AxxonSoft VMS System Security

AxxonSoft software meets the latest demands in information security. Flexible multi-level settings for access rights, channel encryption, secure archives and more are combined with standard IT security procedures to protect our video surveillance systems from both internal and external threats.

Feature Brief

Network setup

A security and video surveillance system based on Axxon Next should be built on a separate network that connects all the major components of the system without any connection to the main network. This significantly reduces the risk of being hacked and losing important data. If for some reason it is not possible to isolate the security system on a separate network, it is recommended that you secure access to it from external networks by using a VPN with dedicated ports and password protection.

User access permissions

Axxon Next offers flexible configuration of user access to system functions and hardware. Users with restricted access will not have permission to access certain interfaces, hardware configurations, archives, and so on.

Integration with LDAP and Active Directory

The Axxon Next VMS supports working with users from LDAP directories and Windows Active Directory. All external users can use the same access rights as Axxon Next users.

Logging user actions

In Axxon Next, all user actions are logged. The system administrator can easily track improper actions and instantly revoke the user's rights.

Encryption

In addition to encryption software, Axxon Next supports hardware encryption of the channels between routers and all network nodes.

Secure archives

The Axxon Next archive uses the proprietary SolidStore file system. An entire physical or virtual disk is allocated to the archive. If a separate disk cannot be allocated for the Axxon Next video archive, this archive can be stored as an ordinary file within the existing Windows file system. The archive can only be viewed in the Axxon Next client application by users with the appropriate access rights.

Protection for exported files

Materials exported from Axxon Next can be password protected and digitally signed. Password protection ensures that forensic materials can only be viewed by the authorized recipient, and the digital signature proves that the video has not been altered during transmission.

Secure remote user access

Users can connect and work with Axxon Next from their mobile devices or from a browser.
The AxxonCloud service can be used to provide a secure SSL connection. In addition, the video signal can be transmitted over the secure HTTPS protocol.