Ocularis 5 Encryption

Date: April 9, 2018

Rev: 00040620181706

-Confirmation-

On-Net Surveillance Systems, Inc. confirms that the communication between the Ocularis Clients and the Ocularis Recorder is encrypted in all Ocularis 5 models (Professional, Enterprise and Ultimate). Ocularis 5 uses the AES encryption with a key length of 128 bit.

Listed below are bullet points regarding the encrypted communication between Ocularis Clients and Ocularis 5 Recorders and vice versa:

- Encrypted transmission

  Encrypted transmission is enabled by default and cannot be switched off

- Password

  The password is always transmitted from the Ocularis Client to the Ocularis 5 Recorder as "salted SHA-512 hash"

- Camera Audio / Video Streaming

  The Streaming of Audio and Video is always from the camera to the Ocularis 5 Recorder Device Manager (DM). Securing the transmission using encryption depends on the camera model used. Streaming using HTTPS must be supported. TLS 1.2 will be used if supported by the camera and implemented by Ocularis Recorder Manager for the appropriate camera model.

- Storing Audio / Video Streams

  Incoming Streams sent to the Ocularis 5 Recorder DM will be forwarded to the local Ocularis 5 MultiMedia Database (MDB). The transmission from the DM to the MDB proceeds within the same server (local TCP STACK) and therefore no encryption is required. Ocularis 5 Recorder stores the streams in one or several file systems in parallel. The file systems are freely configurable. The storage of data in the Ocularis 5 MDB is encrypted in a proprietary format. We assume that the physical and logical access to the storage server is restricted by administrative actions. The export from the MDB protected by either 128 or 256 bit AES (Advanced Encryption Standard) encryption. This ensures that no access to the stream can be made without the password; any alteration of the data exported will result in the password not working and therefore confirms the export is valid. The protection of the raw data prevents a manipulation and ensures the authenticity of the data.

- Audio / Video Streaming to Ocularis Clients

  Streams are only sent to the Clients if needed (e.g. if a camera should be displayed in Live or Browse mode). The Streams are sent over TCP or UDP to the Ocularis Clients and are protected using our own proprietary transmission protocol.

- Video Streaming to the Ocularis 5 Web and Mobile Clients

  The data transmission between the Ocularis 5 Recorder and the Ocularis 5 Web and Mobile Client is encrypted over HTTPS. Transcoded video streams will be sent over RTMP and are not encrypted. A one-time RTSP-URL for the video stream will be generated and sent over the encrypted connection. Audio streams cannot be delivered.