SecurOS™ VMS / Analytics Platform

Cyber Security Guide

v.1.4

July 9st 2021

1. Introduction

ISS has an ongoing commitment to implement data protection features that ensure the highest level of security for any ISS system. Systems today typically access some type of a network, thus magnifying the importance of cyber security. ISS has implemented and will continue to implement cyber security features to mitigate the growing risk on cyber threats. Below are details on the SecurOS™ platform's cyber security features.

2. Password Protection

Protecting passwords stored by SecurOS and exchanged on a network between SecurOS servers, clients, and IP cameras is a basic and important part of cyber security.

1. All passwords stored in SecurOS for the purposes for authenticating to IP cameras, are stored as encrypted data (via AES-256) on the ISS server.
    a. SecurOS supports digest authentication for most camera vendors that support the feature.
2. Passwords sent over the network are encrypted using session-based hash (SHA-2).
3. Passwords used for SecurOS built-in User Rights Management, are also stored encrypted (via AES-256) in the SecurOS SQL database.
4. For another level of security, SecurOS can connect to an Active Directory or LDAP server to authenticate its users. In this case all password data will be stored and secured by the AD server.
5. For passwords used by Windows users on ISS servers/workstations, it is recommended to follow Windows strict password policy.

3. Authentication and Access

SecurOS ensures that all authentication procedures within the system are secured.

3.1. Built-in User Rights Management

Using the SecurOS User Rights Management, create native SecurOS users with different permissions. Limit the amount of administrator users. For operator users, limit what an operator can see in the user interface to only those components that are essential for the operator to be able to do their job.

3.2. LDAP / LDAPS / Active Directory Integration

SecurOS supports integration with Active Directory and LDAP. As an alternate option to using native SecurOS users, AD or LDAP users can connect to a SecurOS system using the permissions configured by SecurOS User Rights Management.

For additional security, SecurOS also supports LDAP over TLS, also known as LDAPS. LDAPS allows for the encryption of LDAP data (which includes user credentials) in transit when a directory bind is established, thereby protecting against credential theft.

3.3. Authorization security

SecurOS supports a limited number and delay between user authentication attempts. After 3 unsuccessful login attempts, the user is locked out from trying to login again for 30 seconds.

3.4. Password based authorization for MCC connection

SecurOS requires admin users to enter a password on the remote site and on the MCC server to complete the authorization process.

4. PostgreSQL Security

PostgreSQL, which is SecurOS's SQL database for storing data, comes with built-in authorization. PG Admin, which is the tool to access the data and perform DB admin functions is password protected, and any established connection strings from SecurOS to PostgreSQL require a valid user name and password.

ISS recommends to change the default PostgreSQL user password, and keep it secure, as this is a fundamental cyber security concept and a requirement across use cases.

5. SecurOS Server / Workstation Secure Identity

All SecurOS video/management servers verify their identity in the system via 2 ways:

- In the system license key by a USB Guardant code or Server hardware hash.
- By their NetBIOS name in the system configuration.

All SecurOS Operator Workstation Clients can identify themselves in the configuration via 2 ways:

- By their NetBIOS name.
- By their IP address (client connections can be limited to predefined IP addresses).

6. Encryption for Data at Rest

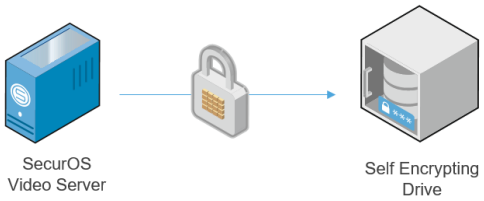
To ensure protection of data at rest, encryption is used.

SecurOS supports 2 types of data encryption methods:

- Hard drive encryption using SED Drives.
- Database encryption.

SED Encryption:

ISS supports the use of certified hardware accelerated encryption technology via Self-encrypting Drives (SED). Video and metadata can be encrypted using SED-compatible drives and controllers. Self-encrypting Drive technology relies on a dedicated chip to encrypt all data with AES-128 or AES-256 and does not occupy CPU resources. SED technology follows the Federal Information Processing Standard (FIPS) 140-2 / 140-3 standards.



Database Encryption:

ISS supports database encryption for certain SecurOS data. All personal data stored by the SecurOS FaceX module is encrypted at rest via PostgeSQL encryption. The extent of database encryption is under user control. The extent of the encryption can have impact on system performance and this should be accounted in the case of full (database) encryption.

7. Digital Signature & Encryption of Exported Video

If video data is exported from SecurOS, authenticity of the exported video must be ensured.

1. SecurOS supports Digital Certificates for the exported video. Certificates are used to authenticate the source of the exported video provided to law enforcement as evidence to be used in court. It is possible to use a trusted certificate issued by a certification authority (as an alternative to self-issued certificates).
2. Exported files are digitally signed using a certificate installed on the exporter server/workstation including SecurOS specific metadata like user account, camera id, etc. This provides proof of the evidence source and guarantees data integrity (that video wasn't tampered and modified in any way). Digital signatures can be verified using the SecurOS Evidence Manager or the SecurOS Digital Signature Verification Utility.
    a. A Certificate used for signing is assigned to a specific Archive Converter Profile (SecurOS module for exporting video).
    b. There is an additional layer of protection when a certificate requires a password to sign anything (can be configured by admin or entered manually by operator).
3. There is an option to encrypt exported files using any encryption provider installed in Windows (for example AES-256) thus protecting files from unauthorized access.

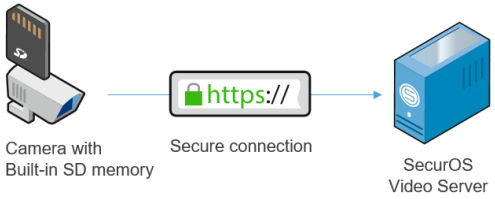
8. SecurOS Secure Communication

8.1. Secure connection between Cameras and Recording Servers

Protecting video data being sent from IP cameras to video recording servers / client workstations is a critical security task in most current day installations. This task becomes increasingly important in bigger systems that include a large number of cameras, servers, local/remote clients, and multiple network infrastructures.

1. SecurOS supports camera digital certificates for most of the major camera vendors who support this feature. Certificates installed in cameras must be trusted by the SecurOS video servers.
    a. Only devices with trusted certificates are allowed to connect to SecurOS.
    b. Trust relationships are managed by a system administrator using the Windows Certificate Store.
2. SecurOS supports digest authentication (actual password is never sent over network).
3. SecurOS ensures secure connection (encrypted and source verified) between camera and video server using HTTPS tunneling.
    a. More specifically RTSP and RTP data gets tunneled through HTTPS.
    b. The HTTP transport is built from two separate HTTP GET and POST requests initiated by the client. There will be two separate connections established between the server and camera. The server then will bind the connections to form a virtual full-duplex connection.
    c. Audio is also encrypted.
    d. An HTTPS session (secured over TLS with a trusted certificate installed in camera) protects video and metadata.

    e. HTTPS must first be enabled on the camera side. Then on the SecurOS VMS side, a setting is enabled to use camera encryption.
    f. HTTPS tunneling is also supported for SecurOS EdgeStorage Sync (ISS module to retrieve video from the camera's SD card).



8.2. Secure connection between all SecurOS Servers

SecurOS supports a secure connection using the TLS 1.2 protocol between all SecurOS servers in a system.

8.3. Secure connection between SecurOS Servers and Thick-clients

SecurOS supports a secure connection using the TLS 1.2 protocol between all SecurOS servers and thick-clients in a system.

8.4. Secure connection between SecurOS Servers and Thin-clients

SecurOS supports a secure HTTPS connection between SecurOS servers and SecurOS thin-clients (SecurOS WebConnect or SecurOS Mobile). The following additional security requirements must be considered:

1. Use HTTPS connections with trusted certificate. To connect server via HTTPS, a TLS certificate is required. To install certificate the following shall be done:
    a. Trusted TLS certificate is installed into your private certificate storage using MMC snap-in.
    b. If you already have a certificate for SecurOS Web/Mobile server then it is recommended to use it.
    c. If not, a trusted certificate can be obtained from a trusted 3rd party certificate authority.
2. A dedicated SecurOS Web/Mobile server is recommended to be used, to provide access for operators connecting over a WAN.
3. All network ports except for those required for the Web/Mobile modules to run, should be blocked in the WAN.
4. SecurOS *User Rights* shall be configured to prevent unauthorized access to SecurOS *Cameras* when logging in from the Web client or Mobile App.
5. Unsecure (passwords must meet standard complexity requirements and be unique) or compromised credentials must never be used for SecurOS users, in order to prevent unauthorized access.

8.5. SecurOS Failover Cluster - secure connection

The connection between the Server Manager and the Cluster Host is encrypted and requires authorization under Windows Administrator.