Video integrity protection

Prevent video evidence tampering and unauthorized exports

Leaks, breaches, and tampered evidence can result in jeopardized security, sanctions, and reputational damage. That's why you need to protect the integrity and confidentiality of your data. Security Center Omnicast™ helps you ensure evidence remains available, and that it is not leaked or tampered with.

Protect against tampering

A digital signature helps protect video footage from alterations. Combined with audit trails and supervised exports, you can maintain a full chain of custody. It also allows you to share admissible and secure files while ensuring that recipients receive legitimate, tamper-free evidence.

Prevent data leaks

Visual watermarking deters users from leaking video by stamping their username and workstation information on live or recorded footage. Add password protection to confidential video exports, and you'll significantly reduce the risk of leakage.

Keep your data confidential

With end-to-end encryption, video remains protected and inaccessible by unauthorized users. Operations are shielded with multiple layers of authentication and authorization.

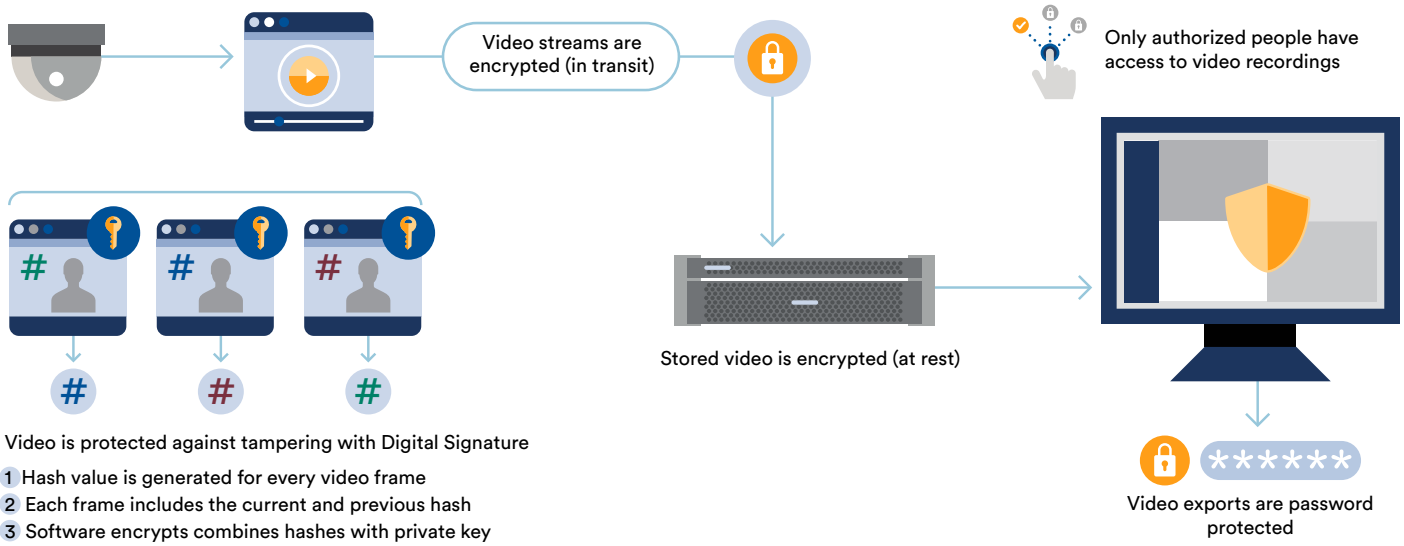
Industry:
Applies to all industries

Applications:
Security Center, Video Surveillance, Clearance

Category:
Security

Key benefits

- Ensure video evidence is admissible in court
- Deter users from leaking private information
- Protect your system with multiple layers of encryption, authentication and authorization
- Maintain a full chain of custody



Video is protected against tampering with Digital Signature

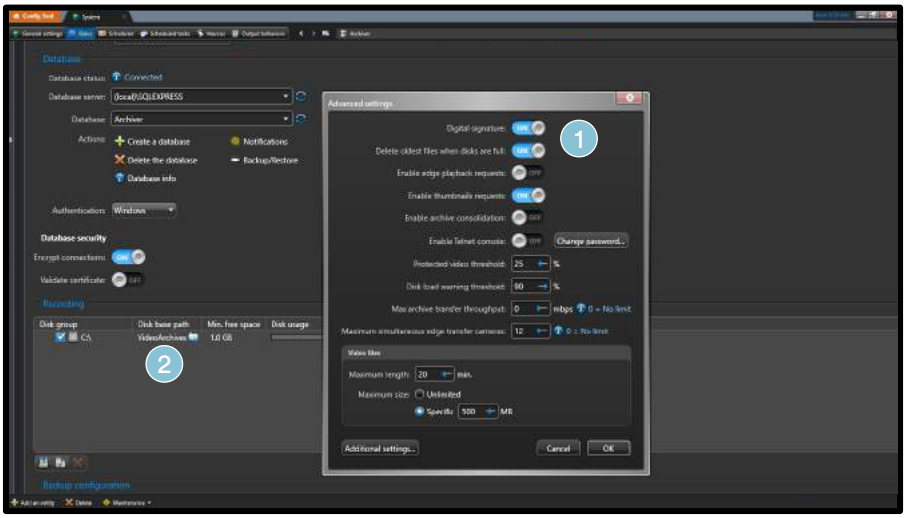
1. Hash value is generated for every video frame
2. Each frame includes the current and previous hash
3. Software encrypts combines hashes with private key

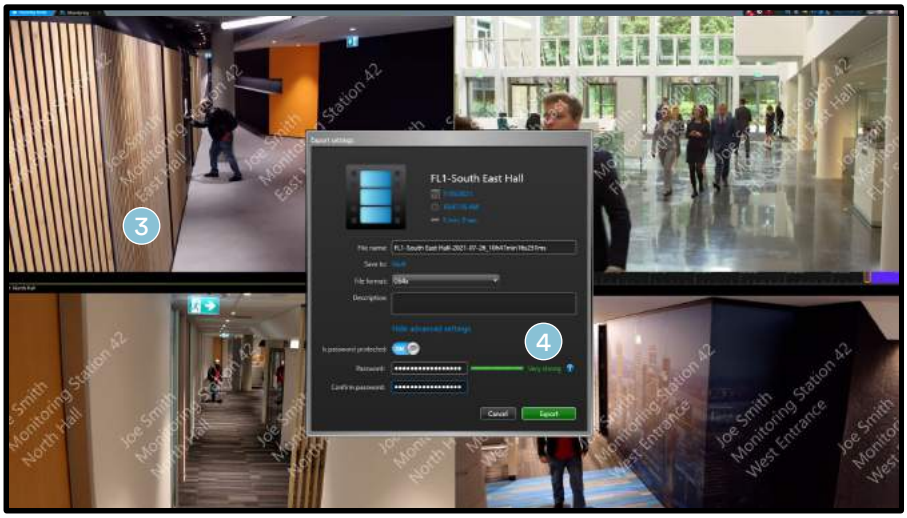
Key features and specifications

- Digital signature with Edwards-curve Digital Signature Algorithm (EdDSA)
- Visual watermarking displaying operator name, date, time, and/or workstation name
- Password-protected video exports
- Video encryption in transit and at rest
- Multi-factor authentication and Active Directory integration
- Detailed permissions and privileges configuration
- Secure portal to share and redact video evidence
- End-to-end audit trails for system and user activity tracking

How it works

1. Digital signature is activated in the Security Center Config Tool and automatically generates cryptographic keys.
2. Next time the Archiver records video, the files will be digitally signed using the cryptographic key.
3. Visual watermarking is applied to each video stream to prevent unauthorized captures or exports.
4. The four-eye principle ensures that two people approve an export before any video leaves the system.





Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

UPDT-08-03-21