SICK Media Server Release: 1.5

Release notes

Document Revision History

Revision: 1.0
Date: August 19, 2025
Author: Engineering
Comment: Initial release of Media Server 1.6, introducing support for enhanced security features, improved certificate management, upgraded libraries, improved rename functionality for SEC/IPCam devices, support for .tif image extensions, seconds-level metadata extraction, and other performance and usability improvements.

This document provides the release notes for SICK Media Server version 1.6, released on August 19 , 2025. SICK Media Server enables the aggregation, storage, and retrieval of package images for operational use. These release notes summarize the new features, improvements, bug fixes, and known issues for this version.

Operating System

- Windows 10 (64 bit)
- Windows 11 (64 bit)
- Windows Server 2016 (64 bit)
- Windows Server 2019 (64 bit)
- Windows Server 2022 (64 bit)
- Ubuntu 22.04 LTS (64 bit)
- Ubuntu 24.04 LTS (64 bit)

Required disk space

- **Installation:**
    - Without MySQL DB: Approximately 700 MB for a fresh installation.
    - With MySQL DB: A minimum of 5 GB is required for installation.
- **Media Storage:** Allocate additional storage space based on the estimated amount of media and retention period. It is recommended to use dedicated drives for image storage.
- **Database Indexing:** Allocate an extra 10% of the total media storage space for database indexing. For example, if 1 TB of media storage is required, allocate 1.1 TB to account for indexing.

Required disk type

- Solid State Drives (SSDs) with high-write endurance are highly recommended

Processor

- **Minimum:** Lower-spec CPUs are supported, but high-volume sites are recommended to use better-performing CPUs (e.g., Intel Core i7 or equivalent).

Memory (RAM)

- 8 GB DDR3L or higher is recommended

Screen Resolution

- 1920 x 1080 (16:9) aspect ratio is recommended for optimal viewing

Browsers

- Google Chrome (version 127 or higher)
- Mozilla Firefox (version 127 or higher)
- Microsoft Edge (version 123or higher)

Communication and Security

- The software can be integrated with most anti-virus software.
- Certain ports are used by the application and need to be exempted from firewalls and file scanning

- 443 (Media Server port using HTTPS mode)
- 8084 (Media Server port using HTTP mode)
- 8406 (Database communications)
- 3121 (SFTP communications)
- 4121 (FTPS communications)
- 3030 (UDS Server Port)
- 445 (SMB communications)
- 2020 (FileSync SFTP communications)

Pre-requisite software

- Databases
  - MySQL 8.0.33(All records will be migrated to MySQL DB on MS upgrade to v1.6)
- Runtimes and Databases are bundled with the installation package and will be installed/updated if they do not exist on the target machine. Patching existing instance of PA will not upgrade the MySQL.
- Browser Recommended
  - Chrome (Latest version), Firefox (Latest version), Edge (Latest version)

Included Components

SICK MS installer is delivered with the following components:

Component	Version / Comment
SICK MS	1.6

Note: A license file is needed to access the full functionality. This license is supplied separately and on request.

Installation:

Administrator rights are needed to install SICK MS. Installation procedure:

1. Download the file installation.exe
2. Execute the installation.exe file with administrator rights
3. Follow the on-screen instructions to complete the installation
4. Start SICK MS by launching the URL in the address bar.
5. If your license is invalid, outdated, or not located in the correct folder, you will be redirected to a license dialog (also reachable from License & Registration page).
6. Click the “Apply License” button to browse for and apply your license file.

New Features/Improvements and Bug Fixes:

This release introduces the following new features, improvements, and bug fixes:

S.No.	New Features/Improvements	Description
1	**License Field Type Update**	Updated the license column in the license table from TEXT to MEDIUMTEXT to support encrypted licenses generated by Package Analytics 4.6 (approx. 64k characters). The datatype change is applied automatically when a new trusted license is applied, with the config parameter MODIFY_LICENSE_TABLE set to false post-migration.
2	**Enhanced Certificate Management**	Added support for System Security Manager (SSM) to manage Media Server certificates, enhancing certificate handling and automation. Implemented certificate management via a property file (e.g., cert-config.properties) specifying certificate path, alias, and password (obfuscated as cert-strawberry). Supports base64-encoded passwords with the PROPERTIES_PASSWORD_ENCODED parameter under the CERTIFICATE tag set to true. Certificates are updated every 2 months.
3	**IPWorks Library Upgrade**	Upgraded the IPWorks library and performed performance testing with SFTP and FTPS simulation to ensure no degradation in functionality.
4	**TLS Version Control for HTTPS**	Added configuration to restrict HTTPS clients using deprecated TLS versions. The TLS_VERSION and USE_TLS parameters under the HTTPSD tag control allowed versions, defaulting to TLS 1.2. Media Server must be restarted for changes to take effect.
5	**POCO Library Upgrade**	Upgraded the POCO library to version 1.14.1 for Windows and Linux, supporting OpenSSL 3.5 and TLS 1.3. Ensures no performance degradation for all dependent functionalities, with regression testing completed.
6	**OpenSSL Upgrade**	Upgraded Media Server to support OpenSSL 3.x.x, ensuring compatibility with the latest OpenSSL version without errors.
7	**Encodedmultiplemedia Performance**	Optimized the Encodedmultiplemedia API to support wildcard searches without devices configured, improving performance for filename, filename prefix, and partial filename patterns.
8	**Rename Support for FTPS/SFTP**	Added support for the rename command for SEC/IPCam devices over FTPS and SFTP protocols. The rename command works with TLS 1.2 and 1.3, supports out-of-sync renaming, and ensures images are moved to the correct folders with cleanup of temporary control files.
9	**Consolidated Cache-Control Header**	Combined duplicate Cache-Control headers into a single header for all API responses. Cache-Control is added for GET methods with no-cache when missing and ensures no duplicate headers are present.
10	**.tif Image Extension Support**	Added support for images with .tif extensions (in addition to .tiff) from ICR890-4 cameras. This includes error image handling, inventorying, and license commissioning for .tif extensions.
11	**Flexible IPCam Renaming**	Enhanced IPCam renaming functionality to support 1txt/2txt/UDS modes for all licensed file extensions, removing the restriction on three-letter filetypes (e.g., .jpeg) to support other devices.

12	**Seconds-Level Metadata Extraction**	Updated the Metaextractor API to support seconds-level granularity for image metadata searches, improving precision for timestamp-based queries.
13	**HTTP Disable Option**	Introduced a new API (2.0/services) to enable/disable HTTP and HTTPS protocols without requiring a new license. The ENABLED parameter under HTTPD and HTTPSD tags controls protocol states, with both protocols enabled by default and mutual disabling prevented.
14	**Configurable Image Discard Threshold**	Removed the 500 MB memory threshold for image discards, making it optional via the DISCARD_ON_LOW_MEMORY parameter under the STORAGE tag (default: false). The OS now handles memory requirements when the threshold is disabled.
15	**TLS Version Control for FTPS**	Added a TLS_VERSION parameter under the FTPSD header to control TLS versions for FTPS. Default is 1_2 (supports 1.2 and 1.3); setting to 1_3 restricts to TLS 1.3 only. Removed fallback to lower TLS versions for stricter security.
16	**Brute Force Login Protection**	Implemented brute force protection for login attempts at the username level. After 5 consecutive failed attempts (configurable via INVALID_LOGIN_ATTEMPT), login is blocked for 30 seconds (configurable via INVALID_LOGIN_ATTEMPT_INTERVAL). Successful logins reset the counter.
17	**Remove Unnecessary Profile Key**	Removed the unnecessary profile key from the request body of the /3.0/serversettings API call in the frontend, ensuring no impact on full/thumb cleanup profiles.

Important Note While patching:

Limitations and Known Issues: