order specified.	
Hotspot Authentication			If you disable or do not configure this policy setting default	
Lanman Server			cipher suite order is used.	
📔 Lanman Workstation				
Link-Layer Topology Discovery			Link for all the cipherSuites: http://go.microsoft.com/twlink/?	
> in Network Connections				
Network Connectivity Status Ind				
Network Isolation				
Offline Files				
> 🧮 QoS Packet Scheduler				
SNMP				
SSL Configuration Settings				v
2 setting(s)			OK Cancel Apply	

6 Uruchom ponownie usługę Softwire lub uruchom ponownie urządzenie.

7

Pomoc techniczna

Ta sekcja zawiera następujące tematy:

- "Kontakt z Centrum pomocy technicznej Genetec", 110
- "Wsparcie dotyczące oprogramowania", 113
- "Wsparcie sprzętowe", 114
- "Specyfikacje Streamvault", 115
- "Ogólne warunki wsparcia dotyczące Streamvault", 116

Kontakt z Centrum pomocy technicznej Genetec

Centrum Pomocy Technicznej Genetec[™] (GTAC) jest do Twojej dyspozycji w przypadku jakichkolwiek problemów z oprogramowaniem lub sprzętem związanym ze Streamvault[™].

Uwaga: W przypadku zapytań dotyczących problemów z oprogramowaniem Genetec[™] Security Center pomoc techniczna jest oferowana za pośrednictwem naszej regularnej linii pomocy technicznej. Aby znaleźć numer telefonu GTAC i godziny pracy w swoim regionie, przejdź do strony Centrum Pomocy Technicznej Genetec Kontakt

Przydatne informacje

Otwierając zgłoszenie do pomocy technicznej, przygotuj następujące informacje:

- Identyfikator Systemu Licencji Security Center. Aby uzyskać więcej informacji, zobacz Jak znaleźć identyfikator systemu?.
- Twój numer seryjny Genetec lub kod serwisowy sprzętu.
- Twój kod Genetec, który znajduje się na obudowie (nie dotyczy urządzeń typu "wszystko w jednym"). Kod jest wymagany jeśli utracisz dostęp administracyjny do systemu i potrzebujesz obrazu fabrycznego.



• Twój plik dziennika diagnostycznego TSR (jeśli dotyczy).

Kontakt telefoniczny z GTAC

Pomoc telefoniczna dotycząca problemów ze Streamvault[™] jest dostępna dla wszystkich klientów w godzinach pracy w ich regionie.

Dla klientów w Ameryce Północnej, Europie, na Bliskim Wschodzie i w Afryce:

- 1. Odwiedź stronę Centrum Pomocy Technicznej Genetec[™](GTAC) *Kontakt*, aby znaleźć numer telefonu GTAC i godziny pracy w swoim regionie.
- 2. Zadzwoń pod numer telefonu GTAC i wybierz opcję nr 2.

Dla klientów w regionie Azji i Pacyfiku:™

Wsparcie dla regionu APAC jest zapewniane za pośrednictwem Portalu Pomocy Technicznej Genetec (GTAP) za pośrednictwem czatu na żywo i zgłoszeń pomocy technicznej. Godziny pracy: od poniedziałku do piątku w godzinach 8:00 - 20:00 (czasu lokalnego).

Aby uzyskać pomoc w nagłych wypadkach 24 godziny na dobę, 7 dni w tygodniu poza godzinami pracy:

- 1. Zadzwoń pod numer GTAC dla swojego regionu.
- 2. Wprowadź numer identyfikacyjny certyfikatu Genetec.
- 3. Wprowadź numer umowy Genetec Advantage lub numer subskrypcji Genetec.
- 4. Wybierz produkt.

5. Zostaw wiadomość zawierającą Twoje imię i nazwisko, numer telefonu oraz opis problemu. Inżynier dyżurny skontaktuje się z Tobą w ciągu 30 minut

Ważne: Całodobowa pomoc w nagłych wypadkach jest dostępna tylko dla klientów, którzy dodali opcję Genetec Advantage do swojej umowy . Aby uzyskać więcej informacji, skontaktuj się z nami na advantage@genetec.com.

Klienci nieobjęci pakietem Advantage muszą utworzyć zgłoszenie za pośrednictwem Portalu Pomocy Technicznej Genetec (GTAP).

Kontaktowanie się z GTAC poprzez GTAP

Wsparcie dotyczące problemów ze Streamvault[™] jest dostępne dla wszystkich klientów w godzinach pracy w ich regionie za pośrednictwem zgłoszeń online w Portalu pomocy technicznej Genetec[™] (GTAP).

W przypadku klientów nie objętych pakietem Genetec[™] Advantage należy otworzyć sprawę za pośrednictwem Portalu Pomocy Technicznej Genetec (GTAP). Aby uzyskać więcej informacji na temat Genetec Advantage, skontaktuj się z nami advantage@genetec.com.

Aby zgłosić sprawę poprzez portal internetowy:

- 1. Przejdź do Portalu Pomocy Technicznej Genetec
- 2. Zaloguj się przy użyciu firmowego adresu e-mail.
- 3. Kliknij + Utwórz Sprawę



- 4. Z listy Identyfikator systemu wybierz system, którego dotyczy problem.
- 5. W przypadku zwrotu lub naprawy sprzętu dołącz w tytule **Prośba o RMA**, aby nasz zespół mógł łatwo zidentyfikować te zgłoszenia.

Description of the issue

Please Note:

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

Title:

RMA Request [your title here]

Description:

[Your description here]

- 6. Podaj numer seryjny produktu, kod Genetec i plik dziennika diagnostycznego TSR (jeśli dotyczy).
- 7. Kliknij Prześlij sprawę.

Otrzymasz e-mail z potwierdzeniem zgłoszenia z szacowanym czasem odpowiedzi.

Kontaktowanie się z GTAC za pośrednictwem czatu na żywo

Pomoc dotycząca problemów ze Streamvault[™] jest dostępna dla klientów korzystających z usługi Genetec[™] Advantage za pośrednictwem czatu na żywo w Portalu Pomocy Technicznej Genetec (GTAP). Klienci mogą uzyskać pomoc w godzinach pracy w swoim regionie.

W przypadku klientów nie objętych pakietem Genetec Advantage należy otworzyć sprawę za pośrednictwem Portalu Pomocy Technicznej Genetec (GTAP). Aby uzyskać więcej informacji na temat Genetec Advantage, skontaktuj się z nami advantage@genetec.com.

Aby rozpocząć czat na żywo:

- 1. Przejdź do Portalu Pomocy Technicznej Genetec
- 2. Zaloguj się przy użyciu firmowego adresu e-mail.
- 3. Kliknij przycisk rozpocznij chat

🐑 click to chat

- 4. Wybierz preferowany język.
- 5. Wprowadź pełny identyfikator systemu (GSC-xxxxxx-xxxxx), potem kliknij **Sprawdź Identyfikator Systemu**.
- 6. Wybierz, czy chcesz rozmawiać na temat nowej czy istniejącej sprawy.
- 7. Wybierz produkt.
- 8. Kliknij rozpocznij czat.

GTAC - Live Chat				
Support ho Ionday to Status: Onl	Durs for your territory: Friday: 08:00 to 20:00 Eastern Standard Time line			
Welcor Please O En Please	me select your preferred language glish O French enter the System ID *			
i	Please enter the System ID	CHECK SYSTEM ID		
The qual	transcript of your chat session will be retained for lity assurance purposes	START CHAT		

9. Aby zainicjować zgłoszenie RMA, podaj numer seryjny produktu, kod Genetec i plik dziennika diagnostycznego TSR (jeśli dotyczy).

Czas odpowiedzi (dostępny tylko w godzinach pracy w Twoim regionie): Zwykle w ciągu 5 minut.

Wsparcie dotyczące oprogramowania

Oprogramowanie obrazu Streamvault[™] Windows zawiera najnowszą wersję oprogramowania Security Center i panelu sterowania dostępną w momencie tworzenia obrazu. Wsparcie dla obrazu systemu Windows i oprogramowania Security Center jest obsługiwane oddzielnie.

Oprogramowanie Streamvault

- Obraz Streamvault Windows jest objęty gwarancją Streamvault przez cały cykl życia urządzenia.
 Ważne: Aktualizacja systemu operacyjnego Windows nie jest objęta gwarancją. Aktualizacja systemu operacyjnego Windows spowoduje usunięcie niezbędnych sterowników, zabezpieczeń i oprogramowania zainstalowanego wraz z obrazem.
- Obraz zapasowy dostarczony w celu ponownego zobrazowania urządzenia Streamvault obejmuje pierwotny system operacyjny i obraz dostarczony wraz z urządzeniem przy zakupie.
- Obraz Streamvault Windows jest objęty gwarancją Streamvault niezależnie od statusu Genetec[™] Advantage.

Oprogramowanie Security Center

Problemy z oprogramowaniem Security Center są objęte umową dotyczącą poziomu usług (SLA) i procedurami pomocy technicznej opisanymi w następującym dokumencie Genetec[™] Lifecycle Management (GLM): Opis programu Genetec Advantage.

Wsparcie sprzętowe

Gwarancje dotyczące HP i Dell ProSupport są dostępne za pośrednictwem Genetec[™]. W przypadku jakichkolwiek problemów ze sprzętem, Centrum Pomocy Technicznej Genetec[™](GTAC) jest punktem kontaktowym, w którym można zdiagnozować problem i skoordynować działania z HP i Dell ProSupport.

Szczegółowe informacje na temat Gwarancji na Sprzęt Streamvault oferowanych przez Genetec można znaleźć w Przeglądzie Warunków Gwarancji Sprzętowej Genetec.

Specyfikacje Streamvault

Podczas planowania i wdrażania urządzenia Streamvault[™] należy zapoznać się z poniższymi specyfikacjami technicznymi, mechanicznymi i środowiskowymi.

Specyfikacje techniczne, mechaniczne i środowiskowe

Urządzenia typu "all-in-one":

• SV-300E arkusz danych

Urządzenia do montażu na stojaku:

- seria SV-1000E arkusz danych
- seria SV-2000E arkusz danych
- seria SV-4000E arkusz danych

Scentralizowana pamięć masowa o wysokiej dostępności:

• seria SV-7000EX arkusz danych

Stacje robocze

- seria SVW-100E arkusz danych
- seria SVW-300E arkusz danych
- seria SVW-500E arkusz danych

Urządzenia do Monitorowania Pojazdów all-in-one

- seria SVR-300A arkusz danych
- seria SVR-300AR arkusz danych
- seria SVR-500A arkusz danych

Ogólne warunki wsparcia dotyczące Streamvault

Standardowa i Rozszerzona gwarancja na sprzęt Genetec[™] podlega warunkom opisanym w Przeglądzie Gwarancji Sprzętu Genetec.

Glosariusz

manufacturing image

Obraz produkcyjny to obraz Streamvault[™], który jest wysyłany do klientów, gdy kupują urządzenie. Wersje oprogramowania zainstalowane na tym obrazie różnią się w zależności od zamówienia klienta.

Narzędzia SV

Streamvault[™] to urządzenie "pod klucz" z wbudowanym systemem operacyjnym i wcześniej zainstalowanym programem Security Center. Za pomocą urządzeń Streamvault[™] można szybko wdrożyć ujednolicony lub samodzielny system nadzoru wideo i kontroli dostępu.

Narzędzie do przywracania ustawień fabrycznych Streamvault

Narzędzie do przywracania ustawień fabrycznych Streamvault to narzędzie umożliwiające ponowne przywrócenie ustawień fabrycznych urządzenia Streamvault. Pozwala ono także utworzyć klucz USB do uruchomienia systemu za pomocą wymaganego obrazu oprogramowania Streamvault.

obraz odzyskiwania

Obraz odzyskiwania jest używany do ponownego instalowania obrazów na urządzeniach Streamvault[™]." Jest to stały obraz z preinstalowanymi określonymi wersjami oprogramowania.

Panel Sterowania SV

Panel Sterowania SV to aplikacja interfejsu użytkownika, której można użyć do skonfigurowania urządzenia Streamvault[™] do współpracy z kontrolą dostępu i nadzorem wideo w Security Center.

Streamvault[™] hardware

Streamvault[™] hardware to zadanie raportowania w Security Center, którego można użyć do wyświetlenia listy problemów technicznych wpływających na urządzenia Streamvault[™]..

Streamvault[™] hardware monitor

Jednostka monitorująca sprzęt hardware monitor Streamvault[™] służy do monitorowania stanu urządzeń Streamvault[™] i zapewnia otrzymywanie powiadomień w przypadku wystąpienia problemów. Wymagany jest jeden hardware monitor Streamvault[™] na każde urządzenie Streamvault[™].

Streamvault[™] manager

Jednostka Streamvault[™] manager służy do kontrolowania konfiguracji alertów dla grupy podmiotów w Streamvault[™] Agent. W każdym systemie dozwolony jest tylko jeden Streamvault[™] manager.

SV-1000E

SV-1000E to ekonomiczne urządzenie zabezpieczające do montażu na stojaku, przeznaczone do systemów zabezpieczeń średniej wielkości. Pomaga przejść na ujednolicony system bezpieczeństwa łączący nadzór wideo, kontrolę dostępu, automatyczne rozpoznawanie tablic rejestracyjnych, komunikację, nieautoryzowane wtargnięcia i analizy w jednym urządzeniu. Model SV-1000E jest wyposażony w Security Center i wcześniej zainstalowany Panel Sterowania SV.

SV-100E

SV-100E to subkompaktowe urządzenie typu "all-in-one", które jest dostarczane z preinstalowanym systemem Microsoft Windows, Centrum zabezpieczeń i Panelem sterowania SV. SV-100E przeznaczony jest do instalacji na małą skalę, na jednym serwerze i może obsługiwać zarówno kamery, jak i czytniki kontroli dostępu.

SV-2000E

SV-2000E to urządzenie zabezpieczające do montażu w szafie przemyslowej które umożliwia łatwe wdrożenie zunifikowanego systemu łączącego nadzór wideo, kontrolę dostępu, automatyczne rozpoznawanie tablic rejestracyjnych i komunikację. Model SV-2000E jest wyposażony w Security Center i wcześniej zainstalowany Panel Sterowania SV.

SV-300E

SV-300E to kompaktowe, kompleksowe urządzenie "pod klucz", które jest dostarczane z zainstalowanym wcześniej systemem Microsoft Windows, Security Center i Panelem Sterowania SV. Dzięki wbudowanym

techdocs.genetec.com | Podręcznik Użytkownika Narzędzia Streamvault[™] PL.803.003 | Ostatnio zaktualizowany: 30 Kwiecień, 2025

kartom przechwytującym z enkoderem analogowym możesz wykorzystać urządzenie do szybkiego wdrożenia samodzielnego systemu nadzoru wideo lub kontroli dostępu lub systemu ujednoliconego.

SV-350E

SV-350E to kompleksowe, gotowe do użycia urządzenie zabezpieczające, które ułątwia przejście do ujednoliconego systemu łączącego nadzór wideo, kontrolę dostępu, wykrywanie włamań i komunikację. Jest dostarczany z preinstalowanym systemem Microsoft Windows, Security Center i Panelem Sterowania SV. Natomiast RAID 5 umożliwia przechowywania plików wideo w sytuacjach mających krytyczne znaczenie.

SV-4000E

SV-4000E to urządzenie montowane na stelażu, które zapewnia wydajność i niezawodność dla przedsiębiorstwa. Certyfikowane konfiguracje sprzętowe i gotowe zabezpieczenia przed zagrożeniami cybernetycznymi upraszczają projektowanie i wdrażanie nowego systemu bezpieczeństwa. Model SV-4000E jest wyposażony w Security Center i zainstalowany wcześniej Panel sterowania SV.

SV-7000E

SV-7000E to urządzenie do montażu na stelażu, jego zastosowanie obejmuje dużą liczbę kamer, użytkowników i wydarzeń o wysokiej rozdzielczości. Model SV-7000E jest wyposażony w Security Center i wcześniej zainstalowany Panel Sterowania SV.

SVA-100E

SVA-100E to kompaktowe urządzenie, za pomocą którego można łatwo ulepszyć system bezpieczeństwa za pomocą analizy wideo KiwiVision[™]. Projekt jest zoptymalizowany pod kątem zastosowania większej liczby strumieni analitycznych w systemie nadzoru wideo, niezależnie od tego, czy jest to analityczny strumień pojedynczy czy wielo-strumieniowy na kamerę.

SVW-300E

Stacja robocza SVW-300E to gotowe rozwiązanie przeznaczone do monitorowania małych i średnich systemów bezpieczeństwa, które może obsłużyć większą ilość monitorów ekranowych. Urządzenie SVW-300E jest dostarczane z preinstalowanym programem Security Center.

SVW-500E

Stacja robocza SVW-500E to wysoko wydajne rozwiązanie przeznaczone dla użytkowników potrzebujących możliwości wyświetlania obrazu z kamer w bardzo wysokiej rozdzielczości na monitorach i ścianach wideo 4K. Urządzenie SVW-500E jest dostarczane z preinstalowanym programem Security Center.

Usługa Streamvault

Usługa Streamvault to usługa systemu Windows umożliwiająca użytkownikom konfigurowanie urządzenia Streamvault[™], np. poprzez stosowanie profili wzmacniających bezpieczeństwo.

Gdzie znaleźć informacje o produkcie

Możesz znaleźć naszą dokumentację dotyczącą produktu w następujących miejscach:

• Genetec TechDoc Hub: Najnowsza dokumentacja jest dostępna w TechDoc Hub.

Nie możesz znaleźć tego, czego szukasz? Skontaktuj się z documentation@genetec.com.

- **Pakiet instalacyjny:** Wytyczne dotyczące Instalacji oraz Informacje o Wersji są dostępne w folderze Dokumentacja w zakładce pakiet instalacyjny. Dokumenty te mają również bezpośredni link umożliwiający pobranie najnowszej wersji dokumentu.
- **Pomoc:** Aplikacje klienckie i internetowe Security Center oferują pomoc w zrozumieniu działania produktu, oraz zawierają instrukcje dotyczące możliwości korzystania z jego funkcji. Aby uzyskać dostęp do pomocy, stuknij **Pomoc**, stuknij F1 lub **?** (znak zapytania) w różnych aplikacjach klienckich.