

Ghidul utilizatorului pentru dispozitivul Streamvault™

Faceți clic [aici](#) pentru cea mai recentă versiune a documentului.

Ultima actualizare a documentului: 5 iunie 2025

Mențiuni legale

©2025 Genetec Inc. Toate drepturile rezervate.

Genetec Inc. distribuie acest document cu software care include un acord de licență pentru utilizatorul final și este furnizat sub licență și poate fi utilizat doar în conformitate cu termenii acordului de licență. Conținutul acestui document este protejat prin legea privind drepturile de autor.

Conținutul acestui ghid este furnizat doar cu titlu informativ și poate fi modificat fără notificare prealabilă. Genetec Inc. nu își asumă nicio responsabilitate sau răspundere pentru orice erori sau inexactități care pot apărea în conținutul informațional conținut în acest ghid.

Această publicație nu poate fi copiată, modificată sau reprodusă sub nicio formă sau în niciun scop și nici nu poate fi creată nicio lucrare derivată din aceasta fără acordul scris prealabil al Genetec Inc.

Genetec Inc. își rezervă dreptul de a revizui și îmbunătăți produsele după cum consideră de cuviință. Acest document descrie starea unui produs la momentul ultimei revizuirii a documentului și este posibil să nu reflecte produsul în toate momentele din viitor.

În nici un caz Genetec Inc. nu va fi răspunzătoare față de orice persoană sau entitate cu privire la orice pierdere sau daune care sunt incidente sau în consecință instrucțiunilor găsite în acest document sau a produselor software și hardware descrise aici.

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™, siglele lor respective, precum și sigla Mobius Strip sunt mărci comerciale ale Genetec Inc. și pot fi înregistrate sau în curs de înregistrare în mai multe jurisdicții.

Alte mărci comerciale utilizate în acest document pot fi mărci comerciale ale producătorilor sau ale furnizorilor produselor respective.

În curs de brevetare. Genetec™ Security Center, Omnicast™, AutoVu™, Stratocast™, Genetec Citigraf™, Genetec Clearance™ și alte produse Genetec™ fac obiectul cererilor de brevet în curs și pot face obiectul brevetelor eliberate, în Statele Unite și în alte jurisdicții din întreaga lume.

Toate specificațiile sunt supuse modificărilor fără înștiințare prealabilă.

Informații despre document

Titlu document: Ghidul utilizatorului pentru dispozitivul Streamvault™

Număr document inițial: EN.803.003

Număr document: RO.803.003

Data de actualizare a documentului: 5 iunie 2025

Puteți să trimiteți comentariile, corecțiile și sugestiile cu privire la acest ghid către documentation@genetec.com.

Despre acest ghid

Acest ghid explică cum să configurați dispozitivul Streamvault pentru a funcționa cu Security Center pentru controlul accesului și supravegherea video, utilizând versiunea actuală a panoului de control SV. Acest ghid completează Ghidul administratorului Security Center și Ghidul de configurare a dispozitivului Synergis™.

Acest ghid este scris pentru integratorul care efectuează configurarea inițială a dispozitivului SV. Se presupune că sunteți familiarizat cu terminologia și conceptele utilizate în Security Center.

Note și notificări

Următoarele note și notificări pot apărea în acest ghid:

- **Sfat:** Sugerează modul de aplicare a informațiilor într-o temă sau etapă.
- **Notă:** Explică un caz special sau extinde un aspect important.
- **Important:** Evidențiază informațiile critice referitoare la o temă sau o etapă.
- **Atenție:** Indică faptul că o acțiune sau o etapă poate cauza pierderea datelor, probleme de securitate sau probleme de performanță.
- **Avertisment:** Indică faptul că o acțiune sau o etapă ar putea să aibă drept rezultat vătămare corporală sau să provoace deteriorarea echipamentului hardware.

IMPORTANT: Conținutul din acest ghid care face referire la informații găsite pe site-urile web ale terților era exact în momentul publicării, cu toate acestea, aceste informații pot fi modificate fără notificare prealabilă din partea Genetec Inc.

Cuprins

Preface

Mențiuni legale.	ii
Despre acest ghid.	iii

Cap. 1. Introducere pentru dispozitivul Streamvault

Noțiuni de bază despre dispozitivul dvs. Streamvault.	2
Porturi implicite utilizate de Streamvault.	4
Despre actualizarea software-ului SV în SV Control Panel.	7
Conectarea componentelor dispozitivului Streamvault.	8
Carduri de codificare analogică Genetec.	8
Dezactivarea intrărilor camerei pe cardurile de codificare de pe un dispozitiv Streamvault.	9
Intrările și ieșirile de alarmă ale unui dispozitiv Streamvault.	10
Despre conturile de utilizator Streamvault.	12
Informații de conectare pentru conturile de utilizator implicite de pe unStreamvault aparat.	12
Conectarea la un dispozitiv Streamvault.	14
Despre serviciul Streamvault.	15
Despre întărirea Streamvault.	16
Aparate cu capacități de gestionare a întăririi.	16

Cap. 2. Noțiuni de bază despre panoul de control SV

Despre SV Control Panel.	19
Configurați-vă aparatul în SV Control Panel.	19
Activarea licenței Security Center pe un dispozitiv.	22
Activarea manuală a unei licențe de la Server Admin.	23
Activarea monitorului de disponibilitate a sistemului.	25
Activarea funcțiilor video și de control al accesului din Security Center.	26
Despre Instrumentul de înscriere a unității.	29
Deschiderea Instrumentului de înscriere a unității.	29
Configurarea setărilor de înscriere a unității.	29
Se adaugă unități.	30
Golirea unităților adăugate.	30
Ignorarea unităților.	31
Eliminarea unităților din lista de unități ignorate.	31
Configurarea setărilor implicite ale camerei.	32
Crearea de programe de înregistrare personalizate.	34
Despre backup și restaurare.	35
Realizarea unei icopii de rezervă a bazei de date Directory.	36
Restaurarea bazei de date Directory.	37
Alegerea metodei de creare a rolurilor Archiver și partițiilor.	38
Adăugarea rolurilor Archiver în SV Control Panel.	38
Adăugarea manuală a partițiilor și a rolurilor Archiver.	40
Criptarea unității sistemului de operare.	43
Crearea unei chei de recuperare.	44
Colectarea jurnalelor de asistență.	47

Cap. 3. Noțiuni de bază despre plugin-ul de întreținere Streamvault

Despre plugin-ul Întreținerea Streamvault.	50
Descărcarea și instalarea plugin-ului.	51
Privilegii Streamvault Genetec.	52
Crearea rolului de plugin.	54
Configurarea unei entități monitor hardware Streamvault.	55
Configurarea unei entități manager Streamvault.	59
Despre fila Management.	62
Revizuirea sănătății dispozitivului Streamvault.	63
Coloanele panoului de raport pentru comanda hardware Streamvault.	64
Crearea de evenimente către acțiuni pentru evenimentele de sănătate Streamvault.	65

Cap. 4. Referința panoului de control SV

Pagina de pornire a SV Control Panel.	68
Pagina de configurare a SV Control Panel.	70
Pagina Securitate a SV Control Panel.	73
Pagina Despre din SV Control Panel.	76

Cap. 5. Resurse suplimentare

Garanția produsului pentru dispozitivul Streamvault.	79
Configurarea parolei BIOS.	80
Schimbarea parolei implicite iDRAC.	83
Adăugarea unui nou utilizator iDRAC cu privilegii de administrator.	84
Dezactivarea utilizatorului root iDRAC.	85
Reimaginarea unui dispozitiv Streamvault.	86
Găsirea ID-ului sistemului și a versiunii imaginii unui dispozitiv Streamvault.	87
Permiterea distribuției fișierelor pe un dispozitiv Streamvault.	88
Permiterea conexiunilor Remote Desktop la un dispozitiv Streamvault.	89

Cap. 6. Depanare

Efectuarea unei resetări din fabrică pe un Streamvault dispozitiv All-in-one.	91
Crearea unei chei USB de resetare din fabrică pentru un dispozitiv Streamvault All-in-one.	91
Resetarea imaginii software pe un dispozitiv All-in-one.	93
Efectuarea unei resetări din fabrică pe o Streamvaultstație de lucru sau un dispozitiv server.	101
Crearea unei chei USB de resetare din fabrică pentru o stație de lucru Streamvault sau un dispozitiv server.	101
Resetarea imaginii software pe o Streamvaultstație de lucru sau un dispozitiv server.	103
Controlerele Mercury EP rămân offline atunci când TLS 1.1 este dezactivat.	106
Activarea Transport Layer Security (TLS).	107
Remote Desktop nu se poate conecta la un dispozitiv Streamvault.	110
Eliminarea restricțiilor de la conturile de utilizatori non-administratori.	114
Conturile locale nu pot accesa Desktop la distanță, serviciul de partajare a fișierelor și gestionarea de la distanță.	115
Activarea serviciilor legate de Smart Card.	116
Activarea suportului pentru controlerele Mercury EP și LP firmware 1.x.x.	117
Activarea suportului pentru integrarea Synergis IX.	119
Modificarea GPO-urilor locale pentru conturile de utilizator non-administrator.	120
Dezactivarea paravanului de protecție Windows.	123

Cap. 7. Asistență tehnică

Streamvault Contactarea Centrului de asistență tehnică Genetec.	126
Contactarea GTAC prin telefon.	126
Contactarea GTAC prin intermediul GTAP.	127
Contactarea GTAC prin chat live.	127
Asistență software.	129
Suport hardware.	130
Specificații pentru Streamvault.	131
Termeni și condiții de asistență Streamvault.	132
Glosar	133
Unde puteți găsi informații despre produs	135

Introducere pentru dispozitivul Streamvault

Această secțiune include următoarele subiecte:

- ["Noțiuni de bază despre dispozitivul dvs. Streamvault"](#), pagină 2
- ["Porturi implicite utilizate de Streamvault"](#), pagină 4
- [" Despre actualizarea software-ului SV în SV Control Panel "](#), pagină 7
- ["Conectarea componentelor dispozitivului Streamvault"](#), pagină 8
- ["Despre conturile de utilizator Streamvault"](#), pagină 12
- ["Conectarea la un dispozitiv Streamvault "](#), pagină 14
- ["Despre serviciul Streamvault"](#), pagină 15
- [" Despre întărirea Streamvault"](#), pagină 16

Noțiuni de bază despre dispozitivul dvs. Streamvault

Puteți implementa dispozitivul Streamvault™ cu Security Center urmând o succesiune de pași.

Prezentare generală a implementării

Etapă Comandă	Unde puteți găsi mai multe informații
Înțelegeți condițiile prealabile și problemele cheie înainte de implementare	
1 Deschideți porturile de rețea necesare pentru a conecta sistemele de bază din Security Center și modulele din Streamvault. Conectați perifericele, precum monitorul, tastatura, placa de codificare analogică și dispozitivele la intrări și ieșiri. Conectați dispozitivul la rețeaua dumneavoastră.	<ul style="list-style-type: none"> • Porturi implicite utilizate de Streamvault, pagină 4. • Conectarea componentelor dispozitivului Streamvault, pagină 8. • Carduri de codificare analogică Genetec, pagină 8. • Dezactivarea intrărilor camerei pe cardurile de codificare de pe un dispozitiv Streamvault, pagină 9. • Intrările și ieșirile de alarmă ale unui dispozitiv Streamvault, pagină 10.
2 Înainte de a vă instala dispozitivul, aflați despre conținutul versiunii dvs. de imagine.	<ul style="list-style-type: none"> • Conținutul fiecărei versiuni de imagine Streamvault.
3 Conectați-vă la Windows ca administrator folosind parola tipărită pe dispozitiv, apoi schimbați parola.	<ul style="list-style-type: none"> • Conectarea la un dispozitiv Streamvault, pagină 14.
4 Configurați parola BIOS pe dispozitivul dvs.	<ul style="list-style-type: none"> • Configurarea parolei BIOS, pagină 80.
5 Dacă dispozitivul dumneavoastră este compatibil cu iDRAC, schimbați imediat parola implicită iDRAC. Pentru o securitate sporită, este recomandat să creați un cont de utilizator alternativ cu privilegii administrative și să dezactivați contul de utilizator root.	<ul style="list-style-type: none"> • Schimbarea parolei implicite iDRAC, pagină 83. • Adăugarea unui nou utilizator iDRAC cu privilegii de administrator, pagină 84. • Dezactivarea utilizatorului root iDRAC, pagină 85.
Completați expertii de configurare	
6 Finalizați expertul de configurare <i>Panoul de control Streamvault</i> . Notă: Remote Desktop este dezactivat în mod implicit. Pentru a activa desktop-ul la distanță, activați setarea serviciului Desktop la distanță de pe pagina <i>Securitate</i> din SV Control Panel.	<ul style="list-style-type: none"> • Configurați-vă aparatul în SV Control Panel, pagină 19. • Permiterea conexiunilor Remote Desktop la un dispozitiv Streamvault, pagină 89.
7 Activați-vă licența Security Center. <ul style="list-style-type: none"> • Dacă dispozitivul este conectat la internet, activați licența utilizând expertul de activare <i>Panoul de control Streamvault</i>. 	<ul style="list-style-type: none"> • Activarea licenței Security Center pe un dispozitiv, pagină 22. • Activarea manuală a unei licențe de la Server Admin, pagină 23.

Etapă Comandă	Unde puteți găsi mai multe informații
<ul style="list-style-type: none"> Dacă dispozitivul nu este conectat la internet, activați licența manual din Server Admin. 	
8 Activați Monitorul de disponibilitate a sistemului	<ul style="list-style-type: none"> Activarea monitorului de disponibilitate a sistemului, pagină 25.
9 Configurați Genetec™ Update Service astfel încât să puteți obține cea mai recentă versiune a Security Center și SV Control Panel. Dacă există actualizări, instalați-le.	<ul style="list-style-type: none"> Configurarea Genetec Update Service.
10 Dacă SV Control Panel indică faptul că sunt disponibile mai multe actualizări, instalați-le acum.	<ul style="list-style-type: none"> Despre actualizarea software-ului SV în SV Control Panel, pagină 7.
11 Criptați unitatea sistemului de operare de pe dispozitiv cu BitLocker și creați o cheie de recuperare.	<ul style="list-style-type: none"> Criptarea unității sistemului de operare, pagină 43.
12 Pentru un dispozitiv Archiver, creați numărul de roluri Archiver de care aveți nevoie pentru a susține numărul de camere și lățimea de bandă totală a rețelei planificate pentru implementarea.	<ul style="list-style-type: none"> Pentru seriile SV-1000E, SV-2000E, SV-4000E: Adăugarea rolurilor Archiver în SV Control Panel, pagină 38. Pentru SV-7000EX și pentru all-in-one: Adăugarea manuală a partițiilor și a rolurilor Archiver, pagină 40.
13 Conectați-vă la Config Tool și configurați funcțiile video și de control al accesului ale Security Center.	<ul style="list-style-type: none"> Activarea funcțiilor video și de control al accesului din Security Center, pagină 26. Configurarea setărilor de înscriere a unității, pagină 29.
14 Efectuați o copie de rezervă a configurației Security Center.	<ul style="list-style-type: none"> Realizarea unei icopii de rezervă a bazei de date Directory, pagină 36.

Porturi implicite utilizate de Streamvault

Porturile de rețea necesare trebuie să fie deschise pentru a permite funcționarea corectă a următoarelor componente Streamvault™.

Porturi necesare pentru pluginul Întreținere Streamvault

Următorul port trebuie deschis pe un firewall extern pentru traficul de intrare, astfel încât pluginul de întreținere Streamvault™ să poată comunica cu hardware-ul Streamvault. Această cerință se aplică numai dacă sunt îndeplinite următoarele trei condiții:

- Conexiunea de trecere a sistemului de operare intern la iDRAC este dezactivată
- iDRAC utilizează un port LAN dedicat
- Există un firewall între rețea iDRAC și rețea gazdă

În orice altă situație, această cerință poate fi ignorată.

Modul	Port de intrare	Utilizarea portului
Monitor hardware Streamvault	65116	Utilizat pentru comunicarea HTTPS prin rețea între Security Center și controlerul de gestionare a plăcii de bază iDRAC al hardware-ului Streamvault.

Porturi necesare pentru SV Control Panel

Porturile de trafic de ieșire enumerate mai jos trebuie să fie deschise pentru a permite componentelor Streamvault Control Panel să se conecteze la serviciile cloud Genetec™.

Port de ieșire	Utilizarea portului	URL destinație
TCP 443	Comunicare HTTPS cu serviciile de backup Genetec	svbackupservices.genetec.com genetecbackupservice.blob.core.windows.net

Porturi necesare CylancePROTECT

Porturile de trafic de ieșire enumerate mai jos trebuie să fie deschise pentru a permite agentului desktop CylancePROTECT să comunice cu consola de administrare Genetec și să primească actualizările agentului.

Port de ieșire	Utilizarea portului	URL destinație
TCP 443	Comunicarea HTTPS în America de Nord	cement.cylance.com data.cylance.com protect.cylance.com update.cylance.com api.cylance.com download.cylance.com venueapi.cylance.com

Port de ieșire	Utilizarea portului	URL destinație
TCP 443	Comunicarea HTTPS în Asia-Pacific Nord-Est	ciment-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	Comunicarea HTTPS în Asia-Pacific Sud-Est	ciment-au.cylance.com ciment-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	Comunicarea HTTPS în Europa Centrală	ciment-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	Comunicarea HTTPS în America de Sud	ciment-sae1.cylance.com data-sae1.cylance.com protect-sae1.cylance.com update-sae1.cylance.com api.cylance.com download.cylance.com venueapi-sae1.cylance.com
TCP 443	Comunicarea HTTPS în GovCloud	ciment.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

Port de ieșire	Utilizarea portului	URL destinație
		venueapi.us.cylance.com
TCP 443	Comunicare HTTPS pentru a activa Cylance după reinstalare	svservices.genetec.com

Notă: Dacă nu doriți să deschideți conexiunile de ieșire de mai sus, CylancePROTECT poate fi trecut în modul deconectat. În modul deconectat, CylancePROTECT primește actualizări ale agentului de la Genetec™ Update Service (GUS).

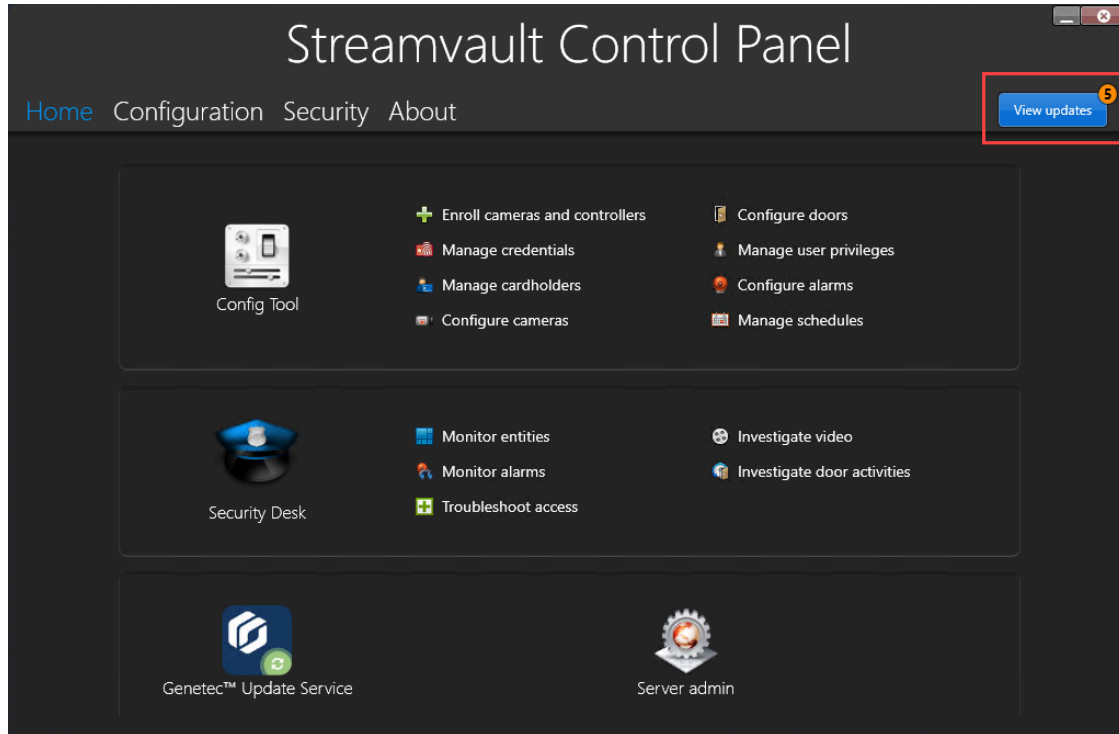
Pentru mai multe informații despre modurile în care dispozitivul Streamvault comunică cu serviciile de gestionare Genetec, consultați [Pagina Securitate a SV Control Panel](#), pagină 73.

Despre actualizarea software-ului SV în SV Control Panel

Genetec™ Update Service (GUS) este integrat în SV Control Panel pentru a vă asigura că componentele software ale dispozitivului dvs. sunt actualizate.

Atunci când sunt disponibile actualizări, butonul **Vezi actualizări** este afișat cu o insignă care indică câte actualizări sunt disponibile. Dacă dați clic pe butonul **Vizualizare actualizări**, se lansează GUS într-un browser.

Notă: Culoarea insignei variază în funcție de importanța actualizărilor. O insignă portocalie indică actualizări recomandate, iar o insignă roșie indică actualizări critice.



Principalele funcții ale GUS sunt următoarele:

- Actualizați-vă produsele Genetec™ atunci când este disponibilă o nouă versiune.
- Verificați dacă există actualizări la intervale regulate.
- Configurați actualizările pentru a fi descărcate în fundal, dar tot trebuie să le instalați manual.
- Vizualizați când a avut loc ultima verificare a actualizărilor.
- Actualizează automat licența în fundal pentru a se asigura că aceasta este valabilă și că data de expirare este actualizată.
- Activați diverse funcții, precum Programul de îmbunătățire Genetec.
- Vă analizează firmware-ul și vă recomandă actualizări sau vă notifică cu privire la vulnerabilități.

Pentru mai multe informații despre modul de utilizare a GUS, consultați [Ghidul de utilizare Genetec™ Update Service](#) pe TechDoc Hub.

Conectarea componentelor dispozitivului Streamvault

Pentru a pregăti dispozitivul Streamvault™ pentru utilizare, trebuie să conectați perifericele necesare (monitor, tastatură și mouse), perifericele opționale, rețeaua și o sursă de alimentare.

Înainte de a începe

Eliberați spațiul din jurul butonului de alimentare. Pentru a preveni oprirea accidentală a dispozitivului, asigurați-vă că nimic nu atinge sau nu se află prea aproape de butonul de pornire.

Procedură

- 1 Conectați cablul monitorului de afișare la o intrare video acceptată: VGA, HDMI sau conector DisplayPort. Cel puțin un monitor trebuie să fie conectat la aparat. Puteți conecta până la trei monitoare la același dispozitiv.
- 2 Conectați monitorul la o priză de curent alternativ și porniți-l.
- 3 Conectați tastatura și mouse-ul la un port USB disponibil.
- 4 (Opțional) Conectați perifericele opționale:
 - Difuzoare
 - [Camere analogice](#)
 - [Intrări și ieșiri de alarmă](#)
- 5 Conectați un cablu Ethernet la portul Ethernet de pe aparat. Conectați celălalt capăt al cablului la mufa RJ-45 a rețelei IP.
- 6 Pentru aparatele Streamvault™ SV-100E, introduceți fișa de curent continuu în mufa de intrare de 19,5 V a aparatului și celălalt capăt în cărămida de alimentare. Conectați cablul de la cărămidă la o priză electrică.
- 7 Pentru a porni dispozitivul Streamvault, apăsați butonul de pornire.

După ce termini

[Conectați-vă la dispozitivul Streamvault.](#)

Carduri de codificare analogică Genetec

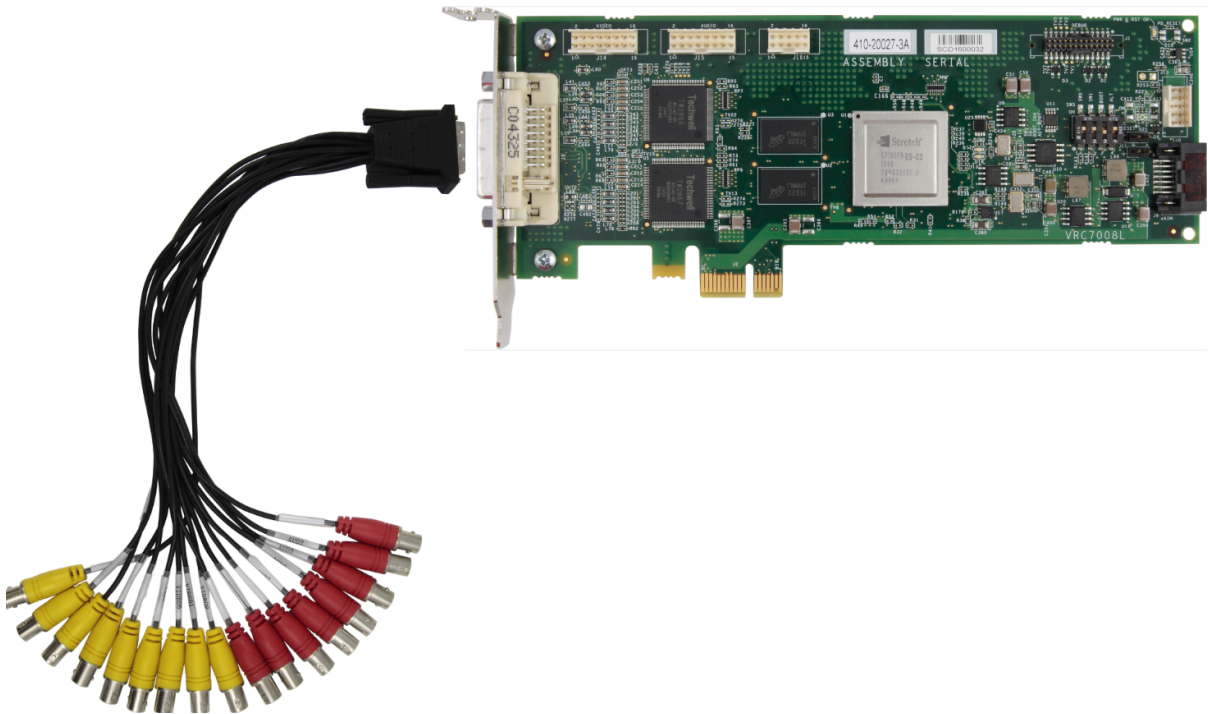
Dacă utilizați un dispozitiv Streamvault pentru a implementa un sistem de management video cu camere analogice, trebuie să conectați camerele la placa de codificare analogică Genetec™ de pe dispozitiv.

Specificațiile cardului de codificare analogică

Următoarele specificații se aplică dispozitivelor Streamvault care includ placa video analogică:

- 8 sau 16 intrări video analogice, în funcție de cartela instalată
- Rezoluție video maximă 4CIF
- Rata maximă a cadrelor: 30 fps
- Suportă formatul de compresie H.264

Limitare: Pentru ca placa de codificare analogică să poată înregistra, dispozitivul Streamvault trebuie să aibă o conexiune de rețea. Dacă nu este disponibilă o conexiune de rețea, trebuie să configurați o interfață loopback pentru ca placa de codificare să poată funcționa corect.



Despre conectarea camerelor analogice

Dacă aparatul dvs Streamvault include cardul codificator analogic Genetec, acesta este livrat cu un cablu de breakout cu conectori BNC. Conectorii BNC sunt utilizați pentru a conecta camerele analogice direct la placa de codare încorporată.

Despre adăugarea de camere analogice în Security Center

Pentru a adăuga camere analogice în Security Center, trebuie să utilizați instrumentul de înregistrare a unității. Pentru mai multe informații, consultați [Despre instrumentul de înregistrare a unității](#).

Luați în considerare următoarele aspecte atunci când adăugați camere analogice:

- Nu puteți adăuga camere analogice în Security Center folosind metoda *Adaugare manuală*. Utilizați Instrumentul de înregistrare a unității.
- Pentru a detecta noi unități și a utiliza Instrumentul de înregistrare a unităților, trebuie să vă conectați la Config Tool la nivel local.
- Atunci când selectați producătorul camerei în instrumentul de înregistrare a unității, puteți găsi toate camerele analogice listate sub producătorul plăcii de *codare Genetec*.

Dezactivarea intrărilor camerei pe cardurile de codificare de pe un dispozitiv Streamvault

Pentru a actualiza o licență de conectare a camerei de la analog la IP, trebuie să dezactivați intrările camerei de pe placa de codificare.

Procedură

- 1 De pe pagina de pornire a Config Tool, dați clic pe fila *Despre*.

- 2 Dați clic pe fila **Omnicast™** și verificați numărul de camere listate lângă *Număr de camere și monitoare analogice*.
De exemplu: 16 / 16.
- 3 Deschideți comanda *Video*.
- 4 În arborele de entități, dați clic pe unitatea video care corespunde plăcii de codificare.
- 5 Dați clic pe fila **Periferice** și selectați camerele pe care trebuie să le dezactivați.
Puteți selecta mai multe camere apăsând Ctrl și dând clic pe camerele respective.
- 6 În partea de jos a paginii *Periferice*, dați clic pe cercul roșu (●) pentru a dezactiva camerele, apoi dați clic pe **Aplicare**.
Camerele dezactivate sunt gri, iar în stânga fiecărei camere dezactivate din listă este afișat un punct roșu.
- 7 Pe pagina *Despre*, verificați dacă numărul de camere este corect.
Este posibil să fie necesar să reporniți Config Tool pentru a actualiza numărul de camere.
Notă: Dacă o cameră pe care ați dezactivat-o a înregistrat imagini video, camera este afișată în arborele de entități din comanda Security Desk *Monitorizare*. Puteți vizualiza redarea de la camera respectivă.

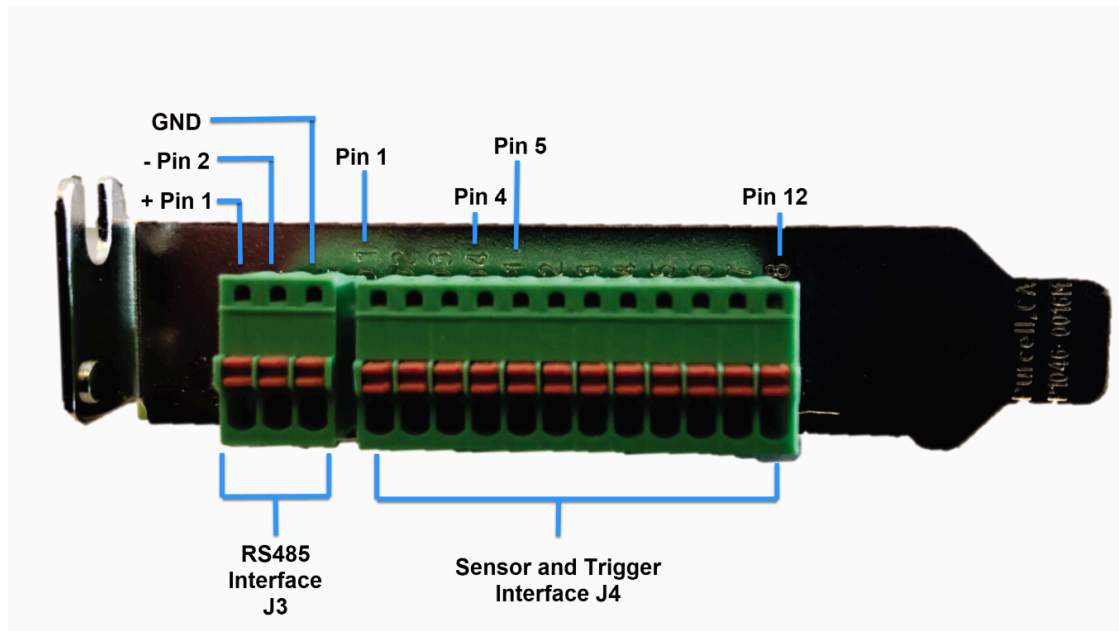
Intrările și ieșirile de alarmă ale unui dispozitiv Streamvault

Dacă utilizați un dispozitiv Streamvault pentru a implementa un sistem de control al accesului, puteți utiliza cardul I/O pentru a conecta intrările de alarmă hardware direct la dispozitiv, iar apoi puteți controla ieșirile acestuia utilizând evenimente la acțiuni în Security Center.

Specificațiile cardului I/O

Următoarele specificații se aplică modelelor Streamvault care includ placa de I/O:

- 4 ieșiri de declanșare
- 8 intrări de alarmă
- Port de comunicații RS-485



Despre conectarea intrărilor I/O

Puteți conecta firele de intrare și de ieșire de la dispozitivele hardware direct la cartela I/O de pe spatele Streamvault dispozitivului. Firele trebuie introduse cu ajutorul unei șurubelnițe mici cu cap plat pentru a împinge clemele de tensiune de pe conector.

Despre crearea de evenimente pentru acțiuni

Pentru informații privind modul de creare a evenimentelor la acțiuni pentru Streamvault, consultați [Crearea evenimentelor la acțiuni](#) pe TechDoc Hub.

Despre conturile de utilizator Streamvault

Există două tipuri de conturi de utilizator Streamvault™: administrator local și non-administrator local. În funcție de tipul de cont de utilizator cu care vă conectați la Panoul de control SV, vedeți doar acele caracteristici care sunt relevante pentru dvs.

Administrator local

Contul de utilizator de administrator local (Admin) este creat implicit. O persoană conectată ca administrator are drepturi administrative complete la Panoul de control SV. Administratorul poate configura toate setările legate de sistem și securitate în Panoul de control SV și poate crea conturi de utilizator non-administrator.

Non-administrator local

Contul de utilizator local implicit non-administrator pentru dispozitivele și stațiile de lucru All-in-one este contul de operator. O persoană conectată ca Operator are acces restricționat la funcțiile Panoului de control SV. Operatorul poate lansa Config Tool și Security Desk, poate vizualiza informații despre sistem și licențiere și poate accesa documentația produsului.

O persoană conectată ca administrator poate crea alte conturi care nu sunt de administrator, care au, de asemenea, acces limitat la Panoul de control SV.

Notă: Este posibil să eliminați restricțiile de acces implicite aplicate pentru toate conturile de utilizator care nu sunt administrator. Pentru informații despre cum să faceți acest lucru, consultați [Eliminarea restricțiilor de la conturile de utilizatori non-administratori](#), pagină 114.

Informații de conectare pentru conturile de utilizator implicite de pe unStreamvault aparat

La prima pornire a dispozitivului Streamvault, sunt create conturile de utilizator Windows Admin și Operator. Aceste conturi au drepturi de acces diferite și parole implicite. Server Admin are o parolă implicită.

Următoarele parole implicite sunt pentru autentificarea inițială. În timpul instalării, vă creați propria parolă pentru Config Tool și Security Desk.

Nume utilizator	Parolă implicită	Acces permis la	Acces interzis la
Administrator	admin	Acces complet la sistem: <ul style="list-style-type: none"> Windows: toate funcțiile de sistem și administrative Security Center SV Control Panel 	Nu se aplică
Operator	operator	<ul style="list-style-type: none"> Coșul de reciclare Biblioteci Computerul meu C: unitate Pagina de pornire a SV Control Panel, pagina de configurare Doar setări regionale, pagina Despre 	<ul style="list-style-type: none"> Windows: închideți și reporniți Setări de sistem Partiție video

Nume utilizator	Parolă implicită	Acces permis la	Acces interzis la
		<ul style="list-style-type: none"> Server Admin: necesită o parolă de administrator pentru drepturi complete 	
Nu se aplică	genetecfactory	Server Admin	Notă: Această opțiune nu este disponibilă pentru dispozitivele Stații de lucru.

Pentru a schimba contul de utilizator Windows, aplicația client sau parola Server Admin, conectați-vă la SV Control Panel folosind contul de utilizator Windows Admin. Pe pagina *Securitate*, în secțiunea *Acreditări*, vă puteți gestiona toate parolele.

Notă: Contul Operator nu este creat cu un șablon. Dacă creați un nou cont de utilizator, acesta nu va avea aceleași restricții în mod implicit.

Security Center Server Admin

- Doar utilizatorii administratori se pot conecta la Server Admin.
- Pentru a vă conecta de pe calculatorul local, dați clic pe comanda rapidă **Server Admin** de pe desktop.
- Pentru a vă conecta la Server Admin de la distanță, aveți nevoie de numele DNS sau adresa IP a serverului, portul serverului web și parola serverului. Atunci când introduceți parola implicită, vi se solicită să o modificați.

IMPORTANT: Pentru a asigura securitatea sistemului dvs., schimbați imediat toate parolele implicite. Utilizați bunele practici din industrie pentru crearea de parole puternice.

Subiecte conexe

[Modificarea GPO-urilor locale pentru conturile de utilizator non-administrator](#), pagină 120

Conectarea la un dispozitiv Streamvault

Prima dată când porniți dispozitivul Streamvault™, vi se solicită să schimbați parola de administrare implicită. De asemenea, trebuie să schimbați parola implicită a operatorului. Apoi vă puteți conecta ca utilizator Operator sau Admin.

Înainte de a începe

[Aflați ce drepturi de acces au conturile Operator și Admin.](#)

Ce ar trebui să știți

Conectați-vă ca utilizator administrator pentru a configura dispozitivul în SV Control Panel.

IMPORTANT: Parolele trebuie să îndeplinească următoarele cerințe:

- Minimum de 14 caractere
Lungimea minimă este de 10 caractere pentru aparatele cu versiuni de imagine care nu au serviciul Streamvault. Pentru informații despre ce aparate au serviciul Streamvault și care nu, consultați [Aparate cu capacități de gestionare a întăririi](#), pagină 16.
- Cel puțin trei caractere din următoarele patru categorii:
 - Majuscule
 - Litere mici
 - Cifre de bază 10 (0-9)
 - Caractere nonalfanumerice (precum \$, %, !)

Procedură

- 1 Alimentați cu energie dispozitivul.
- 2 Conectați-vă folosind numele de utilizator Admin și parola implicită care sunt tipărite pe dispozitiv.
- 3 Introduceți o nouă parolă de administrator.
Sunteți conectat ca utilizator administrator.
Notă: Unele modele au în mod implicit doar contul de administrator.
- 4 Deconectați-vă, apoi conectați-vă folosind numele de utilizator Operator și parola implicită care sunt tipărite pe dispozitiv.
- 5 Introduceți o nouă parolă de operator.
Sunteți conectat ca utilizator Operator.
- 6 Continuați sesiunea de operator sau deconectați-vă și conectați-vă din nou ca utilizator administrator.

După ce termini

[Lansați configurarea inițială a dispozitivului dumneavoastră.](#)

Despre serviciul Streamvault

Serviciul Streamvault este un serviciu Windows care permite utilizatorilor să configureze un dispozitiv Streamvault™, precum aplicarea profilurilor de întărire.

Serviciul Streamvault poate aplica următoarele profiluri de întărire pe aparate:

- Linii de bază de securitate Microsoft
- Linii de bază de securitate Microsoft cu profilul Center for Internet Security (CIS) Nivel 1
- Linii de bază de securitate Microsoft cu profilul CIS Nivelul 2
- Linii de bază de securitate Microsoft cu profilul Ghid de implementare tehnică de securitate (STIG).

Vezi [Despre întărirea Streamvault](#), pagină 16 pentru mai multe informații despre profilele de întărire.

Când un utilizator Admin selectează un profil de întărire în Panoul de control SV, serviciul Streamvault aplică profilul la aparat.

Actualizările pentru serviciul Streamvault sunt disponibile periodic și pot fi aplicate prin Genetec™ Update Service (GUS) sau Genetec Technical Assistance Portal (GTAP). Când este disponibilă o actualizare, apare o notificare în Panoul de control SV. Aplicarea actualizărilor este opțională, dar recomandată pentru a accesa versiuni noi ale profilurilor de întărire.

Despre întărirea Streamvault

Întărirea îmbunătățește securitatea dispozitivului dvs. Streamvault™ prin aplicarea unui set specific de setări de securitate.

Atunci când vă întăriți aparatul, îl optimizați pentru mai multă securitate, dar, potențial, în detrimentul unei anumite utilizări sau performanțe. Cât de mult vă întăriți dispozitivul depinde de modelul dvs. de amenințare și de sensibilitatea informațiilor dvs.

Întărirea se aplică pe *Securitate* pagina Panoului de control SV. Există patru profile de întărire predefinite din care puteți alege.

În mod implicit, toate aparatele sunt livrate cu Microsoft cu profilul de întărire CIS Nivelul 2 aplicat.

Profil de întărire	Descriere
Microsoft (doar)	Acest profil de întărire aplică liniile de bază de securitate Microsoft sistemului dumneavoastră. Liniile de bază de securitate Microsoft sunt un grup de setări de configurare recomandate de Microsoft care se bazează pe feedback-ul de la echipele de inginerie de securitate Microsoft, grupurile de produse, partenerii și clienții. Liniile de bază Microsoft care sunt implementate pe dispozitivele Streamvault sunt linia de bază Windows și linia de bază Microsoft Edge.
Microsoft cu CIS Nivelul 1	Acest profil de întărire aplică liniile de bază de securitate Microsoft și profilul Center for Internet Security (CIS) Nivel 1 (CIS L1) la sistemul dumneavoastră. CIS L1 oferă cerințe de securitate esențiale care pot fi implementate pe orice sistem cu un impact redus sau deloc asupra performanței sau funcționalitate redusă.
Microsoft cu CIS Nivelul 2	Acest profil de întărire aplică liniile de bază de securitate Microsoft și profilurile CIS L1 și Level 2 (L2) sistemului dumneavoastră. Profilul CIS L2 oferă cel mai înalt nivel de securitate și este destinat organizațiilor în care securitatea este de maximă importanță. Securitatea strictă pe care o aduce acest profil de întărire poate reduce funcționalitatea sistemului și poate face mai dificilă administrarea de la distanță a serverului.
Microsoft cu STIG	Acest profil de întărire aplică liniile de bază de securitate Microsoft și Ghidurile de implementare tehnică de securitate (STIG) ale Agenției pentru Sisteme Informaționale de Apărare (DISA) sistemului dumneavoastră. DISA STIG se bazează pe standardele Institutului Național de Standarde și Tehnologie (NIST) și oferă protecție avansată de securitate pentru sistemele Windows pentru Departamentul de Apărare al SUA.

Notă: Profilele de întărire sunt disponibile numai pe aparatele care au [Serviciul Streamvault](#). Pentru mai multe informații, consultați [Despre serviciul Streamvault](#), pagină 15.

Aparate cu capacități de gestionare a întăririi

Numai acele aparate cu serviciul Streamvault™ au capacități de gestionare a întăririi. Tipul aparatului și imaginea determină dacă serviciul Streamvault este disponibil.

Tabelul de mai jos prezintă ce aparate au serviciul Streamvault și care nu.

Tip dispozitiv	Versiuni de imagini cu serviciul Streamvault	Versiuni de imagini fără serviciul Streamvault
All-in-one	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 16 17 18 19
SVW	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 0010.4 0011.2 0012.2 0013.2
SVA	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 0010.4 0011.2 0012.2 0013.2
SVR	<ul style="list-style-type: none"> 10.2021.2 11.2024.2 	<ul style="list-style-type: none"> 0012.2.X
Alte dispozitive Streamvault	<ul style="list-style-type: none"> WS.2022.1 	<ul style="list-style-type: none"> 2016.1.B 2016.1.C 2019.1 2019.4.C 2022.1.C

Notă: Pentru informații despre găsirea versiunii imagine a aparatului dvs., consultați [Găsirea ID-ului sistemului și a versiunii imaginii unui dispozitiv Streamvault](#), pagină 87.

Noțiuni de bază despre panoul de control SV

Noțiuni introductive prezintă panoul de control SV și oferă informații despre cum să configurați dispozitivul Streamvault.

Această secțiune include următoarele subiecte:

- ["Despre SV Control Panel"](#), pagină 19
- [" Activarea licenței Security Center pe un dispozitiv "](#), pagină 22
- [" Activarea manuală a unei licențe de la Server Admin "](#), pagină 23
- ["Activarea monitorului de disponibilitate a sistemului"](#), pagină 25
- [" Activarea funcțiilor video și de control al accesului din Security Center "](#), pagină 26
- ["Despre Instrumentul de înscriere a unității"](#), pagină 29
- [" Configurarea setărilor implicite ale camerei "](#), pagină 32
- [" Crearea de programe de înregistrare personalizate "](#), pagină 34
- [" Despre backup și restaurare "](#), pagină 35
- [" Alegerea metodei de creare a rolurilor Archiver și partițiilor "](#), pagină 38
- [" Criptarea unității sistemului de operare "](#), pagină 43
- [" Colectarea jurnalelor de asistență "](#), pagină 47

Despre SV Control Panel

The SV Control Panel este o aplicație de interfață cu utilizatorul pe care o puteți utiliza pentru a configura dispozitivul Streamvault™ pentru a funcționa cu controlul de acces și supravegherea video Security Center.

ATENȚIE: Modificările de configurare efectuate în SV Control Panel va suprascrie modificările de configurare efectuate în afara SV Control Panel, inclusiv setările personalizate ale Windows.

SV Control Panel poate fi rulat în următoarele moduri:

- Modul de expansiune pentru configurațiile care rulează pe un server de expansiune.
- Modul client pentru configurațiile care rulează pe dispozitive stații de lucru.
- Modul Directory pentru configurațiile care rulează pe serverul principal.

SV Control Panel include următoarele funcții:

- Expertul de *Setare a panoului de control Streamvault* pentru a vă ajuta să vă configurați rapid dispozitivul.
- *Expertul de activare din Streamvault Control Panel* pentru a vă ajuta să vă activați dispozitivul.
- *Asistent de instalare Security Center* pe care îl puteți utiliza pentru a configura Security Center.
- *Experții Streamvault Control Panel Backup și Streamvault Control Panel Restore* pentru a vă ajuta să creați copii de rezervă ale bazei de date Directory și ale configurațiilor și să restaurați aceste fișiere în sistem, dacă este cazul.
- Genetec™ Update Service (GUS), care verifică periodic dacă există actualizări de software.
- Comenzi rapide pentru sarcinile utilizate în mod obișnuit în Config Tool și Security Desk.
- Linkuri către portalul de asistență tehnică Genetec (GTAP) și documentația produsului.
- Opțiunea de a alege modul de funcționare pentru software-ul antivirus Cylance furnizat împreună cu dispozitivul dvs. Streamvault™. Opțiunile sunt listate pe *Securitate* pagina de configurare.
- Posibilitatea de a crea mai multe roluri Archiver și partiții pentru configurații pe serverele de expansiune.

Notă:

- Acest ghid este aplicabil pentru versiunea 3.2.1 a Panoului de control SV, pe care o puteți descărca de pe GTAP.
- Versiunile 3.0 și ulterioare ale Panoului de control SV sunt compatibile cu dispozitivele care nu au serviciul Streamvault. Totuși, aceste aparate nu au acces la profilurile de întărire.

Configurați-vă aparatul în SV Control Panel

Prima dată când vă conectați la dispozitivul Streamvault™, SV Control Panel deschide expertul *Configurarea panoului de control Streamvault* pentru a vă ghida în configurarea inițială.


Înainte de a începe

Conectați dispozitivul la internet.

Ce ar trebui să știți

- Setările aplicate în cadrul expertului pot fi modificate ulterior pe pagina *Configurare* din SV Control Panel.
- Pentru un Archiver, date analitice, stație de lucru sau orice alt dispozitiv care este un server de expansiune Security Center, nu vi se solicită să schimbați parolele utilizatorilor.

Procedură

- 1 Porniți dispozitivul.
SV Control Panel începe cu expertul *Configurarea panoului de control Streamvault* deschis.
Notă: SV Control Panel se deschide automat doar la prima pornire a dispozitivului. La repornirile ulterioare, utilizatorii trebuie să se conecteze folosind acreditările lor de administrator și să pornească SV Control Panel.
- 2 Pe pagina *Introducere*, dați clic pe **Mai departe**.
- 3 Pe pagina *Rețea*, configurați setările de conexiune IP:
 - a) Dacă utilizați DHCP pentru a obține automat un IP (implicit) și adresa IP lipsește, faceți clic pe **Refresh**  pentru a obține o adresă IP nouă. Apoi faceți clic pe **Reîncercare**.
 - b) Dacă în câmpul **Stare** se afișează altceva decât "Conectat la Internet", dați clic pe **Reîncercare**.
 - c) Când în câmpul **Stare** se afișează "Conectat la Internet", dați clic pe **Mai departe**.
- 4 Pe pagina *Configurare computer*, completați câmpurile din secțiunile *Informații generale* și *Setări regionale*.
- 5 Pentru a schimba interfața cu utilizatorul într-o altă limbă:
 - a) Din **Limba produsului**, alegeți limba dvs.
 - b) Reporniți SV Control Panel.
 - c) Când se redeschide expertul de *configurare Streamvault Control Panel*, faceți clic pe **Următorul** pe pagina *Configurare computer*.
- 6 Pe pagina *Configurare CylancePROTECT*, alegeți un mod de comunicare:
 - **Online (recomandat):** Atunci când este online, agentul CylancePROTECT comunică cu Genetec pentru a raporta noi amenințări, pentru a-și actualiza agentul și pentru a trimite date care să ajute la îmbunătățirea modelelor sale matematice. Această opțiune oferă cel mai înalt nivel de protecție.
 - **Deconectat:** Modul deconectat este pentru un dispozitiv fără conexiune la internet. În acest mod, CylancePROTECT nu se poate conecta sau trimite informații către serviciile de gestionare Genetec din cloud. Dispozitivul dumneavoastră este protejat împotriva majorității amenințărilor. Întreținerea și actualizările sunt disponibile prin intermediul Genetec™ Update Service (GUS).
 - **Oprirea alimentării:** Selectați acest mod pentru a dezinstala definitiv CylancePROTECT din dispozitivul dumneavoastră. Dispozitivul dvs. va utiliza Microsoft Defender pentru protecția și detectarea amenințărilor. Nu recomandăm dezactivarea CylancePROTECT dacă dispozitivul nu poate primi actualizări ale definițiilor de viruși pentru Microsoft Defender.
- 7 Clic **Activați gestionarea carantinei** pentru a adăuga capabilități suplimentare pictogramei Cylance din bara de activități, inclusiv **Ștergeți în carantină** opțiunea de a șterge fișierele pe care Cylance le-a pus în carantină.
- 8 În pagina *Acreditări*, dați clic pe **Modificare parolă** pentru a configura parolele pentru următoarele aplicații:
 - **Security Center (utilizator Admin):** Parola utilizatorului administrator pentru Security Desk, Config Tool și Genetec™ Update Service.
 - **Server Admin:** Parola pentru aplicația Genetec™ Server Admin.

Dacă dispozitivul dvs. este un server de expansiune Security Center, nu vi se solicită să schimbați nicio parolă. Selectați **Sari peste acest pas** dacă nu doriți să setați parole noi.
- 9 Pe pagina *Întărire*, selectați unul dintre următoarele profiluri de întărire:
 - **Microsoft (doar):** Acest profil de întărire aplică liniile de bază de securitate Microsoft sistemului dumneavoastră. Liniile de bază de securitate Microsoft sunt un grup de setări de configurare recomandate de Microsoft care se bazează pe feedback-ul de la echipele de inginerie de securitate Microsoft, grupurile de produse, partenerii și clienții.
 - **Microsoft cu CIS Nivelul 1:** Acest profil de întărire aplică liniile de bază de securitate Microsoft și profilul Center for Internet Security (CIS) Nivel 1 (CIS L1) la sistemul dumneavoastră. CIS L1 oferă cerințe de securitate esențiale care pot fi implementate pe orice sistem cu un impact redus sau deloc asupra performanței sau funcționalitate redusă.
 - **Microsoft cu CIS Nivelul 2:** Acest profil de consolidare aplică liniile de bază de securitate Microsoft și profilurile CIS L1 și Level 2 (L2) sistemului dumneavoastră. Profilul CIS L2 oferă cel mai înalt nivel de securitate și este destinat organizațiilor în care securitatea este de maximă importanță.

Notă: Securitatea strictă pe care o aduce acest profil de întărire poate reduce funcționalitatea sistemului și poate face mai dificilă administrarea de la distanță a serverului.

- **Microsoft cu STIG:** Acest profil de întărire aplică liniile de bază de securitate Microsoft și Ghidurile de implementare tehnică de securitate (STIG) ale Agenției pentru Sisteme Informaționale de Apărare (DISA) sistemului dumneavoastră. DISA STIG se bazează pe standardele Institutului Național de Standarde și Tehnologie (NIST) și oferă protecție avansată de securitate pentru sistemele Windows pentru Departamentul de Apărare al SUA.

Notă: Pagina *Întărire* este disponibilă numai pentru aparatele cu serviciul Streamvault.

10 Pe pagina *Monitor de disponibilitate a sistemului*, alegeți o metodă de colectare a datelor:

- **Nu colectați datele:** Agentul Monitorul de disponibilitate a sistemului este instalat, dar nu colectează date.
- **Datele vor fi colectate în mod anonim:** Nu este necesar niciun cod de activare. Datele privind sănătatea sunt trimise către un serviciu dedicat de monitorizare a sănătății, unde numele entităților sunt criptate și nu pot fi urmărite. Aceste date sunt utilizate doar de Genetec Inc. pentru statistici și nu pot fi accesate prin intermediul GTAP.
- **Datele vor fi colectate și conectate la sistemul meu:** Este necesar un cod de activare. Datele privind sănătatea care sunt colectate sunt legate de un sistem înregistrat cu un acord de întreținere a sistemului (SMA) activ.

11 Citiți acordul de confidențialitate, bifați caseta de selectare **Accept termenii acordului de confidențialitate** și dați clic pe **Aplică**.

12 Pe pagina *Concluzie*, dați clic pe **Închidere**.

Opțiunea **Porniți expertul de activare după configurare** este selectată în mod implicit. Dacă îl ștergeți, vi se reamintește să activați produsul.

După ce termini

[Activați dispozitivul](#) înainte de utilizare.

Activarea licenței Security Center pe un dispozitiv

Expertul de *activare a Panoului de control Streamvault* vă ajută să vă activați licența Security Center pe dispozitivul Streamvault™.

Înainte de a începe

- Conectați-vă dispozitivul la internet.
- Asigurați-vă că aveți ID-ul de sistem și parola care v-au fost trimise după ce ați cumpărat licența.

Ce ar trebui să știți

- Această comandă se aplică doar dispozitivelor care au o conexiune la internet. Pentru un dispozitiv fără internet, [activați manual licența dvs. Security Center din Server Admin](#).
- Trebuie să activați licența Security Center numai pe dispozitivul care găzduiește rolul Directory, nu și pe dispozitivele server sau stație de lucru de expansiune.

Procedură

- 1 Din SV Control Panel, dați clic pe **Sistemul nu este activat. Dați clic aici pentru a activa**.
Se deschide expertul de *activare a panoului de control Streamvault*.
Notă: Dacă vedeți mesajul *Accesul la internet este necesar pentru activare*, dispozitivul dvs. nu este conectat în prezent la internet. Fie conectați dispozitivul acum, fie activați licența manual din Server Admin.
- 2 Pe pagina *Activare*, dați clic pe **ID sistem** și dați clic pe **Mai departe**.
- 3 Pe pagina *ID sistem*, introduceți ID-ul de sistem și parola și dați clic pe **Mai departe**.
- 4 Pe pagina *Rezumat*, verificați dacă ID-ul de sistem este corect și dați clic pe **Activare**.
Pagina *Rezultat* se deschide și indică faptul că activarea a avut succes.
- 5 Dați clic pe **Mai departe**.
- 6 (Opțional) Pe pagina *Actualizări*, efectuați una dintre următoarele acțiuni:
 - Dacă nu sunt disponibile actualizări, dați clic pe **Deschideți asistentul de instalare Security Center**.
 - Dacă sunt disponibile actualizări, dați clic pe **Vezi actualizările** pentru a deschide Genetec™ Update Service și a instala actualizările.
 - Dacă verificarea actualizării a eșuat deoarece Directory nu răspunde, dați clic pe **Deschideți Server Admin** și asigurați-vă că Directory este pregătit.

Notă: Dacă Genetec Update Service nu era pregătit, verificarea actualizării ar putea eșua. Apare mesajul *În acest moment nu se poate verifica dacă există actualizări. Vom încerca din nou mai târziu*.
- 7 Pe pagina *Funcții suplimentare*, activați sau dezactivați Synergis™ Softwire și Genetec™ Mobile.
Aceste funcții sunt afișate doar dacă sunt instalate pe dispozitivul dumneavoastră. Funcția Genetec Mobile este disponibilă doar pentru Security Center 5.8 și versiunile anterioare.
- 8 Închideți expertul de activare *Streamvault Control Panel*.

După ce termini

- (Opțional) [Activați agentul Monitorul de disponibilitate a sistemului](#).
- [Configurați setările Security Center cu ajutorul asistentului de instalare al Security Center](#)

Subiecte conexe

[Activarea manuală a unei licențe de la Server Admin](#), pagină 23

[Pagina Despre din SV Control Panel](#), pagină 76

Activarea manuală a unei licențe de la Server Admin

Dacă dispozitivul Streamvault™ nu are acces la Internet, trebuie să activați manual licența Security Center din Server Admin.

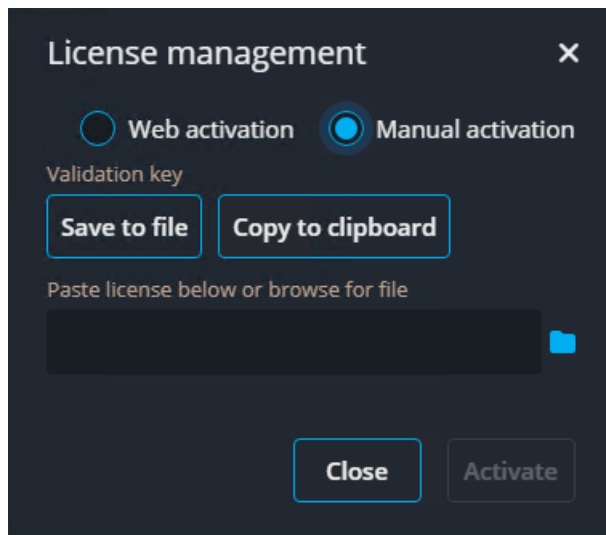
Procedură

1 Salvați cheia de validare:

- a) Din dispozitiv, deschideți SV Control Panel.
- b) De pe pagina de pornire, dați clic pe pictograma **Server Admin**.
- c) Conectați-vă la Server Admin.

Dacă parola Server Admin este diferită de parola de administrator Windows, conectați-vă la Server Admin utilizând acreditările specificate în expertul de *Configurare a panoului de control Streamvault*.

- d) Pe pagina *Licență*, dați clic pe **Modificare**.
- e) În caseta de dialog *Gestiunea licențelor*, selectați **Activare manuală** > **Salvare în fișier**.
Numele implicit al fișierului este *validation.vk*.



- f) Copiați fișierul *validation.vk* pe o cheie USB.
 - g) Ejectați cheia USB din computer.
- 2 Obțineți licența de la Portalul de asistență tehnică Genetec™ (GTAP):
- a) Conectați cheia USB la un alt computer care are acces la internet.
 - b) Conectați-vă la [GTAP](#).
 - c) Pe pagina *Autentificare GTAP*, introduceți ID-ul de sistem și parola care v-au fost atribuite atunci când ați achiziționat licența, apoi dați clic pe **Autentificare**.
 - d) Din pagina *Informații sistem*, în secțiunea **Informații licență**, dați clic pe *Activare licență*.
 - e) În caseta de dialog care se deschide, inserați cheia de validare sau căutați fișierul.
 - f) În caseta de dialog *Activare*, navigați până la fișierul *validation.vk* de pe cheia USB, apoi dați clic pe **Trimite**.
Se afișează mesajul *Licența dvs. a fost activată cu succes*.
 - g) Dați clic pe **Descărcare licență**, apoi salvați cheia de licență.
Numele implicit al fișierului este ID-ul de sistem, urmat de *_Directory_License.lic*.
 - h) Copiați fișierul *_Directory_License.lic* pe cheia USB.
 - i) Ejectați cheia USB din computer.

- 3 Activați-vă licența.
 - a) Conectați cheia USB la dispozitivul dumneavoastră.
 - b) Reveniți la Server Admin.
 - c) Pe pagina *Licență*, dați clic pe **Modificare**.
 - d) În caseta de dialog *Gestiunea licențelor*, selectați **Activare manuală**.
 - e) Lipiți informațiile despre licență din fișierul *License.lic* (deschideți cu un editor de text) sau căutați fișierul *License.lic*, apoi dați clic pe **deschidere**.
 - f) Dați clic pe **Activare**.

Subiecte conexe

[Activarea licenței Security Center pe un dispozitiv](#), pagină 22

Activarea monitorului de disponibilitate a sistemului

Pentru a monitoriza disponibilitatea sistemului și problemele de sănătate ale GTAP, puteți seta Monitorul de disponibilitate a sistemului să colecteze date despre dispozitivul dumneavoastră și să le trimită la Serviciile de monitorizare a sănătății.

Înainte de a începe

Pentru a colecta și a raporta informații despre starea de sănătate a dispozitivului dumneavoastră, trebuie să fie generat un cod de activare pe [GTAP](#). Pentru informații despre cum să faceți acest lucru, consultați [Generarea codurilor de activare pentru System Availability Monitor Agent](#) pe TechDoc Hub.

Procedură

- 1 Deschideți SV Control Panel.
- 2 Pe *Configurare* pagină, faceți clic **Configurați** în *Monitorul disponibilității sistemului* secțiune.
- 3 În fereastra *Agent monitor de disponibilitate a sistemului Genetec*, dați clic pe **Modificare**.
- 4 Verificați dacă este selectată caseta de selectare **Datele vor fi colectate și conectate la sistemul meu**.
- 5 În câmpul **Cod de activare**, introduceți codul dispozitivului dumneavoastră.
- 6 Dați clic pe **OK**.

Activarea funcțiilor video și de control al accesului din Security Center

Expertul *asistent de instalare al Security Center* vă ghidează prin configurarea principalelor funcții de gestionare video și de control al accesului.

Ce ar trebui să știți

Setările pe care le aplicați în asistent pot fi modificate ulterior în Config Tool.

Se aplică: Dispozitivelor care găzduiesc rolul Directory, precum dispozitivele all-In-one

Procedură

- 1 Conectați-vă ca utilizator Administrator.

SFAT: Dacă parola dvs. de la Security Center este diferită de parola de administrator pentru Windows, conectați-vă la Security Center folosind parola de acces specificată în expertul *Configurarea Panoului de control Streamvault*.

Asistentul de instalare a Security Center se deschide.

- 2 După ce ați citit pagina *Introducere*, dați clic pe **Mai departe**.

- 3 Pe pagina *Funcții disponibile*, alegeți funcțiile dorite și dați clic pe **Mai departe**.

Funcțiile de bază sunt activate în mod implicit. Puteți activa și dezactiva funcțiile mai târziu pe pagina *Funcții* din vizualizarea **Setări generale** a comenzii *Sistem*.

Notă: Dacă licența dvs. nu acceptă o funcție, funcția respectivă nu apare în listă.

- 4 Pe pagina *Securitate cameră*, specificați numele de utilizator și parola implicită care sunt utilizate pentru toate camerele dvs. și apoi dați clic pe **Mai departe**.

SFAT: Pentru mai multă securitate, selectați **Utilizare HTTPS**.

- 5 Pe pagina *Setări calitate cameră*, configurați următoarele opțiuni:

- **Rezoluție:**

- **Mare:** 1280x720 și mai mare
- **Standard:** Mai mult de 320x240 și mai puțin de 1280x720
- **Redus:** 320x240 și mai mic
- **Implicit:** Setările implicite ale producătorului

Camera utilizează întotdeauna cea mai mare rezoluție pe care o poate suporta din categoria aleasă. În cazul în care camera nu acceptă nicio rezoluție din categoria aleasă, aceasta utilizează cea mai mare rezoluție pe care o poate accepta din categoria următoare. De exemplu, în cazul în care camera nu poate suporta o rezoluție înaltă, aceasta utilizează cea mai mare rezoluție pe care o poate suporta din grupul Standard.

Setările de pe această pagină pot fi modificate ulterior din pagina *Setări implicite ale camerei* a rolului Arhivar.

- 6 Pe pagina *Setări de înregistrare*, selectați setările de înregistrare implicite care se aplică tuturor camerelor:

- **Oprit:** Înregistrarea este oprită
- **Continuu:** Camerele înregistrează continuu. Aceasta este setarea implicită.
- **La mișcare/manual:** Camerele înregistrează atunci când sunt declanșate de o acțiune (cum ar fi Pornire înregistrare, Adăugare marcaj sau Declanșare alarmă), de detectarea mișcării sau manual de către un utilizator.
- **Manual:** Camerele înregistrează atunci când sunt declanșate de o acțiune (cum ar fi Pornire înregistrare, Adăugare marcaj sau Declanșare alarmă) sau manual de către un utilizator.

Notă: Când se utilizează setarea **Manual**, atunci mișcarea nu declanșează nicio înregistrare.

- **Personalizat:** Puteți seta un program pentru momentul în care are loc înregistrarea.

7 Dați clic pe **Mai departe**.

8 Pe pagina *Securitatea unității de control al accesului*, specificați numele de utilizator și parola implicită pentru toate unitățile de control al accesului și dați clic pe **Mai departe**.

9 Pe pagina *Titulari de card*, selectați modul în care doriți să adăugați acreditările (cardurile) și titularii de carduri.

a) Selectați dacă doriți să adăugați titularii de carduri (la închiderea asistentului de instalare a Security Center) de la comanda *Managementul titularilor de carduri* sau utilizând instrumentul Import.

b) Dați clic pe **Mai departe**.


10 Pe pagina *Utilizatori*, adăugați mai mulți utilizatori în sistem:

a) Introduceți numele de utilizator.

b) Selectați **Tip de utilizator**:

- **Operator:** Un operator poate să utilizeze comanda *Monitorizare*, să vizualizeze videoclipuri și să gestioneze vizitatorii în Security Desk.
- **Raportare:** Un utilizator de raportare poate utiliza aplicația Security Desk și poate executa cele mai elementare acțiuni de raportare, cu excepția sarcinilor pentru AutoVu™ ALPR. Un utilizator care are doar drepturi de raportare nu poate vizualiza niciun video, nu poate controla niciun dispozitiv fizic sau raporta incidente.
- **Investigator:** Un investigator poate să utilizeze comanda *Monitorizare*, să vizualizeze videoclipul, să controleze camerele PTZ, să înregistreze și să exporteze videoclipuri, să adăuge marcaje și incidente, să utilizeze sarcini de investigare, să administreze alarme și vizitatori, să suprascrie programul de deblocare a ușilor, să salveze comenzi etc.
- **Supraveghetor:** Un supraveghetor poate să utilizeze comanda *Monitorizare*, să vizualizeze videoclipul, să controleze camerele PTZ, să înregistreze și să exporteze videoclipuri, să adăuge marcaje și incidente, să utilizeze comenzi de investigare, să administreze alarme și vizitatori, să suprascrie programul de deblocare a ușilor, să salveze sarcini etc. Un supraveghetor poate și să utilizeze acțiuni de întreținere, să gestioneze titularii de carduri și acreditările, să modifice câmpurile personalizate, să stabilească nivelurile de pericol, să blocheze camere și să numere persoanele.
- **Provizionare:** Un utilizator de provizionare are majoritatea drepturilor de configurare, cu excepția următoarelor: gestionarea rolurilor, a macrocomenzilor, a utilizatorilor, a grupurilor de utilizatori, a evenimentelor personalizate, a traseelor de activitate, a nivelurilor de pericol și a fișierelor audio. Utilizatorul de provizionare este, de obicei, un instalator de sistem.
- **Operator AutoVu de bază:** Acest tip de utilizator este destinat operatorilor care utilizează AutoVu ALPR. Utilizatorul AutoVu de bază poate să utilizeze sarcinile ALPR, să configureze entități ALPR, să creeze reguli ALPR, să monitorizeze evenimente ALPR etc.
- **Utilizator Patroller:** Acest tip de utilizator este destinat utilizatorilor Genetec Patroller™ care utilizează AutoVu ALPR. Utilizatorul Patroller poate să utilizeze sarcinile ALPR, să configureze entități ALPR, să creeze reguli ALPR, să monitorizeze evenimente ALPR etc. Un utilizator Patroller nu are acces la alte aplicații Security Center, de exemplu, Config Tool și Security Desk. Utilizatorul Patroller nu poate modifica rapoartele sau parola Patroller.

11 Introduceți și confirmați **parola**, apoi dați clic pe **Adăugare**.

Noul utilizator este adăugat la lista de utilizatori din partea dreaptă a casetei de dialog. Pentru a șterge un utilizator, selectați un utilizator din listă și dați clic pe .

Modificați profilurile utilizatorilor în vizualizarea **Utilizatori** de la comanda *Gestionarea utilizatorilor*. Pentru informații, consultați [Ghidul administratorului Security Center](#) pe TechDoc Hub.

12 Dați clic pe **Mai departe**.

13 Confirmați că informațiile de pe pagina *Rezumat* sunt corecte, apoi dați clic pe **Aplicare** sau dați clic pe **Înapoi** pentru a corecta eventualele erori.

14 Pe pagina *Concluzie*, dați clic pe **Repornire**.

Config Tool repornește pentru a aplica setările.

Notă: Opțiunea **Deschideți Instrumentul de înscriere a unității după închiderea expertului** este selectată în mod implicit. Puteți șterge această opțiune și deschide ulterior instrumentul de înscriere a unității, dând clic pe comanda rapidă **Înscrieți camerele și controlorii** de pe pagina *Acasă* din SV Control Panel.

După ce termini

[Adăugați unități la sistemul](#), utilizând Instrumentul de înscriere a unităților.

Subiecte conexe

[Configurarea setărilor implicite ale camerei](#), pagină 32

[Crearea de programe de înregistrare personalizate](#), pagină 34

[Pagina de pornire a SV Control Panel](#), pagină 68

Despre Instrumentul de înscriere a unității

Înscrierea unităților este un instrument pe care îl puteți utiliza pentru a detecta unitățile IP (video și de control al accesului) conectate la rețeaua dvs., pe baza producătorului și a proprietăților de rețea ale acestora (port de detectare, interval de adrese IP, parolă etc.). După ce ați detectat o unitate, o puteți adăuga la sistemul dumneavoastră.

- Instrumentul de înscriere a unității se deschide automat după *Asistentul de instalare a Security Center*, cu excepția cazului în care ați dezactivat opțiunea **Deschideți instrumentul de înscriere a unității după expert**.
- Atunci când adăugați unități de control al accesului, numai unitățile HID și Synergis™ pot fi înrolate cu instrumentul de înrolare a unităților. Pentru detalii complete privind modul de înscriere a unităților Synergis, consultați *Ghidul de configurare a dispozitivelor Synergis™*.

Deschiderea Instrumentului de înscriere a unității

Există trei moduri de a deschide instrumentul de înscriere a unităților.

Procedură

- Efectuați una dintre următoarele:
 - Din pagina de pornire a SV Control Panel, dați clic pe **+ Înscriere camere și controlere**.
 - Din pagina de pornire a SV Control Panel dați clic pe pictograma **Config Tool**, apoi pe **Tasks > Unit enrollment**.
 - De pe pagina de pornire din SV Control Panel, dați clic pe pictograma **Config Tool**, apoi dați clic pe pictograma **Adăugați starea unității** din bara de notificare a Config Tool.



Configurarea setărilor de înscriere a unității

Puteți utiliza butonul **Setări și producători** din instrumentul Înscriere unități pentru a specifica ce producători să includeți atunci când căutați unități noi. De asemenea, puteți configura setările de detectare pentru unități și puteți specifica numele de utilizator și parolele pentru unități, astfel încât acestea să poată fi înregistrate cu ușurință.


Procedură

- 1 De pe pagina de pornire, dați clic pe **Instrumente > Înscriere unitate**.
- 2 În caseta de dialog *Înrolare unitate*, dați clic pe **Setare și producători** (⚙️).
- 3 Utilizați opțiunea **Refuzați autentificarea de bază** de a activa sau dezactiva autentificarea de bază (doar unități video). Acest lucru este util dacă ați dezactivat autentificarea de bază în Security Center InstallShield, dar trebuie să o reporniți pentru a efectua o actualizare de firmware sau pentru a înscrie o cameră care acceptă doar autentificarea de bază. Pentru a activa din nou autentificarea de bază, trebuie să comutați opțiunea **Refuzați autentificarea de bază** la **Oprit**.

Notă: Această opțiune este disponibilă doar pentru utilizatorii cu privilegii de administrator.

- 4 Dați clic pe **Adaugă producător** (+) pentru a adăuga un producător la lista de unități care vor fi detectate.


Pentru a șterge un producător din listă, selectați-l și dați clic pe ✖️.

- 5 Configurați setările individuale pentru toți producătorii pe care i-ați adăugat. Pentru a face acest lucru, selectați producătorul și dați clic pe .
- IMPORTANT:** Trebuie să introduceți numele de utilizator și parola corecte pentru ca unitatea să se înscrie corect.
- 6 (Opțional) Eliminați unitățile din lista unităților ignorate (vezi [Eliminarea unităților din lista de unități ignorate](#), pagină 31).
- 7 Dați clic pe **Salvare**.

Se adaugă unități

După ce au fost detectate noi unități, puteți utiliza instrumentul de înscriere a unităților pentru a le adăuga în sistem.

Procedură

- 1 De pe pagina de pornire, dați clic pe **Instrumente > Înscriere unitate**.
- 2 Există trei moduri de a adăuga unități nou detectate:
 - Adăugați toate noile unități detectate în același timp, dând clic pe butonul **Adaugă toate**  din partea dreaptă jos a casetei de dialog.
 - Dați clic pe o singură unitate din listă, apoi dați clic pe **Adăugare** în coloana **Stare**.
 - Dați clic dreapta pe o singură unitate din listă și dați clic pe **Adăugare sau Adăugare unitate**

Atunci când o unitate video nu are numele de utilizator și parola corecte, **Stare** pentru unitatea respectivă va fi afișat ca **Conectare greșită** și vi se va solicita să introduceți informațiile corecte atunci când adăugați unitatea. Dacă doriți să utilizați același nume de utilizator și aceeași parolă pentru toate camerele din sistem, selectați opțiunea **Salvare ca autentificare implicită pentru toți producătorii**.

De asemenea, puteți adăuga o unitate manual, dând clic pe butonul **Adăugare manuală** din partea de jos a casetei de dialog *Instrument de înscriere unitate*.

Notă:

- Pentru unitățile video, dacă camera adăugată este un codificator cu mai multe fluxuri disponibile, fiecare flux este adăugat cu șirul *Camera - n* adăugat la numele camerei, *n* reprezentând numărul fluxului. Pentru o cameră IP cu un singur flux disponibil, numele camerei nu este modificat.
- Dacă adăugați un SharpV, în mod implicit, unitățile de cameră includ un certificat auto-semnat care utilizează numele comun al SharpV (de exemplu, SharpV12345). Pentru a adăuga SharpV la Archiver, trebuie să generați un nou certificat (semnat sau auto-semnat) care utilizează adresa IP a camerei în loc de numele comun.

Golirea unităților adăugate

Puteți șterge unitățile care au fost deja adăugate în sistem, astfel încât acestea să nu fie afișate de fiecare dată când utilizați Instrumentul de înscriere a unităților pentru a detecta unitățile din sistem.

Ce ar trebui să știți

Opțiunea **Eliminare finalizată** din instrumentul de înscriere a unității este permanentă, nu poate fi anulată.

Procedură

- 1 Adăugați unitățile detectate dorite la sistemul dumneavoastră, consultați [Se adaugă unități](#), pagină 30.
- 2 După ce au fost adăugate unitățile, dați clic pe **Eliminare finalizată**.
Orice unitate care are **Adăugat** afișat în coloana **Stare** va fi ștersă din lista de unități detectate.

Ignorarea unităților

Puteți alege să ignorați unitățile, astfel încât acestea să nu apară în lista de unități detectate din instrumentul de înscriere a unităților.

Procedură

- 1 De pe pagina de pornire, dați clic pe **Instrumente** > **Înscriere unitate**.
Instrumentul de înscriere a unităților se deschide cu lista unităților care au fost detectate în sistem.
- 2 Dați clic dreapta pe unitatea pe care doriți să o ignorați și selectați **Ignorare**.
Unitatea este eliminată din listă și va fi ignorată atunci când Instrumentul de înscriere a unităților detectează noi unități. Pentru informații privind eliminarea unei unități din lista unităților ignorate, vezi [Eliminarea unităților din lista de unități ignorate](#), pagină 31.

Eliminarea unităților din lista de unități ignorate

Puteți elimina o unitate din lista unităților ignorate, astfel încât aceasta să nu fie ignorată atunci când instrumentul de înscriere a unităților efectuează o detectare.

Procedură

- 1 De pe pagina de pornire, dați clic pe **Instrumente** > **Înscriere unitate**.
- 2 În colțul din dreapta sus al casetei de dialog *Înscriere unitate*, dați clic pe **Setare și producători** (⚙️).
- 3 Dați clic pe **Unități ignorate** și dați clic pe **Îndepărtați toate unitățile ignorate**, sau puteți selecta o singură unitate și dați clic pe butonul **Îndepărtați unitatea ignorată** (✖️).

Configurarea setărilor implicite ale camerei

Din *Setări implicite cameră*, puteți modifica setările implicite de înregistrare și de calitate video aplicate tuturor camerelor controlate de Arhivar. Inițial, aceste setări sunt configurate pe pagina *Setări de calitate a camerei* din asistentul de instalare Security Center.

Ce ar trebui să știți


De asemenea, puteți aplica setările video și de înregistrare pentru o cameră în Config Tool folosind fila **Video și înregistrare** a unității. Setările efectuate pentru o cameră individuală au prioritate față de setările care sunt aplicate în asistentul de instalare Security Center sau pe pagina *Setări implicite ale camerei*.

Procedură

- 1 De pe pagina de pornire a Config Tool, deschideți comanda *Video*.
- 2 Selectați rolul Arhivar, apoi dați clic pe fila **Setări implicite cameră**.
- 3 La **Calitatea video (aceeași pentru toate arhivatoarele)**, configurați următoarele:

- **Rezoluție:**
 - **Mare:** 1280x720 și mai mare
 - **Standard:** Mai mult de 320x240 și mai puțin de 1280x720
 - **Redus:** 320x240 și mai mic
 - **Implicit:** Setările implicite ale producătorului

Camera utilizează întotdeauna cea mai mare rezoluție pe care o poate suporta din categoria aleasă. În cazul în care camera nu acceptă nicio rezoluție din categoria aleasă, aceasta utilizează cea mai mare rezoluție pe care o poate accepta din categoria următoare. De exemplu, în cazul în care camera nu poate suporta o rezoluție înaltă, aceasta utilizează cea mai mare rezoluție pe care o poate suporta din grupul Standard.

- 4 La **Înregistrare**, dați clic pe  pentru a adăuga un program.
Programele disponibile includ:
 - Programele care au fost create cu ajutorul vizualizării **Programe** din task-ul *Sistem*.
 - Un program personalizat, dacă a fost creat unul în asistentul de instalare Security Center.
- 5 Din meniul derulant **Mod**, selectați un mod pentru programul de înregistrare:
 - **Oprit:** Înregistrarea este oprită
 - **Continuu:** Camerele înregistrează continuu. Aceasta este setarea implicită.
 - **La mișcare/manual.:** Camerele înregistrează atunci când sunt declanșate de o acțiune (cum ar fi Pornire înregistrare, Adăugare marcaj sau Declanșare alarmă), de detectarea mișcării sau manual de către un utilizator.
 - **Manual:** Camerele înregistrează atunci când sunt declanșate de o acțiune (cum ar fi Pornire înregistrare, Adăugare marcaj sau Declanșare alarmă) sau manual de către un utilizator.

Notă: Când se utilizează setarea **Manual**, atunci mișcarea nu declanșează nicio înregistrare.

 - **Personalizat:** Puteți seta un program pentru momentul în care are loc înregistrarea.

6 Configurați următoarele opțiuni:

- **Înregistrare audio:** Activați această opțiune atunci când doriți să înregistrați audio împreună cu video. O entitate de microfon trebuie atașată la camerele dvs. ca această opțiune să funcționeze.
- **Arhivare duplicitară:** Activați această opțiune atunci când doriți ca atât serverul principal, cât și cel secundar să arhiveze video în același timp. Această setare este eficientă doar dacă este configurat transferul.
- **Curățare automată:** Activați această opțiune atunci când doriți să ștergeți înregistrările video după un anumit număr de zile. Înregistrarea video este ștearsă indiferent dacă spațiul de stocare al arhivarului este plin sau nu.
- **Durată de înregistrare înainte de un eveniment:** Utilizați cursorul pentru a seta numărul de secunde pe care doriți să le înregistrați înainte de un eveniment. Această memorie tampon este salvată de fiecare dată când pornește înregistrarea, asigurând faptul că întregul conținut semnalat de înregistrare este capta și în înregistrarea video.
- **Durata de înregistrare după o mișcare:** Setați numărul de secunde în care doriți ca înregistrarea să continue după un eveniment de mișcare. În această perioadă, utilizatorul un poate opri înregistrarea.
- **Lungime implicită înregistrare manuală :** Setați numărul de minute pe care doriți să le înregistrați atunci când un utilizator începe înregistrarea. Utilizatorul poate opri înregistrarea în orice moment înainte de expirarea duratei. Această valoare este, de asemenea, utilizată de acțiunea Start recording (Începe înregistrarea), atunci când este selectată durata implicită de înregistrare.


7 Dați clic pe **Aplicare**.8 Dacă doriți să aplicați noile setări la toate camerele existente, dați clic pe **Da**.**Subiecte conexe**


[Activarea funcțiilor video și de control al accesului din Security Center](#), pagină 26

Crearea de programe de înregistrare personalizate

Creați programe de înregistrare personalizate din asistentul de instalare al Security Center pentru a permite camerelor să înregistreze în diferite moduri de înregistrare pentru un anumit interval de timp.

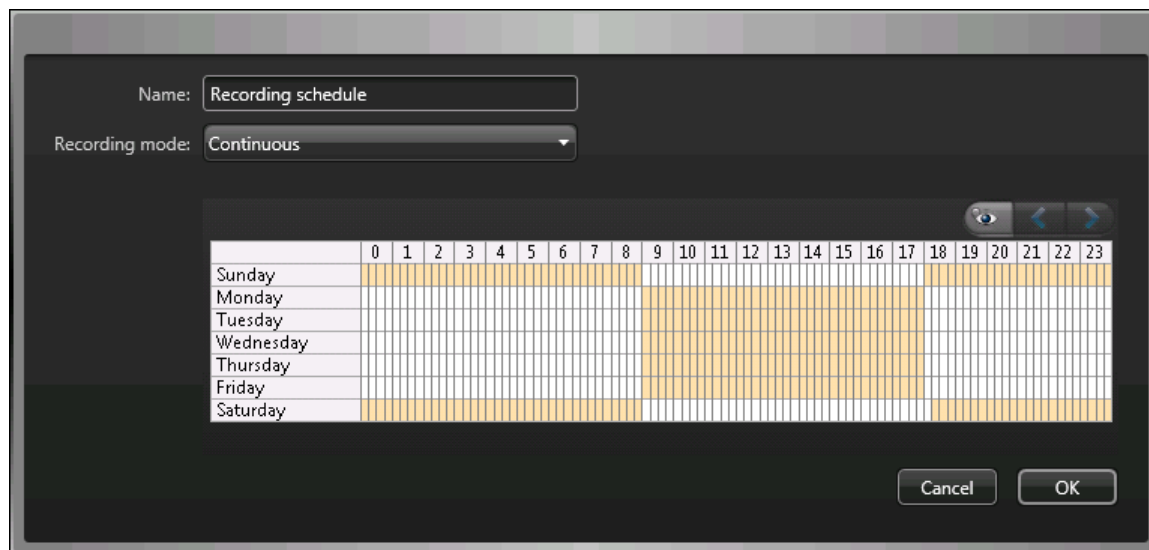
Procedură

- 1 Pe pagina *Setări de înregistrare*, dați clic pe  de la **Program de înregistrare**.
- 2 Introduceți un nume pentru noul program.
- 3 Din lista **Mod de înregistrare**, selectați unul dintre următoarele:
 - **Oprit:** Înregistrarea este oprită
 - **Continuu:** Camerele înregistrează continuu. Aceasta este setarea implicită.
 - **La mișcare/manual.:** Camerele înregistrează atunci când sunt declanșate de o acțiune (cum ar fi Pornire înregistrare, Adăugare marcaj sau Declanșare alarmă), de detectarea mișcării sau manual de către un utilizator.
 - **Manual:** Camerele înregistrează atunci când sunt declanșate de o acțiune (cum ar fi Pornire înregistrare, Adăugare marcaj sau Declanșare alarmă) sau manual de către un utilizator.
- 4 Pentru fiecare zi a săptămânii, specificați intervalul de timp pentru înregistrare:
 - Dați clic și trageți pentru a selecta un bloc de timp.
 - Dați clic dreapta și trageți pentru a șterge un bloc de timp.
 - Folosiți tastele cursor pentru a vă deplasa pe linia de timp de 24 de ore.

SFAT: Pentru a trece la modul de înaltă rezoluție, în care fiecare bloc reprezintă 1 minut, dați clic pe 

Exemplu

Exemplul următor prezintă un program în care înregistrarea are loc continuu de la 18:00 la 9:00 în weekend și de la 9:00 la 17:00 în zilele lucrătoare.



Subiecte conexe

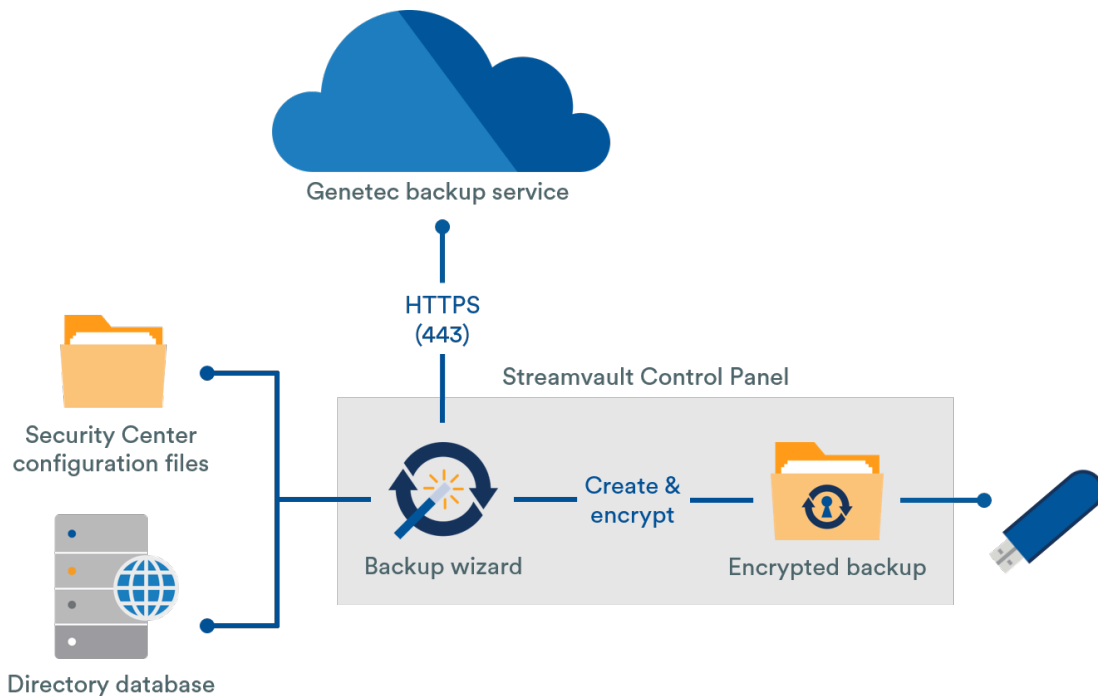
[Activarea funcțiilor video și de control al accesului din Security Center](#), pagină 26

Despre backup și restaurare

Cu ajutorul SV Control Panel, puteți face o copie de rezervă sigură a bazei de date Directory și a fișierelor de configurare. Ulterior, le puteți restaura la același ID de sistem în cazul unei defecțiuni de sistem sau al unei actualizări hardware.

Cum funcționează backup-ul și restaurarea în SV Control Panel

Creați copii de rezervă ale bazei de date Directory și ale fișierelor de configurare și le stocați în cloud sau local. Următoarea diagramă de arhitectură prezintă modul în care funcționează backup-ul în SV Control Panel:



Beneficiile copiei de rezervă și de restaurare

-
- Restaurați cu ușurință oricare dintre cele cinci copii de rezervă în cloud sau oricare dintre copiile de rezervă locale la același ID de sistem utilizând expertul *Restaurare*.
- Toate fișierele copie de rezervă
- Sistemul se blochează după cinci încercări eșuate de conectare.
- Nu este necesar să fiți înscris în programul Genetec Advantage pentru a utiliza această funcție.

Limitări ale copiei de rezervă și ale restaurării

- O copie de rezervă exclude fișierele de licență, arhivele video sau alte baze de date.
- Nu puteți restaura o copie de rezervă pe o versiune anterioară a Security Center. De exemplu, nu puteți restaura o copie de rezervă de la un sistem Security Center 5.10 la un sistem Security Center 5.9.
- Nu puteți restaura fișierele de configurare dacă restaurați între versiunile majore ale Security Center. De exemplu, nu puteți restaura fișierele de configurare dintr-o copie de rezervă a sistemului Security Center 5.9 pe un sistem Security Center 5.10.

Subiecte conexe

[Realizarea unei icopii de rezervă a bazei de date Directory](#), pagină 36

[Restaurarea bazei de date Directory](#), pagină 37

Realizarea unei icopii de rezervă a bazei de date Directory

Puteți utiliza backup și restaurare pentru a salva în siguranță baza de date Directory și fișierele de configurare. Copierea de rezervă și restaurarea ușurează configurarea sistemului după o actualizare hardware și vă poate restaura configurațiile după o defecțiune a sistemului.

Înainte de a începe

Asigurați-vă că sunt respectate următoarele:

- Este instalat Security Center 5.9 sau o versiune ulterioară.
- Genetec™ Server rulează.
- Aveți o licență valabilă și activă.

Ce ar trebui să știți

- Doar administratorii pot efectua o copie de rezervă, iar toate copiile de rezervă în cloud trebuie să fie autentificate.

Procedură

- 1 În SV Control Panel, dați clic pe fila **Configurare**.
- 2 La *Directory copie de rezervă/restaurare și configurații*, dați clic pe **Expert copie de rezervă > Mai departe**.
- 3 Pe pagina *Metoda pentru copia de rezervă*, selectați fie **Cloud**, fie **Local**, apoi dați clic pe **Mai departe**.
 - Dacă ați selectat **Cloud**, faceți următoarele:
 - a. Pe pagina *Autentificare*, introduceți fie ID-ul de sistem, fie acreditările GTAP pentru a autentifica copia de rezervă.
Notă: După ce v-ați introdus acreditările pentru prima dată, nu vi se va mai cere din nou pentru viitoarele copii de rezervă.
 - b. Pe pagina *Securitate*, selectați una dintre următoarele două opțiuni:
 - **Lăsați Genetec să-mi gestioneze securitatea:** Nu este necesar să furnizați o parolă. Serviciul de backup în cloud de la Genetec Inc. vă criptează datele.
 - **Utilizați propria parolă:** Creați și să vă rețineți propria parolă pentru a o utiliza ulterior pentru criptarea fișierelor de backup.
IMPORTANT: Dacă vă pierdeți sau uitați parola, Genetec Inc. nu poate recupera parola pierdută.
 - Dacă ați selectat **Local**, procedați după cum urmează:
 - a. Pe pagina *Dosar de destinație*, introduceți un nume pentru copia de rezervă și navigați până la dosarul în care doriți să stocați copia de rezervă.
 - b. Pe pagina *Securitate*, creați o parolă pentru a vă cripta fișierul de backup. Și puteți selecta **Nu cripta copia de rezervă**, deși nu este recomandat.
- 4 Urmăriți restul pașilor din expertul pentru a finaliza copia de rezervă.

Subiecte conexe

[Despre backup și restaurare](#), pagină 35

[Restaurarea bazei de date Directory](#), pagină 37

Restaurarea bazei de date Directory

Dacă ați făcut o copie de rezervă a bazei de date Directory și a fișierelor de configurare folosind funcția copie de rezervă și de restaurare din SV Control Panel, puteți restaura cu ușurință fișierele de rezervă la același ID de sistem. Fișierele de rezervă pot fi restaurate în cazul unei defecțiuni de sistem sau al unei actualizări hardware.

Înainte de a începe

Asigurați-vă că sunt respectate următoarele:

- Este instalat Security Center 5.9 sau o versiune ulterioară.
- Genetec™ Server rulează.
- Aveți o licență valabilă și activă.

Ce ar trebui să știți

- Dacă ați făcut o copie de rezervă a fișierelor în cloud, puteți restaura oricare dintre ultimele cinci copii de rezervă la același ID de sistem.
- Dacă ați făcut o copie de rezervă a fișierelor la nivel local, puteți restaura oricare dintre copiile de rezervă la același ID de sistem.
- Dacă v-ați creat propria parolă pentru fișierele copie de rezervă criptate în timpul procesului de backup, veți avea nevoie de ea pentru a vă restaura fișierele.

Procedură

- 1 În SV Control Panel, dați clic pe fila **Configurare**.
- 2 La *Directorul copie de rezervă/restaurare și configurații*, dați clic pe **Expert de restaurare > Mai departe**.
- 3 Pe pagina *Metoda de restaurare*, selectați fie **Cloud**, fie **Local**.
Dacă ați selectat Cloud, pe pagina *Autentificare*, introduceți fie ID-ul de sistem, fie acreditările GTAP, în funcție de cel pe care l-ați utilizat pentru autentificarea copiei de rezervă. Dacă vă folosiți acreditările GTAP, vi se trimite un cod de activare pe adresa de e-mail.
- 4 Pe pagina *Selecția copie de rezervă*, selectați fișierul pe care doriți să îl restaurați în sistem.
- 5 Pe pagina *Restore*, dacă ați ales să creați o parolă în timpul procesului de backup, trebuie să introduceți parola aici.
- 6 Urmați restul pașilor din asistentul pentru a finaliza procesul de restaurare.

Subiecte conexe

[Realizarea unei icopii de rezervă a bazei de date Directory](#), pagină 36

[Despre backup și restaurare](#), pagină 35

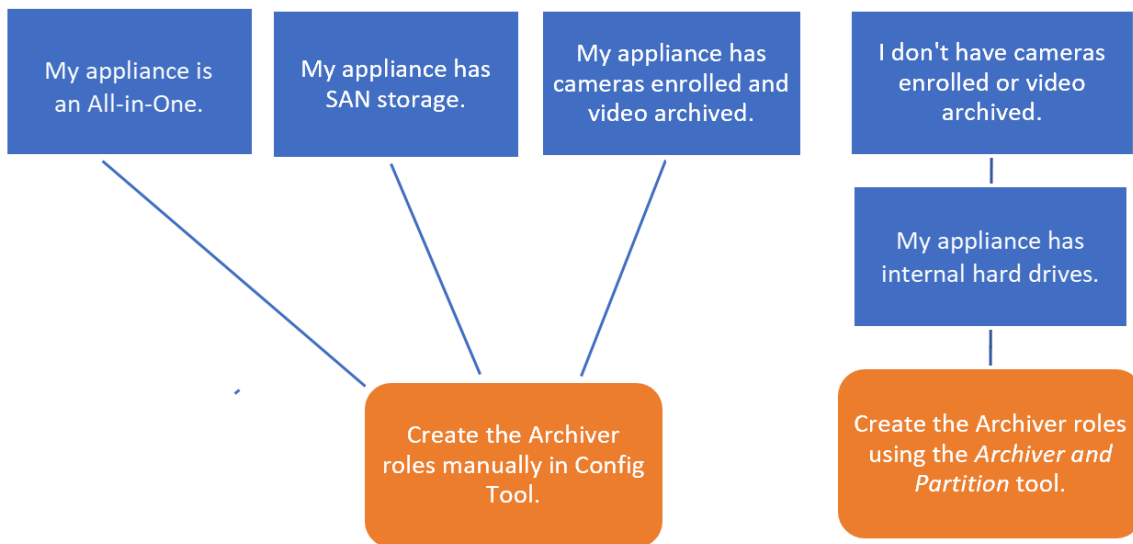
Alegerea metodei de creare a rolurilor Archiver și partițiilor

Pentru a vă configura dispozitivul pentru numărul de camere și pentru utilizarea lățimii de bandă preconizate, trebuie să creați suficiente roluri Archiver. În funcție de tipul și starea dispozitivului dumneavoastră, puteți alege între două metode.

- [Utilizând instrumentul Roluri Archiver și partiții.](#)
- [Crearea manuală a partițiilor și a rolurilor Archiver.](#)

Alegerea metodei pentru situația dumneavoastră

Utilizați următorul arbore de decizie pentru a vă ajuta să decideți ce metodă să utilizați:



Despre instrumentul Roluri Archiver și partiții

Puteți accesa instrumentul Roluri și partiții de arhivare din SV Control Panel. Instrumentul calculează câte roluri Archiver aveți nevoie pe baza numărului de camere pe care intenționați să le implementați și a lățimii de bandă preconizate.

Acest instrument este disponibil doar pe modelele Streamvault™ care au un hard disk intern. Dacă configurați un dispozitiv de stocare extern, precum SAN pe un dispozitiv Streamvault™ din seria SV-7000EX, urmați pașii de la [Adăugarea manuală a partițiilor și a rolurilor Archiver](#), pagină 40.

Atunci când instrumentul creează partiții, toate volumele locale, cu excepția C: sunt șterse, iar rolurile Archiver existente și camerele înscrise sunt eliminate din Security Center. Deci, dacă dispozitivul dvs. are camere și înregistrări video pe care doriți să le păstrați, [adăugați manual partițiile și rolurile Archiver](#).

Adăugarea rolurilor Archiver în SV Control Panel

Utilizați instrumentul Roluri și partiții de Archiver pentru a adăuga suficiente roluri de Archiver pentru a susține traficul video preconizat. Acest instrument este disponibil pe dispozitivele Archiver din seriile Streamvault™ 1000, 2000 și 4000.

Înainte de a începe

- [Alegeți metoda adecvată pentru crearea rolurilor Archiver și partițiilor.](#)
- Faceți o copie de rezervă a datelor importante de pe unitatea pe care intenționați să o partiționați.
ATENȚIE: Instrumentul Roluri Archiver și partiții poate șterge datele existente, inclusiv configurația rolului Archiver și toate fișierele de pe unitatea D:.

Procedură

- 1 În SV Control Panel, dați clic pe fila **Configurare**.
- 2 La *Roluri Arhivar și partiții*, dați clic pe **Configurare**.
Se deschide caseta de dialog *Roluri Archiver și partiții*.
- 3 Selectați una dintre următoarele opțiuni pentru a configura numărul de roluri Archiver și partiții:
 - Pentru a permite instrumentului să calculeze numărul de roluri, numărul de partiții și dimensiunea partiției de care aveți nevoie, selectați **Scenariu sugerat**. Introduceți numărul de camere pe care vă așteptați să le implementați și debitul preconizat al fiecărei camere.
 - Pentru a specifica numărul de roluri și partiții Archiver de creat, selectați **Scenariu personalizat**. Introduceți numărul de roluri de Archiver, numărul de partiții și dimensiunea partiției.

Numărul de partiții trebuie să fie un multiplu al numărului de roluri Archiver.

ATENȚIE: Fișierele de pe unitatea pe care o partiționați sunt șterse.
- 4 Dați clic pe **Creați partiții și roluri**.

Archiver Roles and Partitions

An Archiver role can support:

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

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

- 400 cameras
- 400 Mbps

Suggested scenario

Number of cameras: 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

Create partitions/roles

- 5 În fereastra *Avertizare*, selectați cazul de selectare pentru a confirma că doriți să continuați.
- 6 Dați clic pe **OK**.
Se deschide fereastra *Rezultat* și afișează numele și locațiile rolurilor Archiver și partițiilor. Fiecărui rol Archiver i se atribuie automat o literă de unitate.

Adăugarea manuală a partițiilor și a rolurilor Archiver

Pentru a configura dispozitivul SV-7000E sau SV-300E all-in-one pentru prima dată, trebuie să creați manual partiții. Puteți adăuga manual și roluri Archiver la un dispozitiv care are deja date, astfel încât datele să nu se piardă.

Înainte de a începe

Alegeți o metodă de creare a partițiilor pe dispozitivul dvs.

Ce ar trebui să știți

Formatarea unui volum șterge datele de pe partiție. Pentru a păstra datele, micșorați volumul și apoi creați volume noi.

Procedură

- 1 Dacă dispozitivul are deja camere înregistrate, înregistrări video arhivate sau date de control al accesului, procedați după cum urmează:
 - a) [Efectuați o copie de rezervă a bazei de date Directory folosind SV Control Panel.](#)
 - b) Generați un raport *Configurație cameră* pentru a obține o imagine instantanee a configurației actuale a camerei. Pentru informații, consultați [Vizualizarea setărilor camerei](#) pe TechDoc Hub.
- 2 Creați volumele de care aveți nevoie pentru rolurile Archiver pe care intenționați să le creați pe dispozitiv.
 - Pe dispozitivele care se conectează la stocare SAN, cum ar fi dispozitivele din seria SV-7000EX, creați un număr de unitate logică (LUN) pentru fiecare rol Archiver.
 - Pe dispozitivele care au unități de stocare interne, precum SV-1000E, SV-2000E și SV-4000E, utilizați instrumentul Windows *Disk Management* pentru a configura volumele.

3 În Security Center, creați un rol de Archiver:

- De pe pagina de pornire a Config Tool, deschideți comanda *Sistem* și dați clic pe vizualizarea **Roluri**.
- Faceți clic pe **Adaugă o entitate** și selectați **Archiver**.
Se deschide expertul de configurare a rolului Archiver.
- Pe pagina *Informații specifice*, introduceți un nume pentru **baza de date** a rolului Archiver și dați clic pe **Mai departe**.
Fiecare rol Archiver trebuie să aibă o bază de date dedicată.

Creating a role: Archiver

Specific info

Basic information

Creation summary

Entity creation outcome

Database server: (local)\SQLEXPRESS

Database: Archiver5

- Pe secțiunea **Informații de bază**, introduceți **Numele entității** și dați clic pe **Mai departe**.
Cea mai bună practică este ca numele bazei de date a rolului Archiver să se potrivească cu numele entității.

Creating a role: Archiver

Specific info

Basic information

Creation summary

Entity creation outcome

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

Entity name: Archiver5

Entity description:

- Verificați dacă informațiile de pe pagina *Rezumat creare* sunt corecte și dați clic pe **Creare**.

4 Configurați rolul Archiver.

- În browserul de entități, selectați noul rol Archiver și dați clic pe **Resurse**.
- Dați clic pentru a extinde secțiunea *Server* și selectați un card de interfață a rețelei (NIC) din lista **Card de rețea**.
Toate rolurile Archiver trebuie să utilizeze aceeași NIC.


Server: VM9084

Network card: 10.2.110.157 - Ethernet0

RTSP port: 558 and 608 Telnet port: 5605

- La *Înregistrare*, selectați sau creați un **Grup de unități** sau **Localizare de rețea** pentru rolul Archiver.
Fiecare rol Archiver are nevoie de o locație de înregistrare dedicată. Dacă arhivarul A scrie pe discurile A, B și C, atunci arhivarul B ar trebui să scrie pe discurile D, E și F. Un rol poate deține mai multe partiții, dar două roluri nu ar trebui să utilizeze niciodată aceeași partiție.
- Dați clic pe **Aplicare**.

5 Repetați pașii 3 și 4 pentru a crea fiecare rol Archiver.

- 6 Adăugați-vă camerele la rolul lor de Archiver desemnat:
- a) De pe pagina de pornire a Config Tool, deschideți comanda *Video*.
 - b) În browserul Entitate, selectați rolul Archiver căruia doriți să îi atribuiți camera, apoi dați clic pe **Unitate video** .
 - c) În caseta de dialog care se deschide, introduceți informațiile necesare referitoare la cameră și faceți clic pe **OK**.
Notă: Este nevoie de câteva secunde pentru a adăuga camerele. În cazul în care rolul nu poate adăuga o cameră în intervalul de timp dat, se indică o stare de eșec, iar camera este eliminată.
 - d) Dați clic pe **Aplicare**.

Criptarea unității sistemului de operare

Pentru a păstra în siguranță dispozitivul Streamvault™ și parola de administrator Windows, trebuie să criptați unitatea sistemului de operare (C:) cu BitLocker.

Înainte de a începe

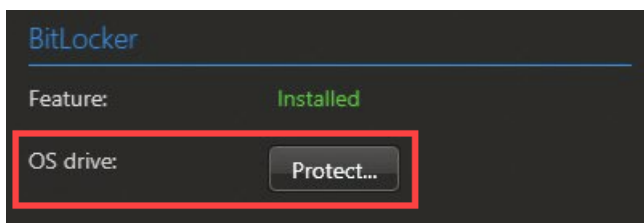
Când unitatea sistemului de operare este criptată cu BitLocker, cheia de decriptare este salvată pe un cip Trusted Platform Module (TPM) situat pe placa de sistem a dispozitivului Streamvault. Dacă unitatea sistemului de operare ar fi scoasă sau placa de sistem ar fi înlocuită, informațiile de pe unitatea sistemului de operare s-ar pierde. Unitatea sistemului de operare nu ar putea accesa cheia de decriptare de pe TPM. Puteți crea o cheie de recuperare care poate fi utilizată pentru a decripta unitatea în aceste scenarii. Fără o cheie de recuperare, dispozitivul trebuie re-creat și software-ul trebuie reinstalat.

Discul de stocare este utilizat în principal pentru stocarea arhivelor video și nu este criptat cu BitLocker. Puteți utiliza funcțiile Centrului de securitate pentru a cripta arhivele video în repaus.

Notă: Funcția BitLocker este disponibilă începând cu SV Control Panel 3.2. Funcția introduce și o actualizare a profilului de consolidare pentru [aparate cu capacități de gestionare a securității](#). Puteți obține această actualizare descărcând [Serviciul Streamvault](#) din Serviciul de actualizare Genetec™ (GUS) sau GTAP. Pentru a beneficia pe deplin de funcția BitLocker, vă încurajăm să criptați unitatea sistemului de operare și să aplicați actualizarea profilului de securizare, dacă este cazul.

Procedură

- 1 În Panoul de control SV, faceți clic pe **Securitate** filă.
- 2 În *BitLocker* secțiune, faceți clic **Proteja** lângă **Unitate de sistem de operare** domeniu.



Notă: Dacă unitatea sistemului de operare este deja criptată, **Proteja** butonul este înlocuit de un *Protejat* statut.

- 3 Când vi se întreabă dacă doriți să activați BitLocker, faceți clic pe **Da**.
Unitatea sistemului de operare este criptată, cheia de decriptare este salvată pe TPM și este creată o cheie de recuperare. În mod implicit, cheia de recuperare este salvată pe o unitate de date fixă. Dacă nu există o unitate de date fixă, cum ar fi pe o stație de lucru, cheia de recuperare este salvată pe un stick USB.
IMPORTANT: Dacă salvați cheia de recuperare pe o unitate de date fixă, asigurați-vă că mutați cheia într-o locație sigură și o ștergeți din dispozitiv.
- 4 (Opțional) Dacă nu există o unitate de date fixă sau un stick USB, puteți alege dacă doriți să continuați cu criptarea fără a crea o cheie de recuperare. Efectuați una dintre următoarele:
 - Clic **Da** pentru a continua fără a crea o cheie de recuperare.
 - Clic **Nu** pentru a anula criptarea.

Notă: Dacă alegeți să nu creați o cheie de recuperare, puteți crea una ulterior. Pentru mai multe informații, consultați [Crearea unei chei de recuperare](#), pagină 44.

Crearea unei chei de recuperare

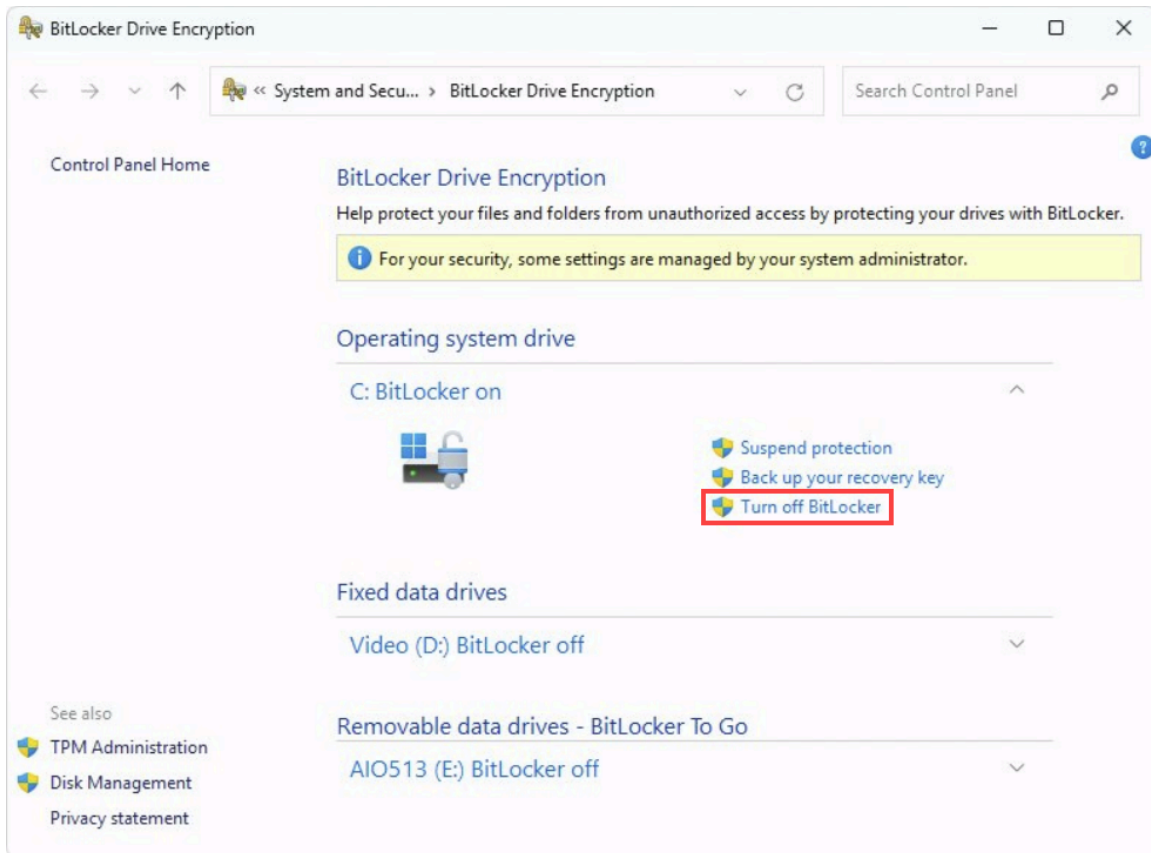
Dacă ați criptat unitatea sistemului de operare de pe dispozitivul Streamvault™ cu BitLocker, dar nu ați salvat o cheie de recuperare, puteți crea una cu Windows BitLocker Drive Encryption.

Ce ar trebui să știți

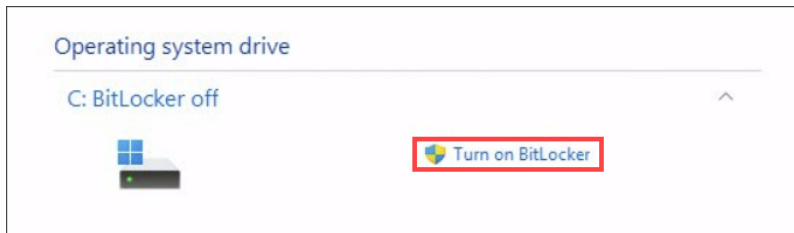
Această procedură presupune că ați criptat unitatea sistemului de operare prin intermediul Panoului de control SV.

Procedură

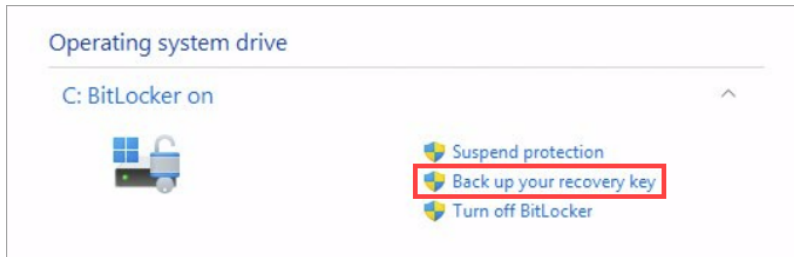
- 1 Din meniul Start din Windows, tastați **BitLocker** și selectați **Gestionați BitLocker** din rezultate. Cel/Cea/Cei/Cele *Cripare unitate BitLocker* se deschide fereastra. Sunt listate toate unitățile conectate la dispozitiv.
- 2 În *Unitatea sistemului de operare* secțiune, faceți clic **Dezactivați BitLocker** și așteptați ca unitatea sistemului de operare să fie decriptată. Acest proces durează câteva minute.



- 3 După ce unitatea sistemului de operare este decriptată, faceți clic pe **Activați BitLocker** și așteptați ca unitatea sistemului de operare să fie recriptată cu BitLocker.



- 4 După ce unitatea sistemului de operare este criptată, faceți clic pe **Faceți o copie de rezervă a cheii de recuperare** lângă unitatea sistemului de operare (C:).

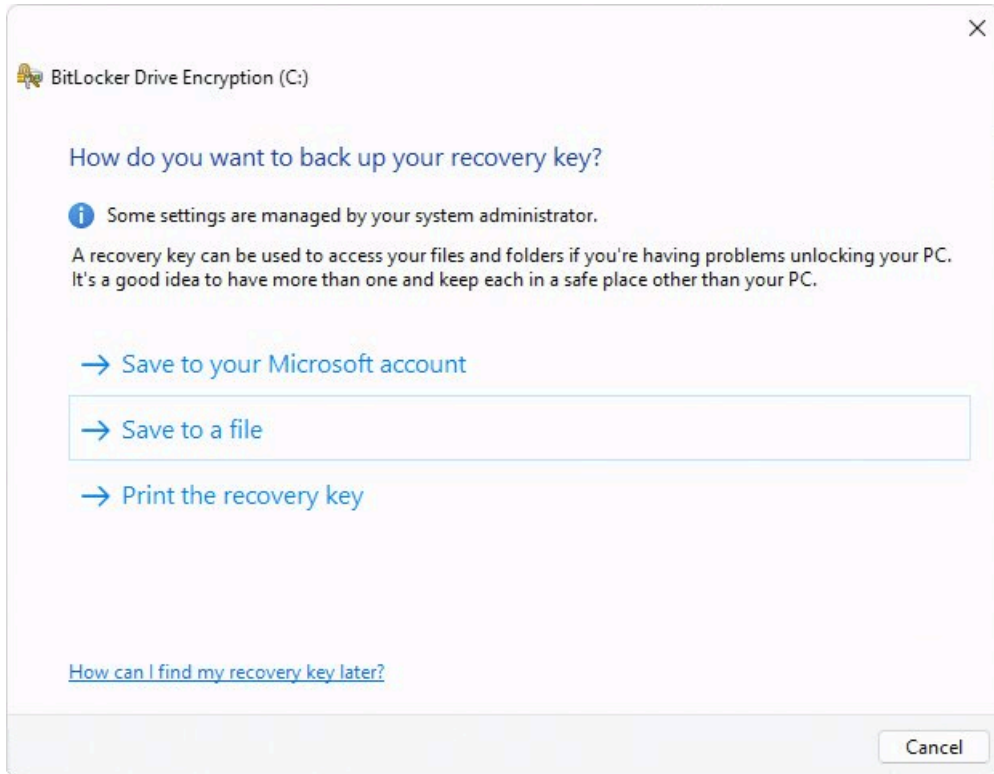


Cel/Cea/Cei/Cele *Cripare unitate BitLocker* se deschide expertul.

5 Alegeți cum doriți să creați o copie de rezervă a cheii de recuperare:

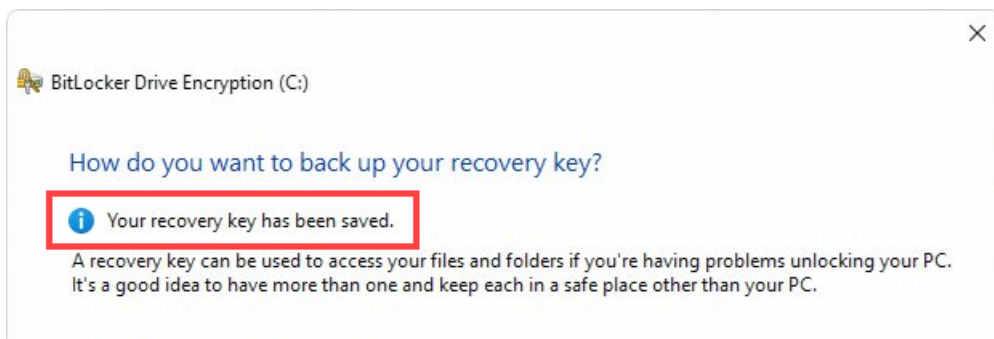
- **Salvați în contul dvs. Microsoft:** Salvați cheia de recuperare în *biblioteca de chei de recuperare* din contul dvs. Microsoft.
- **Salvați într-un fișier:** Salvați cheia de recuperare ca fișier text simplu pe o unitate de date fixă necriptată de pe dispozitiv sau pe o cheie USB.
- **Imprimați cheia de recuperare:** Imprimați o copie fizică a cheii de recuperare.

Notă: Dacă selectați **Salvați într-un fișier**, asigurați-vă că aveți la dispoziție o unitate de date fixă sau un stick USB pentru a salva cheia de recuperare.



6 Dacă salvați cheia de recuperare într-un fișier, selectați locația în care doriți să salvați cheia și faceți clic pe **Salva**.

Vei fi notificat(ă) că recuperarea a fost salvată.



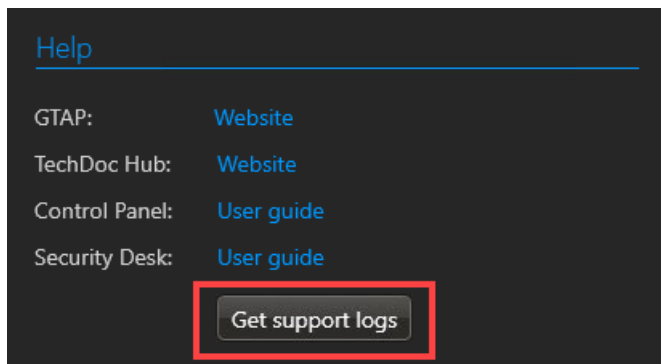
7 Clic **Termina** pentru a ieși din expert.

Colectarea jurnalelor de asistență

Centrul de asistență tehnică Genetec™ (GTAC) poate utiliza jurnalele Streamvault™ și alte jurnale de aplicații pentru a depana problemele dispozitivului dumneavoastră. Puteți descărca aceste jurnale de asistență din Panoul de control SV.

Procedură

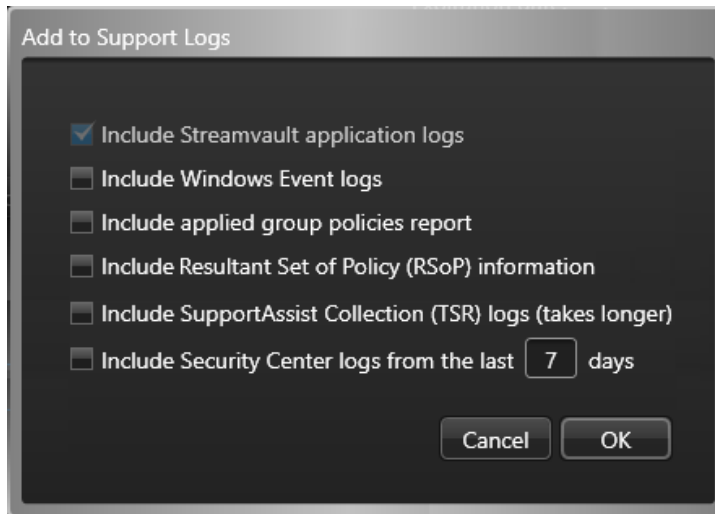
- 1 În Panoul de control SV, faceți clic pe **Despre** filă.
- 2 În *Ajutor* secțiune, faceți clic **Obțineți jurnale de asistență**.



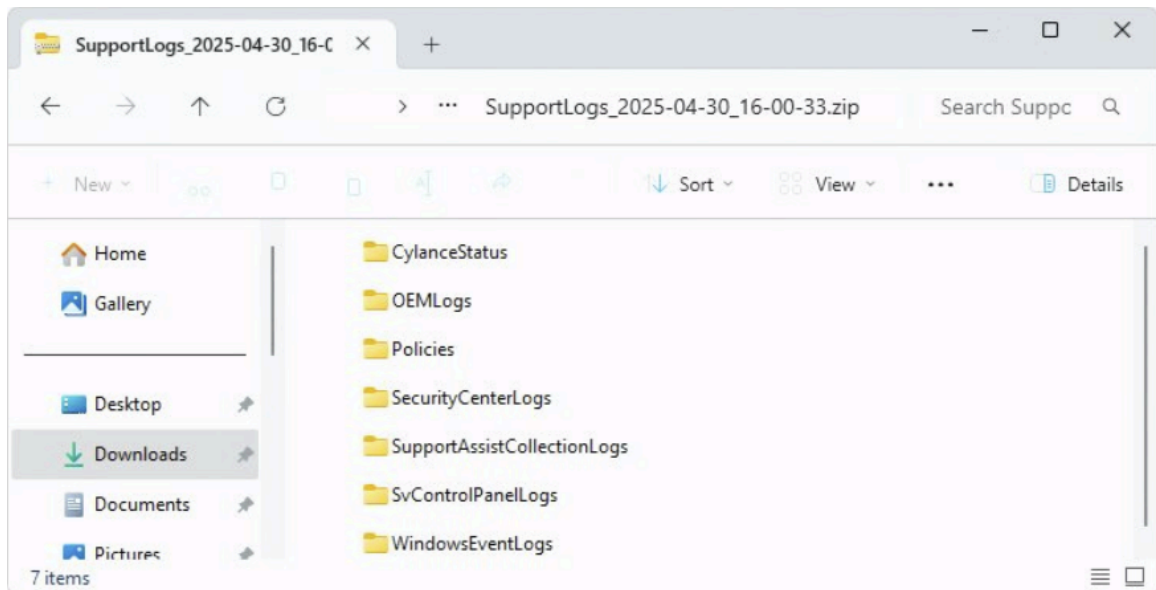
- 3 În *Adăugați la jurnalele de asistență* caseta de dialog care se deschide, selectați jurnalele pe care doriți să le descărcați:
 - **Jurnalele aplicației Streamvault:** Aceste jurnale includ fișierele jurnal Cylance, OEM, politici, Softwire și ale panoului de control SV. Această opțiune este selectată în mod implicit și nu poate fi debifată.
 - **Jurnalele de evenimente Windows:** Aceste jurnale includ evenimente de aplicație, securitate și sistem Windows.
 - **Raportul privind politicile de grup aplicate:** Acest raport este pentru sistemele care fac parte din domeniu. Raportul listează toate obiectele de politică de grup (GPO) care sunt aplicate în prezent și specifică dacă acestea sunt aplicate la nivel local sau de domeniu.
 - **Informații despre setul rezultat de politici (RSOP):** Acest raport HTML include toate setările de sistem configurate prin politicile de grup. Pentru sistemele care nu sunt conectate la un domeniu, această opțiune este selectată în mod implicit. Pentru sistemele conectate la un domeniu, această opțiune este debifată în mod implicit, deoarece raportul conține informații sensibile, cum ar fi numele domeniului, numele de gazdă al dispozitivului și așa mai departe.
 - **Jurnalele de colectare SupportAssist (TSR):** Aceste jurnale sunt pentru sistemele care pot crea o colecție SupportAssist, cunoscută și sub denumirea de Raport de asistență tehnică (TSR). Serverele Dell PowerEdge, cum ar fi serverele Streamvault din seriile 1000, 2000, 4000 și 7000, pot crea colecții

SupportAssist. Această opțiune este disponibilă numai pentru serverele Streamvault care acceptă iDRAC.

- **Jurnalele Centrului de Securitate din ultimele X zile:** În mod implicit, sunt colectate jurnalele Centrului de securitate din ultimele 7 zile. Introduceți numărul preferat de zile.



- 4 Dați clic pe **OK**.
- 5 În *Căutați folderul* caseta de dialog, selectați folderul în care doriți să salvați jurnalele și faceți clic pe **Bine**. Jurnalele dvs. de asistență sunt salvate într-un . zip pliant.



Noțiuni de bază despre plugin-ul de întreținere Streamvault

Noțiuni introductive prezintă plugin-ul Întreținerea Streamvault și oferă informații despre cum se configurează plugin-ul.

Această secțiune include următoarele subiecte:

- ["Despre plugin-ul Întreținerea Streamvault "](#), pagină 50
- ["Descărcarea și instalarea plugin-ului"](#), pagină 51
- ["Privilegii Streamvault Genetec"](#), pagină 52
- [" Crearea rolului de plugin "](#), pagină 54
- ["Configurarea unei entități monitor hardware Streamvault"](#), pagină 55
- ["Configurarea unei entități manager Streamvault"](#), pagină 59
- [" Despre fila Management "](#), pagină 62
- ["Revizuirea sănătății dispozitivului Streamvault"](#), pagină 63
- ["Coloanele panoului de raport pentru comanda hardware Streamvault"](#), pagină 64
- ["Crearea de evenimente către acțiuni pentru evenimentele de sănătate Streamvault"](#), pagină 65

Despre plugin-ul Întreținerea Streamvault

Plugin-ul Streamvault™ Maintenance este utilizat pentru a monitoriza starea de sănătate a dispozitivelor Streamvault și pentru a vă asigura că primiți notificări atunci când apar probleme.

Notă: Acest ghid se aplică pluginului Streamvault Maintenance 2.0.

Extensia Întreținerea Streamvault include următoarele componente:

- **Rolul Streamvault:** Rolul de plugin utilizat pentru a rula fie monitorul hardware, fie entitatea manager. Este necesar un rol pentru fiecare aparat Streamvault pe care trebuie să îl monitorizați.
- **Monitor hardware Streamvault™:** Entitate utilizată pentru a defini configurațiile de alertă pentru fiecare dispozitiv Streamvault.
- **Manager Streamvault™:** Entitate utilizată pentru controlul în masă al configurațiilor pentru un grup de dispozitive Streamvault. Poate fi creată o singură instanță de manager Streamvault.
- **Hardware Streamvault™:** Comanda Raport din Security Center utilizată pentru a vizualiza o listă de probleme de sănătate care afectează dispozitivele Streamvault.

Configurațiile entității plugin-ului constau în următoarele setări:

- **Configurații de alertă:** utilizate pentru a defini tipurile de **evenimente**, nivelurile de **severitate** și tipurile de **notificare** care afectează alertele care abordează starea de sănătate a serverelor Streamvault.
- **Destinatarii e-mailului:** utilizat pentru a selecta utilizatorii și grupurile de utilizatori care primesc notificări prin e-mail.
- **Remote management credentials:** utilizate pentru a controla crearea de profiluri de utilizator în iDRAC.
- **Integrare iDRAC (Integrated Dell Remote Access Controller)** (pentru modelele Streamvault care acceptă iDRAC): utilizată pentru a exercita un control mai precis asupra gestionării acreditărilor. Această caracteristică poate fi găsită în fila **Management** a plugin-ului.

Pentru mai multe informații, consultați <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

IMPORTANT:

- Pentru sistemele cu servere compatibile iDRAC, firmware-ul iDRAC trebuie să fie la versiunea 6.0 sau ulterioară.
- Pentru dispozitivele care acceptă iDRAC, pluginul Întreținerea Streamvault accesează datele de sănătate utilizând o conexiune internă, atât timp cât este instalat software-ul Dell iDRAC Service Module (iSM). iSM este instalat în mod implicit pe modelele care acceptă iDRAC.

Dacă iSM nu este disponibil, pluginul utilizează comunicarea în afara benzii cu iDRAC. În acest caz, trebuie să existe o conexiune de rețea între portul dedicat iDRAC și cel puțin un port LAN dacă nu se utilizează partajarea porturilor. Portul iDRAC dedicat este dezactivat în mod implicit. Pentru mai multe informații, consultați următoarele: <https://www.dell.com/support/kbdoc/en-ca/000177212/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip>.

Descărcarea și instalarea plugin-ului

Pentru a integra plugin-ul Streamvault™ Maintenance în Security Center, trebuie să instalați plugin-ul pe un server Directory, pe serverele Streamvault pe care doriți să le monitorizați și pe toate stațiile de lucru client de pe care doriți să configurați plugin-ul.

Înainte de a începe

Asigurați-vă că este instalată o versiune compatibilă a Security Center. Pentru informații, consultați [Pluginuri acceptate în Security Center](#) din TechDoc Hub.

Ce ar trebui să știți

- **CELE MAI BUNE PRACTICĂ:** Instalați rolul Streamvault pe fiecare server pe care trebuie să îl monitorizați.
- **IMPORTANT:** Asigurați-vă că modulul iDRAC al fiecărui server este conectat la rețea și poate comunica cu sistemul gazdă. În mod implicit, modulul iDRAC împarte același port LAN cu sistemul gazdă și este configurat să obțină o adresă IP prin DHCP.
- **IMPORTANT:** Asigurați-vă că modulul iDRAC este actualizat la firmware-ul 6.00 sau la o versiune ulterioară și că BIOS-ul serverului este actualizat la cea mai recentă versiune înainte de a continua.
- Plugin-ul este acceptat doar pe serverele pe care rulează software-ul de server Security Center.
- **Notă:** Plugin-ul [Întreținerea Streamvault](#) este preinstalat pe toate serverele Streamvault compatibile. Din acest motiv, majoritatea utilizatorilor trebuie doar să creeze rolurile și entitățile în Security Center. Dacă serverul dvs. a fost livrat înainte ca acest plugin să fie disponibil sau dacă a fost deinstallat, urmați acești pași pentru a-l instala.

Procedură

- 1 Deschideți pagina GTAP [Descărcare produs](#).
- 2 La **Download Finder**, selectați versiunea dvs. de Security Center.
- 3 Din secțiunea *Genetec Plugins*, descărcați pachetul pentru produsul dumneavoastră.
- 4 Rulați fișierul .exe, apoi dezarhivați fișierul.
În mod implicit, fișierul este dezarhivat în C:\Genetec.
- 5 Deschideți dosarul extras, dați clic dreapta pe fișierul *setup.exe* și dați clic pe **Rulare ca administrator**.
- 6 Urmați instrucțiunile de instalare.
- 7 Pe pagina *Expert instalare finalizat*, dați clic pe **Terminare**.
IMPORTANT: Opțiunea **Reporniți serverul Genetec™** este selectată în mod implicit. Puteți șterge această opțiune dacă nu doriți să reporniți imediat serverul Genetec™. Cu toate acestea, trebuie să reporniți serverul Genetec™ pentru a finaliza instalarea.
- 8 Închideți și apoi deschideți toate instanțele Config Tool și Security Desk.

Privilegii Streamvault Genetec

Pentru a utiliza comenzile *Monitor Hardware* și *Manager* asociate cu dispozitivul Streamvault™, conturile de utilizator trebuie să primească privilegiile necesare.

Configurarea privilegiilor de utilizator pentru Streamvault

Unele grupuri de utilizatori, precum administratorii, beneficiază de privilegii implicite.

În comanda *Gestionare utilizatori* a Config Tool, puteți configura sau modifica privilegiile utilizatorului sau ale grupului de utilizatori pe pagina *Privilegii* a utilizatorului sau a grupului de utilizatori.

Pentru a afla mai multe despre ierarhia privilegiilor, moștenirea privilegiilor și atribuirea de privilegii, consultați [Ghidul de administrare Security Center](#) și [Ghidul de întărire Security Center](#) pe TechDoc Hub.

Notă: Pentru o listă a tuturor privilegiilor disponibile pentru Security Center, consultați foaia de calcul [Privilegii pentru Security Center](#). Puteți sorta și filtra această listă în funcție de necesități.

Privilegii de rol pentru pluginul Streamvault

Privilegiile rolului de plugin Streamvault acordă acces la sarcinile asociate cu Streamvault *Hardware monitor* și *Manager*.

În mod implicit, administratorii au toate privilegiile. Dacă creați un cont de utilizator din unul dintre celelalte șabloane de privilegii, contul de utilizator necesită următoarele privilegii de rol de plugin Streamvault pentru Config Tool în Streamvault.

Subcategorie de privilegii	Include privilegiile pentru	Acțiuni care pot fi efectuate
Monitor hardware	Modificați monitoare hardware	<ul style="list-style-type: none"> Configurații alertă modificare Modificați destinatarii de e-mail Modificarea acreditărilor de gestionare la distanță Modificați setările portului
	Adăugați monitoare hardware	Creați o nouă entitate monitor hardware și atribuiți-o unui server Streamvault
	Ștergeți monitoare hardware	Ștergerea unei entități monitor hardware existente
	Vizualizați monitoare hardware	Vizualizați o configurație a monitorului hardware
Manager	Modifică managerul	<ul style="list-style-type: none"> Modificarea în bloc a configurațiilor de alertă Modificarea în bloc a destinatarilor de e-mail
	Adăugați managerul	Creați entitatea manager și atribuiți-o unui server Streamvault

Subcategorie de privilegii	Include privilegii pentru	Acțiuni care pot fi efectuate
	Ștergeți managerul	Ștergeți entitatea manager
	Vezi manager	Vizualizați configurația managerului

Crearea rolului de plugin

Înainte de a putea configura și utiliza pluginul, trebuie să creați rolul pluginului Streamvault™ Maintenance în Config Tool.

Înainte de a începe

[Descărcați și instalați plugin.](#)

Ce ar trebui să știți

Plugin-ul Întreținerea Streamvault conține două roluri de plugin:

- **Monitor hardware Streamvault™** Entitatea monitor hardware Streamvault™ este utilizat pentru a monitoriza starea de sănătate a dispozitivelor Streamvault™ și pentru a vă asigura că primiți notificări atunci când apar probleme. Este necesar un monitor hardware Streamvault™ pentru fiecare dispozitiv Streamvault™.
- **Manager Streamvault™** Entitatea Manager Streamvault™ este utilizată pentru a controla configurațiile de alertă pentru un grup de entități Agent Streamvault™. Este permis un singur Manager Streamvault™ pentru fiecare sistem.
- **Notă:** Dacă serverele Directory sunt mașini virtuale sau servere care nu sunt Streamvault, creați un rol pentru aceste servere doar dacă doriți să utilizați entitatea Manager.

Procedură

- 1 De pe pagina de pornire a Config Tool, deschideți comanda *Plugins*.
- 2 În comanda *Plugins*, dați clic pe **Adaugă o entitate** (+) și selectați **Plugin**.
Se deschide expertul de creare a pluginului.
- 3 Pe pagina *Informații specifice*, selectați serverul pe care este găzduit rolul de plugin și tipul de plugin, apoi dați clic pe **Mai departe**.
Dacă nu utilizați servere de expansiune în sistem, opțiunea **Server** nu este afișată.
- 4 Pe pagina *Informații de bază*, specificați informațiile despre rol:
 - a) Introduceți **Nume entitate**.
 - b) Introduceți **Descriere entitate**.
 - c) Selectați **Partiție** pentru rolul de plugin.
Dacă nu folosiți partiții în sistemul dumneavoastră, opțiunea **Partiție** nu este afișată. Partițiile sunt grupări logice utilizate pentru a controla vizibilitatea entităților. Doar utilizatorii care sunt membri ai partiției respective pot vizualiza sau modifica rolul.
 - d) Dați clic pe **Mai departe**.
- 5 Pe pagina *Rezumat creare*, examinați informațiile, apoi dați clic pe **Creare** sau **Înapoi** pentru a face modificări.
După crearea rolului de plugin, se afișează următorul mesaj: Operațiunea a avut succes.
- 6 Dați clic pe **Închidere**.

După ce termini

- [Configurați entitatea de monitorizare hardware Streamvault.](#)
- [Configurați entitatea manager Streamvault.](#)

Configurarea unei entități monitor hardware Streamvault

Puteți configura o entitate monitor hardware Streamvault™ pentru a monitoriza starea de sănătate a unui dispozitiv Streamvault și pentru a seta notificări care să fie transmise atunci când apar probleme.

Înainte de a începe

- Înscrieți-vă dispozitivele Streamvault.
- [Creați rolul Streamvault Plugin.](#)

IMPORTANT: Un monitor hardware Streamvault este creat automat pe fiecare server Streamvault care găzduiește un rol Streamvault. Dacă entitatea monitorului hardware nu este prezentă în sistemul dvs. după ce ați creat rolul, trebuie să creați manual monitorul hardware. Monitorul hardware poate rula doar pe un server Streamvault.

Ce ar trebui să știți

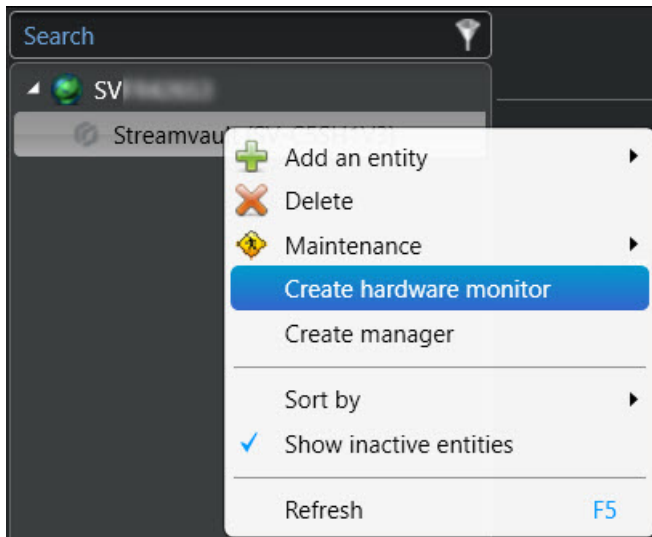
Opțiunile de configurare sunt diferite, în funcție de faptul că aveți servere compatibile iDRAC sau alte servere non-iDRAC.

- [Configurarea unui server activat iDRAC.](#)
- [Configurarea unui server non-iDRAC.](#)

Procedură

Pentru a configura un server activat iDRAC:

- 1 În Config Tool, navigați la comanda *Plugins* și selectați rolul pluginului Streamvault.
- 2 Dați clic dreapta pe rolul de plugin Streamvault și dați clic pe **Creare monitor hardware**.



- 3 În fila **Identitate**, introduceți un nume pentru monitorul hardware Streamvault în câmpul **Nume**.
- 4 Selectați fila **General**.
- 5 (Opțional) Dacă ați creat o entitate de manager Streamvault pentru sistemul dvs., bifați caseta de selectare **Use manager settings** pentru a utiliza setările profilului de configurare a alertelor din managerul Streamvault.

- 6 În secțiunea *Profil configurare alertă* , bifați caseta de selectare **Monitorul hardware gestionează configurațiile de alertă iDRAC** pentru a gestiona configurațiile de alertă prin intermediul monitorului hardware Streamvault.
- 7 Selectați casetele de selectare care se corelează cu **evenimentele**, nivelurile de **severitate** și tipurile de **notificare** pe care doriți să le includeți pentru acest monitor hardware Streamvault.

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

- 8 În secțiunea *Destinatarii e-mailului* , alegeți ce utilizatori și grupuri de utilizatori primesc notificări prin e-mail când este îndeplinită o condiție din secțiunea *Profil de configurare alertă* .

User/Group	Selected
Admin	<input type="checkbox"/>
Administrators	<input checked="" type="checkbox"/>
AutoVu	<input type="checkbox"/>
AutoVu operators	<input type="checkbox"/>
Patroller	<input type="checkbox"/>
Patroller users	<input type="checkbox"/>

No email configured for this group

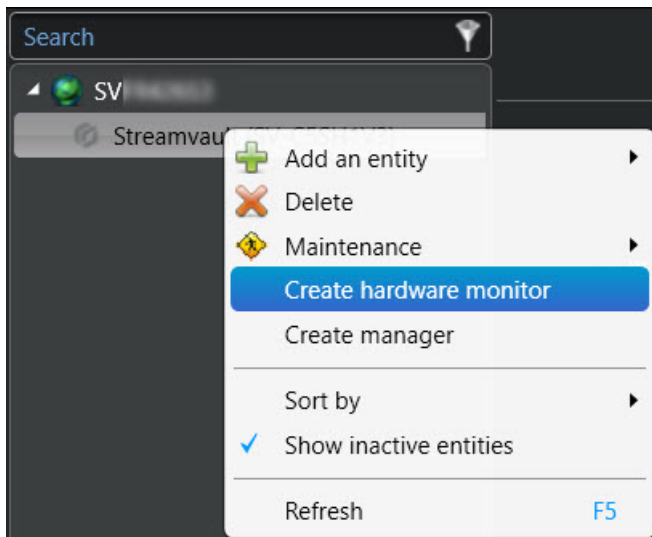
- 9 În secțiunea *Crediente de gestionare la distanță* , efectuați una dintre următoarele acțiuni:
 - Selectați caseta de selectare **Monitor hardware gestionează conturile iDRAC** pentru a gestiona acreditările direct prin plugin.
 - Debifați caseta de selectare **Monitor hardware gestionează conturile iDRAC** pentru a utiliza iDRAC pentru a controla crearea de utilizatori și parole.
- 10 (Opțional) Dacă ați debifat caseta de selectare **Monitor hardware gestionează conturile iDRAC** , navigați la fila **Management** și configurați acreditările direct în iDRAC.

- 11 (Opțional) În secțiunea *Setări*, puteți modifica **portul** de intrare implicit de la 65115 în alegerea dvs. preferată. Pentru mai multe informații, consultați [Porturi implicite utilizate de Streamvault](#), pagină 4.

- 12 Dați clic pe **Aplicare**.

Pentru a configura un server non-iDRAC:

- 1 În Config Tool, navigați la comanda *Plugins* și selectați rolul pluginului Streamvault.
- 2 Dați clic dreapta pe rolul de plugin Streamvault și dați clic pe **Creare monitor hardware**.



- 3 În fila **Identitate**, introduceți un nume pentru monitorul hardware Streamvault în câmpul **Nume**.
- 4 Selectați fila **General**.
- 5 (Opțional) Dacă ați creat o entitate de manager Streamvault pentru sistemul dvs., bifați caseta de selectare **Use manager settings** pentru a utiliza setările profilului de configurare a alertelor din managerul Streamvault.
- 6 În secțiunea *Profil de configurare alertă*, bifați casetele de selectare corelate cu tipurile de **evenimente** și **notificări** pe care doriți să le Întreținerea Streamvault aplicați instanțelor plugin controlate de managerul Streamvault.
- 7 La **Configurare**, setați **Pragul de uzură %** al unității solid-state drive (SSD) la care doriți să primiți o notificare care să vă informeze că trebuie să înlocuiți SSD-ul în curând.

- 8 În secțiunea *Destinatarii e-mailului*, alegeți ce utilizatori și grupuri de utilizatori primesc notificări prin e-mail când este îndeplinită o condiție din secțiunea *Profil de configurare alertă*.

☐ Use manager settings

Alert configuration profile

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

Email recipients

☐ Admin

☒ Administrators No email configured for this group

☐ AutoVu

☐ AutoVu operators

☐ Patroller

☐ Patroller users

- 9 Dați clic pe **Aplicare**.

Subiecte conexe

[Despre fila Management](#), pagină 62

Configurarea unei entități manager Streamvault

Puteți configura o entitate manager Streamvault™ pentru a controla configurațiile de alertă ale unui grup de monitoare hardware Streamvault dintr-o singură locație. De asemenea, puteți configura notificări care să fie transmise atunci când apar probleme. Utilizarea entității manager Streamvault este opțională.

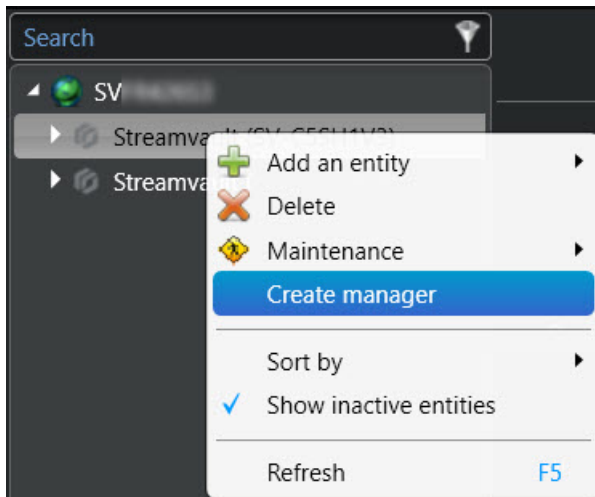
Înainte de a începe

- Înscrieți-vă dispozitivele Streamvault.
- [Creați rolul Streamvault Plugin.](#)

Notă: Entitatea manager Streamvault poate rula pe orice server (Streamvault sau non-Streamvault) sau mașină virtuală din sistemul Security Center. În sistem poate fi adăugată o singură entitate Streamvault manager.

Procedură

- 1 În Config Tool, navigați la comanda *Plugins* și selectați rolul pluginului Streamvault.
- 2 Dați clic dreapta pe rolul de plugin Streamvault și dați clic pe **Create manager**.



- 3 Selectați entitatea manager Streamvault și dați clic pe fila **General**.
Se afișează următoarele secțiuni:
 - Secțiunea *Profilul de configurare a alertelor iDRAC* gestionează serverele cu iDRAC din sistemul dumneavoastră.
 - Secțiunea *Profilul de configurare a alertelor Non-iDRAC* este utilizată pentru a gestiona alte servere non-iDRAC din sistem.

Ambele secțiuni sunt afișate întotdeauna, indiferent dacă aveți un sistem iDRAC sau un sistem non-iDRAC.

- 4 (Dacă este cazul) În secțiunea Profil de configurare a alertei *iDRAC*, configurați următoarele:
- Pentru a gestiona configurațiile de alertă iDRAC prin intermediul monitorului hardware Streamvault al serverului selectat, selectați caseta de selectare **Monitorul hardware gestionează configurațiile de alertă iDRAC**.
 - Selectați casetele de selectare care se corelează cu nivelurile de **Evenimente**, **Severitate** și **Notificare** pe care doriți să le aplicați instanțelor de Întreținerea Streamvault plugin controlate de managerul Streamvault.

iDRAC alert configuration profile

☒ Hardware monitor manages iDRAC alert configurations

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

Hardware monitors using Streamvault™ manager configuration

Streamvault (SV-C5SH1V3) - Streamvault™ hardware monitor

Notă: Monitoarele hardware ale căror configurații sunt stabilite de managerul Streamvault sunt listate la **Monitoare hardware care utilizează configurația managerului Streamvault™**. Monitoarele hardware care utilizează configurații proprii sunt listate la **Monitoare hardware care utilizează configurații personalizate**.

- 5 (Dacă este cazul) În secțiunea *Non-iDRAC alert configuration profile*, configurați următoarele:
 - a) Selectați casetele de selectare care se corelează cu tipurile de **Evenimente** și **Notificare** pe care doriți să le aplicați instanțelor de plugin Întreținerea Streamvault controlate de managerul Streamvault.
 - b) La **Configurare**, setați **Pragul de uzură %** al unității solid-state drive (SSD) la care doriți să primiți o notificare care să vă informeze că trebuie să înlocuiți SSD-ul în curând.

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

Hardware monitors using Streamvault™ manager configuration

Streamvault (SVFR426S3) - Streamvault™ hardware monitor

Notă: Monitoarele hardware ale căror configurații sunt stabilite de managerul Streamvault sunt listate la **Monitoare hardware care utilizează configurația managerului Streamvault™**. Monitoarele hardware care utilizează configurații proprii sunt listate la **Monitoare hardware care utilizează configurații personalizate**.

- 6 În secțiunea *Destinatari e-mail*, alegeți utilizatorii și grupurile de utilizatori care primesc notificări prin e-mail atunci când este îndeplinită o condiție din secțiunea **Profil de configurare alertă iDRAC** sau **Profil de configurare alertă Non-iDRAC**.

Email recipients

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

- 7 Dați clic pe **Aplicare**.

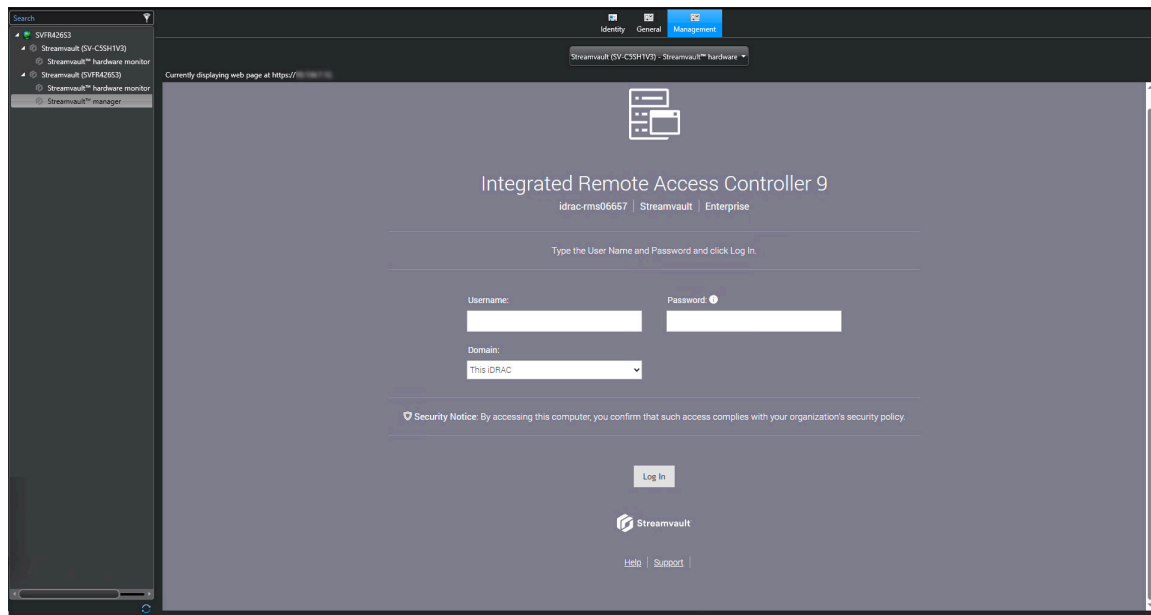
Despre fila Management

În fila **Management** se afișează o pagină web iDRAC prin intermediul căreia puteți configura și gestiona acreditările serverului iDRAC. De asemenea, puteți afla mai multe informații despre serverul iDRAC și puteți configura alte opțiuni care nu sunt disponibile prin interfața de utilizator a pluginului Streamvault™.

Puteți accesa fila **Management** prin intermediul monitorului hardware Streamvault™ al oricărui server compatibil iDRAC sau prin intermediul managerului Streamvault™.

Dacă accesați fila **Management** prin intermediul managerului Streamvault, în partea de sus a paginii este afișată o listă derulantă. Îl puteți utiliza pentru a trece de la un server iDRAC la altul, în loc să trebuiască să treceți manual de la un monitor hardware la altul. Fiecare server iDRAC are propria pagină web iDRAC.

Pentru informații de conectare, dați clic pe **Ajutor** în partea de jos a paginii web.



Notă: Pentru a accesa pagina web iDRAC, aveți nevoie de o conexiune de rețea între sistemul client care rulează Config Tool și adresa IP a serverului iDRAC. Dacă nu este disponibilă o conexiune la rețea, utilizați pagina Config Tool direct de pe dispozitivul Streamvault printr-o sesiune desktop de la distanță sau de consolă locală.

Dacă sistemul dvs. nu are niciun server iDRAC, fila **Management** este goală. Un mesaj indică faptul că nu sunt disponibile monitoare hardware Streamvault cu capacități de gestionare iDRAC.

Notă: Dacă pagina web iDRAC nu se încarcă, dați clic pe o altă filă și apoi reveniți la fila **Management**.

Subiecte conexe

[Configurarea unei entități monitor hardware Streamvault](#), pagină 55

[Configurarea unei entități manager Streamvault](#), pagină 59

Revizuirea sănătății dispozitivului Streamvault

Utilizați comanda **Hardware Streamvault™** pentru a vizualiza o listă a problemelor de sănătate care afectează dispozitivele Streamvault.

Procedură

- 1 De pe pagina de pornire, deschideți comanda *Hardware Streamvault*.
- 2 În filtrul de interogare **Interval de timp**, definiți perioada de timp pe care doriți să o includeți în raport.
- 3 Dați clic pe **Generare raport**.
Proprietățile unității sunt enumerate pe panoul de raportare.

Coloanele panoului de raport pentru comanda hardware Streamvault

După generarea unui raport, rezultatele interogării dvs. sunt enumerate în panoul de raportare. Această secțiune enumeră coloanele disponibile pentru comanda hardware Streamvault™.

- **Imagine:** Pictograma care reprezintă tipul de problemă.
- **Severitate:** Nivelul de gravitate asociat cu problema.
- **Marcaj temporal:** Data și ora la care a apărut problema.
- **Sursă:** Dispozitivul Streamvault afectat de această problemă.
- **MessageID:** Secvență alfanumerică de identificare asociată cu problema raportată.
- **Mesaj:** Descrierea problemei.
- **Descriere:** Descrierea cauzei problemei.

Notă: Pentru mai multe informații despre crearea rapoartelor, consultați [Prezentare generală a spațiului de lucru al comenzilor de raportare](#) pe TechDoc Hub.


Crearea de evenimente către acțiuni pentru evenimentele de sănătate Streamvault

Utilizând un eveniment la acțiune, puteți declanșa acțiuni care să aibă loc atunci când este detectată o problemă hardware Streamvault™.

Înainte de a începe

- [Creați rolul pluginului Streamvault Maintenance..](#)
- [Configurați o entitate](#) de monitorizare hardware Streamvault.

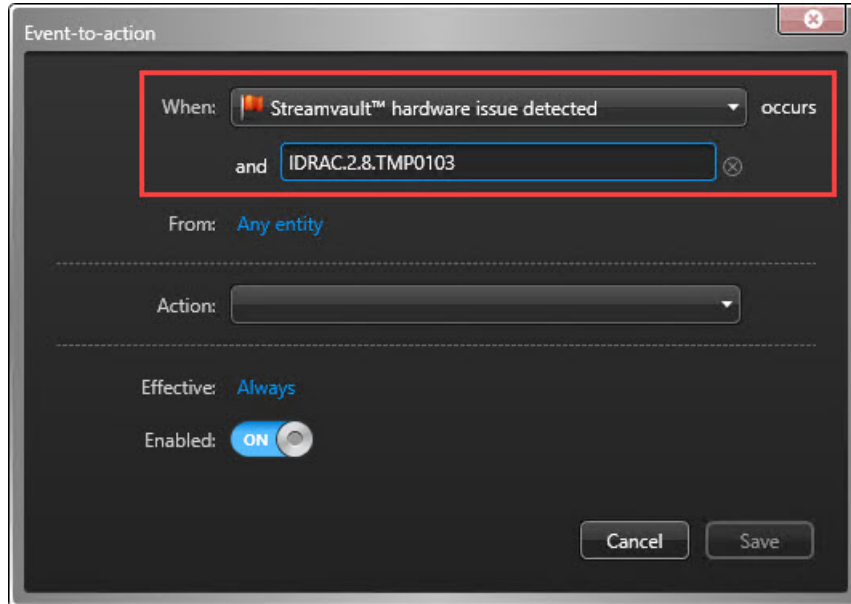
Procedură

- 1 Din pagina de pornire Config Tool, faceți clic pe sarcina *Automatizare* și apoi pe vizualizarea **Acțiuni** .
- 2 Dați clic pe **Adaugați un element** ().

3 Configurați evenimentul la acțiune:

- a) Din meniul derulant **Când**, selectați **Streamvault problemă hardware detectată**.
- b) Faceți clic pe **Specificați o condiție** și introduceți codul de eroare iDRAC. De asemenea, puteți introduce ID-ul complet pentru a preveni orice declanșare falsă.

De exemplu, în captura de ecran de mai jos, codul de eroare este TMP0103, iar ID-ul complet este IDRAC.2.8.TMP0103.



- c) (Opțional) În opțiunea **De la**, selectați pluginul Streamvault™ sau monitorul hardware.

Notă: Deoarece pluginul Streamvault utilizează evenimente personalizate care au sens numai pentru el însuși, nu este nevoie să atribuiți o sursă.

Dacă selectați pluginul Streamvault ca entitate sursă, atunci dacă rolul pluginului este vreodată șters, toate regulile de automatizare legate sunt șterse. Dacă nu este specificată nicio entitate sursă și rolul este șters, regulile de automatizare persistă.

- d) Din meniul derulant **Actiune**, selectați un tip de acțiune și configurați-i parametrii.
- e) (Opțional) În opțiunea **Efectiv**, dați clic pe **Întotdeauna** și selectați un program în care acest eveniment-activitate este activ.

Dacă evenimentul are loc în afara programului definit, atunci acțiunea nu este declanșată.

4 Asigurați-vă că evenimentul la acțiune este activat.

5 Dați clic pe **Salvare**.

Notă: Pentru o listă completă a codurilor de eroare iDRAC, consultați <https://developer.dell.com/apis/2978/versions/5.xx/docs/Error%20Codes/EEMRegistry.md>.

Referința panoului de control SV

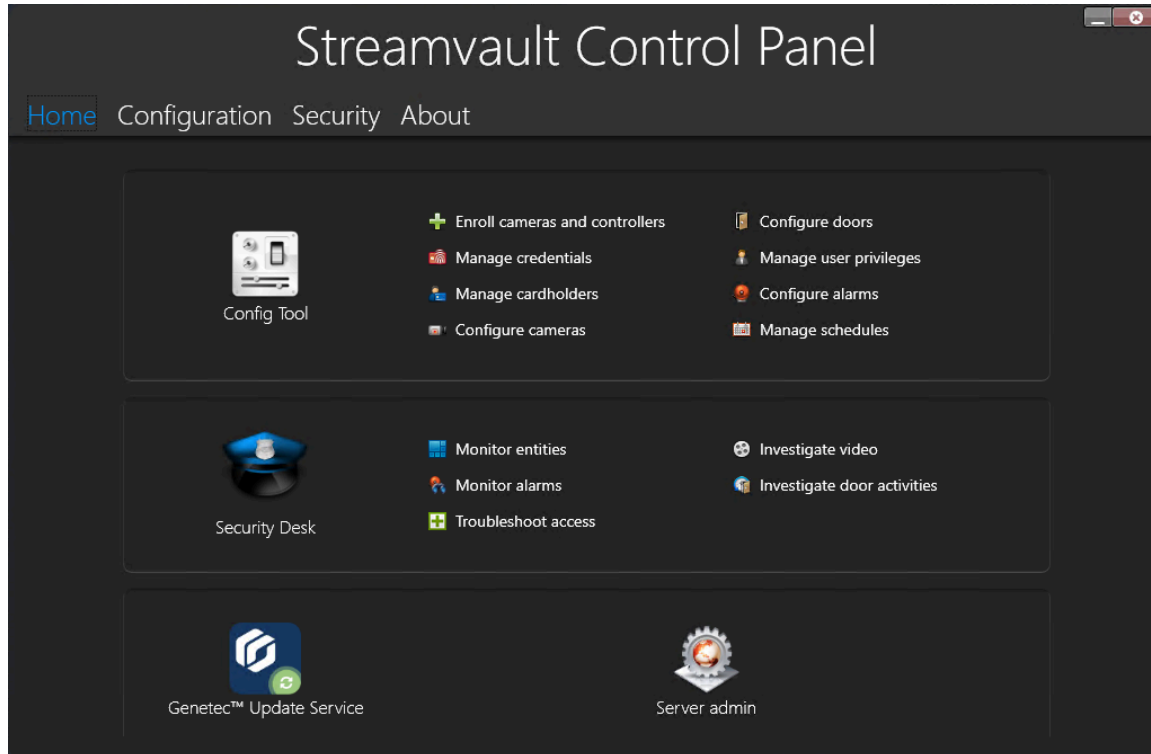
Aceste pagini de referință vă ajută să înțelegeți panoul de control SV.

Această secțiune include următoarele subiecte:

- ["Pagina de pornire a SV Control Panel"](#), pagină 68
- ["Pagina de configurare a SV Control Panel"](#), pagină 70
- ["Pagina Securitate a SV Control Panel"](#), pagină 73
- ["Pagina Despre din SV Control Panel"](#), pagină 76

Pagina de pornire a SV Control Panel

Utilizați pagina de pornire a SV Control Panel pentru a accesa sarcinile de bază necesare pentru configurarea și utilizarea sistemului dumneavoastră. Puteți da clic pe pictogramele interfeței pentru a accesa aplicațiile Config Tool, Security Desk, Server Admin sau Genetec™ Update Service.



Alternativ, puteți da clic pe comenzile rapide Config Tool sau Security Desk pentru a deschide comenzile asociate.

Pentru sistemele care rulează în modul Client, comanda rapidă Server Admin nu este disponibilă. De asemenea, scurtăturile Config Tool și Security Desk sunt limitate.

Notă: Notă: În cazul în care sistemul dvs. nu este activat, apare un banner roșu pentru a vă anunța. Dați clic pe **Sistemul nu este activat. Dați clic aici pentru a activa**, pentru a deschide expertul de activare Streamvault™ Control Panel.

Comenzi rapide ale Instrumentului de configurare

Utilizați comenzile rapide pentru a deschide principalele sarcini din aplicația Config Tool. Comenzile rapide care sunt disponibile depind de opțiunile de licență pe care le aveți.

Comandă rapidă	Acțiune
Instrument configurare	Deschide Instrumentul de configurare.
Înregistrați camere și controlere	Deschide instrumentul de înregistrare a unității, unde vă puteți înscrie camerele și controlerele.
Administrare acreditări	Deschide comanda <i>Managementul acreditărilor</i> , în care puteți gestiona acreditările utilizatorului.

Comandă rapidă	Acțiune
Administrare titulari de card	Deschide comanda <i>Gestionarea titularilor de card</i> , în care puteți gestiona deținătorii de carduri.
Configurați camere	Deschide comanda <i>Video</i> , unde puteți adăuga și gestiona camere.
Configurați uși	Deschide comanda <i>Vedere zonă</i> , în care puteți adăuga și gestiona uși.
Gestionați privilegiile utilizatorului	Deschide comanda <i>Managementul utilizatorilor</i> , unde puteți adăuga și gestiona privilegiile utilizatorului.
Configurați alarme	Deschide comanda <i>Alarme</i> , unde puteți configura alarme.
Gestionați programele	Deschide comanda <i>Sistem</i> , unde puteți crea și gestiona programe.

Comenzi rapide de Security Desk

Utilizați comenzile rapide pentru a deschide principalele acțiuni din aplicația Security Desk. Comenzile rapide care sunt disponibile depind de opțiunile de licență pe care le aveți.

Comandă rapidă	Acțiune
Security Desk	Deschide Security Desk.
Monitorizare entităților	Deschide comanda <i>Monitorizare</i> ca să monitorizați evenimentele sistemului în timp real.
Monitorizare alarme	Deschide comanda <i>Monitorizare alarmă</i> unde puteți monitoriza și răspunde la alarmele active și pentru a vizualiza alarmele anterioare.
Acces depanare	Deschide instrumentul Access troubleshooter, care permite diagnosticarea și accesarea problemelor de configurare. Notă: Această comandă rapidă nu este disponibilă pentru sistemele care rulează în modul Client.
Investigați video	Deschide comanda <i>Arhive</i> , unde puteți căuta arhive video. Notă: Această comandă rapidă nu este disponibilă pentru sistemele care rulează în modul Client.
Investigați activitățile ușilor	Deschide comanda <i>Activități ușă</i> unde poți investiga evenimentele de la ușile selectate. Notă: Această comandă rapidă nu este disponibilă pentru sistemele care rulează în modul Client.

Comandă rapidă Genetec Update Service

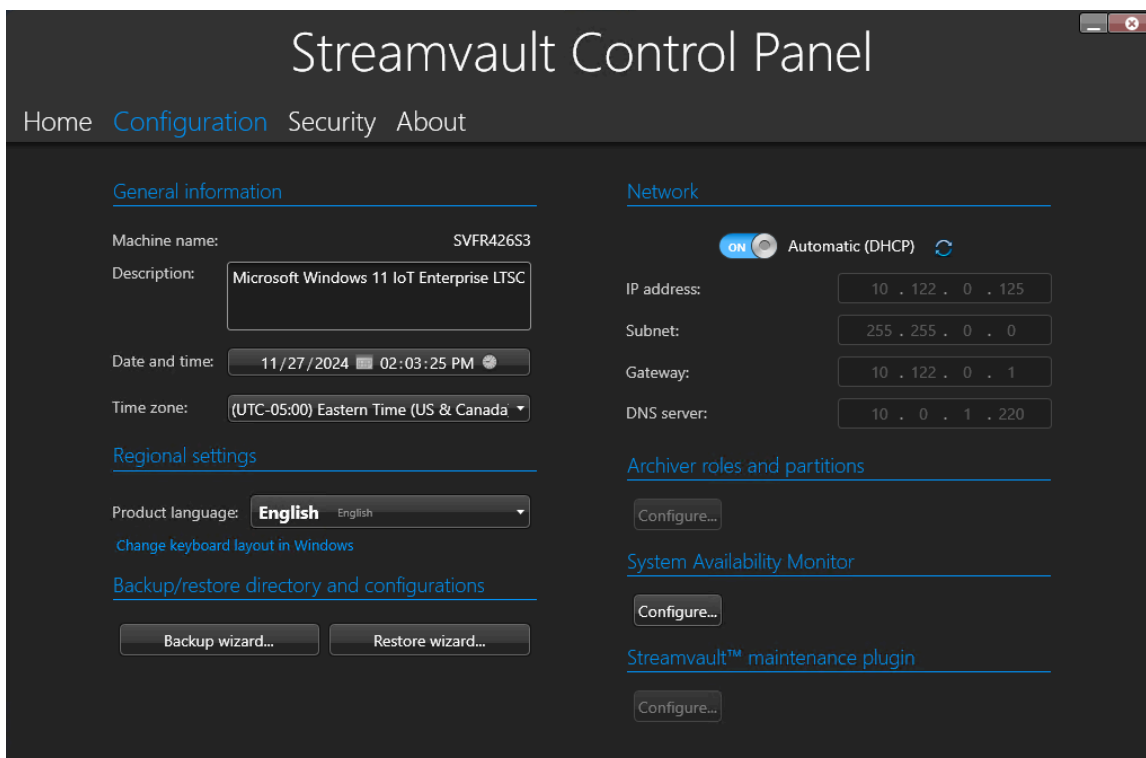
Utilizați Genetec Update Service pentru a vă asigura că componentele software ale dispozitivului dumneavoastră sunt actualizate.

Comandă rapidă pentru administratorul serverului

Utilizați aplicația Server Admin pentru a aplica manual o licență sau pentru a vizualiza și modifica configurația serverului.

Pagina de configurare a SV Control Panel

Utilizați pagina *Configurare* din Streamvault™ Control Panel pentru a modifica setările generale, precum setările regionale, setările de rețea și setările Monitorul de disponibilitate a sistemului.



Pentru sistemele care rulează pe un server de expansiune sau în modul Client, nu sunt disponibile secțiunile *Monitorul de disponibilitate a sistemului* și *Director copie de rezervă/restaurare și configurații*.

Setări pentru informații generale

Utilizați secțiunea *Informații generale* pentru a modifica setările generale, cum ar fi numele dispozitivului Streamvault.

- **Nume mașină:** Afișează numele mașinii SV.
- **Descriere:** Introduceți o descriere semnificativă pentru a ajuta la identificarea mașinii.
- **Data și ora:** Dați clic în câmp pentru a configura valorile datei și orei afișate pe dispozitiv. Alternativ, puteți da clic pe pictograma calendarului sau a ceasului din câmp pentru a configura setările.
- **Fus orar:** Selectați un fus orar din lista derulantă.

Setări regionale

Utilizați secțiunea *Setări regionale* pentru a modifica setările de limbă ale configurației tastaturii sistemului.

- **Limba produsului:** Selectați o limbă din listă pentru a schimba limba din Config Tool și Security Desk.
IMPORTANT: Pentru ca modificările să intre în vigoare, trebuie să reporniți aplicațiile Security Center.
- **Modificarea aspectului tastaturii în Windows:** Dați clic pe această opțiune pentru a deschide pagina de setări *Limbă și regiune* pentru a modifica aspectul tastaturii.
IMPORTANT: Pentru ca modificările să intre în vigoare, trebuie să reporniți computerul.

Notă: SV Control Panel este disponibil în limba engleză, franceză și spaniolă.

Copiere de rezervă și restabilire

Folosiți secțiunea *Director copie de rezervă/restaurare și configurații* pentru a accesa expertul *Copie de rezervă* și expertul *Restaurare*.

Copiile de rezervă și restaurarea sunt o caracteristică a SV Control Panel. Vă permite să faceți o copie de rezervă în siguranță a bazei de date și a fișierelor de configurare ale Directoratului și să le restaurați ulterior pe același ID de sistem. Rezerva și restaurarea pot fi utilizate în cazul unei defecțiuni a sistemului sau al unei actualizări hardware. Această funcție nu face o copie de rezervă a fișierului de licență, a arhivelor video sau a altor baze de date.

Această secțiune nu este disponibilă pentru sistemele care rulează pe un server de expansiune sau în modul Client.

- **Expert Copie de rezervă:** Dați clic pe **Expert copie de rezervă** pentru a crea o copie de rezervă a bazei de date Directory și a fișierelor de configurare.
- **Expert de restaurare:** Dați clic pe **Expert de restaurare** pentru a restaura o copie de rezervă a bazei de date Directory și a fișierelor de configurare pe sistemul dvs.

IMPORTANT: Trebuie să deschideți portul necesar pentru a vă asigura că funcția *Directory copie de rezervă/restaurare și configurații* poate comunica cu SV Control Panel. Pentru mai multe informații, consultați [Porturi implicite utilizate de Streamvault](#), pagină 4.

Setări de rețea

Folosiți secțiunea *Rețea* pentru a modifica setările de rețea, precum adresa IP a dispozitivului Streamvault.

- **Automat (DHCP):** În mod implicit, Protocolul de configurare dinamică a gazdelor (DHCP) este utilizat pentru a atribui automat adresa IP, subrețea, gateway-ul și serverul DNS. Dezactivați această opțiune dacă nu doriți ca adresa IP să fie atribuită dinamic de serverul dvs. DHCP.

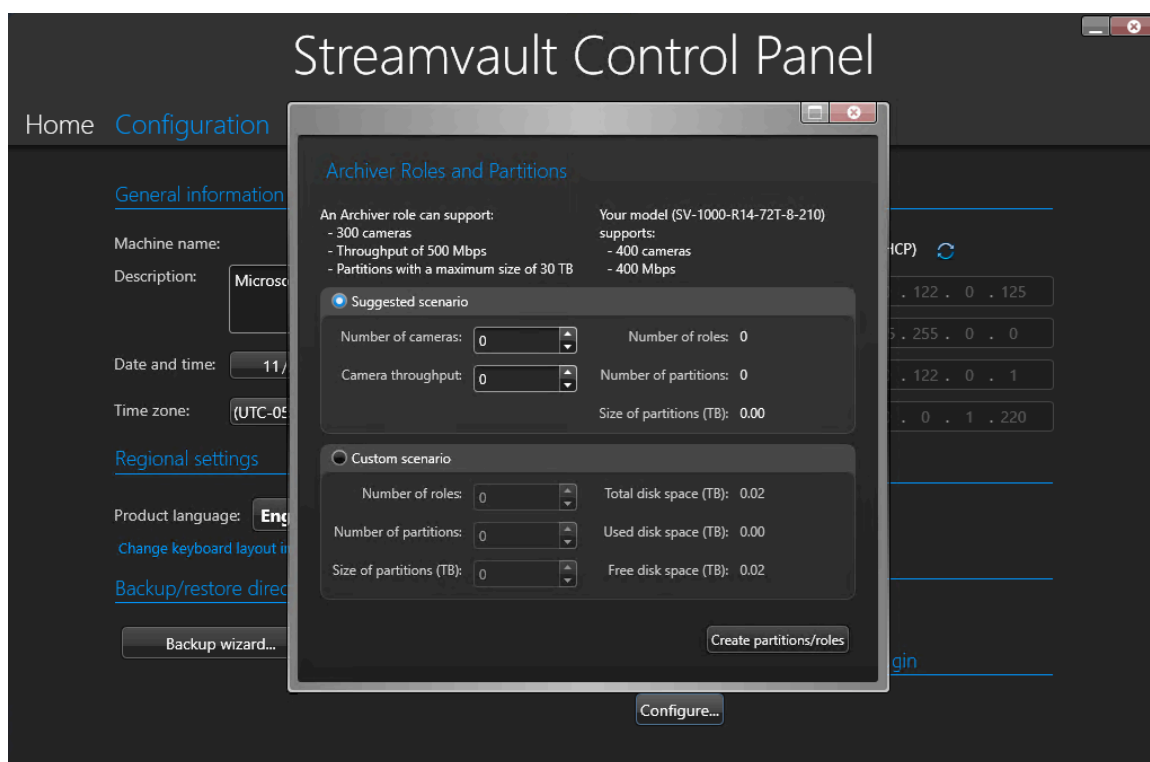
Dați clic pe **Refresh**  pentru a reîmprospăta setările DHCP și a obține o nouă adresă IP.

- **Adresă IP:** Adresa IP a mașinii.
- **Subnet:** Masca de subrețea a mașinii.
- **Gateway:** Adresa IP a gateway-ului.
- **Server DNS:** Adresa IP a serverului DNS.

Roluri Arhivar și partiții

Utilizați secțiunea *Roluri de arhivare și partiții* pentru a configura sisteme care necesită mai mult decât numărul maxim de camere și debit suportate de un singur arhivar.

Această secțiune este disponibilă pentru sistemele care rulează Security Center 5.9 și o versiune ulterioară pe un server de expansiune.



- **Un rol de Archiver poate susține:** Afișează numărul maxim de camere, cantitatea de debit și dimensiunea partițiilor acceptate de un singur rol Archiver
- **Modelul dumneavoastră acceptă:** Afișează numărul maxim de camere și cantitatea maximă de debit suportate de modelul de dispozitiv Streamvault.
- **Scenariul sugerat:** Calculează automat numărul de roluri, partiții și dimensiunea partițiilor necesare pentru numărul dorit de camere și pentru debitul dorit.
- **Scenariu personalizat:** Alegeți numărul de roluri, partiții și dimensiunea partițiilor dorite pentru configurația sistemului dumneavoastră.

Pentru mai multe informații despre utilizarea acestei funcții, consultați [Adăugarea rolurilor Archiver în SV Control Panel](#), pagină 38.

Setări Monitor disponibilitate sistem

Utilizați secțiunea *Monitor disponibilitate sistem* pentru a configura setările pentru agentul Monitor disponibilitate sistem de pe dispozitivul Streamvault. De exemplu, setarea metodei de colectare a datelor și activarea agentului.

De asemenea, puteți verifica următoarele:

- Dacă dispozitivul comunică cu Security Center
- Când a avut loc ultimul punct de control
- Ce erori și avertismente recente au fost raportate în jurnalele de aplicații și servicii

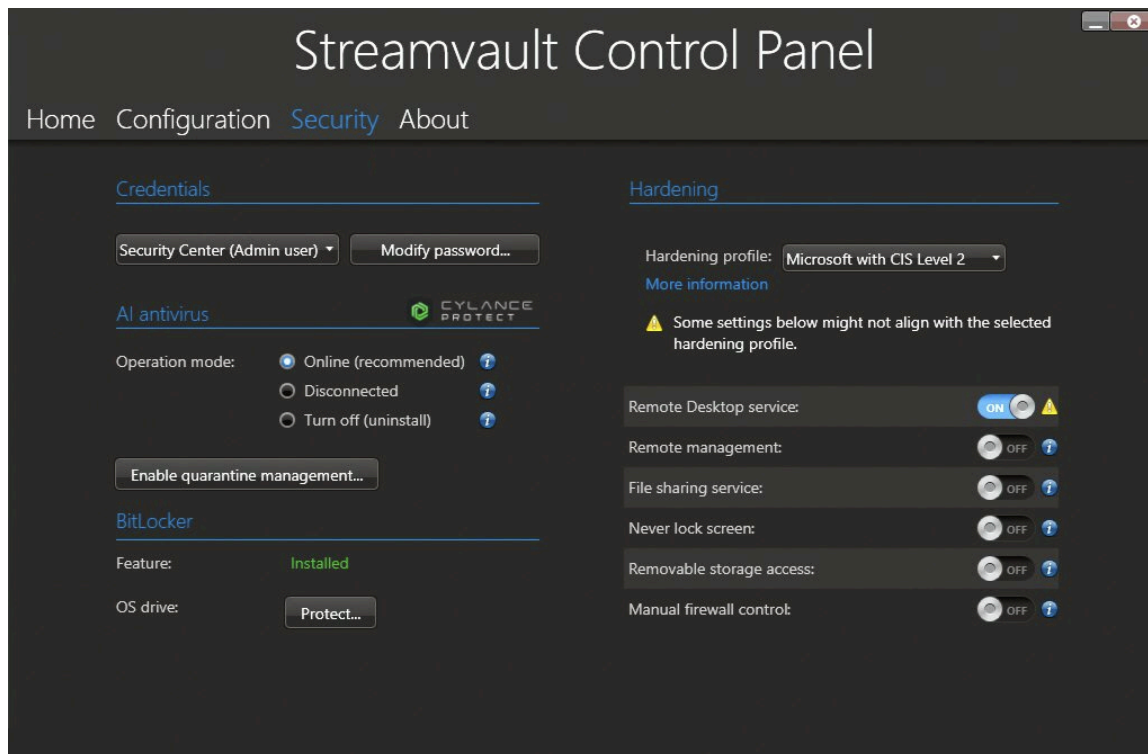
Această secțiune nu este disponibilă pentru sistemele care rulează pe un server de expansiune sau în modul Client.

Setări plug-in Streamvault Maintenance

Utilizați secțiunea *Plugin de întreținere Streamvault* pentru a înscrie pluginul în Centrul de securitate, dacă acesta nu a fost deja înscris.

Pagina Securitate a SV Control Panel

Utilizați pagina *Securitate* pentru a modifica parolele utilizatorului, alegeți modul de comunicare între agentul CylancePROTECT și Genetec™ și aplicați profiluri de întărire și setări de securitate a sistemului la dispozitivul dvs. Streamvault™.



Setări parolă

Utilizați secțiunea *Acreditări* din pagina *Securitate* pentru a modifica parolele conturilor de utilizator pentru dispozitivul Streamvault.

Notă: Atât pe un server principal și pe un server de extindere sunt disponibile diferite opțiuni de parolă pentru utilizatorul curent. Pe un server de expansiune, administratorul poate schimba doar parolele Windows, nu și parolele aplicațiilor Security Center.

Definiți o parolă pentru fiecare tip de utilizator:

- **Security Center (utilizator Admin):** Parola utilizatorului administrator pentru Security Desk, Config Tool și Genetec™ Update Service.
- **Server Admin:** Parola pentru aplicația Genetec™ Server Admin.
- **Operator Windows:** Dați clic pe **Modificare parolă** pentru a modifica parola operatorului pentru Windows.

Setări antivirus

Utilizați *Antivirus AI* pentru a alege modul în care agentul CylancePROTECT comunică cu Genetec.

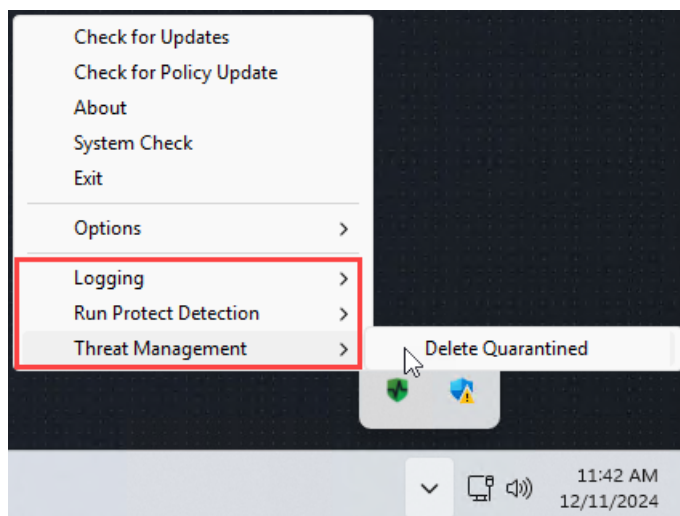
CylancePROTECT este software-ul antivirus bazat pe inteligență artificială, utilizat pentru protecția și detectarea amenințărilor.

Puteți alege dintre următoarele moduri de funcționare:

- **Online (recomandat):** Atunci când este online, agentul CylancePROTECT comunică cu Genetec pentru a raporta noi amenințări, pentru a-și actualiza agentul și pentru a trimite date care să ajute la îmbunătățirea modelelor sale matematice. Această opțiune oferă cel mai înalt nivel de protecție.
- **Deconectat:** Modul deconectat este pentru un dispozitiv fără conexiune la internet. În acest mod, CylancePROTECT nu se poate conecta sau trimite informații către serviciile de gestionare Genetec din cloud. Dispozitivul dumneavoastră este protejat împotriva majorității amenințărilor. Întreținerea și actualizările sunt disponibile prin intermediul Genetec™ Update Service (GUS).
- **Oprirea alimentării:** Selectați acest mod pentru a dezinstala definitiv CylancePROTECT din dispozitivul dumneavoastră. Dispozitivul dvs. va utiliza Microsoft Defender pentru protecția și detectarea amenințărilor. Nu recomandăm dezactivarea CylancePROTECT dacă dispozitivul nu poate primi actualizări ale definițiilor de viruși pentru Microsoft Defender.

ATENȚIE: Comutarea între opțiuni poate necesita o repornire a computerului, ceea ce poate cauza întreruperi ale sistemului.

Dați clic **Activați gestionarea carantinei** a adauga **Managementul amenințărilor** în meniul clic dreapta al pictogramei Cylance din bara de activități Windows. Această opțiune vă permite să ștergeți elementele aflate în carantină. **Înregistrare** și **Run Protect Detection** sunt adăugate și în meniul de clic dreapta. Aceste opțiuni vă permit să accesați jurnalele și, respectiv, să declanșați scanări.



Setări criptare

Folosește *BitLocker* secțiune pentru a instala funcția BitLocker și a cripta unitatea sistemului de operare de pe dispozitivul Streamvault.

- **Caracteristică:** Funcția BitLocker este preinstalată pe Windows 10 și Windows 11. Dacă aveți Windows Server, trebuie să faceți clic pe **Instala** pentru a instala funcția.
- **Unitate de sistem de operare:** Clic **Proteja** pentru a cripta unitatea sistemului de operare (C:) cu BitLocker. Cheia de decriptare este salvată pe un cip Trusted Platform Module (TPM) situat pe placa de sistem a dispozitivului Streamvault. Dacă unitatea sistemului de operare ar fi scoasă sau placa de sistem ar fi înlocuită, informațiile de pe unitatea sistemului de operare s-ar pierde. Unitatea sistemului de operare nu ar putea accesa cheia de decriptare de pe TPM. Puteți crea o cheie de recuperare care poate fi utilizată pentru a decripta unitatea în aceste scenarii. Fără o cheie de recuperare, dispozitivul trebuie re-creat și software-ul trebuie reinstalat. Criptarea unității sistemului de operare ajută, de asemenea, la protejarea parolei de administrator Windows împotriva accesului neautorizat.

Pentru mai multe informații, consultați [Criptarea unității sistemului de operare](#).

Setări de întărire

Utilizați *întărire* pentru a alege un profil de întărire și a seta setările de securitate ale sistemului pentru dispozitivul dvs. Streamvault.

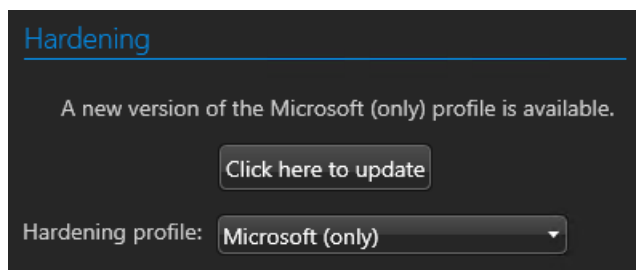
Notă: Profilele de întărire sunt disponibile numai la aparatele care au [Serviciul Streamvault](#). Pentru mai multe informații, consultați [Despre serviciul Streamvault](#), pagină 15.

Există patru profile de întărire predefinite:

- **Microsoft (doar):** Acest profil de întărire aplică liniile de bază de securitate Microsoft sistemului dumneavoastră. Liniile de bază de securitate Microsoft sunt un grup de setări de configurare recomandate de Microsoft care se bazează pe feedback-ul de la echipele de inginerie de securitate Microsoft, grupurile de produse, partenerii și clienții.
- **Microsoft cu CIS Nivelul 1:** Acest profil de întărire aplică liniile de bază de securitate Microsoft și profilul Center for Internet Security (CIS) Nivel 1 (CIS L1) la sistemul dumneavoastră. CIS L1 oferă cerințe de securitate esențiale care pot fi implementate pe orice sistem cu un impact redus sau deloc asupra performanței sau funcționalitate redusă.
- **Microsoft cu CIS Nivelul 2:** Acest profil de consolidare aplică liniile de bază de securitate Microsoft și profilurile CIS L1 și Level 2 (L2) sistemului dumneavoastră. Profilul CIS L2 oferă cel mai înalt nivel de securitate și este destinat organizațiilor în care securitatea este de maximă importanță.
Notă: Securitatea strictă pe care o aduce acest profil de întărire poate reduce funcționalitatea sistemului și poate face mai dificilă administrarea de la distanță a serverului.
- **Microsoft cu STIG:** Acest profil de întărire aplică liniile de bază de securitate Microsoft și Ghidurile de implementare tehnică de securitate (STIG) ale Agenției pentru Sisteme Informaționale de Apărare (DISA) sistemului dumneavoastră. DISA STIG se bazează pe standardele Institutului Național de Standarde și Tehnologie (NIST) și oferă protecție avansată de securitate pentru sistemele Windows pentru Departamentul de Apărare al SUA.

Notă: În mod implicit, toate aparatele sunt livrate cu Microsoft cu profilul de întărire CIS Nivelul 2 aplicat.

Când este disponibilă o nouă versiune a profilului de întărire selectat, apare butonul **Dați clic aici pentru a actualiza**. Dați clic pe butonul pentru a aplica actualizarea.



Pe lângă profilurile de întărire, pot fi setate următoarele setări de securitate a sistemului:

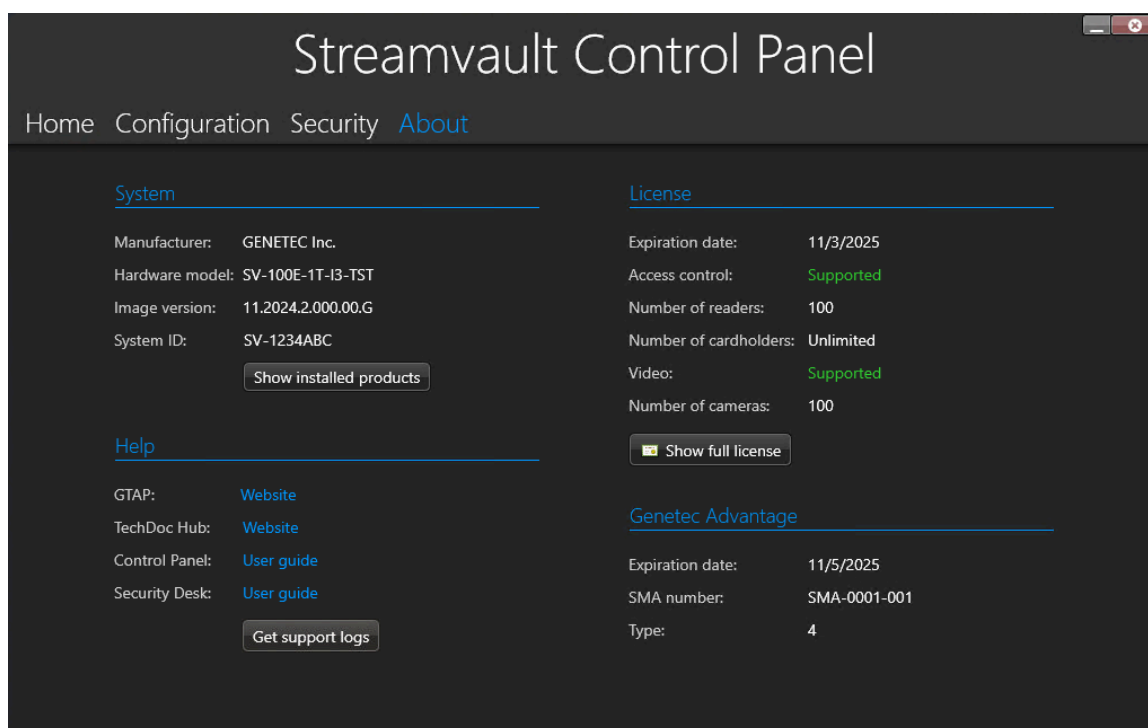
- **Serviciul Remote Desktop:** Permiteți persoanelor din rețeaua dvs. să se conecteze la dispozitivul folosind o aplicație *Remote Desktop*. Pentru a preveni ca programele malițioase să afecteze dispozitivul, această opțiune a fost dezactivată în mod implicit.
- **Management de la distanță:** Activați suportul la distanță pentru instrumentele de gestionare Microsoft, precum Windows Admin Center, Microsoft Server Manager și Remote PowerShell.
- **Serviciu de partajare a fișierelor:** Permiteți persoanelor din rețeaua dvs. să partajeze fișiere și foldere care se află pe aparat. Pentru a preveni ca programele malițioase să afecteze dispozitivul, această opțiune a fost dezactivată în mod implicit.
- **Nu blocați niciodată ecranul:** Dacă această opțiune este activată, Windows va păstra un utilizator conectat, chiar și după 15 minute de inactivitate.
- **Acces la spațiul de stocare detașabil:** Activați accesul la o cheie USB sau la un hard disk USB conectat din Windows.
Notă: Utilizatorii cu privilegii administrative au automat acces la spațiul de stocare detașabil.
- **Control manual al firewall-ului:** În mod implicit, Paravanul de protecție Windows Defender utilizează obiecte de politică de grup (GPO) din profilurile de consolidare pentru a securiza sistemul. Activați această opțiune pentru a controla manual politicile firewall-ului. Toate obiectele GPO vor fi dezactivate.

Pentru mai multe informații, consultați [Dezactivarea paravanului de protecție Windows](#), pagină 123.

Pagina Despre din SV Control Panel

Utilizați pagina *Despre* pentru a vizualiza informații utile dacă aveți nevoie de asistență cu dispozitivul Streamvault™. Pagina *Despre* include informații despre sistem, linkuri către portalul de asistență tehnică Genetec™ (GTAP) și documentația produsului, informații despre licență și informații despre Contractul de întreținere software (SMA).

Pentru sistemele care rulează pe un server de expansiune sau care sunt în modul Client, sunt disponibile doar secțiunile *Sistem* și *Ajutor*.



Informații sistem

Utilizați secțiunea *Sistem* pentru a vizualiza informații despre sistem.

- **Producător:** Afișează producătorul hardware-ului.
- **Model hardware:** Afișează modelul hardware.
- **Versiune imagine:** Afișează versiunea sau imaginea software-ului.
- **ID sistem:** Afișează ID-ul de sistem.
- **Afișați produsele instalate:** Dați clic pentru a afișa versiunea de software a componentelor Genetec instalate pe dispozitiv.

Informații de ajutor

Utilizați secțiunea *Ajutor* pentru a accesa link-uri utile către GTAP și documentația produsului.

- **GTAP:** Dați clic pe link pentru a deschide [GTAP](#) și forumurile de asistență.
Notă: Trebuie să aveți un nume de utilizator și o parolă valabile pentru a vă conecta la GTAP.
- **TechDoc Hub:** Dați clic pe link pentru a deschide [Genetec TechDoc Hub](#).
- **Control Panel:** Faceți clic pe link pentru a deschide *Ghidul utilizatorului dispozitivului Streamvault*, care conține informații despre SV Control Panel.
- **Security Desk:** Faceți clic pe link pentru a deschide *Ghidul utilizatorului Security Center*.

- **Obțineți jurnale de asistență:** Faceți clic pentru a selecta jurnalele de asistență pe care doriți să le descărcați în scopul depanării.

Informații de licență

Utilizați secțiunea *Licență* pentru a vedea informații despre licență. Informațiile care sunt afișate variază în funcție de opțiunile de licență.

- **Data de expirare:** Se afișează când vă expiră licența Security Center.
- **Control acces:** Afișează dacă sunt acceptate sau nu funcțiile de control al accesului.
- **Număr de cititoare:** Afișează câte cititoare sunt acceptate pe sistemul dvs.
- **Număr de titulari de card:** Afișează numărul de titulari de carduri acceptate de sistemul dumneavoastră.
- **Înregistrare video:** Afișează dacă sunt acceptate sau nu funcțiile video.
- **Număr de camere:** Afișează câte camere sunt acceptate pe sistemul dumneavoastră.
- **Arată licența completă:** Dați clic pentru a afișa mai multe informații despre licență.

Această secțiune nu este disponibilă pentru sistemele care rulează pe un server de expansiune sau în modul Client.

Genetec Advantage information

Utilizați *Avantajul Genetec* secțiune pentru a vizualiza informații despre SMA.

- **Data de expirare:** Afișează data de expirare a Contractului de întreținere a software-ului.
- **Numărul SMA:** Afișează numărul SMA.
- **Tip:** Afișează tipul SMA.

Această secțiune nu este disponibilă pentru sistemele care rulează pe un server de expansiune sau în modul Client.

Resurse suplimentare

Această secțiune include următoarele subiecte:

- ["Garanția produsului pentru dispozitivul Streamvault"](#), pagină 79
- [" Configurarea parolei BIOS "](#), pagină 80
- [" Schimbarea parolei implicite iDRAC "](#), pagină 83
- ["Adăugarea unui nou utilizator iDRAC cu privilegii de administrator"](#), pagină 84
- ["Dezactivarea utilizatorului root iDRAC"](#), pagină 85
- ["Reimaginarea unui dispozitiv Streamvault"](#), pagină 86
- ["Găsirea ID-ului sistemului și a versiunii imaginii unui dispozitiv Streamvault"](#), pagină 87
- ["Permiterea distribuirea fișierelor pe un dispozitiv Streamvault"](#), pagină 88
- ["Permiterea conexiunilor Remote Desktop la un dispozitiv Streamvault"](#), pagină 89

Garanția produsului pentru dispozitivul Streamvault

Dispozitivul Streamvault™ este acoperit de o garanție standard de 3 ani pentru hardware și software, cu o prelungire opțională de 2 ani.

Pentru o descriere detaliată a termenilor și condițiilor de garanție a produsului Genetec™, consultați [Prezentare generală a garanției produsului Genetec™](#).

Configurarea parolei BIOS

Pentru a proteja datele de pe dispozitivul Streamvault™ împotriva accesului neautorizat, trebuie să setați o parolă BIOS.

Ce ar trebui să știți

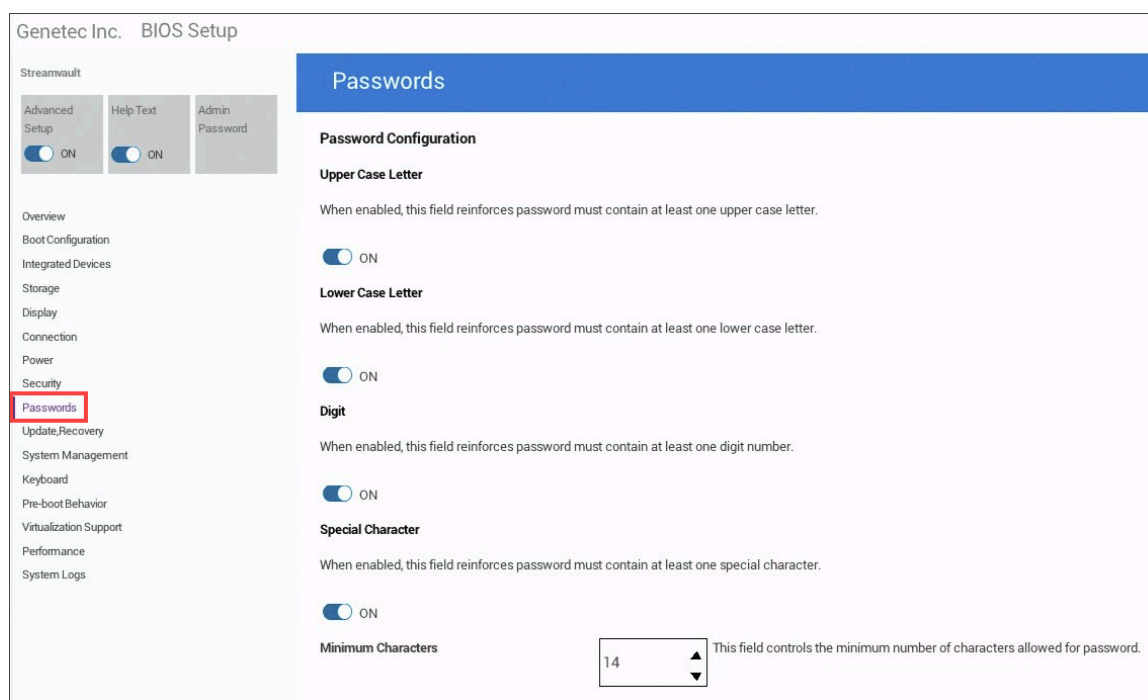
Pașii pentru configurarea unei parole BIOS diferă în funcție de modelul dispozitivului. Urmăriți procedura aplicabilă aparatului dumneavoastră.

- [Setați parola BIOS pe dispozitivul sau stația de lucru Streamvault All-in-one.](#)
- [Setați parola BIOS pe dispozitivul din seria SV-1000, SV-2000, SV-4000 sau SV-7000 \(PowerEdge\).](#)

Procedură

Pentru a seta parola BIOS pe dispozitivul sau stația de lucru Streamvault All-in-one:

- 1 Porniți sau reporniți aparatul și apăsați F2 în mod repetat până când *Configurarea BIOS-ului* apare meniul.
- 2 Selectați **Parole** din meniul din partea stângă a ecranului.
- 3 Pe *Parole* pagină, derulați în jos până la *Configurarea parolei* secțiune și configurați următoarele setări:
 - Porniți **Majusculă**, **Literă mică**, **Cifră** și **Caracter special** opțiuni.
 - Setări **Caractere minime** câmp la 14.



- 4 Derulați până în partea de sus a *Parole* pagina și introduceți o nouă parolă BIOS sub **Parolă de administrator**.

Passwords

Admin Password

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

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

Successful changes to this password take effect immediately.

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

Enter the old password:

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

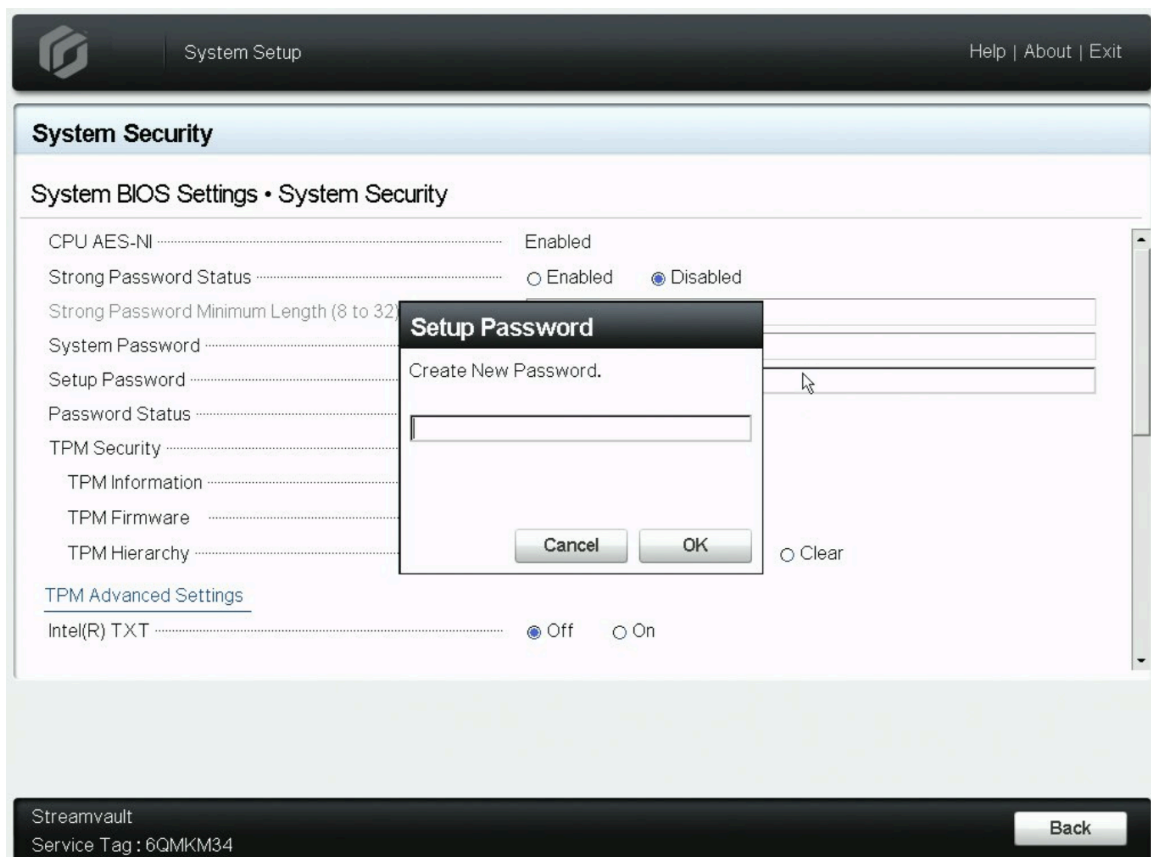
Enter the new password:

- 5 Clic **Îșire**.
Modificările sunt salvate și aparatul repornește.

Pentru a seta parola BIOS pe dispozitivul din seria SV-1000, SV-2000, SV-4000 sau SV-7000 (PowerEdge):

- 1 Porniți sau reporniți aparatul și apăsați F2 în mod repetat până când *Configurarea sistemului* apare meniul.
- 2 În *Meniul principal de configurare a sistemului*, faceți clic **BIOS-ul sistemului**.
- 3 În *Setări BIOS sistem*, faceți clic **Securitatea sistemului**.
- 4 În **Configurare parolă** câmp, faceți clic în interiorul casetei de text.

- 5 În *Configurare parolă* caseta de dialog care se deschide, introduceți o parolă nouă și faceți clic pe **Bine**.



- 6 În **Starea parolei** câmp, selectați **Blocat** pentru a solicita introducerea parolei de configurare înainte de schimbarea parolei de sistem.
- 7 Clic **Spate** > **Termina** > **Termina**.
Modificările sunt salvate și aparatul repornește.

Schimbarea parolei implicite iDRAC

Dacă dispozitivul Streamvault™ este compatibil cu iDRAC, este recomandat să modificați imediat parola iDRAC implicită pentru utilizatorul root pentru a preveni accesul neautorizat la dispozitiv.

Procedură

- 1 Lansați browserul web Microsoft Edge și accesați `https://idrac.local`.
- 2 Pe *Controler de acces la distanță integrat* pagina de conectare, utilizați numele de utilizator și parola implicite pentru a vă conecta:
 - Sub **Nume de utilizator**, introduceți rădăcină.
 - Sub **Parolă**, introduceți parola care se află pe eticheta de service a aparatului.
- 3 După ce v-ați conectat, vi se va solicita să configurați o nouă parolă pentru utilizatorul root. Selectați **Schimbați parola implicită**, introduceți și confirmați noua parolă și faceți clic pe **Continua** pentru a salva modificările.

După ce termini

Pe lângă schimbarea parolei implicite pentru utilizatorul root, este recomandat să creați un utilizator iDRAC alternativ cu privilegii administrative și să dezactivați utilizatorul root. Pentru mai multe informații, consultați [Adăugarea unui nou utilizator iDRAC cu privilegii de administrator](#).

Adăugarea unui nou utilizator iDRAC cu privilegii de administrator

Utilizatorul root iDRAC este bine cunoscut, iar utilizarea sa prezintă riscuri de securitate, chiar dacă ați modificat parola implicită. Prin urmare, este recomandat să adăugați un utilizator nou cu privilegii de administrator pentru a accesa iDRAC.

Ce ar trebui să știți

Puteți adăuga un utilizator local sau puteți utiliza Microsoft Active Directory pentru a crea un cont de utilizator.

Procedură

- Adăugați un utilizator nou într-unul din următoarele moduri:
 - Pentru a adăuga un utilizator local, consultați [Configurarea utilizatorilor locali folosind interfața web iDRAC](#) în Dell *Ghidul utilizatorului iDRAC*.
 - Pentru a utiliza Microsoft Active Directory pentru a crea un utilizator nou, consultați [Configurarea utilizatorilor Active Directory](#) în Dell *Ghidul utilizatorului iDRAC*.

Notă: Când configurați privilegiile utilizatorului, asigurați-vă că **Rolul utilizatorului** este setat la **Administrator**.

După ce termini

Pentru o siguranță sporită, [dezactivați utilizatorul root iDRAC](#).

Dezactivarea utilizatorului root iDRAC

Dacă ați creat un nou utilizator iDRAC cu privilegii de administrator, dezactivați utilizatorul root pentru a vă asigura că nimeni nu se poate conecta cu acel nume de utilizator.

Înainte de a începe

- [Schimbați parola iDRAC implicită pe dispozitivul Streamvault.](#)
- [Adăugați un nou utilizator iDRAC cu privilegii de administrator.](#)

Ce ar trebui să știți

Puteți dezactiva utilizatorul root editând privilegiile utilizatorului.

Procedură

- Pentru detalii despre cum se editează privilegiile utilizatorului root iDRAC, consultați [Configurarea utilizatorilor locali folosind interfața web iDRAC](#) în Dell *Ghidul utilizatorului iDRAC*.

Notă: Când editați privilegiile utilizatorului root, asigurați-vă că configurați următoarele:

- Setați **Rolul utilizatorului** la **Nici unul**.
- Set **Nivel de privilegii LAN** la **Fără acces**.
- Set **Nivel de privilegii al portului serial** la **Fără acces**.
- Set **Serial prin LAN** la **Persoane cu dizabilități**.

Reimaginarea unui dispozitiv Streamvault

Pentru a reimagina un dispozitiv Streamvault™, aveți nevoie de [certificatul de autenticitate Microsoft \(COA\)](#) al acestuia pentru a determina ce imagine poate fi utilizată cu dispozitivul. Fiecare dispozitiv Streamvault are aplicată o etichetă COA, care indică ediția de Windows care rulează pe dispozitiv.

Consultați [Notele de lansare Streamvault](#) pentru o listă de imagini compatibile cu dispozitivul dvs., în funcție de ediția Windows. Nu utilizați imaginea software dacă dispozitivul dvs. rulează o ediție de Windows diferită de cea indicată în notele de lansare.

Următorul este un exemplu de etichetă COA tipică cu informații despre ediția Windows și informații despre certificat ștampilate. Produsele care conțin versiuni încorporate de software Microsoft au o etichetă COA.



Notă: Fiecare imagine Streamvault este concepută pentru a funcționa cu versiunea respectivă a Security Center, așa cum este indicat în [Notele de lansare Streamvault](#). Retrogradarea Security Center la o versiune anterioară poate necesita reducerea nivelului de întărire a dispozitivului.

Pentru o prezentare generală a disponibilității produsului, a asistenței și a serviciilor disponibile, consultați pagina [Ciclul de viață al produsului din GTAP](#).

Găsirea ID-ului sistemului și a versiunii imaginii unui dispozitiv Streamvault

Atunci când contactați Centrul de asistență tehnică Genetec™ (GTAC), aveți nevoie de ID-ul sistemului și de versiunea imaginii a software-ului Genetec™ instalat pe aparat.

Înainte de a începe

Conectați-vă la Windows ca administrator.

Ce ar trebui să știți

În plus față de ID-ul sistemului și versiunea imaginii, GTAC poate solicita numărul de certificare și numărul de serie. Pentru a găsi aceste informații, căutați o etichetă pe dispozitivul Streamvault™.

Procedură

- 1 De pe desktop-ul Windows, deschideți **Genetec™ SV Control Panel**.
- 2 Dacă vi se solicită, introduceți parola pentru utilizatorul Admin.
- 3 Dați clic pe **Despre**.
- 4 În secțiunea *Sistem*, notați **ID-ul sistemului** și **versiunea imaginii**.

Subiecte conexe

[Efectuarea unei resetări din fabrică pe un Streamvault dispozitiv All-in-one](#), pagină 91

[Efectuarea unei resetări din fabrică pe o Streamvaultstație de lucru sau un dispozitiv server](#), pagină 101

Permiterea distribuirea fișierelor pe un dispozitiv Streamvault

Pentru a distribui fișierele și dosarele de pe dispozitivul dvs. cu persoane din rețea, trebuie să activați distribuirea fișierelor în SV Control Panel.

Înainte de a începe

Pe dispozitiv, conectați-vă la Windows ca utilizator administrator.

Ce ar trebui să știți

- Pentru o securitate maximă, distribuirea fișierelor este dezactivată în mod implicit.
- Calculatoarele de la distanță și dispozitivul dvs. trebuie să fie conectate la aceeași rețea IP.

Procedură

- 1 Pe pagina *Securitate* SV Control Panel, porniți opțiunea **Serviciu de partajare a fișierelor**.
- 2 Dați clic pe **Aplicare**.
- 3 Pentru a distribui un dosar sau un fișier cu alte persoane, dați clic dreapta pe un dosar sau un fișier în Windows File Explorer și dați clic pe **Distribuie**.

Permiterea conexiunilor Remote Desktop la un dispozitiv Streamvault

Pentru a controla un dispozitiv de pe orice computer sau mașină virtuală din rețea, trebuie mai întâi să activați accesul la distanță pe dispozitiv.

Înainte de a începe

Pe dispozitiv, conectați-vă la Windows ca utilizator administrator.

Ce ar trebui să știți

- Pentru o securitate maximă, accesul la distanță este dezactivat în mod implicit.
- Dispozitivul și computerul de la distanță trebuie să fie conectate la aceeași rețea.

Procedură

- 1 Pe pagina *Securitate* pagina SV Control Panel, porniți opțiunea **Serviciu Desktop la distanță**.
- 2 Dați clic pe **Aplicare**.

Subiecte conexe

[Remote Desktop nu se poate conecta la un dispozitiv Streamvault](#), pagină 110

Depanare

Această secțiune include următoarele subiecte:

- "Efectuarea unei resetări din fabrică pe un Streamvault dispozitiv All-in-one ", pagină 91
- "Efectuarea unei resetări din fabrică pe o Streamvaultstație de lucru sau un dispozitiv server", pagină 101
- "Controlerele Mercury EP rămân offline atunci când TLS 1.1 este dezactivat", pagină 106
- "Activarea Transport Layer Security (TLS)", pagină 107
- "Remote Desktop nu se poate conecta la un dispozitiv Streamvault", pagină 110
- "Eliminarea restricțiilor de la conturile de utilizatori non-administratori", pagină 114
- "Conturile locale nu pot accesa Desktop la distanță, serviciul de partajare a fișierelor și gestionarea de la distanță ", pagină 115
- "Activarea serviciilor legate de Smart Card", pagină 116
- "Activarea suportului pentru controlerele Mercury EP și LP firmware 1.x.x", pagină 117
- "Activarea suportului pentru integrarea Synergis IX", pagină 119
- "Modificarea GPO-urilor locale pentru conturile de utilizator non-administrator", pagină 120
- "Dezactivarea paravanului de protecție Windows", pagină 123

Efectuarea unei resetări din fabrică pe un Streamvault dispozitiv All-in-one

Dacă software-ul de pe un dispozitiv Streamvault™ All-in-one nu pornește sau nu mai funcționează conform așteptărilor, puteți efectua o resetare din fabrică utilizând o cheie USB.

Înainte de a începe

- [Faceți o copie de rezervă a bazei de date Directly în SV Control Panel](#)
- Aveți licența corectă pentru versiunea de Security Center pe care doriți să o reparați sau să o instalați.
- Aveți ID-ul de sistem și parola care v-au fost trimise prin e-mail atunci când ați achiziționat dispozitivul. Consultați [Găsirea ID-ului sistemului și a versiunii imaginii unui dispozitiv Streamvault](#), pagină 87.
- (Recomandat) Conectați dispozitivul la internet utilizând o conexiune Ethernet cu fir, astfel încât sistemul să poată valida conectivitatea.
Notă: Validarea eșuează dacă nu este disponibilă nicio conexiune la internet, dar puteți continua să utilizați dispozitivul.

Ce ar trebui să știți

O resetare din fabrică șterge și suprascrie toate datele aflate în prezent pe unitatea Windows (C:), inclusiv bazele de date și jurnalele. Fișierele video de pe alte unități nu sunt afectate.

Procedură

- 1 [Creați o cheie USB de resetare din fabrică care conține imaginea software.](#)
- 2 [Cu ajutorul cheii USB, resetați imaginea de pe dispozitiv.](#)

După ce termini

[Reconfigurați-vă aparatul.](#)

Subiecte conexe

[Găsirea ID-ului sistemului și a versiunii imaginii unui dispozitiv Streamvault](#), pagină 87

Crearea unei chei USB de resetare din fabrică pentru un dispozitiv Streamvault All-in-one

Înainte de a putea reseta imaginea unui dispozitiv Streamvault, trebuie să pregătiți o cheie USB bootabilă care conține imaginea software-ului Streamvault necesară.

Înainte de a începe

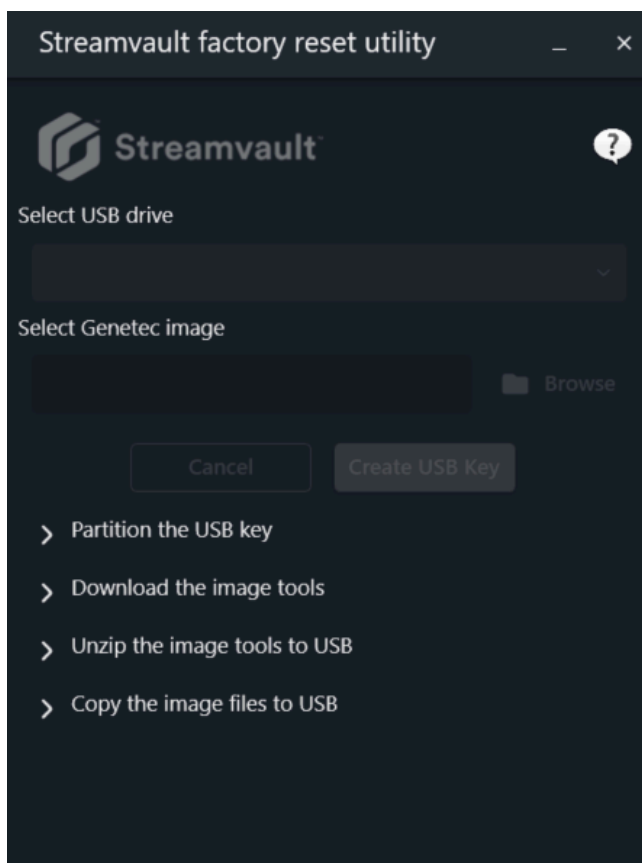
- Obțineți o cheie USB cu cel puțin 32 GB de stocare. Unele chei USB nu reușesc să pornească imaginea; în acest caz, încercați să utilizați o altă marcă sau un alt model de cheie.
ATENȚIE: Toate datele de pe cheia USB sunt șterse atunci când creați o unitate bootabilă.

Procedură

- 1 Contactați [Genetec™ Technical Assistance Center \(GTAC\)](#) pentru a obține imaginea de recuperare. Imaginea de recuperare vine în unul dintre următoarele trei formate:
 - Un fișier *.zip* care conține fișiere *.swm*.
 - Un fișier *.iso* care conține fișierele *.swm* și interfața de utilizator a *utilitarului de resetare din fabrică Streamvault*, pe care o veți utiliza pentru a reseta imaginea software.
 - Un fișier *.iso* care conține *expertul de instalare Windows*, pe care îl veți utiliza pentru a reseta imaginea software.
- 2 Dacă imaginea de recuperare este un fișier *.zip*, dezarhivați conținutul în orice folder Windows.
- 3 Din pagina [Descărcare produs](#) de pe GTAP, descărcați USB creator al *utilitarului de resetare din fabrică Streamvault*.
 - a) La *Download Finder*, selectați versiunea dvs. de Security Center.
 - b) Din lista *Altele*, descărcați pachetul *utilitarului de resetare din fabrică Streamvault*.



- 4 Introduceți cheia USB într-un port USB.
- 5 Deschideți creatorul USB al *utilitarului de resetare din fabrică Streamvault* pe care l-ați descărcat din TechDoc Hub.
- 6 Din lista **Selectați unitatea USB**, selectați o cheie USB care are cel puțin 32 GB de stocare.



- 7 În secțiunea *Selectați imaginea Genetec*, dați clic pe **Răsfoire** și selectați fișierul *.swm* sau *.iso* descărcat.
Notă: Dacă aveți nevoie de un fișier *.swm*, selectați oricare dintre fișierele dezarhivate din folderul *wim*.
 Toate *.swm* Fișierele din acel folder vor fi copiate pe cheia USB.
- 8 Dați clic pe **Creare cheie USB**.
Utilitarul de resetare din fabrică Streamvault începe să partiționeze cheia USB, să descarce instrumentele de imagine și să copieze fișierele de imagine.

Când descărcarea este finalizată, este afișat următorul mesaj: *Cheia USB a fost creată cu succes.*

Exemplu

Următorul videoclip vă arată cum să creați o cheie USB cu resetare din fabrică cu un *.iso* fișier.



După ce termini

[Resetați imaginea software a Streamvault dispozitivului dvs. All-in-one.](#)

Resetarea imaginii software pe un dispozitiv All-in-one

După ce ați pregătit o cheie USB bootabilă care are imaginea software Streamvault™ necesară, o puteți utiliza pentru a reseta imaginea software pe un dispozitiv Streamvault All-in-one.

Înainte de a începe

- [Asigurați-vă că aveți cheia USB care conține software-ul de recuperare pentru dispozitivul dvs.](#)

Ce ar trebui să știți

- Reinițializarea durează aproximativ 20-30 minute, timp în care se execută mai multe scripturi și dispozitivul repornește de mai multe ori.
- Nu întrerupeți procesul de resetare. Închiderea sau oprirea manuală a dispozitivului poate deteriora recuperarea.

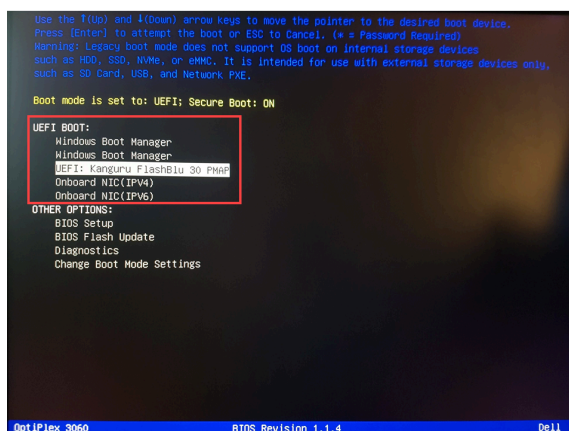
Procedură

Pentru a reseta imaginea software:

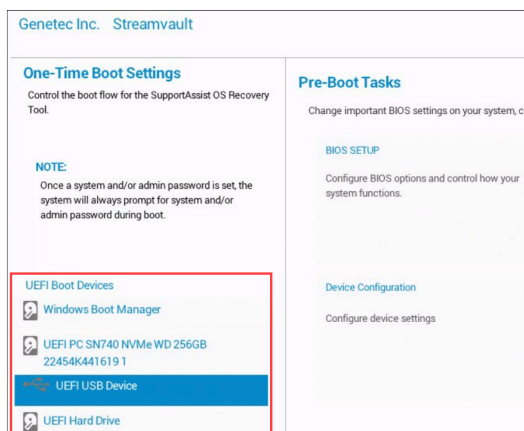
- 1 Închideți dispozitivul.
- 2 Introduceți cheia USB pe care ați creat-o într-un port USB.
- 3 Porniți dispozitivul și apăsați F12 în mod repetat până când apare meniul de pornire.
 În funcție de dispozitiv, se deschide fie meniul UEFI Boot, fie meniul Streamvault One-time Boot.

- 4 Selectați unitatea USB și apăsați Enter.

Notă: Aspectul și senzația meniului de pornire ar putea arăta diferit.



UEFI Boot menu



Streamvault One-time Boot menu

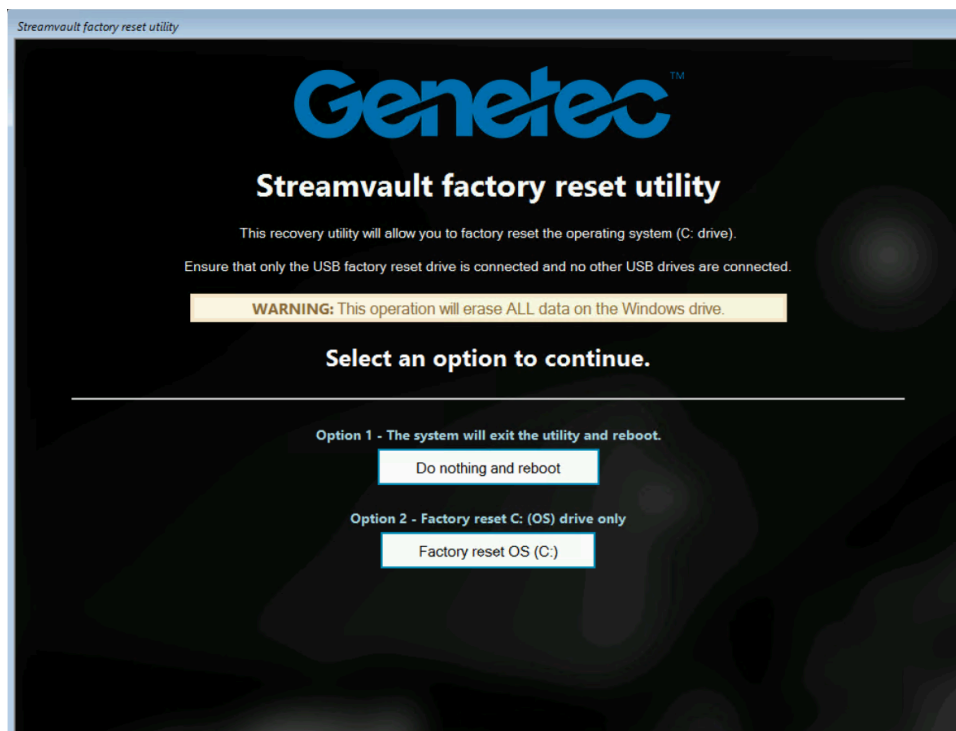
În funcție de imaginea software, se deschide *utilitarul de resetare din fabrică Streamvault* sau expertul *Windows Setup*.

- 5 Resetați imaginea software folosind instrumentul care se aplică aparatului dvs.:

- *Utilitar de resetare din fabrică Streamvault*
- *Expertul Windows Setup*

Pentru a reseta imaginea software folosind utilitarul de resetare din fabrică Streamvault:

- 1 Când USB-ul pornește în modul de recuperare, selectați **Resetare din fabrică OS (C:)** pentru a formata și a reinstala unitatea de sistem a aparatului.



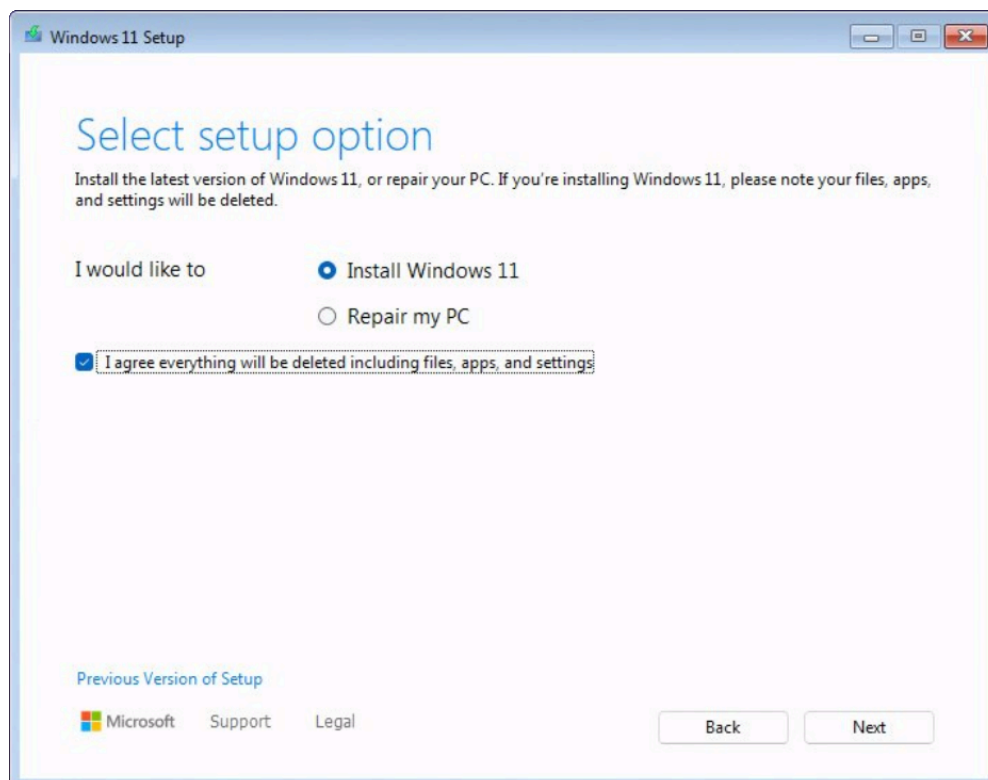
- 2 Când vi se solicită, tastați Da și apăsați Enter. Așteptați ca resetarea din fabrică să se finalizeze.
- 3 Când resetarea din fabrică este finalizată, scoateți cheia USB din dispozitiv și apăsați Enter pentru a reporni.

- 4 În caseta de dialog *Validare produs Genetec™*, introduceți numărul de referință al dispozitivului (Product No.) și numărul de serie Genetec™.
Aceste numere pot fi găsite pe eticheta Genetec situată pe partea superioară a dispozitivului. Dacă nu există o etichetă, puteți introduce orice text pentru a continua.
Apare butonul **Start**.
- 5 Dați clic pe **Pornire**.
Se afișează unul dintre următoarele mesaje de stare:
 - **SUCCES:** Procesul a fost finalizat cu succes. Treceți la pasul următor.
 - **SUCCES - Fără transmisie:** Procesul a fost finalizat cu succes; cu toate acestea, nu a fost disponibilă o conexiune la internet în acel moment. Treceți la pasul următor.
 - **EȘEC:** Procesul a eșuat. Contactați [Genetec™ Technical Assistance Center \(GTAC\)](#).
- 6 Dacă primiți un mesaj **SUCCES** sau **SUCCES - Nicio transmisie**, închideți fereastra *Validator produs Genetec™*.
- 7 Așteptați ca scriptul de fundal să se închidă și apoi reporniți dispozitivul.

Pentru a reseta imaginea software utilizând expertul Windows Setup:

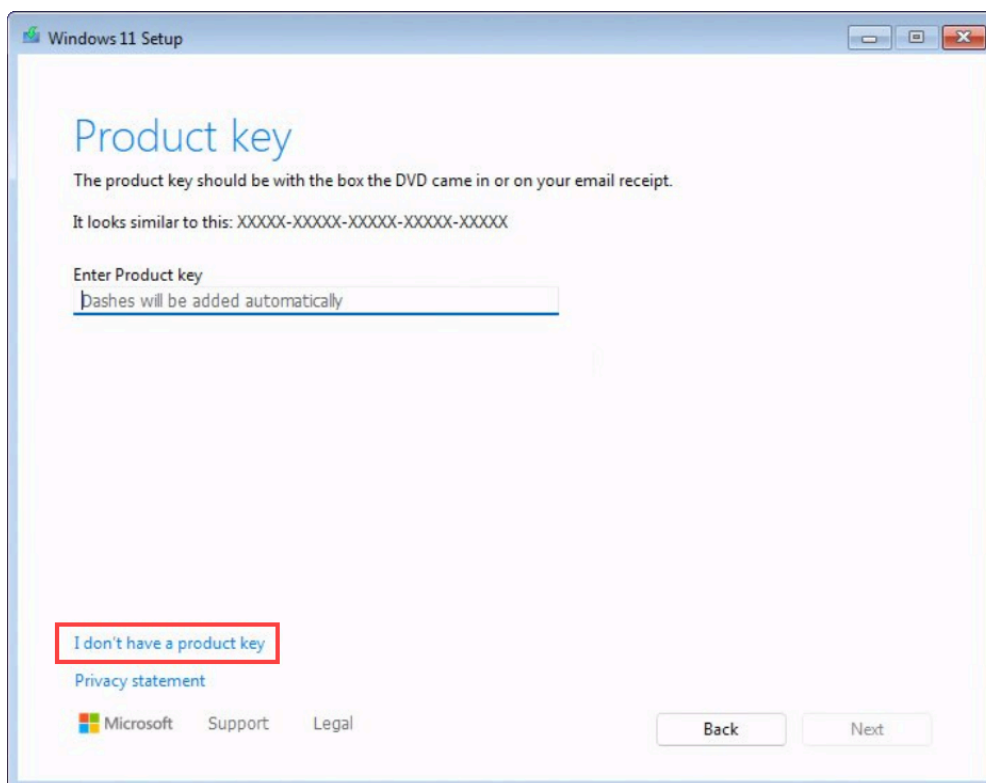
- 1 Pe ecranul *Selectare setări de limbă*, selectați setările de limbă și oră preferate și faceți clic pe **Următorul**.
- 2 Pe ecranul *Selectare setări tastatură*, selectați tastatura preferată și faceți clic pe **Următorul**.
- 3 Pe ecranul *Selectare opțiuni de configurare*, selectați **Instalare Windows X**, unde X reprezintă versiunea Windows pe care o instalați. Confirmați că ștergeți fișierele, aplicațiile și setările dvs. și faceți clic pe **Următorul**.

Notă: Arhivele video stocate pe discul video secundar nu sunt afectate. Numai fișierele de pe discul OS sunt șterse.

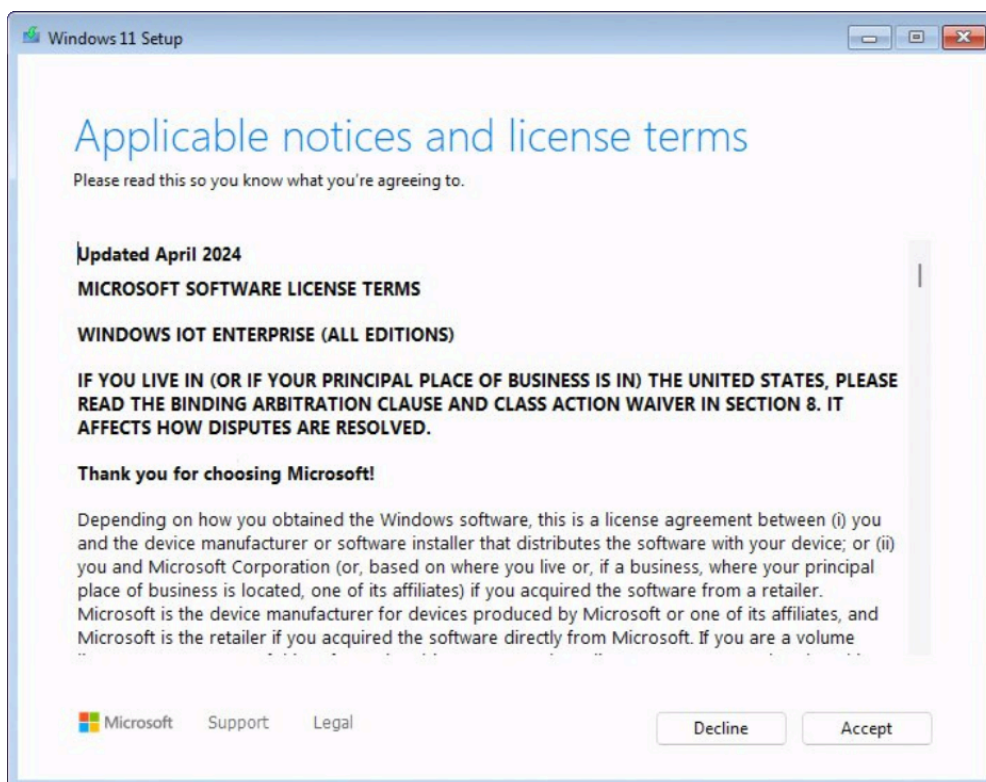


4 Pe ecranul *Cheie produs*, efectuați una dintre următoarele:

- Dacă aparatul este conectat la internet, faceți clic pe **Nu am cheie produs** pentru a continua. Aparatul își preia automat datele de activare de la Microsoft.
- Dacă aparatul nu este conectat la internet, introduceți cheia licenței care se află pe eticheta [Certificatului de autenticitate \(COA\)](#) aplicată pe dispozitiv și faceți clic pe **Următorul**.



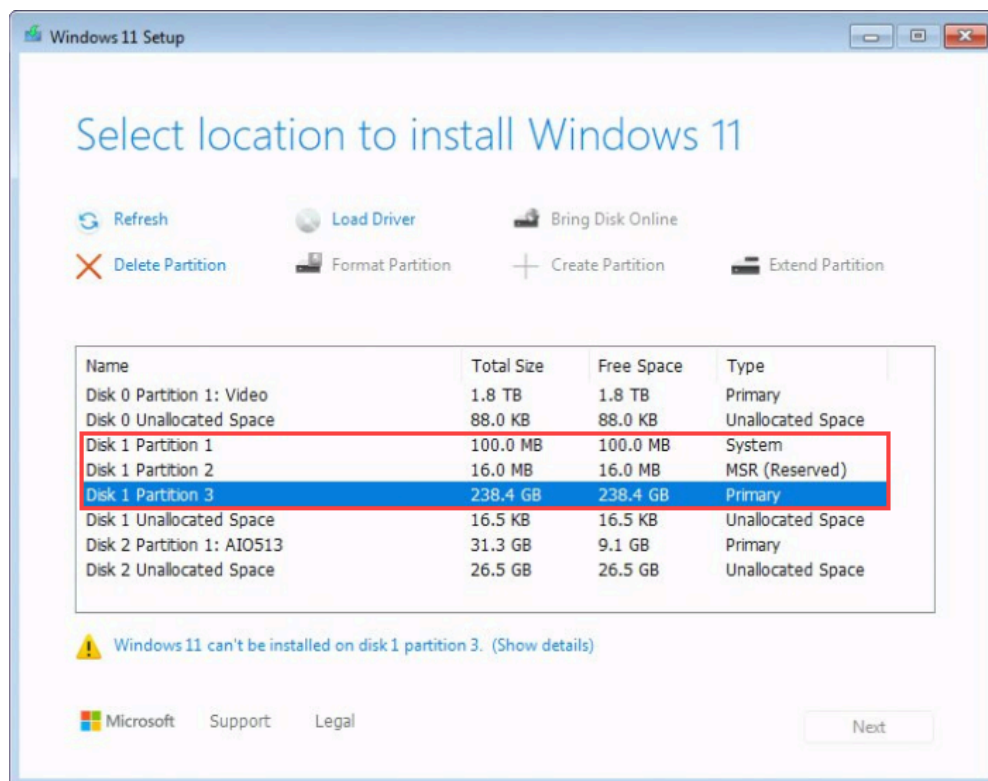
- 5 Pe ecranul *Notificări aplicabile și termeni de licență*, citiți termenii de licență și faceți clic pe **Acceptare**.



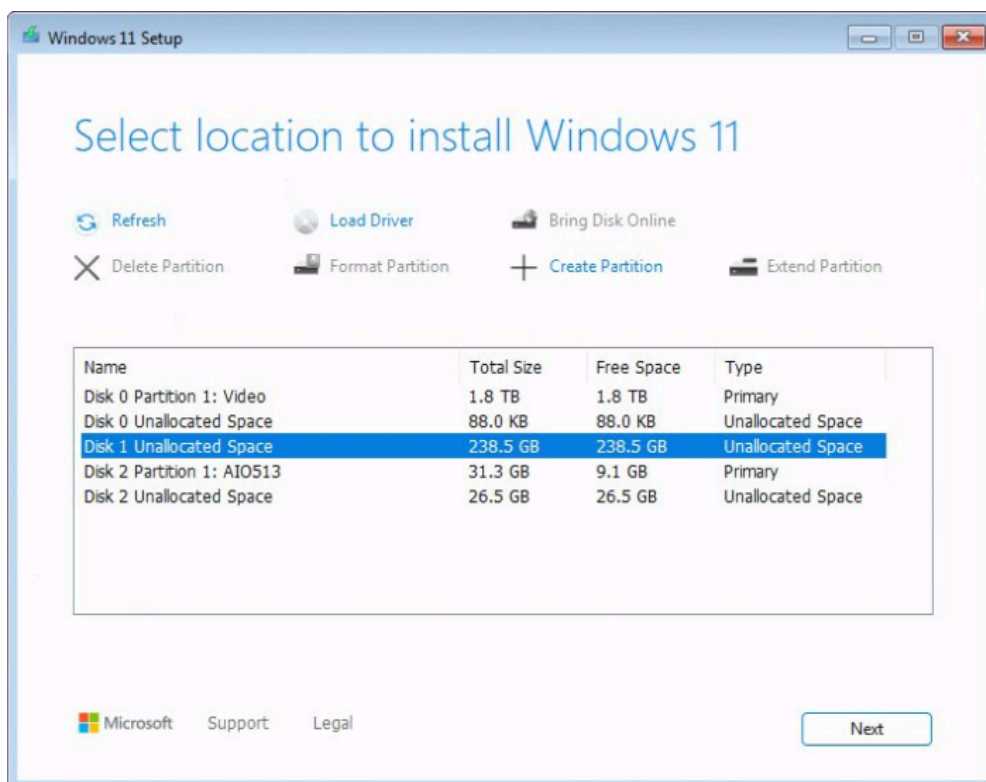
- 6 Pe *Selectați locația pentru instalarea Windows X* ecran, ștergeți partițiile principală, de sistem și MSR (dacă este cazul) de pe discul sistemului de operare.

Pe discul sistemului de operare va rămâne doar spațiul nealocat, iar expertul de instalare Windows va recrea automat partițiile șterse în timpul procesului de instalare.

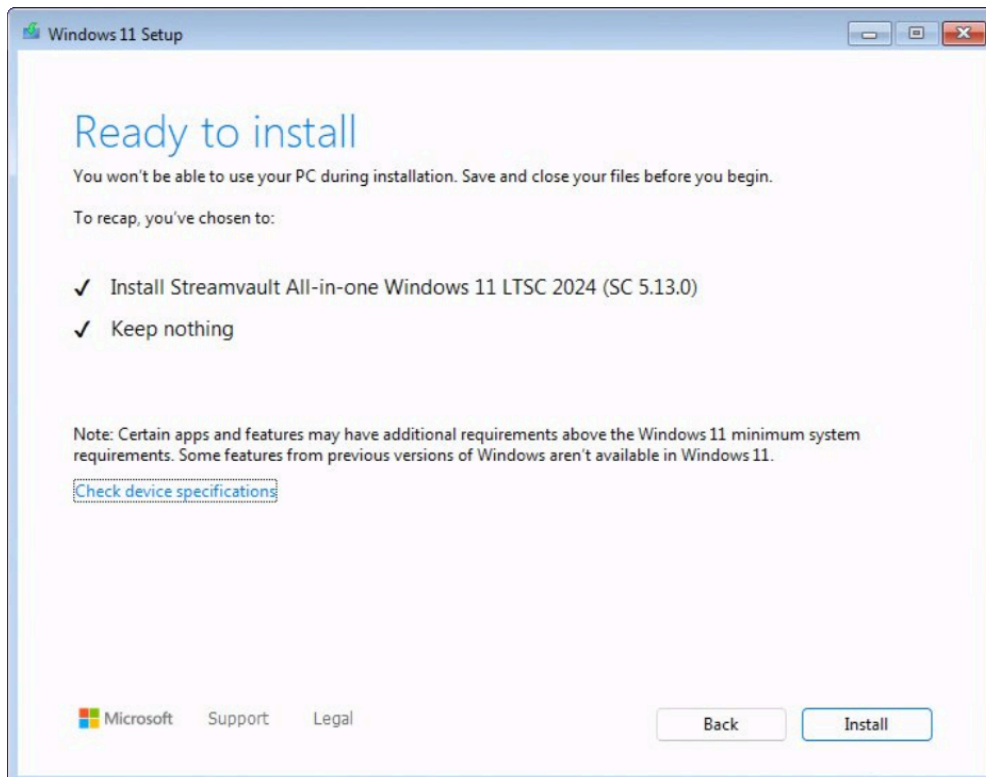
ATENȚIE: Partiția principală de pe discul sistemului de operare are de obicei o dimensiune mai mică de 1 TB. Nu ștergeți partiția principală de pe discul de stocare video, care stochează arhivele video.



- 7 Selectați spațiul nealocat de pe discul sistemului de operare și faceți clic pe **Următorul**.



- 8 Pe ecranul *Gata de instalare*, faceți clic pe **Instalare**.



- 9 Când instalarea este finalizată, sistemul repornește în Windows și rulează automat un script pentru a finaliza instalarea. Când scriptul termină rularea, reporniți dispozitivul.

Exemplu

Urmăriți acest videoclip pentru a învăța cum să resetați imaginea software pe un dispozitiv all-in-one utilizând un USB de pornire care conține fișiere *.swm*.



După ce termini

- Conectați-vă la Windows utilizând numele de utilizator și parola implicită care se află pe autocolantul lipit pe dispozitiv.
- [Activați-vă licența Security Center](#).
- Dacă ați făcut o copie de rezervă a configurațiilor Security Center înainte de resetarea din fabrică, [restaurați configurațiile folosind SV Control Panel](#).
- [Reconfigurați-vă aparatul](#).

Efectuarea unei resetări din fabrică pe o Streamvaultstație de lucru sau un dispozitiv server

Dacă software-ul de pe serverul sau stația de lucru Streamvault™ nu pornește sau nu mai funcționează conform așteptărilor, puteți realiza o resetare din fabrică utilizând o cheie USB.

Înainte de a începe

- Efectuați o copie de rezervă a întregii configurații a Security Center utilizând SV Control Panel. Pentru mai multe informații, consultați [Realizarea unei icopii de rezervă a bazei de date Directory](#) , pagină 36.
- Obțineți o cheie USB cu cel puțin 32 GB de stocare. Unele chei USB nu reușesc să pornească imaginea; în acest caz, încercați să utilizați o altă marcă sau un alt model de cheie.

ATENȚIE: Toate datele de pe cheia USB sunt șterse atunci când creați o unitate bootabilă.

- Aveți licența corectă pentru versiunea de Security Center pe care doriți să o reparați sau să o instalați.
- Aveți ID-ul de sistem și parola care v-au fost trimise prin e-mail atunci când ați achiziționat dispozitivul.

Ce ar trebui să știți

- **Se aplică la:** Toate modelele care încep cu SVW, SVR și SVA și toate serverele cu numerele de model SV-1000E și peste.
- Pentru dispozitivele all-in-one, consultați [Efectuarea unei resetări din fabrică pe un Streamvault dispozitiv All-in-one](#) , pagină 91.
- O resetare din fabrică șterge toate datele aflate în prezent pe unitatea de sistem (OS), dar nu afectează setările implicite din fabrică ale unității RAID.
- Reinițializarea poate eșua atunci când hard disk-urile, unitățile RAID sau partițiile de pe dispozitiv au fost modificate față de setările implicite din fabrică. În astfel de caz, contactați [Genetec™ Technical Assistance Center \(GTAC\)](#).

Procedură

- 1 [Creați o cheie USB de resetare din fabrică.](#)
- 2 [Cu ajutorul cheii USB, reseați imaginea de pe dispozitiv.](#)

După ce termini

[Configurați dispozitivul.](#)

Subiecte conexe

[Găsirea ID-ului sistemului și a versiunii imaginii unui dispozitiv Streamvault](#), pagină 87

Crearea unei chei USB de resetare din fabrică pentru o stație de lucru Streamvault sau un dispozitiv server

Înainte de a putea reseta imaginea unei stații de lucru Streamvault sau un dispozitiv server, trebuie să pregătiți o cheie USB bootabilă care conține imaginea software-ului Streamvault necesară.





Înainte de a începe

Obțineți o cheie USB cu cel puțin 32 GB de stocare. Unele chei USB nu reușesc să pornească imaginea; în acest caz, încercați să utilizați o altă marcă sau un alt model de cheie.

ATENȚIE: Toate datele de pe cheia USB sunt șterse atunci când creați o unitate bootabilă.

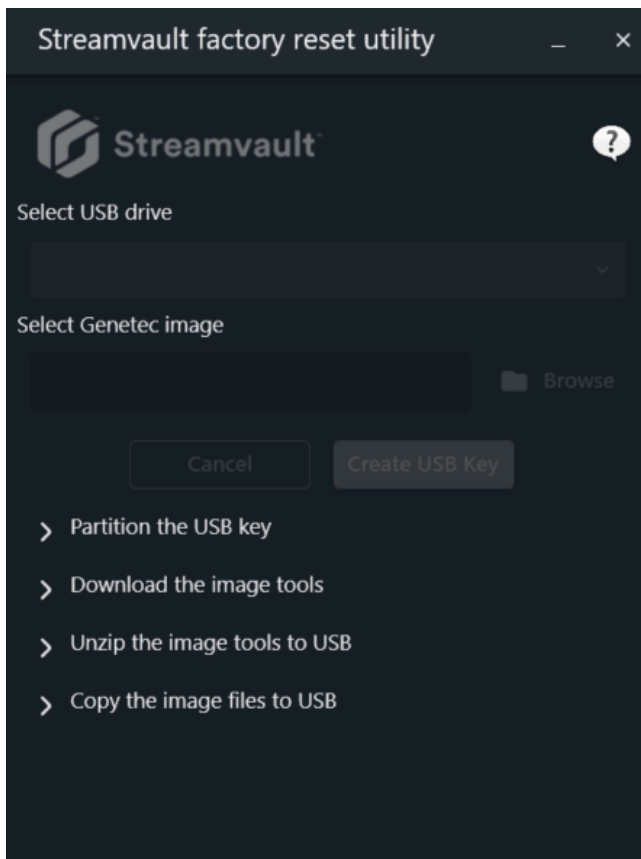
Procedură

- 1 Contactați [Genetec™ Technical Assistance Center \(GTAC\)](#) pentru a obține imaginea de recuperare. Imaginea de recuperare vine în unul dintre următoarele trei formate:
 - Un fișier *.zip* care conține fișiere *.swm*.
 - Un fișier *.iso* care conține fișierele *.swm* și interfața de utilizator a *utilitarului de resetare din fabrică Streamvault*, pe care o veți utiliza pentru a reseta imaginea software.
 - Un fișier *.iso* care conține *expertul de instalare Windows*, pe care îl veți utiliza pentru a reseta imaginea software.
- 2 Dacă imaginea de recuperare este un fișier *.zip*, dezarhivați conținutul în orice folder Windows.
- 3 Din pagina [Descărcare produs](#) de pe GTAP, descărcați USB creator al *utilitarului de resetare din fabrică Streamvault*.
 - a) La *Download Finder*, selectați versiunea dvs. de Security Center.
 - b) Din lista *Altele*, descărcați pachetul *utilitarului de resetare din fabrică Streamvault*.

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

- 4 Introduceți cheia USB într-un port USB.
- 5 Deschideți creatorul USB al *utilitarului de resetare din fabrică Streamvault*.

- 6 Din lista **Selectați unitatea USB**, selectați o cheie USB care are cel puțin 32 GB de stocare.



- 7 În secțiunea *Selectați imaginea Genetec*, dați clic pe **Răsfoire** și selectați fișierul *.swm* sau *.iso* descărcat. Dacă aveți nevoie de un fișier *.swm*, selectați imaginea necesară din folderul *<număr etichetă de serviciu>*.
- 8 Dați clic pe **Creare cheie USB**.
Utilitarul de resetare din fabrică Streamvault începe să partiționeze cheia USB, să descarce instrumentele de imagine și să copieze fișierele de imagine.
- Când descărcarea este finalizată, este afișat următorul mesaj: *Cheia USB a fost creată cu succes.*

Exemplu

Următorul videoclip vă arată cum să creați o cheie USB cu resetare din fabrică cu un *.iso* fișier.



După ce termini

[Resetați imaginea software a Streamvault stației de lucru sau a dispozitivului server.](#)

Resetarea imaginii software pe o Streamvault stație de lucru sau un dispozitiv server

După ce ați pregătit o cheie USB bootabilă care are imaginea software Streamvault™ necesară, o puteți utiliza pentru a reseta imaginea software pe o stație de lucru sau un dispozitiv server.

Înainte de a începe

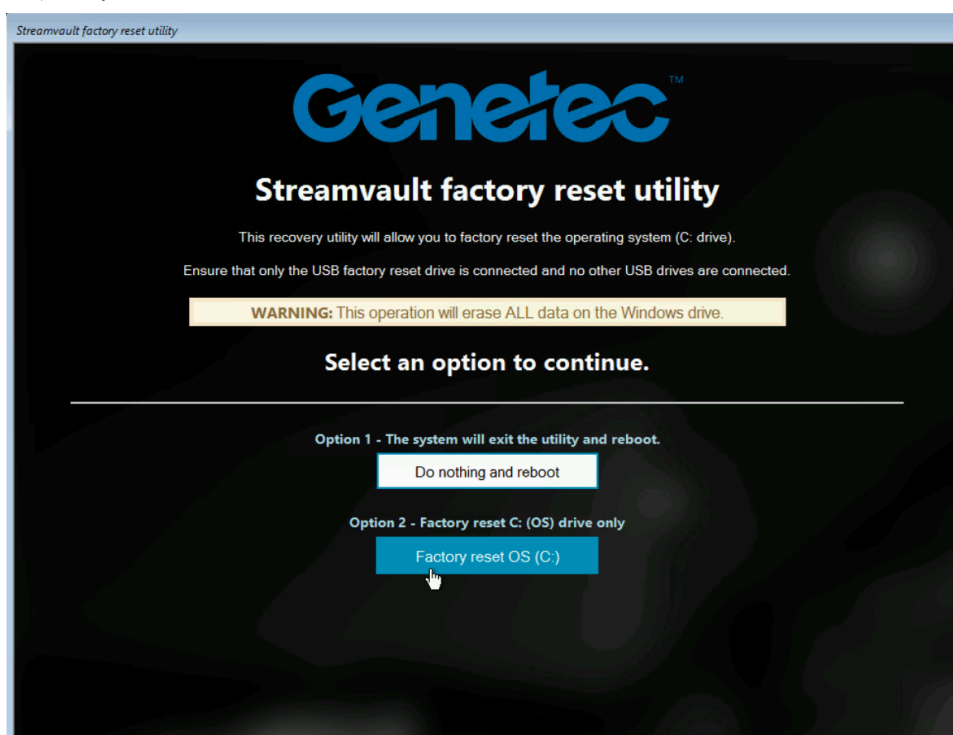
- Asigurați-vă că aveți cheia USB care conține software-ul de recuperare pentru dispozitivul dvs.

Ce ar trebui să știți

- Resetarea nu afectează setările implicite din fabrică ale unității RAID.
- Reinițializarea ar putea eșua dacă hard disk-urile, unitățile RAID sau partițiile de pe dispozitiv au fost modificate față de setările implicite din fabrică. În astfel de caz, contactați [Genetec™ Technical Assistance Center \(GTAC\)](#).

Procedură

- 1 Închideți dispozitivul.
- 2 Introduceți cheia USB bootabilă pe care ați creat-o într-un port USB.
- 3 Alimentați cu energie Streamvault dispozitivul.
- 4 Atunci când vi se solicită, apăsați F12.
Se deschide *Boot Manager*. Dați clic pe **Meniul de bootare One-shot UEFI**.
- 5 Selectați unitatea USB, apoi apăsați Enter.
Se deschide *Utilitarul de resetare din fabrică Streamvault*
- 6 Dați clic pe **Resetarea din fabrică a OS (C:)**.



Se deschide un Prompt de comandă și *Utilitarul de resetare din fabrică Streamvault* analizează sistemul pentru a detecta unitatea de sistem (OS).

- 7 În Promptul de comandă, tastați Da pentru a confirma că a fost detectată unitatea de hard disk corectă și apoi apăsați Enter pentru a începe resetarea din fabrică.
IMPORTANT: Nu întrerupeți, nu opriți și nu reporniți stația de lucru în timpul procesului de reimaginare. Ar putea dura până la 20 minute, în funcție de viteza cheii USB.
- 8 După ce resetarea din fabrică este finalizată, atunci când vi se cere să reporniți stația de lucru, apăsați Enter.
- 9 Scoateți cheia USB din portul USB.

Stația de lucru este acum resetată la starea sa implicită.

Exemplu

Urmăriți acest videoclip pentru a afla cum se resetează imaginea software pe o stație de lucru sau un dispozitiv server Streamvault.



După ce termini

- Conectați-vă la Windows utilizând numele de utilizator și parola implicită care se află pe autocolantul lipit pe dispozitiv.
- [Activați-vă licența Security Center.](#)
- Dacă ați făcut o copie de rezervă a configurațiilor Security Center înainte de resetarea din fabrică, [restaurați configurațiile folosind SV Control Panel.](#)
- [Reconfigurați-vă aparatul.](#)

Controlerele Mercury EP rămân offline atunci când TLS 1.1 este dezactivat

După înscrierea unui controler Mercury EP în Security Center, unitatea nu se activează online.

Nu primiți erori sau avertismente cu privire la această problemă.

Se aplică la:

- Streamvault™ SV-100E 16.3 și versiuni ulterioare
- Streamvault™ SV-300E 16.3 și versiuni ulterioare
- Streamvault™ SV-350E 16.3 și versiuni ulterioare

Cauza

Toate controlerele Mercury EP necesită protocolul Transport Layer Security (TLS) 1.1 pentru a comunica cu Security Center. Cu toate acestea, protocolul este dezactivat pe toate dispozitivele all-in-one Streamvault™ 16.3 și cu versiuni ulterioare.

Soluție

[Activați TLS 1.1.](#)

Activarea Transport Layer Security (TLS)

Protocoalele Transport Layer Security (TLS) 1.0 și 1.1 prezintă mai multe vulnerabilități majore, astfel că sunt dezactivate pe dispozitivele Streamvault™. Atunci când un dispozitiv înscris în Security Center necesită unul dintre aceste protocoale pentru comunicare, trebuie să activați protocolul respectiv pe dispozitivul dumneavoastră.

Ce ar trebui să știți

- TLS 1.1 este dezactivat în imaginea software Streamvault 16.3 și versiuni ulterioare.
- TLS 1.0 este dezactivat în imaginea software Streamvault 16.0 și versiuni ulterioare.
- Activați numai versiunea de TLS care este necesară pentru dispozitivul dumneavoastră.
- Activați TLS în nodurile server (intrare) și client (ieșire).
- Din motive de securitate, opțiunile Proprietăți Internet sunt dezactivate pe dispozitive. Dacă dispozitivul dvs. are serviciul Streamvault, puteți activa TLS din Editorul de politici de grup local. Dacă dispozitivul dvs. nu are serviciul Streamvault, puteți activa TLS numai din Editorul de registru Windows.

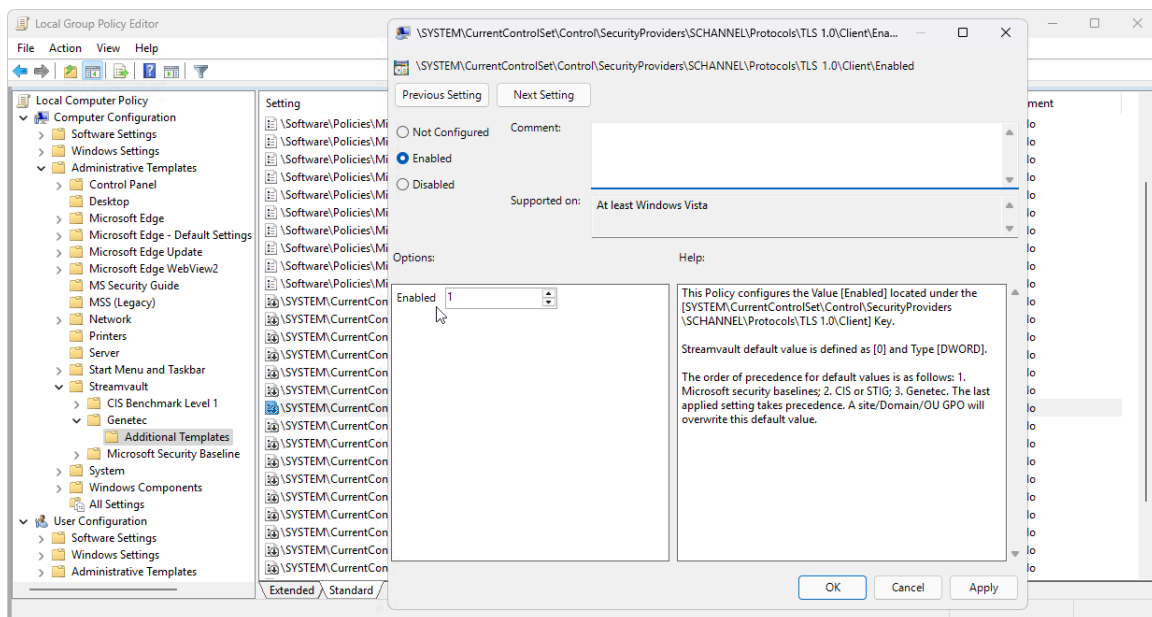
Procedură

Pentru a activa TLS pe un dispozitiv cu serviciul Streamvault:

- 1 Deschideți Promptul de comandă ca administrator și rulați `gpedit.msc`.
Se deschide Editorul de politici de grup local.
- 2 Du-te la **Configurarea computerului > Șabloane administrative > Streamvault > Genetec > Șabloane suplimentare**.
- 3 Activează TLS 1.*n* la client, unde *n* reprezintă numărul versiunii minore:
 - a) Dați clic dreapta pe `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\Enabled` și dați clic pe **Editare**.
 - b) Setati **Activat** la 1 și dați clic **Aplicare > OK**.
 - c) Dați clic dreapta pe `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\DisabledByDefault` și dați clic pe **Editare**.
 - d) Setati **DisabledByDefault** la 0 și dați clic **Aplicare > OK**.

4 Activați TLS 1.n pe server:

- Dați clic dreapta pe `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Server\Enabled` și dați clic **Editare**.
- Setați **Activat** la 1 și dați clic **Aplicare** > **OK**.
- Dați clic dreapta pe `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Server\DisabledByDefault` și dați clic pe **Editare**.
- Setați **DisabledByDefault** la 0 și dați clic **Aplicare** > **OK**.

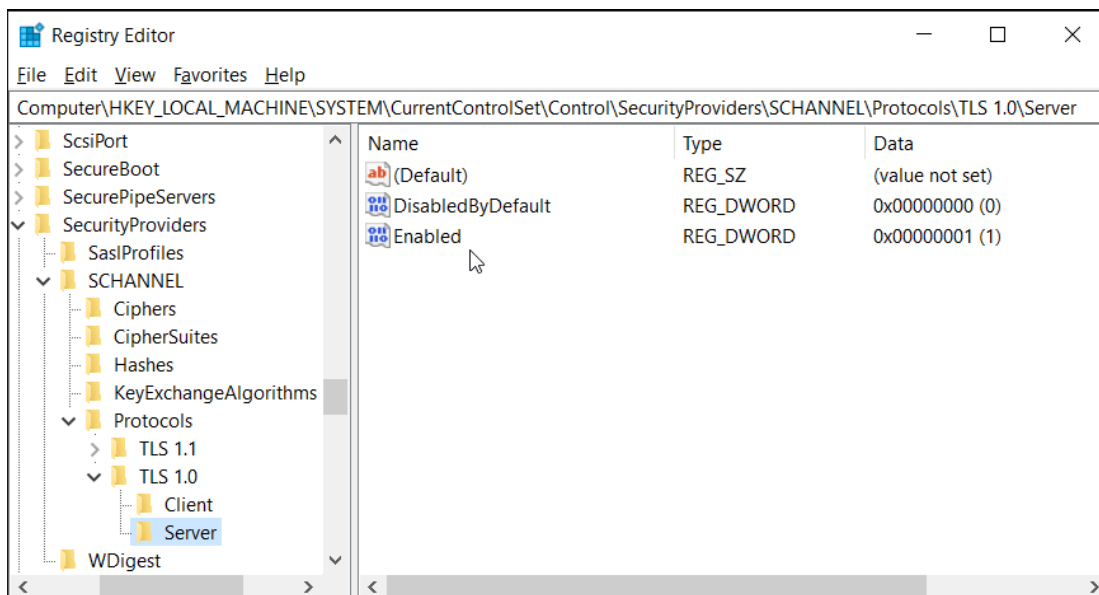


5 Reporniți Windows.

Pentru a activa TLS pe un dispozitiv fără serviciul Streamvault:

- Deschideți Editorul de registru Windows.

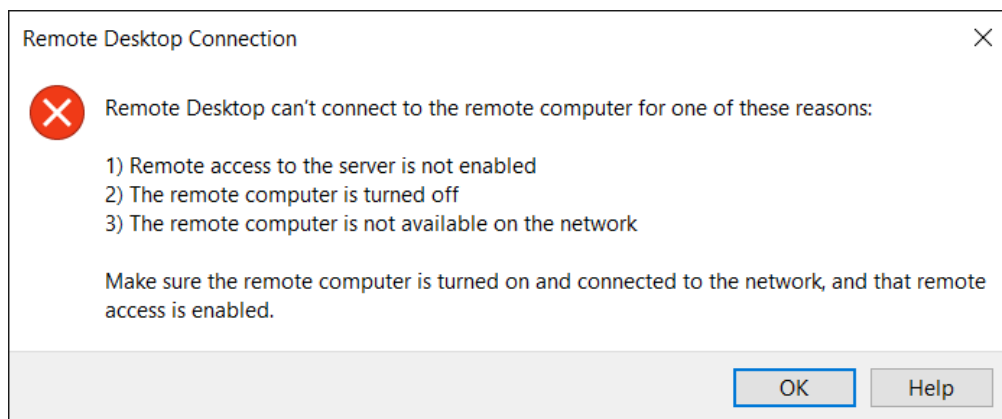
- 2 Activează TLS 1.*n*, unde *n* reprezintă numărul versiunii minore:
 - a) Navigați la `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n`.
 - b) Selectați nodul **Server**, setați **DezactivatImplicit** la 0 și setați **Activat** la 1.
 - c) Selectați nodul **Client**, setați **DezactivatImplicit** la 0 și setați **Activat** la 1.



- 3 Reporniți Windows.

Remote Desktop nu se poate conecta la un dispozitiv Streamvault

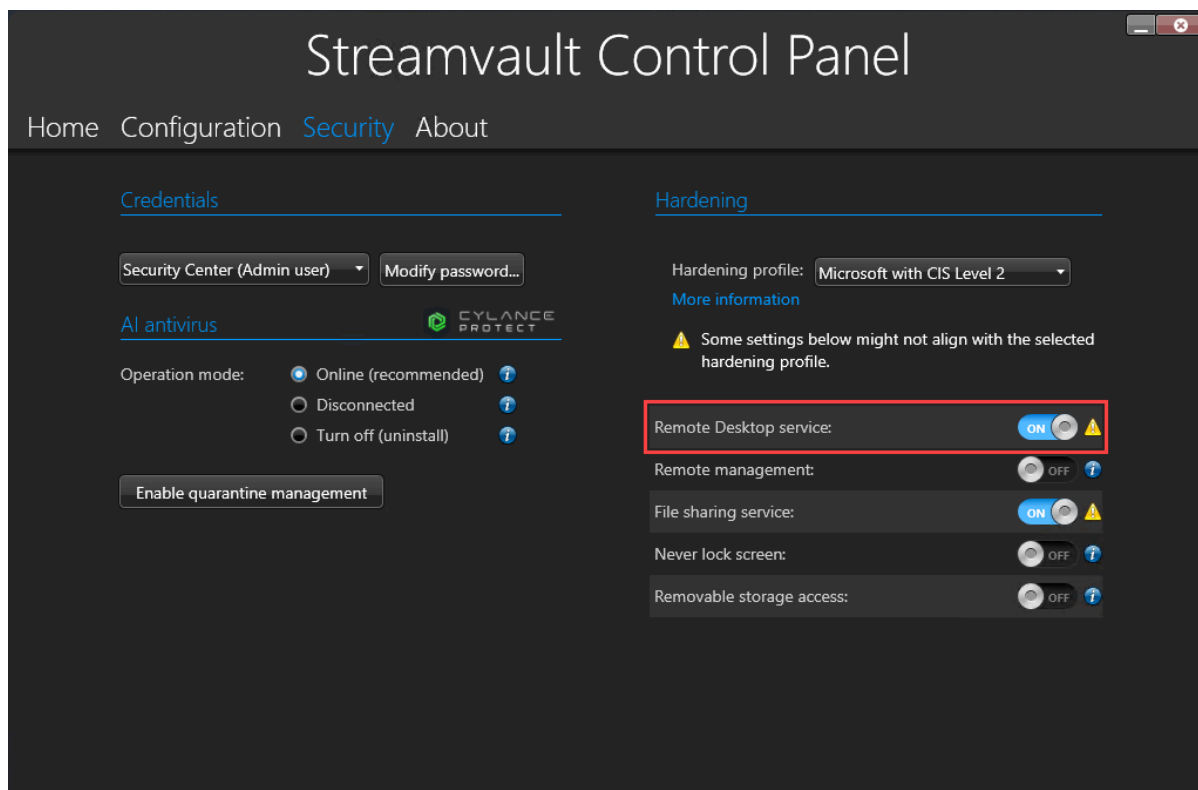
Atunci când încercați să accesați un dispozitiv Streamvault™ utilizând Remote Desktop, primiți un mesaj care indică faptul că Remote Desktop nu se poate conecta la computerul de la distanță.



Serviciul Desktop la distanță este dezactivat în Panoul de control SV

Descriere: Pentru a asigura o securitate maximă, accesul de la distanță este dezactivat în mod implicit pe un dispozitiv.

Soluție: [Activați accesul de la distanță pe dispozitiv](#). Pe pagina *Securitate* Panoului de control SV, porniți **Serviciu Remote Desktop**.



Remote Desktop nu este permis în Windows

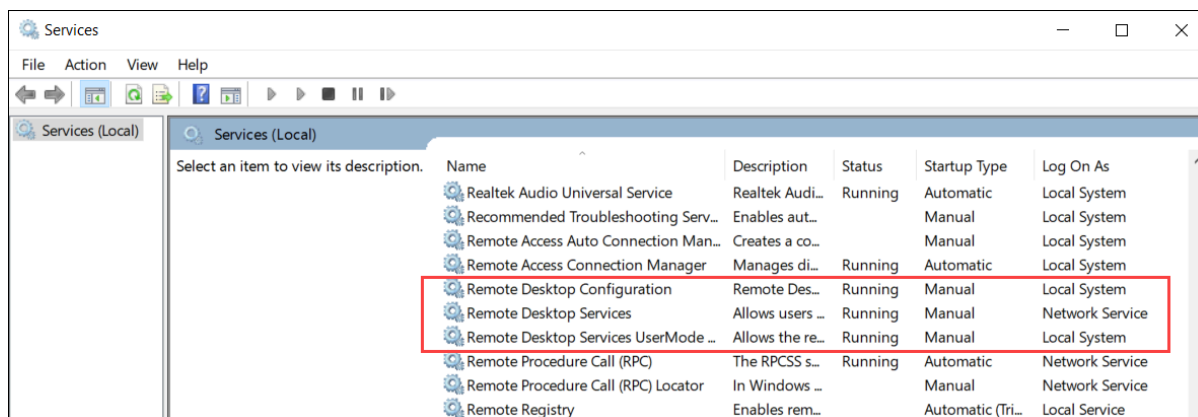
Descriere: Deși **serviciul Remote Desktop** este activat în SV Control Panel, această setare nu este permisă în prezent în Windows.

Soluție: Suprascrieți setarea Windows prin dezactivarea și apoi activarea opțiunii **serviciului Remote Desktop**.

Serviciile Remote Desktop nu rulează

Descriere: Serviciile Remote Desktop au fost oprite în Windows.

Soluție: Deschideți consola Windows Services, asigurați-vă că **Serviciile Remote Desktop** este conectat ca utilizator **Network Service** și asigurați-vă că celelalte servicii Remote Desktop rulează.

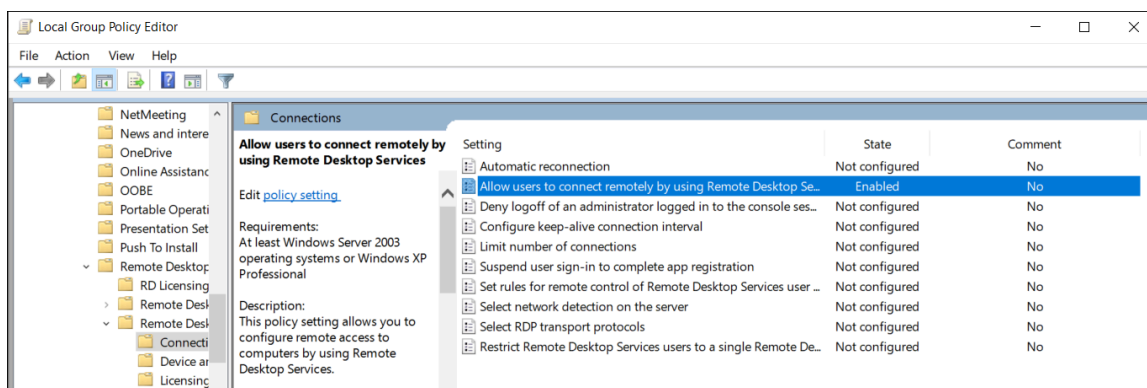


Serviciile Remote Desktop sunt refuzate

Descriere: Windows este configurat pentru a refuza accesul utilizatorilor de la distanță la serviciile Remote Desktop.

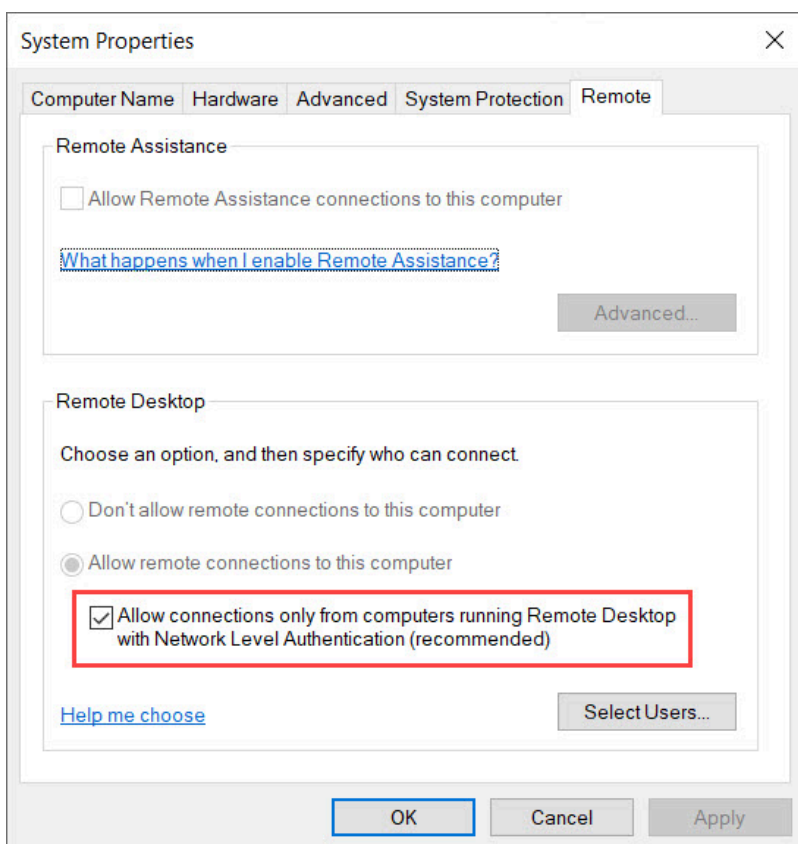
Soluție: Permiteți accesul utilizatorilor de la distanță la dispozitiv utilizând Remote Desktop Services:

1. Deschideți Promptul de comandă ca administrator și rulați `gpedit.msc`.
2. Mergeți la **Configurare computer > Scheme administrative > Componente Windows > Servicii Remote Desktop > Gazdă de sesiune Remote Desktop > Conectări**.
3. Activare **Permite utilizatorilor să se conecteze de la distanță prin intermediul serviciilor Remote Desktop**.



4. În Prompt de comandă, rulați `gpupdate /force`.

5. Din Panoul de control Windows, mergeți la **Sistem și securitate > Permiteți accesul** de la distanță .
Se deschide fereastra *Proprietăți sistem* în fila **Remote** .
6. În secțiunea *Remote Desktop* , asigurați-vă că este selectat **Permite conexiuni numai de la computere care rulează Desktop la distanță cu autentificare la nivel de rețea (recomandat)**.



Politicile de grup locale refuză accesul la distanță

Descriere: Politicile de grup locale Windows sunt configurate pentru a refuza accesul de la distanță la dispozitivul dumneavoastră.

Soluție: Configurați politicile de grup de pe dispozitivul dvs. pentru a permite accesul de la distanță:

1. Deschideți Promptul de comandă ca administrator și rulați `gpedit.msc`.
2. Mergeți la **Configurare computer > Configurare Windows > Configurare securitate > Politici locale > Atribuire drepturi utilizator**.
3. Verificați următoarele setări ale politicii de grup:
 - **Permiteți conectarea prin Servicii la distanță** este setat la **Administratori**.
 - **Interzicerea accesului la acest computer din rețea** este setată la **Oaspeți**.
 - **Refuzați autentificarea prin Servicii Remote Desktop** este setat la **Invitați**.

Autentificarea NTLMv2 nu este acceptată

Descriere: Dispozitivul sau computerul de la distanță nu acceptă autentificarea NTLMv2.

Notă: Dacă toate computerele client acceptă NTLMv2, Microsoft® și mai multe organizații independente recomandă cu tărie politica *Trimiteți NTLMv2 doar răspunsuri*. Consultați Microsoft [Securitatea rețelei: Nivel de autentificare LAN Manager](#) cele mai bune practici și considerații de securitate înainte de a modifica setările.

Soluție: Pentru a vă asigura că mediul dvs. permite autentificarea NTLMv2:

1. Deschideți Promptul de comandă ca administrator și rulați `gpedit.msc`.
2. Accesați **Configurare computer > Configurare Windows > Configurare securitate > Politici locale > Opțiuni de securitate > Securitate rețea: Nivelul de autentificare LAN Manager**.
3. Setati politica la **Send LM & NTLM - utilizați securitatea sesiunii NTLMv2 dacă a fost negociată**.

Contactați-ne

Soluție: Dacă Conexiunea Desktop la distanță nu se poate conecta, [contactați Centrul de asistență tehnică Genetec \(GTAC\)](#).

Subiecte conexe

[Permiterea conexiunilor Remote Desktop la un dispozitiv Streamvault](#), pagină 89

Eliminarea restricțiilor de la conturile de utilizatori non-administratori

În mod implicit, conturile de utilizator care nu sunt administrator, inclusiv Operatorul, au acces limitat la caracteristicile Panoului de control Streamvault™. Puteți elimina restricțiile din acele conturi pentru a le oferi mai mult acces la funcții.

Înainte de a începe

- Doar o persoană conectată ca administrator poate elimina restricțiile din conturile care nu sunt administrator.
- Restricțiile pot fi eliminate numai pe sistemele cu serviciul Streamvault.

Procedură

- 1 Deschideți File Explorer și navigați la *C:\Windows\System32\GroupPolicyUsers*.
- 2 Ștergeți dosarul *S-1-5-32-545* și tot conținutul acestuia. Acest folder conține restricțiile pentru non-administratori.
- 3 Reporniți Windows.

Conturile locale nu pot accesa Desktop la distanță, serviciul de partajare a fișierelor și gestionarea de la distanță

Când **Serviciu Desktop la distanță**, **Management de la distanță**, sau **Serviciu de partajare a fișierelor** opțiunile sunt activate în SV Control Panel, conturile locale încă nu pot accesa funcțiile.

Acest comportament se aplică produselor Windows Server care au SV Control Panel 3.0 și versiuni ulterioare:

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

În mod implicit, serviciul Desktop la distanță, managementul de la distanță și serviciul de partajare a fișierelor sunt dezactivate pentru administratorul local și conturile locale, cum ar fi Operator. Cu versiunile anterioare ale SV Control Panel, administratorul local și conturile locale au avut acces la aceste funcții atunci când au fost activate. Începând cu SV Control Panel 3.0, numai administratorul local are acces atunci când funcțiile sunt activate.

Acest nou comportament este controlat prin intermediul politicii de securitate **Interziceți accesul la acest computer din rețea** și respectă linia de bază de securitate Microsoft pentru Windows Server.

Activarea serviciilor legate de Smart Card

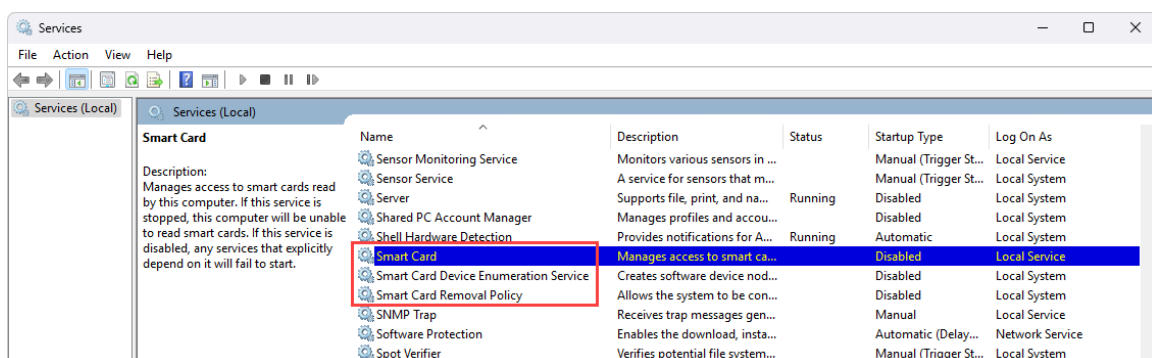
Dacă ați făcut upgrade la SV Control Panel 3.0 de la o versiune mai veche și doriți să activați serviciile legate de Smart Card, puteți face acest lucru prin intermediul aplicației Windows Services.

Ce ar trebui să știți

Opțiunea **Activați suportul pentru carduri inteligente** nu este disponibilă în SV Control Panel 3.0, deoarece serviciile Smart Card sunt activate în mod implicit.

Procedură

- 1 În Windows, rulați *servicii.msc* pentru a deschide aplicația *Servicii*.
- 2 Activați serviciul **Smart Card**.
 - a) Dați clic dreapta pe **Smart Card** service și selectați **Proprietăți**.
Se deschide caseta de dialog *Proprietăți*.
 - b) Pe fila **General**, localizați câmpul **Tip de pornire** și selectați **Automat**.
 - c) Dați clic pe **Aplicare** > **OK**.
- 3 Activați **Serviciul de enumerare a dispozitivelor Smart Card**.
 - a) Dați clic dreapta pe **Serviciul de enumerare a dispozitivelor Smart Card** și selectați **Proprietăți**.
Se deschide caseta de dialog *Proprietăți*.
 - b) Pe fila **General**, localizați câmpul **Tip de pornire** și selectați **Manual**.
 - c) Dați clic pe **Aplicare** > **OK**.
- 4 Activați **Serviciul de enumerare a dispozitivelor Smart Card**.
 - a) Dați clic dreapta pe serviciul **Politica de eliminare a cardurilor inteligente** și selectați **Proprietăți**.
Se deschide caseta de dialog *Proprietăți*.
 - b) Pe fila **General**, localizați câmpul **Tip de pornire** și selectați **Manual**.
 - c) Dați clic pe **Aplicare** > **OK**.



Activarea suportului pentru controlerele Mercury EP și LP firmware 1.x.x

Înainte de a putea integra controlere Mercury EP sau LP firmware 1.xx pe dispozitivul dvs. Streamvault™, trebuie să activați o suită de criptare SSL mai veche.

Ce ar trebui să știți

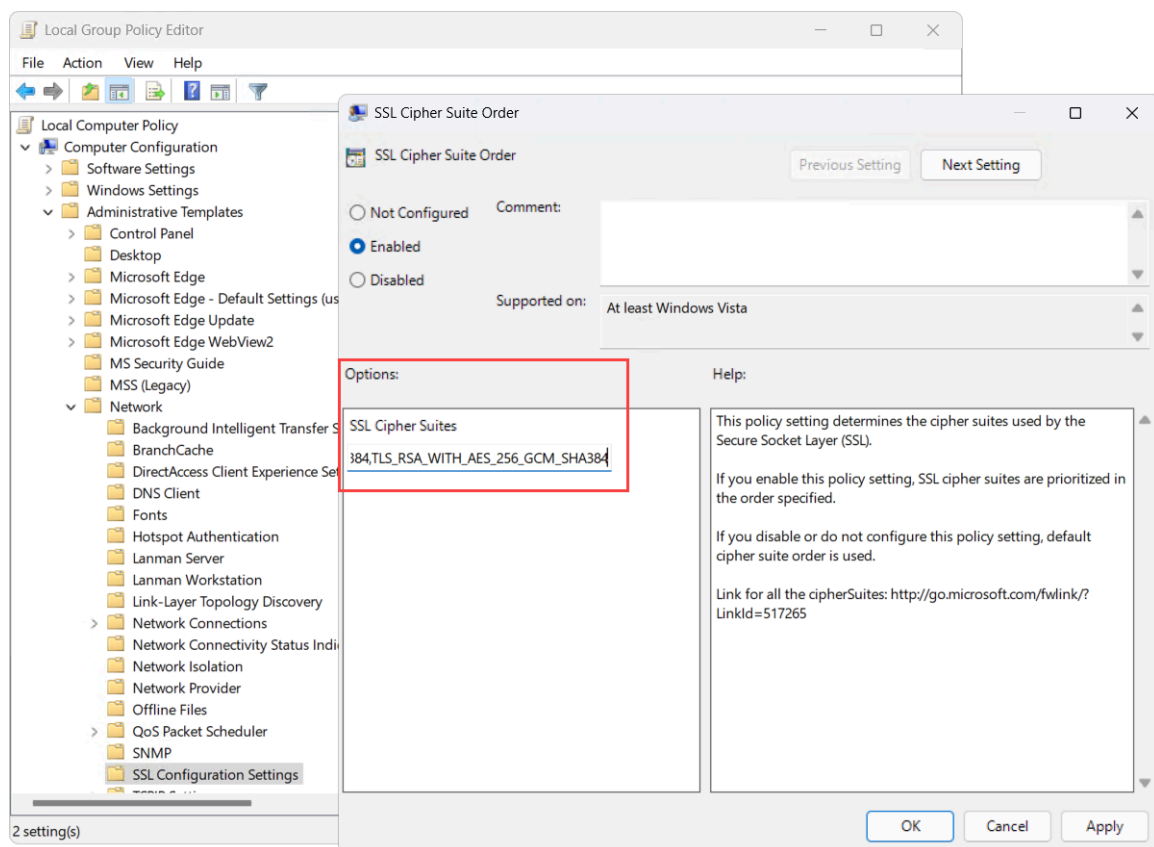
În funcție de integrarea dvs., trebuie adăugată una dintre următoarele suite de criptare pentru a permite unităților să comunice cu aparatul:

- **integrarea controlerului Mercury EP pe firmware-ul 1.29.7 și versiuni anterioare:**
 - TLS_RSA_WITH_AES_256_GCM_SHA384
 - TLS_RSA_WITH_AES_128_GCM_SHA256
- **integrarea controlerului Mercury EP pe firmware-ul 1.29.7 și versiuni anterioare:**
 - TLS_RSA_WITH_AES_256_CBC_SHA

Procedură

- 1 În Windows, rulați `gpedit.msc` pentru a deschide *Editor local de politici de grup*.
- 2 Navigați la **Configurarea computerului > Șabloane administrative > Rețea > Setări de configurare SSL**.
- 3 Dați dublu clic **Comanda SSL Cipher Suite**.
- 4 În *Opțiuni* panou, în **SSL Cipher Suites** câmp, adăugați o virgulă la sfârșitul listei, urmată de suite de criptare aplicabilă integrării dumneavoastră. Nu adăugați niciun spațiu.

- 5 Clic **OK** pentru a salva obiectul de politică de grup (GPO).



- 6 Reporniți Serviciul Software sau reporniți aparatul.

Activarea suportului pentru integrarea Synergis IX

Înainte de a putea înscrie controlere Synergis™ IX pe dispozitivul dvs. Streamvault™, trebuie să adăugați o suită suplimentară de criptare SSL.

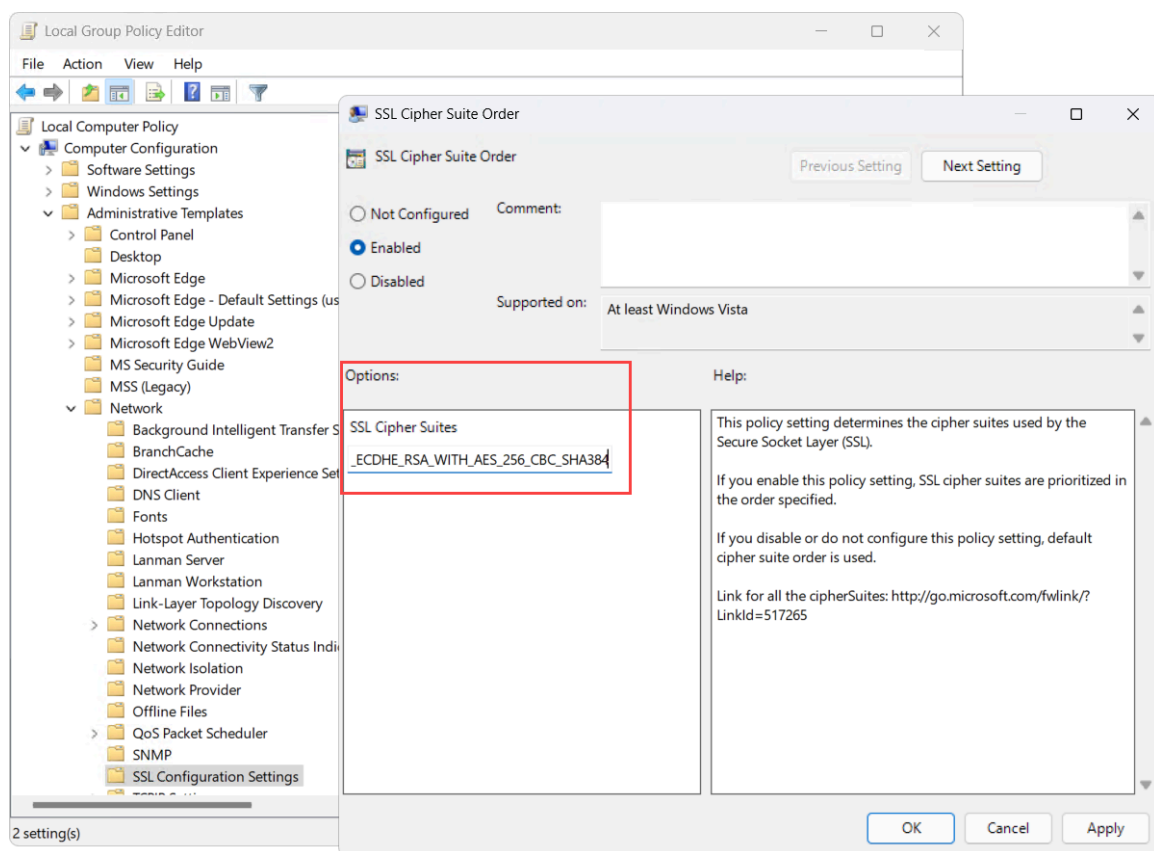
Ce ar trebui să știți

Una dintre următoarele suite de criptare trebuie adăugată pentru a înscrie controlerele Synergis IX pe dispozitivul dvs. Streamvault:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Procedură

- 1 În Windows, rulați `gpedit.msc` pentru a deschide *Editor local de politici de grup*.
- 2 Navigați la **Configurarea computerului** > **Șabloane administrative** > **Rețea** > **Setări de configurare SSL**.
- 3 Dați dublu clic **Comanda SSL Cipher Suite**.
- 4 În *Opțiuni* panou, în **SSL Cipher Suites** câmp, adăugați o virgulă la sfârșitul listei, urmată de TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 sau TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256. Nu adăugați niciun spațiu.
- 5 Clic **OK** pentru a salva obiectul de politică de grup (GPO).



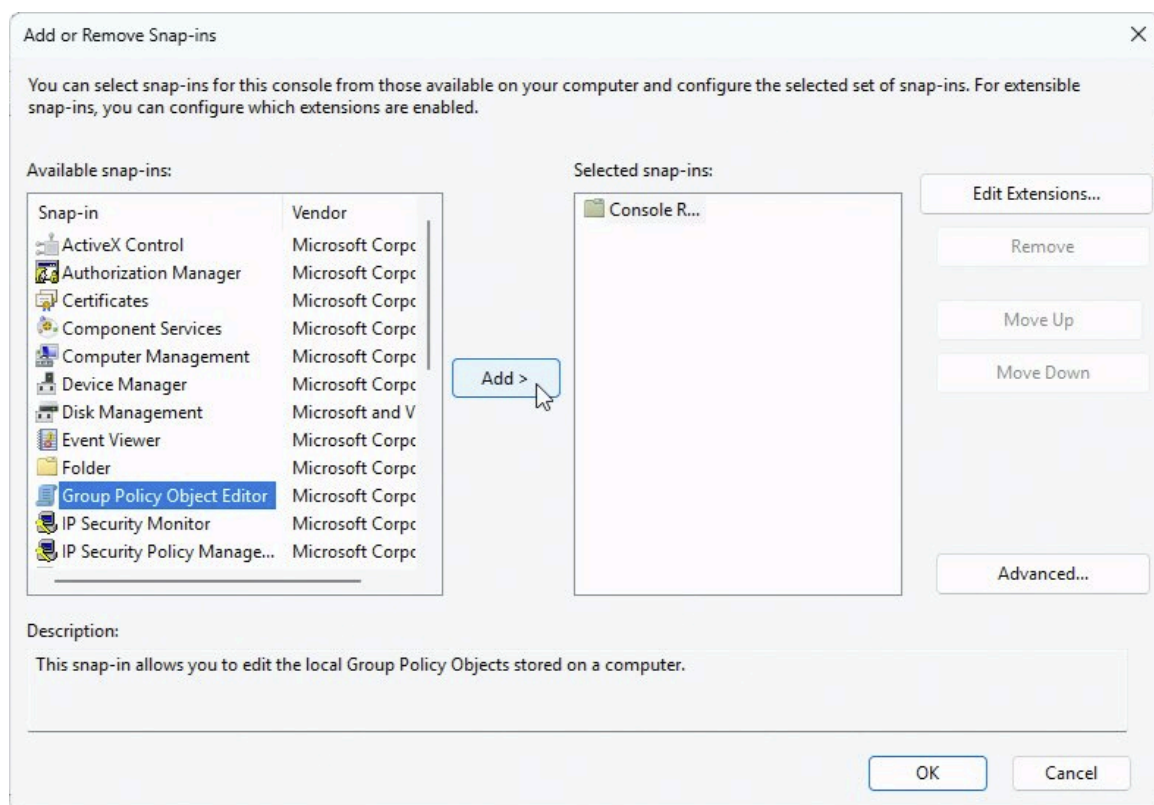
- 6 Reporniți Serviciul Software sau reporniți aparatul.

Modificarea GPO-urilor locale pentru conturile de utilizator non-administrator

În mod implicit, conturile de utilizatori care nu au drepturi de administrator au acces restricționat la funcțiile dispozitivului Streamvault™. Pentru a personaliza permisiunile acestora, puteți modifica obiectele politicii de grup locale (GPO) pentru **Non-administratori** grup prin intermediul Consolei de administrare Microsoft.

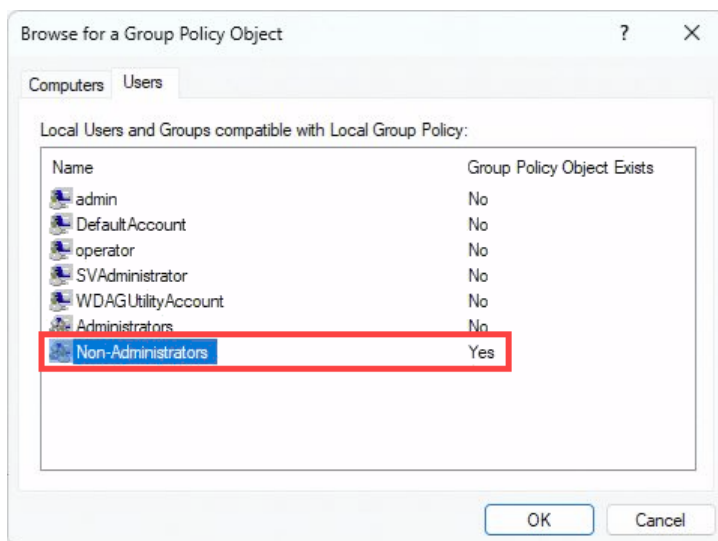
Procedură

- 1 Din meniul Start din Windows, selectați **Aleargă**, apoi tastați `mmc .exe` și faceți clic pe **Bine**. Cel/Cea/Cei/Cele *Consola de administrare Microsoft* se deschide fereastra.
- 2 În panoul din stânga, faceți clic pe **Fișier > Adăugați/Eliminați un snap-in**. Cel/Cea/Cei/Cele *Adăugarea sau eliminarea snap-in-urilor* se deschide o casetă de dialog.
- 3 În **Snap-in-uri disponibile** secțiune, selectați **Editorul de obiecte de politică de grup** și faceți clic **Adăuga**.



- 4 În *Obiect de politică de grup expert*, faceți clic **Răsfoiți**.

- 5 În *Căutare după un obiect de politică de grup* caseta de dialog, faceți clic pe **Utilizatori** fila, selectați **Non-administratori** grup pentru care există un GPO local și faceți clic pe **Bine**.

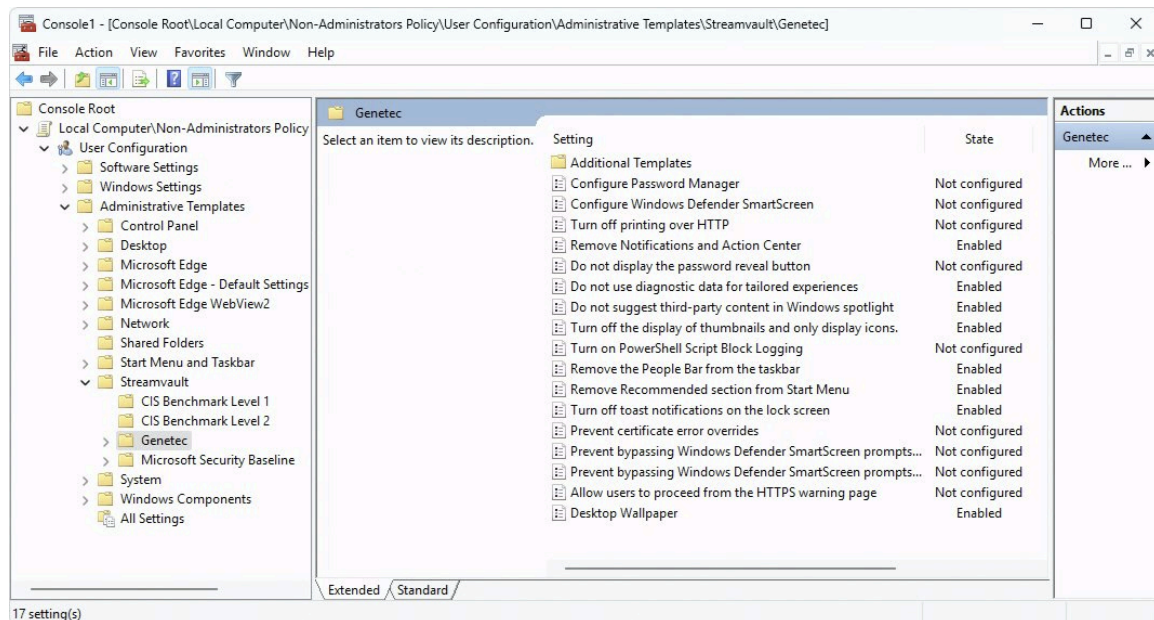


- 6 În *Selectați obiectul politicii de grup* casetă de dialog, faceți clic pe **Termina**.
- 7 Cel/Cea/Cei/Cele *Adăugarea sau eliminarea snap-in-urilor* casetă de dialog, faceți clic pe **Bine**.
- 8 În *Consola de administrare Microsoft* fereastră, mergeți la **Consolă rădăcină** > **Politica pentru computerul local\persoane care nu sunt administratori** > **Configurarea utilizatorului** > **Șabloane administrative** > **Streamvault** > **< profil de întărire >**,

unde < profil de întărire > reprezintă unul dintre cele patru profiluri de consolidare predefinite: CIS Benchmark Nivel 1, CIS Benchmark Nivel 2, Genetec™ și Microsoft Security Baseline.

Toate obiectele GPO configurate pentru conturi non-administrator sunt listate în profilul de securizare selectat.

Notă: Un GPO este configurat dacă starea sa este *Activat* sau *Persoane cu dizabilități*. Un GPO cu o stare de *Neconfigurat* nu este controlat de Streamvault.



- 9 Faceți dublu clic pe obiectele GPO individuale pentru a le vizualiza sau edita.

Subiecte conexe

[Informații de conectare pentru conturile de utilizator implicite de pe unStreamvault aparat](#), pagină 12

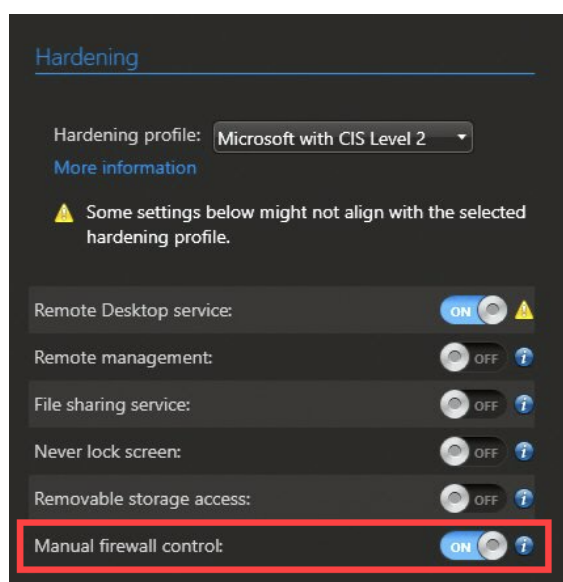
Dezactivarea paravanului de protecție Windows

În mod implicit, Paravanul de protecție Windows utilizează obiecte de politică de grup locală (GPO) din profilurile de consolidare pentru a securiza dispozitivul Streamvault™. Dacă doriți să dezactivați Paravanul de protecție Windows în scopuri de depanare, trebuie mai întâi să activați controlul manual al paravanului de protecție în Panoul de control SV.

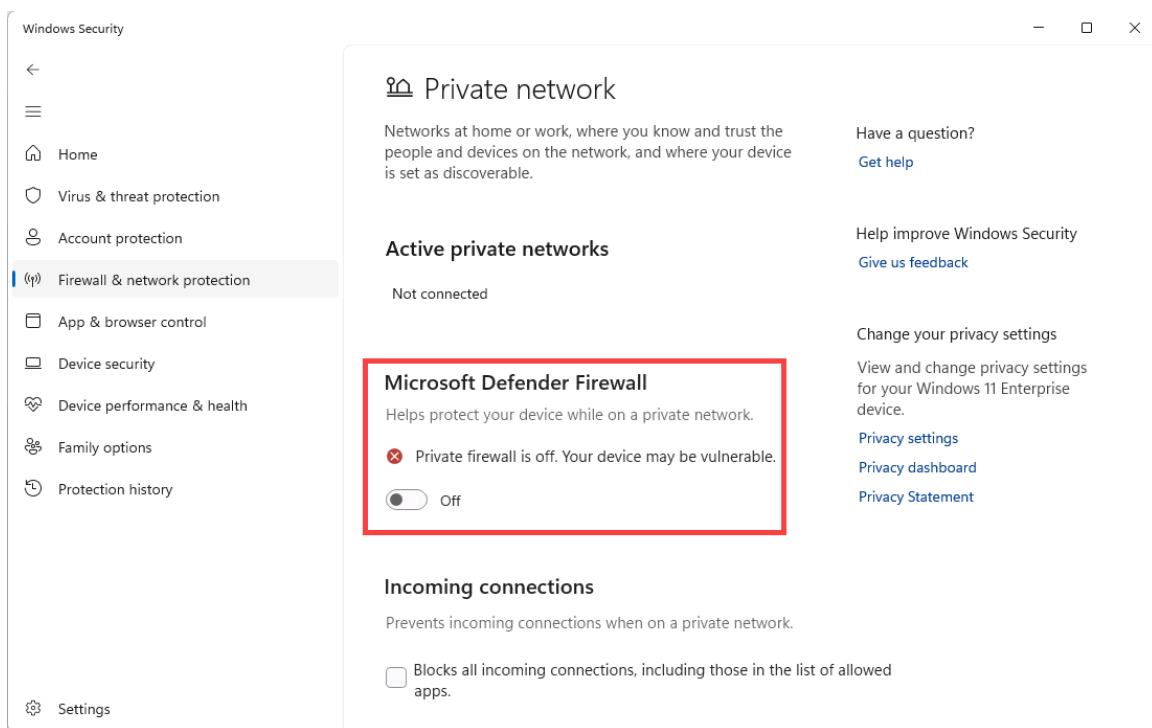
Procedură

- 1 Deschideți Panoul de control SV și accesați *Securitate* pagină.
- 2 În *Întărire* secțiune, porniți **Control manual al firewall-ului** opțiune și faceți clic **Aplică**.
Așteptați ca setarea să fie aplicată.

Notă: Când această opțiune este activată, toate obiectele GPO locale sunt dezactivate. Nicio regulă a firewall-ului nu este afectată.



- 3 Din meniul Start din Windows, deschideți **Firewall& protecția rețelei**.
- 4 Selectați rețeaua pentru care doriți să dezactivați firewall-ul.

5 În *Firewall Microsoft Defender* secțiune, dezactivați firewall-ul.

Notă: De asemenea, puteți dezactiva firewall-ul prin *Firewall Windows Defender cu securitate avansată*.

Asistență tehnică

Această secțiune include următoarele subiecte:

- " [Streamvault Contactarea Centrului de asistență tehnică Genetec](#) ", pagină 126
- " [Asistență software](#) ", pagină 129
- " [Suport hardware](#) ", pagină 130
- " [Specificații pentru Streamvault](#) ", pagină 131
- " [Termeni și condiții de asistență Streamvault](#) ", pagină 132

Streamvault Contactarea Centrului de asistență tehnică Genetec

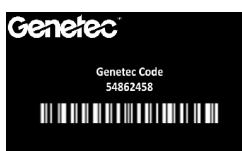
Centrul de asistență tehnică Genetec™ (GTAC) vă stă la dispoziție pentru a vă ajuta cu orice problemă software sau hardware legată de Streamvault™.

Notă: Pentru întrebări legate de problemele legate de software-ul Genetec™ Security Center, asistența tehnică este oferită prin intermediul liniei noastre obișnuite de asistență tehnică. Pentru a afla numărul de telefon și programul de lucru al GTAC din regiunea dumneavoastră, consultați pagina [Genetec Technical Assistance Center Contact us](#).

Informații utile

Atunci când deschideți un caz de asistență, aveți la dispoziție următoarele informații:

- ID-ul de sistem de licență Security Center. Pentru mai multe informații, consultați [Cum îmi găsesc ID-ul de sistem?](#).
- Numărul de serie Genetec sau eticheta de service hardware.
- Codul dumneavoastră Genetec, care se găsește pe șasiu (nu se aplică dispozitivelor all-in-one). Codul este necesar în cazul în care ați pierdut accesul administrativ la sistem și aveți nevoie de o imagine din fabrică.



- Fișierul jurnal TSR de diagnosticare (dacă este cazul). Pentru mai multe informații, consultați [Colectarea jurnalelor de asistență](#).

Contactarea GTAC prin telefon

Asistența telefonică pentru problemele legate de Streamvault™ este disponibilă pentru toți clienții în timpul orelor de program din regiunea lor.

Pentru clienții din America de Nord, Europa, Orientul Mijlociu și Africa:

1. Consultați pagina [Centrul de asistență tehnică Genetec™ \(GTAC\) Contactați-ne](#) pentru a afla numărul de telefon și programul de lucru al GTAC din regiunea dumneavoastră.
2. Sunați la numărul de telefon GTAC și alegeți opțiunea #2.

Pentru clienții din regiunea Asia-Pacific:

Asistența pentru regiunea APAC este furnizată prin intermediul [Portalului de asistență tehnică Genetec \(GTAP\)](#) prin chat live și cazuri de asistență. Orele de funcționare sunt de luni până vineri de la 8:00 - 20:00 (ora locală).

Pentru 24/7 asistență de urgență în afara orelor de program:

1. Sunați la numărul de telefon al GTAC pentru regiunea dumneavoastră.
2. Introduceți numărul de identificare a certificării Genetec.
3. Introduceți numărul de contract Genetec Advantage sau numărul de abonament Genetec.
4. Selectați produsul.

5. Lăsați un mesaj care să conțină numele dumneavoastră, numărul de telefon și o descriere a problemei.
Inginerul de gardă vă contactează în 30 minute.

IMPORTANT: 24/7 asistența de urgență este disponibilă numai pentru clienții care au adăugat această opțiune la contractul Genetec Advantage. Pentru mai multe informații contactați advantage@genetec.com.

Clienții care nu au acoperire Advantage trebuie să deschidă un caz prin intermediul [Portalului de asistență tehnică Genetec \(GTAP\)](#).

Contactarea GTAC prin intermediul GTAP

Asistența pentru problemele Streamvault™ este disponibilă pentru toți clienții în timpul orelor de lucru din regiunea lor prin intermediul cazurilor de asistență online pe [portalul de asistență tehnică Genetec™ \(GTAP\)](#).

Pentru clienții care nu au acoperire Genetec™ Advantage, trebuie să fie deschis un caz prin intermediul [Portalului de asistență tehnică Genetec \(GTAP\)](#). Pentru mai multe informații despre Genetec Advantage, contactați advantage@genetec.com.

Pentru a depune un caz prin intermediul portalului online:

1. Navigați la [Genetec Technical Assistance Portal](#).
2. Autentificați-vă folosind adresa de e-mail a companiei.
3. Dați clic pe **+ Creați cazul**.



4. Din lista **ID-ului de sistem**, selectați sistemul vizat.
5. Pentru returnarea sau repararea hardware-ului, includeți **Cerere RMA** în titlu, astfel încât echipa noastră să poată identifica cu ușurință aceste cereri.

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. Includeți numărul de serie al produsului dumneavoastră, codul Genetec și fișierul jurnal TSR de diagnosticare (dacă este cazul).
7. Dați clic pe **Trimiteți cazul**.

Veți primi o confirmare a cazului prin e-mail cu timpul estimat de răspuns.

Contactarea GTAC prin chat live

Asistența pentru problemele Streamvault™ este disponibilă pentru clienții cu acoperire Genetec™ Advantage prin chat live pe [portalul de asistență tehnică Genetec \(GTAP\)](#). Clienții pot primi asistență în timpul orelor de lucru din regiunea lor.

Pentru clienții care nu au acoperire Genetec Advantage, trebuie să fie deschis un caz prin intermediul [Portalului de asistență tehnică Genetec \(GTAP\)](#). Pentru mai multe informații despre Genetec Advantage, contactați advantage@genetec.com.

Pentru a începe un chat live:

1. Mergeți la [Portalul de asistență tehnică Genetec](#)
2. Autentificați-vă folosind adresa de e-mail a companiei.
3. Dați clic pe butonul **click to chat**.



4. Alegeți limba preferată.
5. Introduceți ID-ul complet de sistem (GSC-xxxxxx-xxxxxx), apoi dați clic pe **Verificare ID sistem**.
6. Alegeți dacă doriți să discutați despre un caz nou sau existent.
7. Selectați produsul.
8. Dați clic pe **Pornire chat**.

9. Pentru a iniția un RMA, includeți numărul de serie al produsului, codul Genetec și fișierul jurnal TSR de diagnosticare (dacă este cazul).
 Timpul de răspuns (disponibil numai în timpul orelor de lucru din regiunea dumneavoastră): De obicei, în 5 minute.

Asistență software

Software-ul de imagine Streamvault™ Windows include cea mai recentă versiune a software-ului Security Center și a panoului de control în momentul creării imaginii. Asistența pentru imaginea Windows și software-ul Security Center sunt abordate separat.

Software Streamvault™

- Imaginea Streamvault™ Windows este acoperită de garanția Streamvault pentru întregul ciclu de viață al dispozitivului.
IMPORTANT: Actualizarea sistemului de operare Windows nu este acoperită de garanție. Actualizarea sistemului de operare Windows șterge driverele necesare, hardening-ul și software-ul instalat împreună cu imaginea.
- Imaginea de rezervă furnizată pentru reimaginarea unui dispozitiv Streamvault include sistemul de operare original și imaginea furnizată împreună cu dispozitivul la cumpărare.
- Imaginea Streamvault Windows este acoperită de garanția Streamvault, indiferent de statutul dumneavoastră Genetec™ Advantage.

Software-ul Security Center

Problemele cu software-ul Security Center sunt acoperite de acordul privind nivelul serviciilor (SLA) și de procedurile de asistență descrise în următorul document Genetec™ Lifecycle Management (GLM): [Genetec Advantage Descriere](#).

Suport hardware

Garanțiile HP și [Dell ProSupport](#) sunt disponibile prin intermediul Genetec™. Pentru orice problemă hardware, Genetec Technical Assistance Center (GTAC) este punctul dvs. de contact pentru a diagnostica problema și pentru a se coordona cu HP și DellProSupport.

Consultați [Prezentare generală a garanției hardware Genetec](#) pentru detalii despre garanțiile hardware Streamvault oferite de Genetec.

Specificații pentru Streamvault

Consultați următoarele specificații tehnice, mecanice și de mediu atunci când planificați și implementați dispozitivul dvs. Streamvault™.

Specificații tehnice, mecanice și de mediu

Dispozitive all-in-one:

- [Fișa tehnică SV-300E](#)

Dispozitive pentru montare în rack:

- [Fișa tehnică a seriei SV-1000E](#)
- [Fișa tehnică a seriei SV-2000E](#)
- [Fișa tehnică a seriei SV-4000E](#)

Stocare centralizată de înaltă disponibilitate:

- [Fișa tehnică a seriei SV-7000EX](#)

Stații de lucru:

- [Fișa tehnică a seriei SVA-100E](#)
- [Fișa tehnică a seriei SVW-300E](#)
- [Fișa tehnică a seriei SVW-500E](#)

Dispozitive de monitorizare a vehiculelor all-in-one:

- [Fișa tehnică a seriei SVR-300A](#)
- [Fișa tehnică a seriei SVR-300AR](#)
- [Fișa tehnică a seriei SVR-500A](#)

Termeni și condiții de asistență Streamvault

Garanțiile hardware standard și extinse Genetec™ sunt guvernate de termenii și condițiile descrise în [Prezentare generală a garanției hardware Genetec](#).

Glosar

Dispozitiv SV

Streamvault™ este un dispozitiv la cheie care vine cu un sistem de operare încorporat și Security Center preinstalat. Puteți utiliza dispozitivele Streamvault™ pentru a implementa rapid un sistem de supraveghere video și de control al accesului unificat sau independent.

Hardware Streamvault™

Hardware Streamvault™ este o comandă de raportare în Security Center pe care o puteți utiliza pentru a vizualiza o listă de probleme de sănătate care afectează dispozitivele Streamvault™.

imagine de fabricație

O imagine de fabricație este o imagine Streamvault™ care este expediată clienților atunci când achiziționează un aparat. Versiunile de software instalate pe această imagine variază în funcție de comanda clientului.

imagine de recuperare

O imagine de recuperare este utilizată pentru reimaginarea dispozitivelor Streamvault™. Este o imagine fixă cu versiuni specifice de software preinstalate.

Manager Streamvault™

Entitatea Manager Streamvault™ este utilizată pentru a controla configurațiile de alertă pentru un grup de entități Agent Streamvault™. Este permis un singur Manager Streamvault™ pentru fiecare sistem.

Monitor hardware Streamvault™

Entitatea monitor hardware Streamvault™ este utilizat pentru a monitoriza starea de sănătate a dispozitivelor Streamvault™ și pentru a vă asigura că primiți notificări atunci când apar probleme. Este necesar un monitor hardware Streamvault™ pentru fiecare dispozitiv Streamvault™.

Serviciul Streamvault

Serviciul Streamvault este un serviciu Windows care permite utilizatorilor să configureze un dispozitiv Streamvault™, precum aplicarea profilurilor de întărire.

SV-1000E

SV-1000E este un dispozitiv de securitate rentabil, montat în rack, conceput pentru sisteme de securitate de dimensiuni medii. Acesta vă ajută să treceți la un sistem de securitate unificat care combină supravegherea video, controlul accesului, recunoașterea automată a plăcuțelor de înmatriculare, comunicațiile, intruziunea și analiza într-un singur dispozitiv. SV-1000E este livrat cu Security Center și SV Control Panel preinstalate.

SV-100E

SV-100E este un dispozitiv subcompact all-in-one care vine cu Microsoft Windows, Security Center și SV Control Panel preinstalate. SV-100E este destinat instalațiilor la scară mică, cu un singur server, și poate suporta atât camere cât și cititoare de control al accesului.

SV-2000E

SV-2000E este un dispozitiv de securitate montat în rack care vă permite să implementați cu ușurință un sistem unificat care combină supravegherea video, controlul accesului, recunoașterea automată a plăcuțelor de înmatriculare și comunicațiile. SV-2000E este livrat cu Security Center și SV Control Panel preinstalate.

SV-300E

SV-300E este un dispozitiv compact, all-in-one, la cheie, care vine cu Microsoft Windows, Security Center și SV Control Panel preinstalate. Cu ajutorul cardurilor de captură a codificatorului analogic încorporat, puteți utiliza dispozitivul pentru a implementa rapid un sistem de supraveghere video sau de control al accesului autonom sau un sistem unificat.

SV-350E

SV-350E este un dispozitiv de securitate "all-in-one", la cheie, care vă ajută să treceți la un sistem unificat care combină supravegherea video, controlul accesului, detectarea intruziunilor și comunicațiile. Vine cu Microsoft Windows, Security Center și SV Control Panel preinstalat. Acesta oferă RAID 5 pentru stocarea video critică.

SV-4000E

SV-4000E este un dispozitiv de securitate montat în rack care oferă performanță și fiabilitate de nivel enterprise. Configurațiile sale hardware certificate și întărirea imediată împotriva amenințărilor cibernetice simplifică proiectarea și implementarea unui nou sistem de securitate. SV-4000E este livrat cu Security Center și SV Control Panel preinstalate.

SV-7000E

SV-7000E este un dispozitiv de securitate montat în rack conceput pentru aplicații care combină un număr mare de camere de înaltă rezoluție, utilizatori și evenimente. SV-7000E este livrat cu Security Center și SV Control Panel preinstalate.

SVA-100E

SVA-100E este un dispozitiv compact pe care îl puteți utiliza pentru a vă îmbunătăți cu ușurință sistemul de securitate cu ajutorul analizei video KiwiVision™. Designul este optimizat pentru a vă permite să aplicați mai multe fluxuri analitice la sistemul de supraveghere video, fie că este vorba de un singur flux analitic sau de mai multe fluxuri analitice, pentru fiecare cameră.

SV Control Panel

SV Control Panel este o aplicație de interfață cu utilizatorul pe care o puteți utiliza pentru a configura dispozitivul Streamvault™ pentru a funcționa cu controlul de acces și supravegherea video Security Center.

SVW-300E

Stația de lucru SVW-300E este o soluție la cheie concepută pentru monitorizarea sistemelor de securitate de dimensiuni mici și medii, cu suport pentru mai multe ecrane. SVW-300E vine cu Security Center preinstalat.

SVW-500E

Stația de lucru SVW-500E este o soluție de înaltă performanță concepută pentru utilizatorii care au nevoie de posibilitatea de a vizualiza camere cu o rezoluție foarte mare pe monitoare 4K și pereți video. SVW-500E vine cu Security Center preinstalat.

Utilitar de resetare din fabrică Streamvault

Utilitarul de resetare din fabrică Streamvault este un instrument care vă permite să reseta un dispozitiv Streamvault la setările din fabrică. Instrumentul vă ajută să creați o cheie USB bootabilă cu ajutorul imaginii software Streamvault.

Unde puteți găsi informații despre produs

Puteți găsi documentația noastră de produs în următoarele locuri:

- **Genetec™ TechDoc Hub:** Cea mai recentă documentație este disponibilă în [TechDoc Hub](#).
Nu găsiți ceea ce căutați? Contactați documentation@genetec.com
- **Pachet de instalare:** Ghidul de instalare și notele de versiune sunt disponibile în folderul pachetului de instalare. Aceste documente dispun de asemenea de un link de descărcare directă către cea mai recentă versiune a documentului.
- **Ajutor:** Clientul Security Center și aplicațiile bazate pe web includ ajutor, care explică modul în care funcționează produsul și oferă instrucțiuni despre cum să utilizați caracteristicile produsului. Pentru a accesa secțiunea de ajutor, faceți clic pe **Ajutor**, apăsați pe F1 sau atingeți ? (semnul întrebării) în diferitele aplicații ale clientului.