USER MANUAL

SICK Media Server

Software to record and maintain media streaming from Media Capturing Devices

SICK
Sensor Intelligence.

Software Versions

Soft-ware / Tool	Function	Ver-sion
SICK Media Server	Introduced Image Disclaimer, a feature that prints configurable disclaimer text on newly acquired images for selected devices. Added Authentication Configuration (OIDC) enabling Single Sign-On (SSO) through external Identity Providers such as Microsoft Entra ID, SICK ID, etc. Upgraded bundled MySQL from 8.4.5 to **8.4.7** to address security vulnera-bilities. Added configurable filename date format for Barcode Counter logs. Enhanced security controls for SFTP/FTPS protocol management.	1.7
SICK Media Server	Added advanced certificate management, TLS 1.2 and 1.3 enforcement, brute-force protection, FTPS/SFTP rename functionality, .tif image support, Metaextractor API, HTTP disable option, automatic certificate updates dur-ing patching, Daylight Saving Time fixes, and optimized media retrieval per-formance.	1.6
SICK Media Server	Added Barcode Counter for XML-based barcode metadata storage, Help Icon for inbuilt user manual, encoded media API for multi-image retrieval, TLS 1.2+ enforcement, vulnerability patches, response header security en-hancements, SQLite database deprecation with MySQL 8.0.33 migration, updated default certificates, crash management improvements, and gMSA service support for Windows.	1.5
SICK Media Server	Added support for SEC 100 devices with JPEG compatibility for Package Analytics.	1.4.2
SICK Media Server	Added crash management to prevent configuration file corruption on power failures, security fixes blocking polyfill.min.js, updated default certificate, and customized HTTP response header support.	1.4.1
SICK Media Server	Added scheduled file archiving, image tagging, rule-based cleanup, en-hanced manual cleanup, 999-day Age-out cleanup, filewriter queue size handling, device grouping and categorization, simplified installer with MySQL, multiple source login, default certificate, properties configuration, custom FTP port range, configuration file protection, IPCam renaming fixes, and command-based version fetch.	1.4

Soft-ware / Tool	Function	Ver-sion
SICK Media Server	Added Ubuntu OS support (18.04, 20.04, 22.04), cleanup improvements for Linux OS, introduced default users for Field Analytics and Facility View authentication, enhanced server settings API with accurate version display, and optimized MySQL connection maintenance.	1.3.2
SICK Media Server	UX improvements for cleanup and maintenance (size-based cleanup, auto disk management, Age-out toggle), performance enhancements (XML retention, media retrieval sequence, failover cleanup), and configurable ratio-based cleanup.	1.3.1
SICK Media Server	Added Samba protocol support for ICR890-4 devices, migrated UI from Angular 1 to React, introduced error response images, FTPS explicit/implicit mode support (beta), improved ETL performance, and fixed trusted license and Internet Explorer UI issues.	1.3
SICK Media Server	Updated patch installation fixing image rejection due to MySQL column size, resizing columns for MySQL/SQLite (filename to 255 characters, device name to 64 characters), and redirecting incoming data to temporary SQLite database during MySQL updates.	1.2.1
SICK Media Server	Added MySQL database support with SQLite migration, HTTPS server support, FTPS/SFTP server support (beta), separate FTP/FTPS/SFTP log files, heartbeat messages to Facility View, certificate properties in UI, API configuration, and optimized media retrieval response time and database query performance.	1.2
SICK Media Server	Added image server configuration details, user profile view, disk usage indicator, manual cleanup by file type, FTP client management (add/delete/list), size- and time-based cleanup and maintenance settings, and license registration. Included MySQL 5.7.23 support. Required a separate license file for full functionality.	1.1

This page left intentionally blank

1 About this Manual

This manual provides detailed documentation on how to install and configure SICK's Media Server software application. The SICK Media Server is used to store and maintain media captured by SICK devices.

2 Security and Usage Disclaimer

Overview

This section describes important security, operational, and usage considerations for the product. The operating entity is responsible for ensuring that the product is deployed, configured, and maintained in a secure and controlled environment.

Network Services and Protocols

A diagram and list of all network services and protocols used by the product are available in the product-specific Release Notes at:
https://support.sick.com

The listed services and protocols represent the best available knowledge. No service or protocol has been intentionally omitted.

Network Security

The operating entity must implement appropriate measures to protect the operating environment and network infrastructure. This includes ensuring secure and trustworthy communication between the product and all connected systems and devices.

Physical Access Protection

The product is not intended for use in easily accessible or public areas.

The operating entity must:

- Protect the product from unauthorized physical access
- Restrict access even for personnel present in the working area
- Ensure that only authorized individuals can access the product

Protection of Installation Environment

The operating entity must prevent unauthorized access to the area in which the product is installed and operated.

Protection of Transmission Media

Transmission media (for example, data cables and network connections) must be protected against unauthorized access, interception, or tampering.

Data Protection and Privacy
The product is technically capable of identifying individuals or capturing personal data.

The operating entity is responsible for ensuring compliance with applicable data protection and privacy regulations.

Protection Against External Force
The product is not designed to protect data or functionality against external force, tampering, or vandalism.

Access Control and User Management
The operating entity must configure access credentials and permissions according to the principle of least privilege. Only the minimum required access rights should be assigned.

External Systems and Services
The product may interact with external systems such as:

- Analytics systems
- FTP servers accessed by the product

These integrations must be secured appropriately.

Cryptographic Data Handling
The product does not store cryptographic secrets that would allow it to access other systems or devices.

Intended Use Limitations
The product is not intended for:

- Safety-critical applications
- Control or authorization of physical access

Responsibility Statement
The operating entity is solely responsible for securing the product, its environment, and ensuring compliant usage.

Important
Failure to implement appropriate security and access control measures may result in unauthorized access, data breaches, or misuse of the product.

SICK Support
For SICK sales and product support visit: www.sick.com
For all SICK technical support visit: https://supportportal.sick.com/

Contents

3 Media Server Overview

SICK auto-identification systems are made up of SICK Intelligent Sensors. These systems include a combination of laser or camera-based barcode readers and scanners, dimensioners, weighing scales and more. For the sensors that acquire and send images along with object data to the controller, the SICK Media Server offers the capability to aggregate, store and retrieve these images for operational purposes.

The SICK Media Server is an application that can be deployed on commonly available operating systems (Windows and Linux) on a real or virtual hardware setup.

System Components

The SICK Media Server works in conjunction with key software components in your facility to aggregate, store, and maintain image data. These are:

- PC/server to host SICK's Analytics software application that needs the Media Server
- PC/server to host SICK Media Server software application. This could also be the same as the hardware hosting the Analytics software.
- Devices to access SICK Analytics Dashboard and/or Media Server configuration.

Media Server Software

The Media Server software application is responsible for aggregating, storing, and managing images acquired by SICK's image-capturing devices. The Media Server can be hosted on the same hardware as the SICK Analytics products or can be installed as a standalone application depending on your architecture requirements. All user access to the Media Server is through the Media Server dashboard.

PC/Server to host the Media Server and/or SICK Analytics Application

A PC or a Server with minimum hardware requirement as mentioned in the section below (Hardware Requirements) to install/deploy the SICK Analytics application and/or the Media Server. All collected images and object data are stored on the host PC.

Device computers

The device computer is any PC connected to the Media Server network. SICK Media Server device dashboards are HTML5 web applications that can be used to access the Media Server configuration.

System Architecture

The illustration below provides a visual representation of the Media Server architecture and illustrates how the system components work together to provide a robust and comprehensive storage tool for media files.

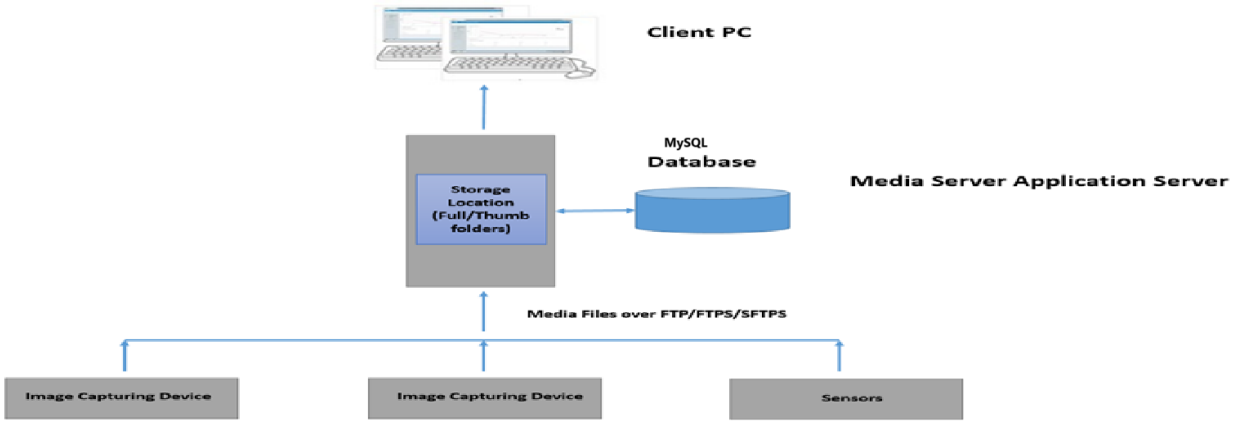


Figure 4.1:1: System Architecture

Hardware Requirements

The following minimum system hardware requirements must be met prior to installation. Note that these are minimum requirements; final hardware configuration is application dependent. Storage duration is application dependent.

Supported Operating Systems	**Recommended:** Windows Server 2022 (64-bit), Ubuntu 24.04 LTS (64-bit) **Supported:** Windows Server 2019 (64-bit), Windows 11 Enterprise (64-bit), Ubuntu 22.04 LTS (64-bit) **Legacy Support:** Windows 10 (64-bit) **Latest (Optional):** Windows Server 2025 (64-bit)
Required Disk Space	Depends on business requirements. Key factors include the number of systems and media capturing devices connected to the Media Server, number of media files generated per day, and retention duration. **Minimum:** 2 GB (base installation)
Required Disk Type	Solid State Drives (SSDs) with high-write endurance are strongly recommended for optimal performance and reliability.
Processor	Depends on workload and data processing requirements. **Minimum:** Intel Core i7 (quad-core, 2.40 GHz or higher) **Recommended:** Multi-core processors (8 cores or above) for production environments
RAM	**Minimum:** 16 GB **Recommended:** 32 GB or higher (based on system load and data volume)
Monitor Resolution	Minimum: 1920 x 1080 (Full HD) Recommended: 2560 x 1440 or higher for better visualization
Supported Browsers	Google Chrome, Mozilla Firefox, Microsoft Edge (latest stable versions)

Table 1: Hardware Requirements

Supported Port/s:

Media Server Software supports the following ports/port ranges:

HTTP	Default Port 8084
HTTPS	Default Port 443
FTP	Default Port 2021. Port range 20,21,1024-65535
SFTP	Default Port 3121. Port range 22,1024-65535
FTPS	Default Port 4121. Port range 21,990,1024-65535
UDS	Default Port 3030
MySQL	Default Port 8406
File Sync	Default Port: 2020
Tagging	Default Port:80

Table 2: Supported Ports

Note:

- This software can be integrated with most anti-virus software. The above-mentioned ports must be exempted from file scanning.
- Conflicts between ports will restrict the initiation of protocol servers attempting to start on a conflicted port.
- All protocol servers are configured to the default ports.
- FTP and HTTP are unsecured protocols. Starting with Media Server 1.6, FTP can be disabled directly from the Media Server UI without requiring a new license.
- HTTP can be disabled through license configuration, configuration file, or directly from the Media Server UI by navigating to **Advanced Settings** → **Properties Configuration**.
- The option to enable or disable HTTP from the UI is available only when the application is accessed over HTTPS.
- When HTTP is disabled, the HTTP port field will not be displayed.
- For detailed steps on how to enable or disable protocols, refer to Section Enable/Disable Protocols.

- It is recommended to use secure alternatives such as SFTP and HTTPS for encrypted communication. For further assistance with disabling these protocols or transitioning to secure alternatives, contact the support team at https://supportportal.sick.com/.

Supported Features:

SICK Media Server 1.7 builds upon the robust foundation of previous versions including 1.6, 1.5, 1.4, 1.3, 1.2, and 1.1, while maintaining full backward compatibility with existing SICK Analytics platforms. This release introduces significant enhancements in authentication, image processing, security, and system management.

Key additions include the **Image Disclaimer** feature, which allows administrators to configure and print customizable disclaimer text on newly acquired images for selected devices. This enables legal, operational, or informational messages to be embedded directly into image outputs.

Media Server 1.7 also introduces **Authentication Configuration using OpenID Connect (OIDC)**, enabling Single Sign-On (SSO) through external Identity Providers such as Microsoft Entra ID, SICK ID, etc. This enterprise-grade authentication mechanism strengthens access control through secure token validation and integration with external identity management systems.

Additional improvements include an upgrade of the bundled **MySQL version from 8.4.5 to 8.4.7** to address identified security vulnerabilities, support for configurable filename date formats for Barcode Counter logs, and Enhanced security controls for SFTP/FTPS protocol management.

Media Server Software supports following features/functionalities:

Features	MS 1.1	MS 1.2	MS 1.3.2	MS 1.4	MS 1.5	MS 1.6	MS 1.7
HTTP Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HTTPS Support	N/A	Yes	Yes	Yes	Yes	Yes	Yes
FTP Device Support	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FTPS Device Support	N/A	Yes	Yes	Yes	Yes	Yes	Yes
SFTP Device Support	N/A	Yes	Yes	Yes	Yes	Yes	Yes

ICR890-4 Support	N/A	N/A	Yes	Yes	Yes	Yes	Yes
Cleanup & Maintenance	Yes	Yes	Yes	Yes	Yes	Yes	Yes
License & Registration	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Certificate Properties	N/A	Yes	Yes	Yes	Yes	Yes	Yes
API Configuration	N/A	Yes	Yes	Yes	Yes	Yes	Yes
Heartbeat Messages	N/A	Yes	Yes	Yes	Yes	Yes	Yes
SQLite Database	Yes	Yes	Yes	Yes	No	No	No
MySQL Database	N/A	Yes	Yes	Yes	Yes	Yes	Yes
File Sync	N/A	N/A	N/A	Yes	Yes	Yes	Yes
Scheduler	N/A	N/A	N/A	Yes	Yes	Yes	Yes
Activity Scheduler	N/A	N/A	N/A	Yes	Yes	Yes	Yes
Rule-based Cleanup	N/A	N/A	N/A	Yes	Yes	Yes	Yes
Selective Manual Cleanup	N/A	N/A	N/A	Yes	Yes	Yes	Yes
Additional Device Type Support	N/A	N/A	N/A	Yes	Yes	Yes	Yes
Tagging	N/A	N/A	N/A	Yes	Yes	Yes	Yes

Barcode Counter	N/A	N/A	N/A	N/A	Yes	Yes	Yes
Image Disclaimer	N/A	N/A	N/A	N/A	N/A	N/A	Yes
OIDC Authentication (SSO)	N/A	N/A	N/A	N/A	N/A	N/A	Yes

Table 3: Supported Features

4 Installation

4.1 Installing SICK Media Server

You can install Media server as a service with the provided executable file. Use full installer for fresh installation of Media Server and apply patch installer over older version of already installed Media servers. Follow the steps below to install the application on your host PC.

4.1.1 To launch the installer on Windows

1. Double click on the executable file

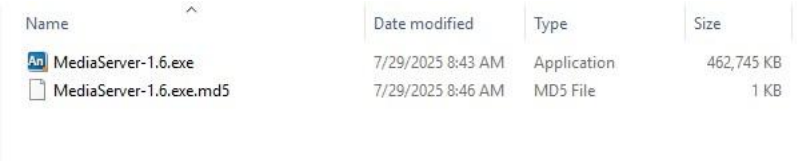


Figure 4.1:1: Media Server Exe

2. **InstallAnywhere** dialog will be displayed.

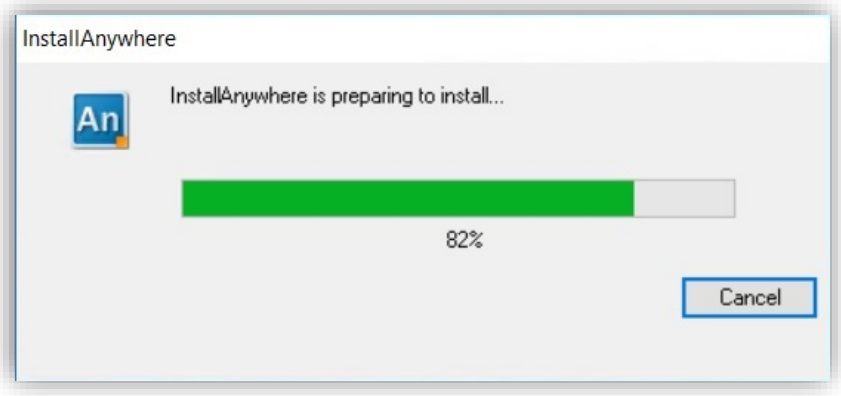


Figure 4.1:2: InstallAnywhere Screen

3. Once the progress on the **InstallAnywhere** dialog reaches 100%, Media Server Installation Wizard will launch with the **Introduction** screen. Click on '**Next**' button to move to the next page.

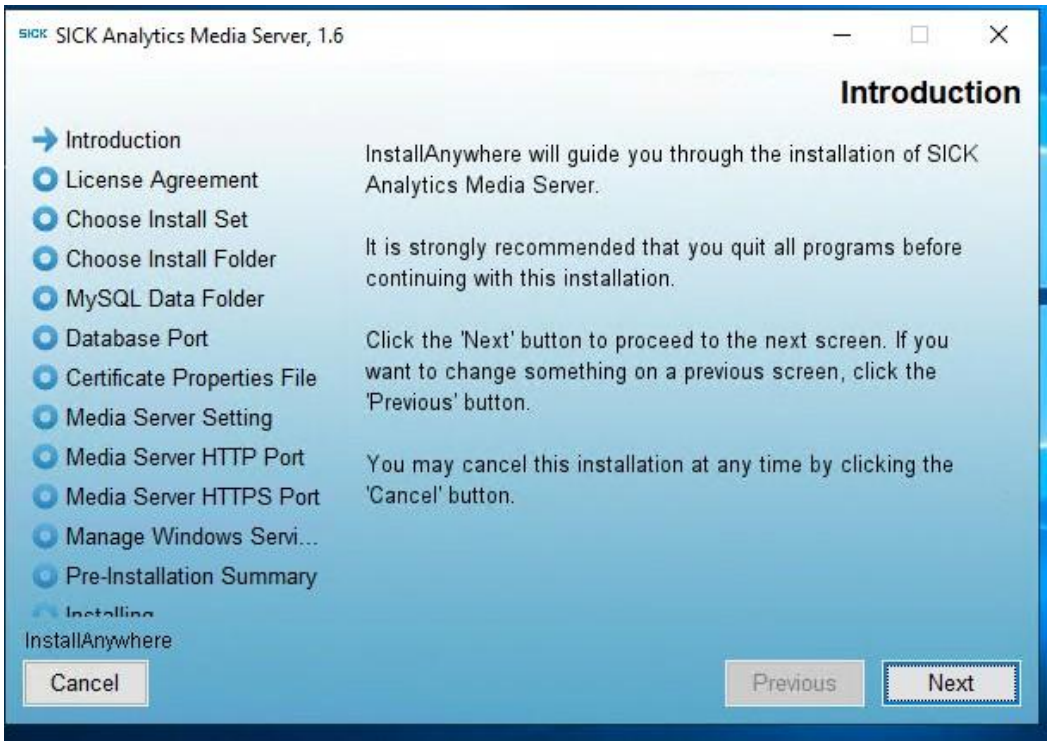


Figure 4.1:2: Introduction Screen

4. License Agreement screen (as shown below) prompts you to read EULA and agree to the terms of License Agreement. Please go through the terms of License Agreement and select the checkbox acknowledging the terms of the license agreement then **Next** button is enabled. Click the **Next** button

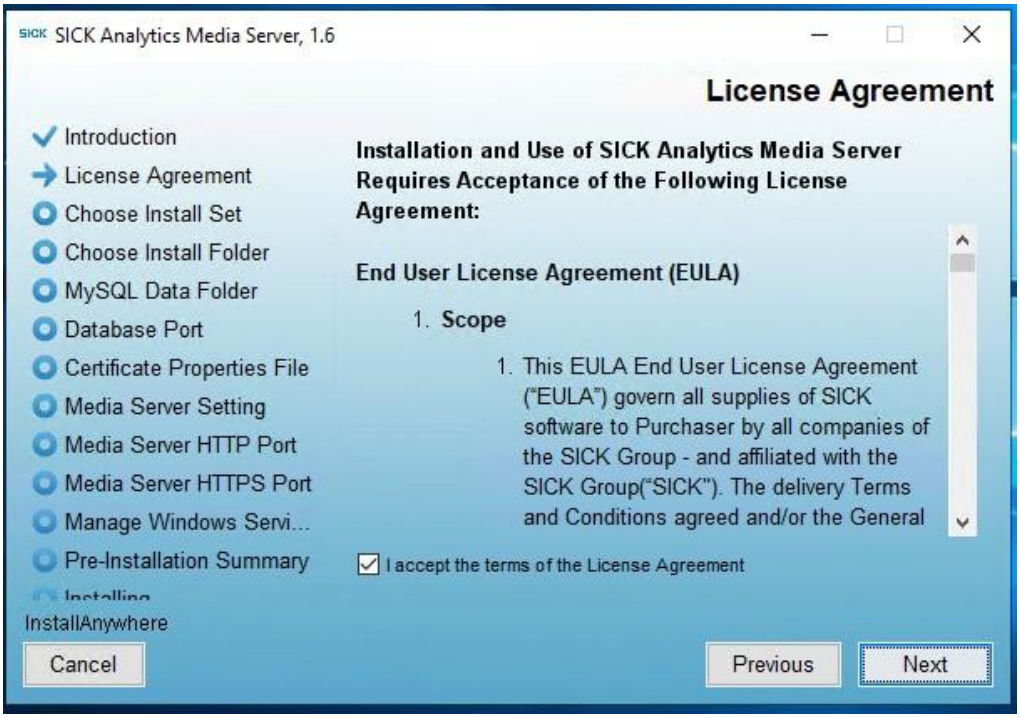


Figure 4.1:3: License and Agreement

5. The Choose Install Set screen appears, allowing you to select from two installation options:
    - **Full Installation** – Installs both Media Server and Database.
    - **Custom Installation** – Allows you to install Media Server with or without the Database.

    After selecting the desired option, click **Next** to proceed or Previous if you need to return to the previous screen.

    Note:

- *If you select Custom Installation without MySQL, you must manually install MySQL* 8.4.5 *and configure Media Server to connect to the database on the remote machine.*
- *If you experience issues switching the database from SQLite to MySQL during installation, see the* ***Troubleshooting*** *section for detailed resolution steps.*

Figure 4.1:4: Choose Install Set

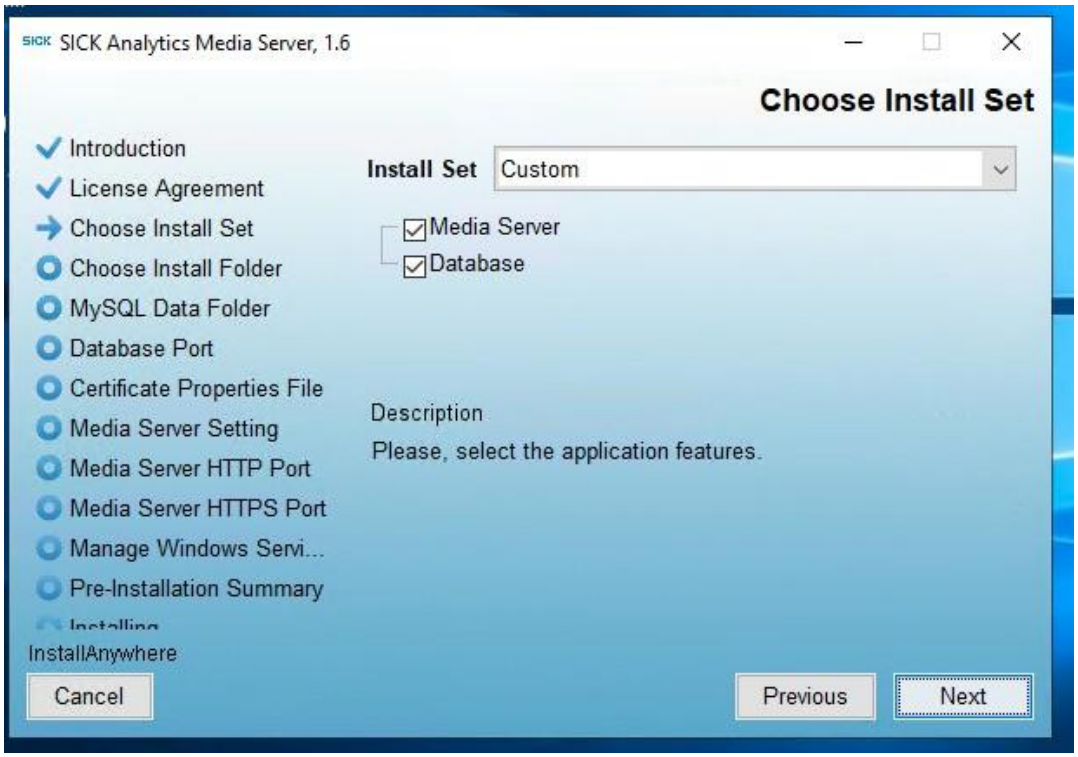


Figure 4.1:5: Install Set – Custom Option

6. The **Choose Install Folder** screen appears, allowing you to specify where to install the Media Server:

   - The default installation path is **C:\Program Files\SICK\Analytics Solutions\Media Server**. To use this location, click **Next**.
   - To select a different directory, click **Choose...** and navigate to the desired folder, or click **Restore Default Folder** to revert to the default location.
   - Click **Next** to proceed or **Previous** to return to the previous screen.

   ***Note**: If the media server is running as a console application, and has started as a non-privileged application, it should be installed outside the Program Files directory tree or else Windows will prevent the Media Server from updating the configuration file. A location like C:\SICK\ must be used for such instances.*

Figure 4.1:6: Choose Install Folder

7. The **MySQL Data Folder** screen appears, prompting you to specify where the MySQL database files should be stored:

    - The default folder path is **C:\Program Files\SICK\Analytics Solutions\MediaServer**. To use this location, click **Next**.
    - To select a different directory, click **Choose...** and navigate to the desired folder, or click **Restore Default Folder** to revert to the default location.
    - Click **Next** to proceed or **Previous** to return to the previous screen.

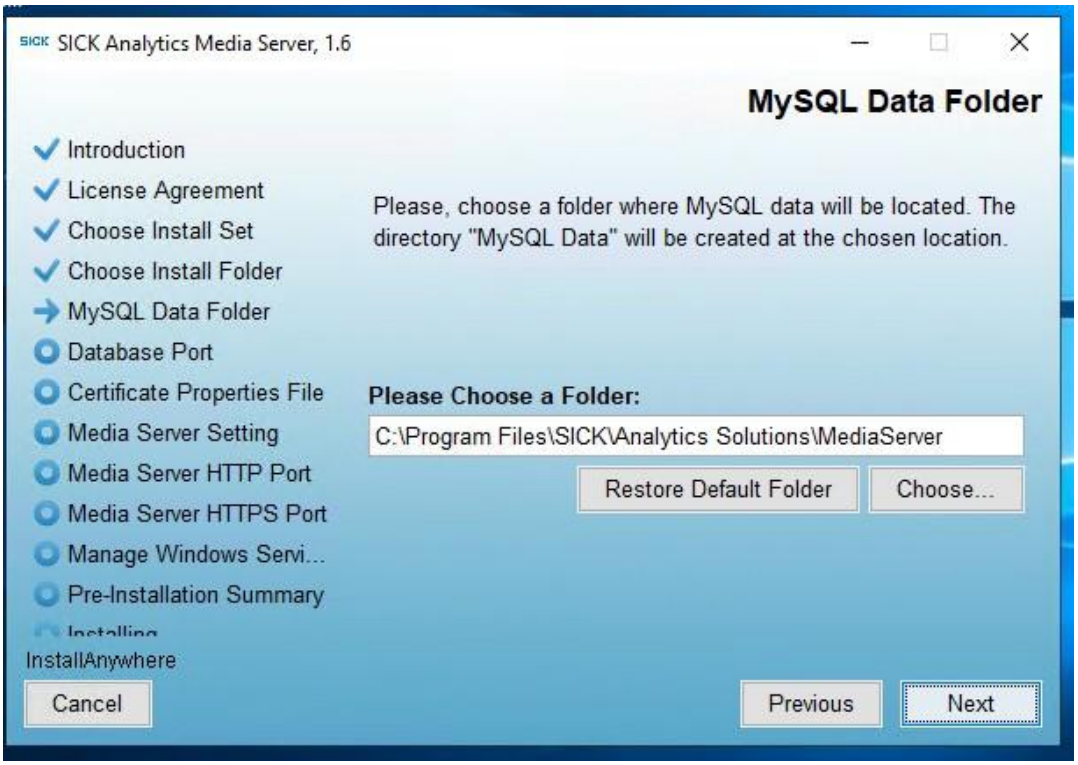


Figure 4.1:7: Choose MySQL Data Folder

8. The Certificate Properties File screen appears, prompting you to specify a certificate properties file:
   - The default file path is **C:\certupdates\cert.properties**. To use this location, click Next.
   - To select a different file, click Choose... and navigate to **the desired. properties file**, or **click Restore Default File** to revert to the default path.
   - Click **Next** to proceed or **Previous** to return to the previous screen.

Figure 2.1:9: Certificate Properties File

9. The **Media Server Setting** screen appears, allowing you to specify the storage location for Media Server files:

   - The default storage location is **C:\media-server-images**. To use this location, click **Next**.
   - To select a different directory, click **Choose...** and navigate to the desired folder, or click **Restore Default** to revert to the default location.
   - Click **Next** to proceed or **Previous** to return to the previous screen.

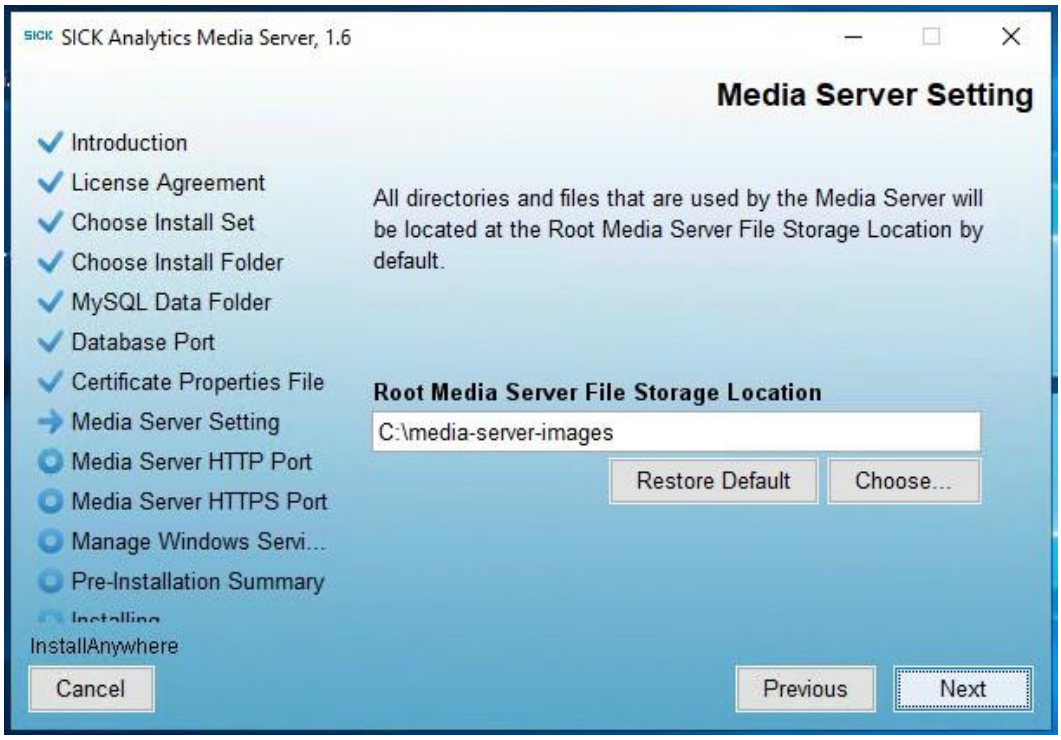


Figure 4.1:8: Media Server Setting

10. The **Manage Product Windows Services as a User** screen appears, allowing you to specify a user account for managing Windows services.

- To manage services as a specific user, select **Manage Product Windows Services as a User** and enter the required credentials:
  - **Domain:** Enter the domain name.
  - **User Name:** Enter the username.
- If left unchecked, the default user is **Local System**.
- Click **Next** to proceed or **Previous** to return to the previous screen.

Note:

- *Ensure the selected user has the necessary permissions to manage Windows services.*
- *Enter the correct password in the next panel; incorrect credentials will prevent services from starting.*

Figure 4.1:9: Manage Product Windows Services as a User

11. Check all the details in Pre-Installation summary page and click on the '**Install**' button to begin final installation of the software.

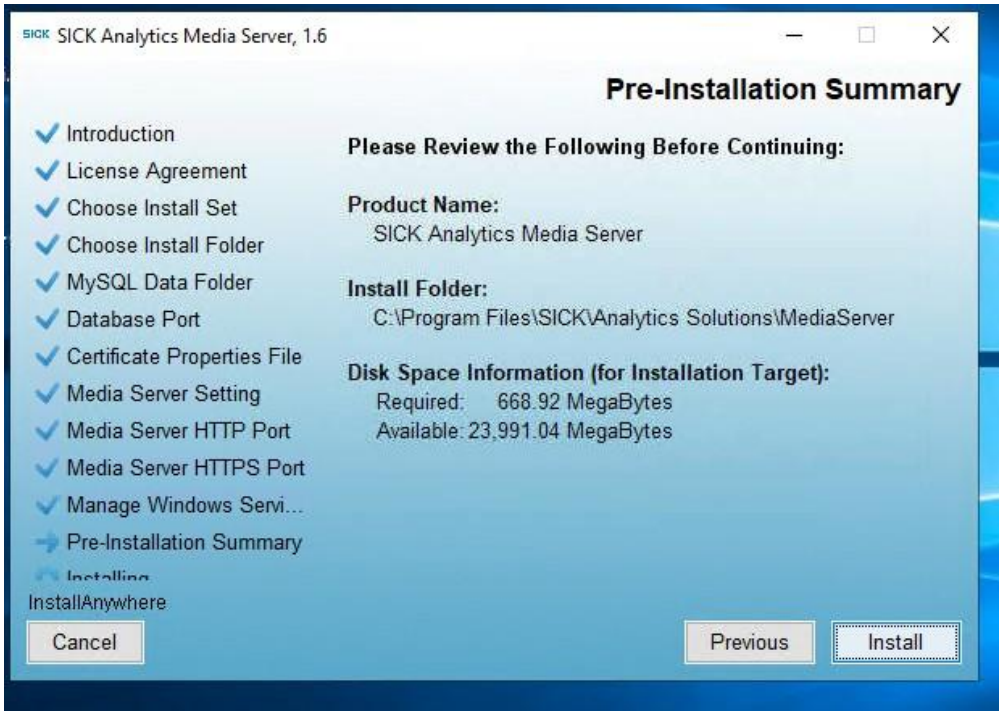


Figure 4.1:10: Pre-Installation Summary

12. Installation will get started and the installation progress can be tracked using the progress bar at the bottom of the screen.

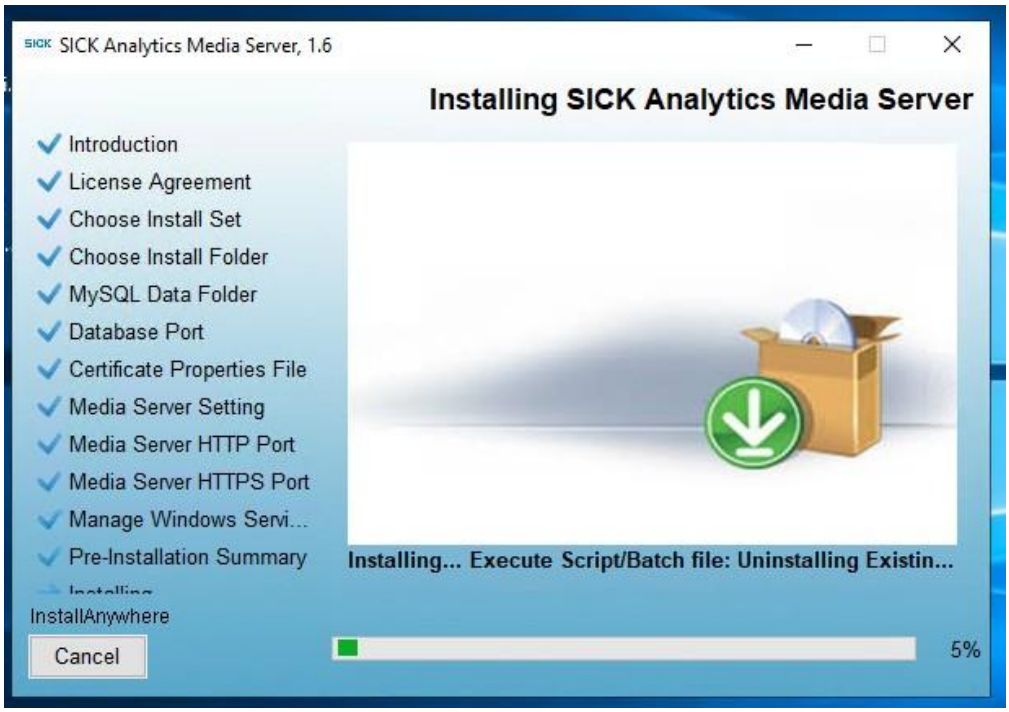


Figure 4.1:11: Installation in Progress

13. Once the installation is completed, **Install Complete** window will be displayed. Click on 'Done' button to complete installation.

Figure 4.1:12: Install Complete

14. If you install Media Server as a standalone application without MySQL, you must manually install **MySQL 8.4.5** and configure Media Server to connect to a remote

database. For detailed steps on configuring the database connection, see 12.1 below

- **Note**
  If the Media Server is unable to connect to MySQL when the service starts for the first time, the application will open in a restricted view called Configure DB. This screen allows you to update or correct the MySQL connection settings.
- *Once valid connection details are provided and saved, a yellow banner will appear stating that a service restart is required. Restart the Media Server service to apply the new database settings and proceed to the normal application interface.*

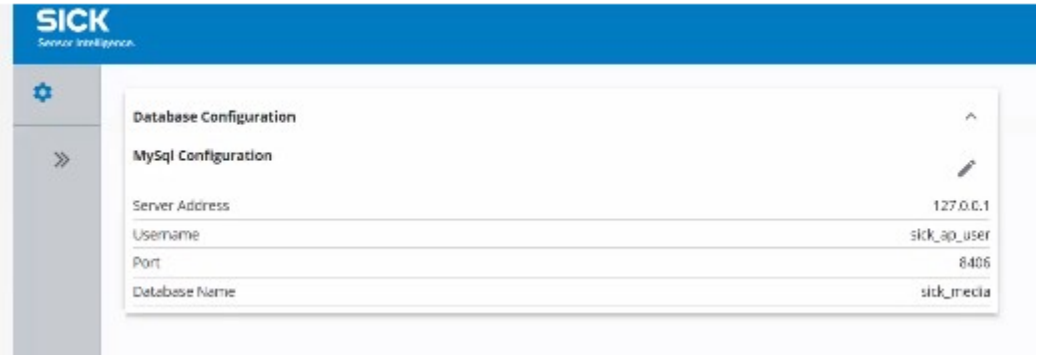


Figure 4.1:13: Configure DB – MySQL Database Configuration Page

- *For detailed instructions on using the Configure DB page, see Section 10.1, Edit or Recover MySQL Configuration.*

4.1.2 To launch the installer on Linux

1. Navigate to the location where Installer .bin file is available
2. Open Terminal in the location where the installer is available
3. Login with root user
4. Grant execution rights to the installer .bin file using command: chmod +xwr <installername.bin>
5. Enter Password
6. Launch the installer using command:/<installername.bin>. The Command will extract the files and will launch the Installer

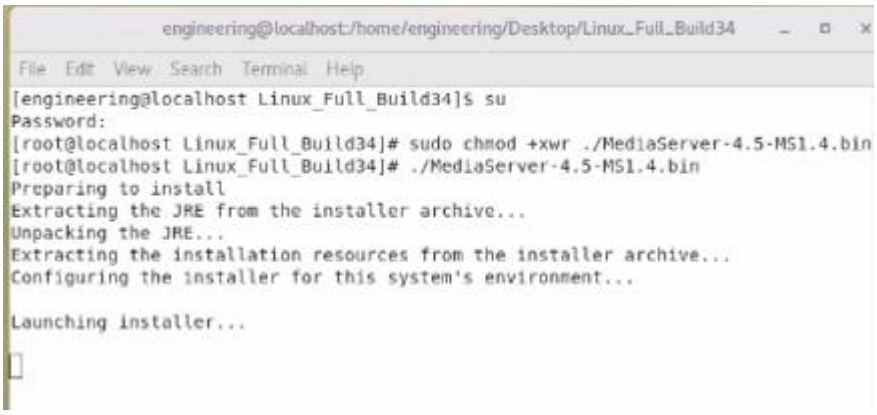


Figure 4.1:13: Linux Installation Terminal

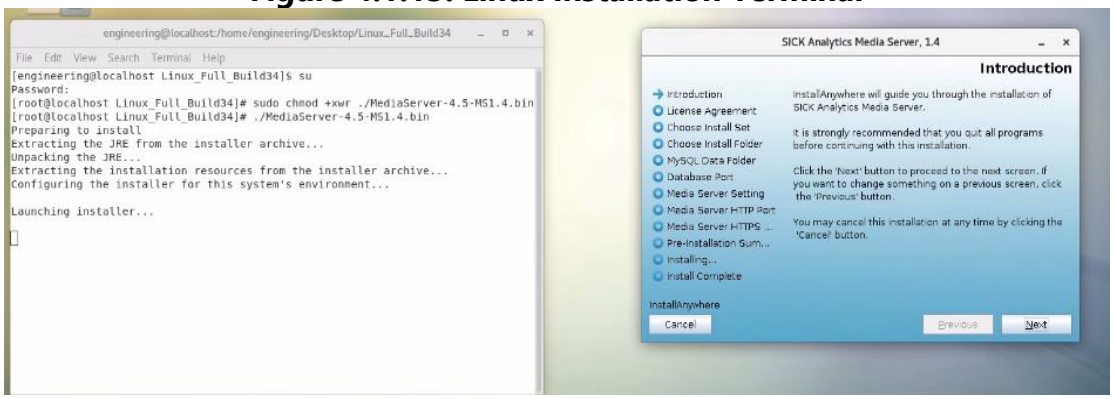


Figure 4.1:14: Linux Installation Window

7. Click on **NEXT** button and follow the same steps as windows installation from step 4- step 10
8. Once installation is completed, to check whether the services are up and running, execute following command: sudo systemctl status SICK_An_Mediaserver.service
9. Similarly, the media server installer will launch Media Server Maintenance window on running command: sudo. /<installername.bin>, if the Media Server is already installed on the machine

4.1.3 To Launch Patch Installer

Note: *When upgrading from Media Server 1.4 or earlier to 1.5 or 1.6, only 339 days of data will be retained; older data will be purged. For more details on migration timelines and database changes, refer to section* *10.2 Points to Note While Switching Database.*

1. **Start Patch Installation**
   - Navigate to the folder containing the **Media Server Patch installer**.
   - Locate the **patch executable file**.
   - **Double-click** the file to launch the patch installer.

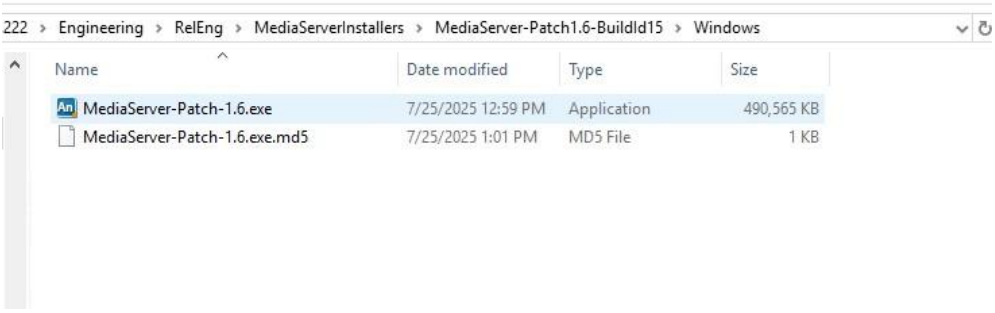


Figure 4.1:15: **Media Server Patch Exe**

2. **InstallAnywhere Loading Screen**
   - Once the patch installer is launched, the **InstallAnywhere** dialog appears.
   - The installation process prepares to start, showing a **progress bar**.
   - Wait until the progress reaches **100%**.

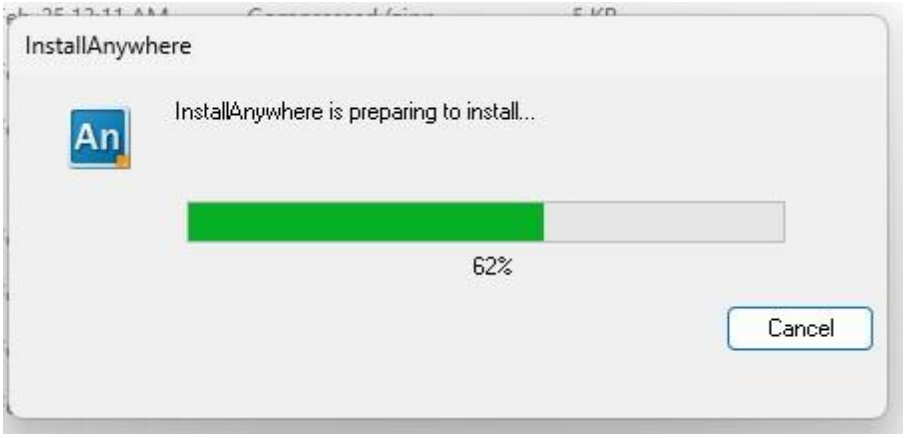


Figure 4.1:16: InstallAnywhere Loading Screen

3. **Introduction Screen**
   - After **InstallAnywhere** completes preparation, the **Introduction Screen** appears.
   - The installer provides an overview of the installation process and recommends closing all running applications before proceeding.
   - Click **Next** to continue.

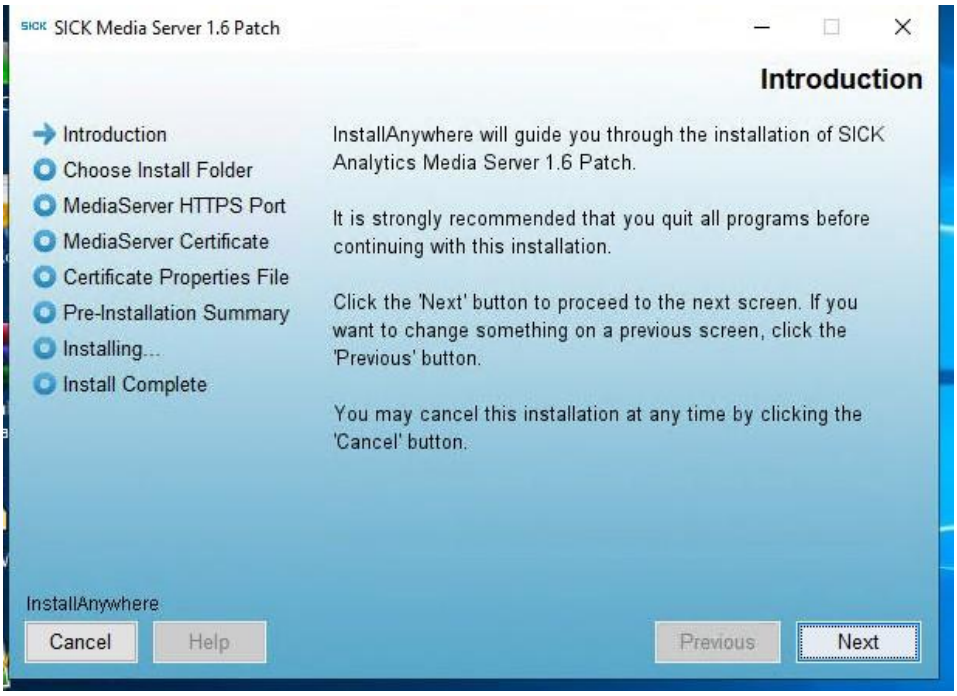


Figure 4.1:17: Introduction Screen

4. **Choose MySQL Data Folder**
    - If the previous Main Installation Package did not install MySQL, you will be prompted to select the MySQL data path.
    - Choose a folder where MySQL data should be stored.
    - **Options:**
        - Click **Restore Default Folder** to use the default path.
        - Click **Choose…** to select a custom location.
    - Click **Next** to proceed.

Figure 4.1:18: MySQL Data Folder Selection

***Note*:** *You have the option to select the **MySQL data path** only if MySQL was not installed during the previous Main Installation Package installation.*

5. **Specify Certificate Properties File:**
   - During patch installation, you will be prompted to select a certificate properties file required for Media Server.
   - This file contains the certificate configuration settings used for secure HTTPS communication.
   - **Options:**
   - **Choose…:** Browse and select the cert.properties file (for example: C:\certupdates\cert.properties).
   - **Restore Default File:** Revert to the default certificate properties file if no custom file is provided.
   - Click **Next** to continue with the selected properties file.

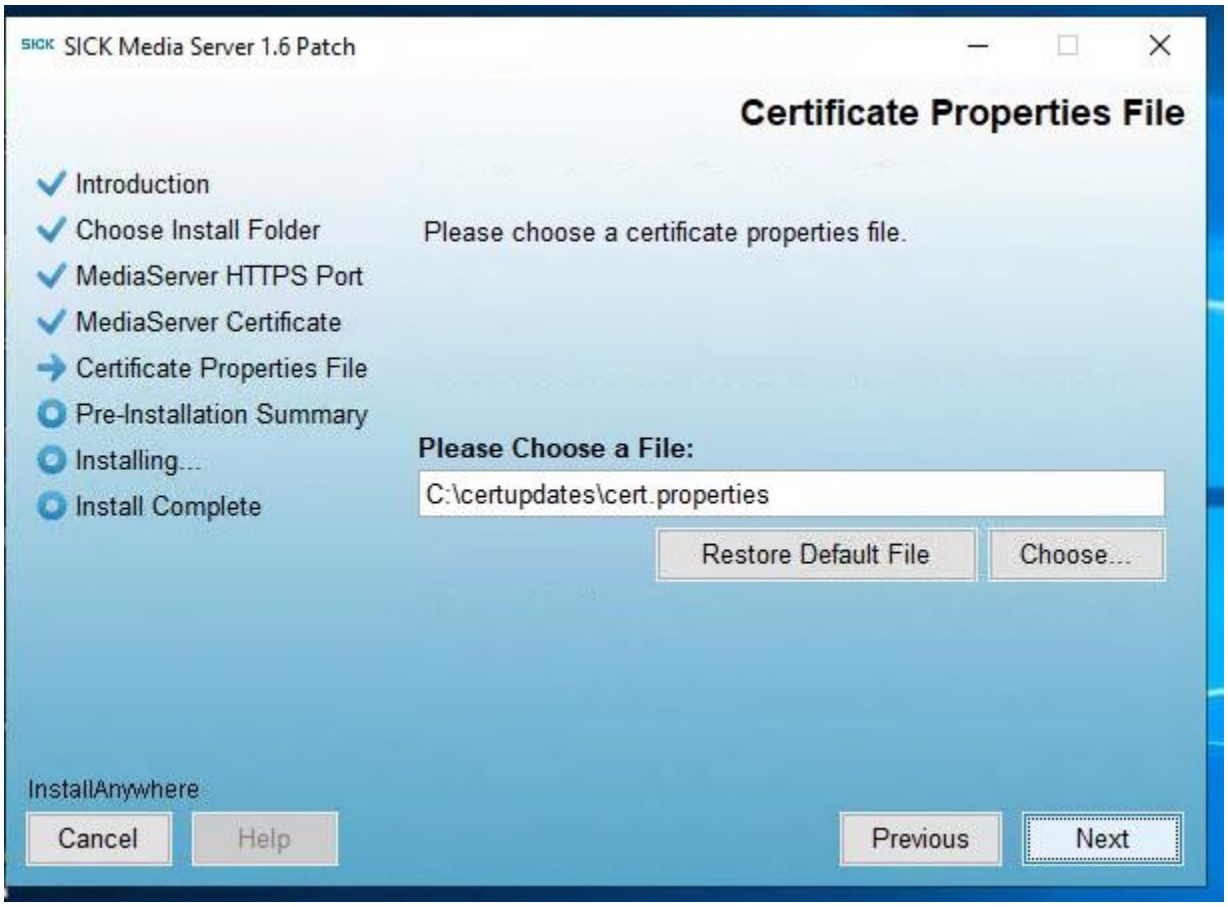


Figure 2.1:19: Media Server Certificate Selection

6. **Pre-Installation Summary**

   - Review the Pre-Installation Summary before proceeding.
   - It displays the Product Name, Install Folder, and Disk Space Information (Required & Available Space).
   - Verify the details and click **Install** to begin.

Figure 4.1:19: Pre-Installation Summary

7. Patch Installation in Progress

- The installer begins patch installation and displays a progress bar.
- JRE and dependencies may be installed or updated.
- Wait until the process reaches **100%.**

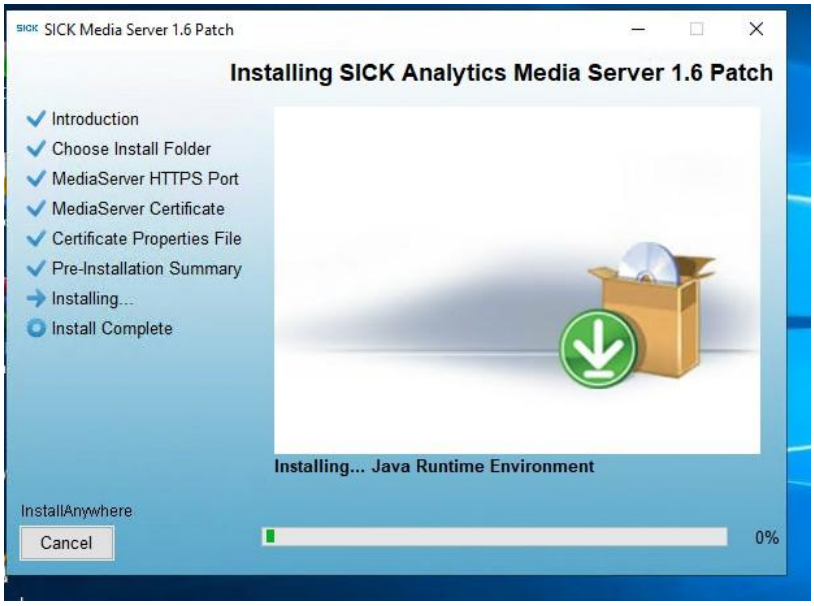


Figure 4.1:20:Patch Installation in Progress

8. **Installation Complete**
    - The **Install Complete** screen confirms that the patch has been successfully installed.
    - The **installation directory** is displayed for reference.
    - Click **Done** to exit the installer.

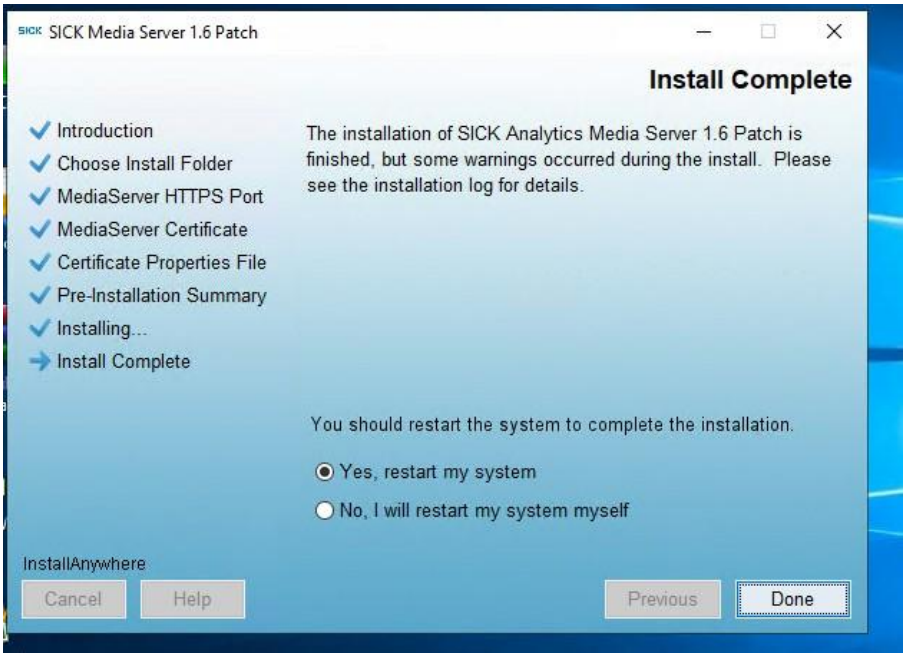


Figure 4.1:21: Install Complete

4.2 Un-installing SICK Media Server

You can uninstall Media server by relaunching the installer with the provided executable file (Please refer To Launch the installer on Windows) or from control panel. Follow the following steps to uninstall the application:

1. Open the **Control Panel**.

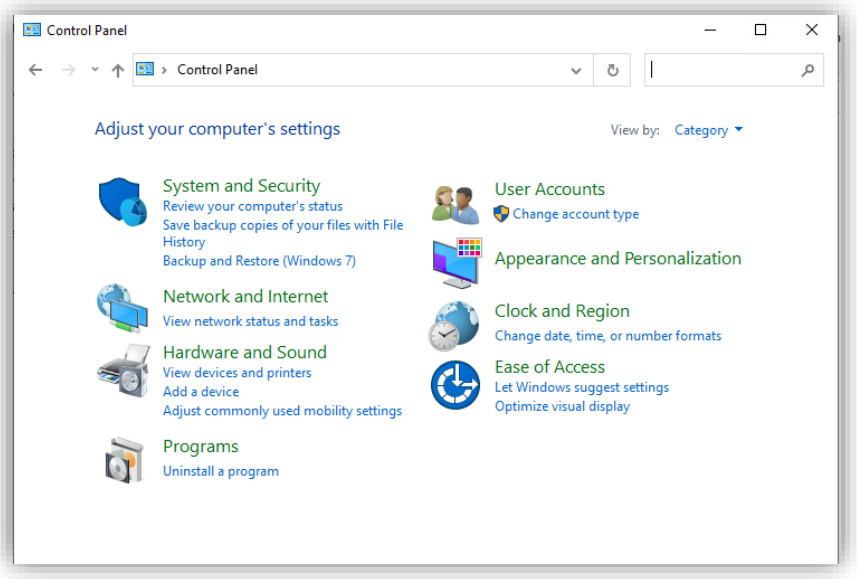


Figure 4.2:1: Control Panel

2. Click on **Programs**.

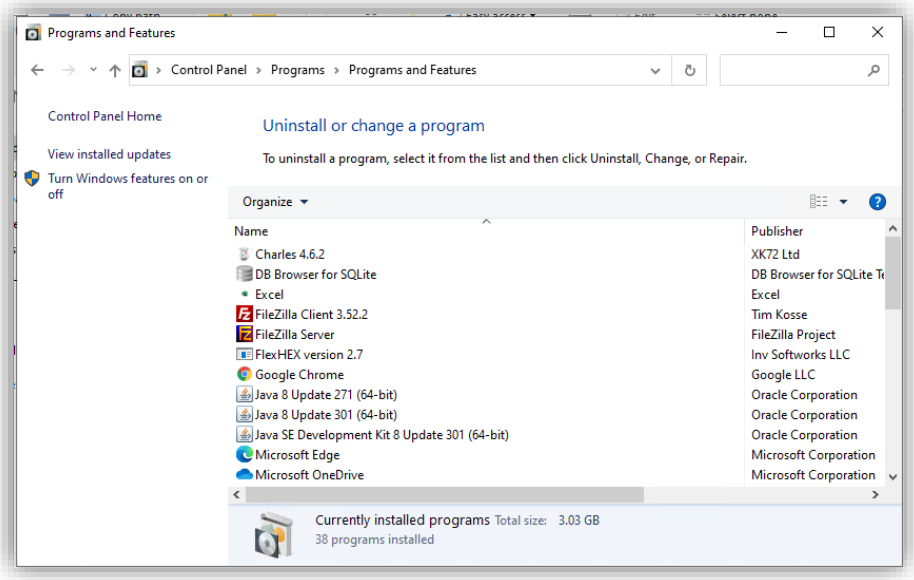


Figure 4.2:2: Programs

3. Under **Programs and Features**, click **Uninstall a Program**.

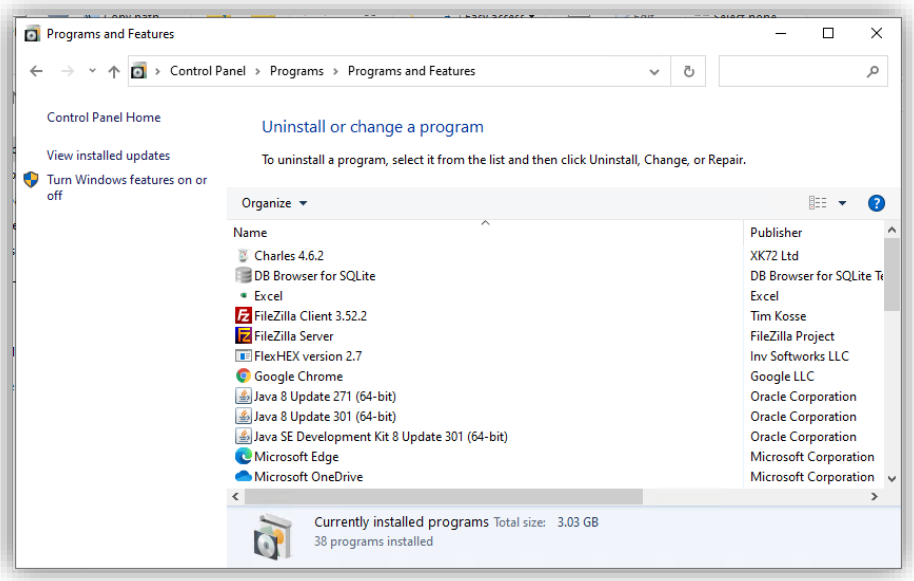


Figure 4.2:3: Uninstall a Program

4. Locate and select **SICK Media Server** from the list of installed applications.
5. Click **Uninstall** to launch the **Maintenance Mode** screen.

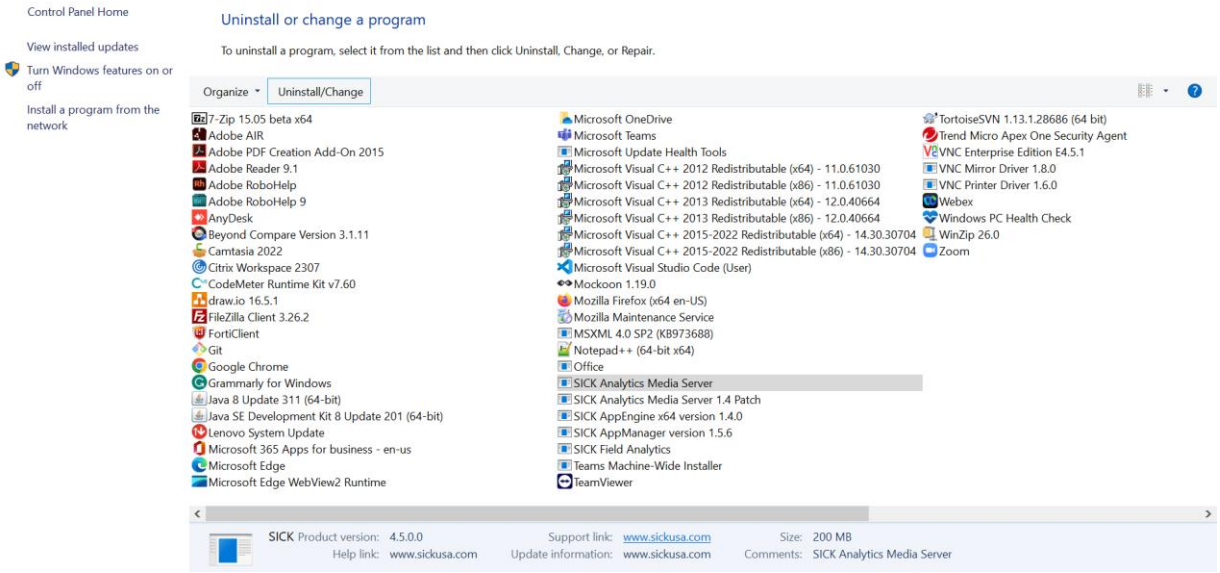


Figure 4.2:4: Launching Media Server Uninstaller

6. On the **Maintenance Mode** screen, select **'Uninstall Product'** and click **'Next'**.

   You will land on the **Maintenance Mode** screen, which displays different options based on the type of uninstallation:

- **Full Installer Maintenance Mode:**
  If you are using the **full uninstaller**, you will see the following options:
  - **Add Features** – Add components to the installed product.
  - **Remove Features** – Remove components from the installed product.
  - **Uninstall Product** – Completely remove the product.

  Select **'Uninstall Product'** and click **'Next'**.

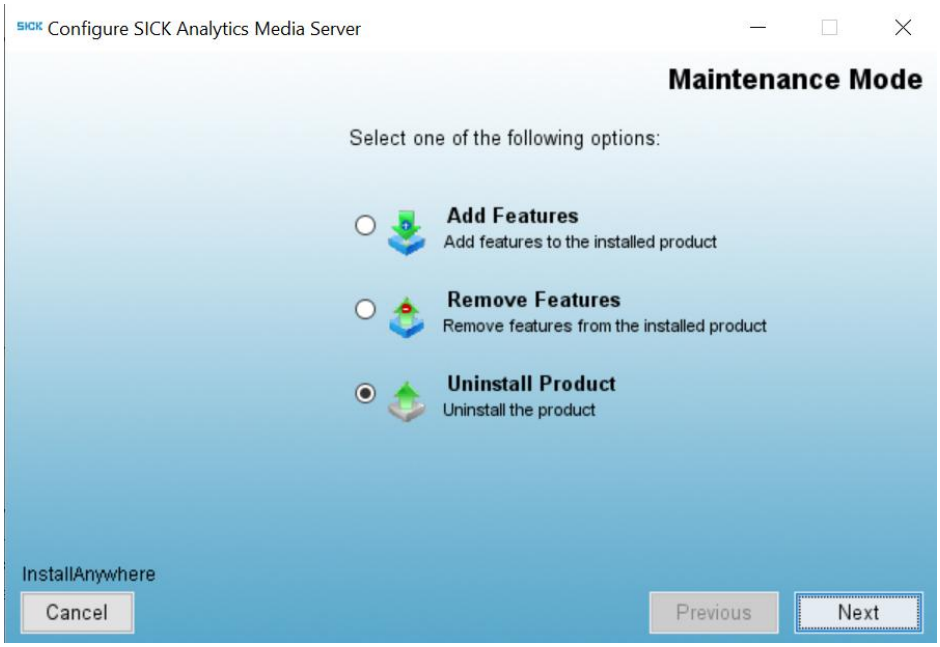


Figure 4.2:5: Full Installer Maintenance Mode Options

- **Patch Uninstaller Maintenance Mode:**
  If you are using the **patch uninstaller**, you will see the **'Uninstall Product'**

option.

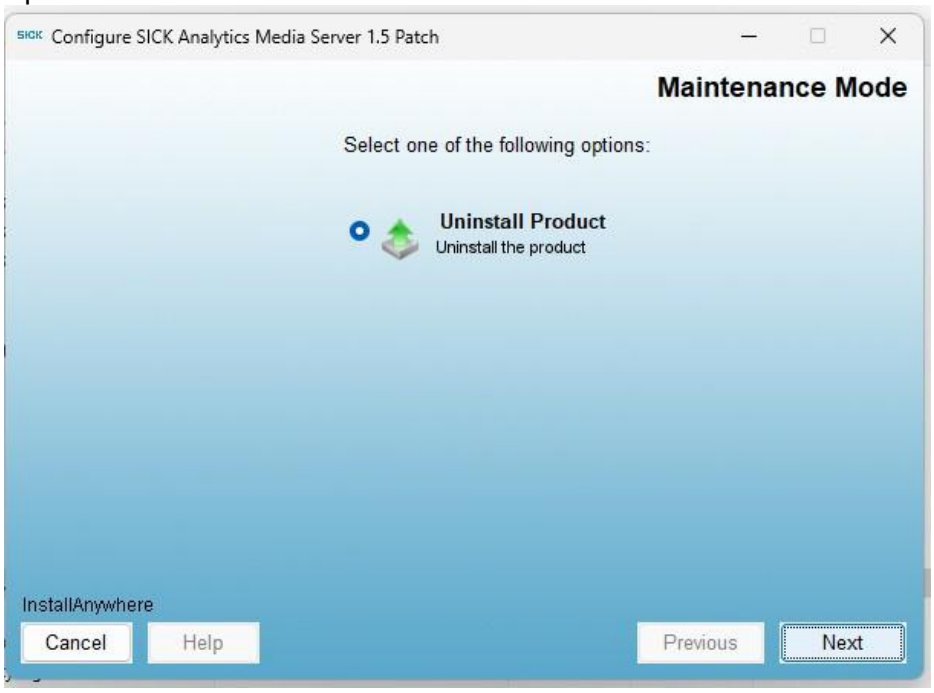


Figure 4.2:6:Patch Uninstaller Maintenance Mode

Note: The full installer removes the entire application, whereas the patch uninstaller only removes the applied patches while keeping the core installation intact.

7. On the **Patches Uninstallation** dialog, review the content and click **OK**.

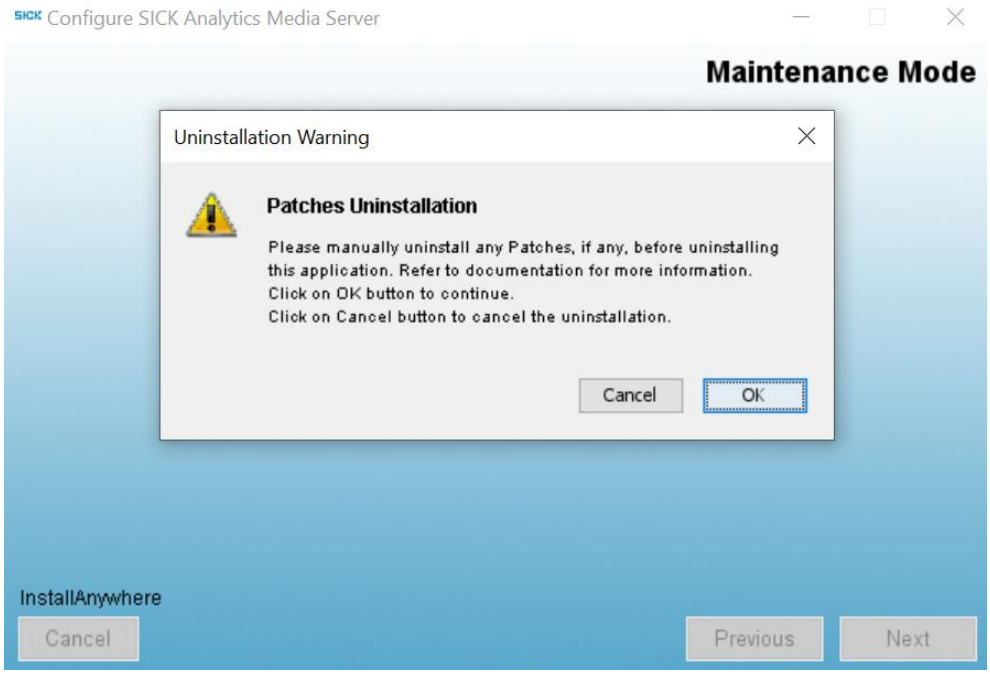


Figure 4.2:7: Patches Uninstallation

8. On the **Uninstall SICK Analytics Media Server** screen, click **Next**.

Figure 4.2:8: Uninstall Screen

9. The **Index File and Images** screen appears with the prompt:
   "Do you want to delete the media server index file and images?"
   - Select **Delete** to remove the index file and images.
   - Select **Keep** to retain the index file and images.
10. The uninstallation process begins, displaying the progress in the **progress bar**.

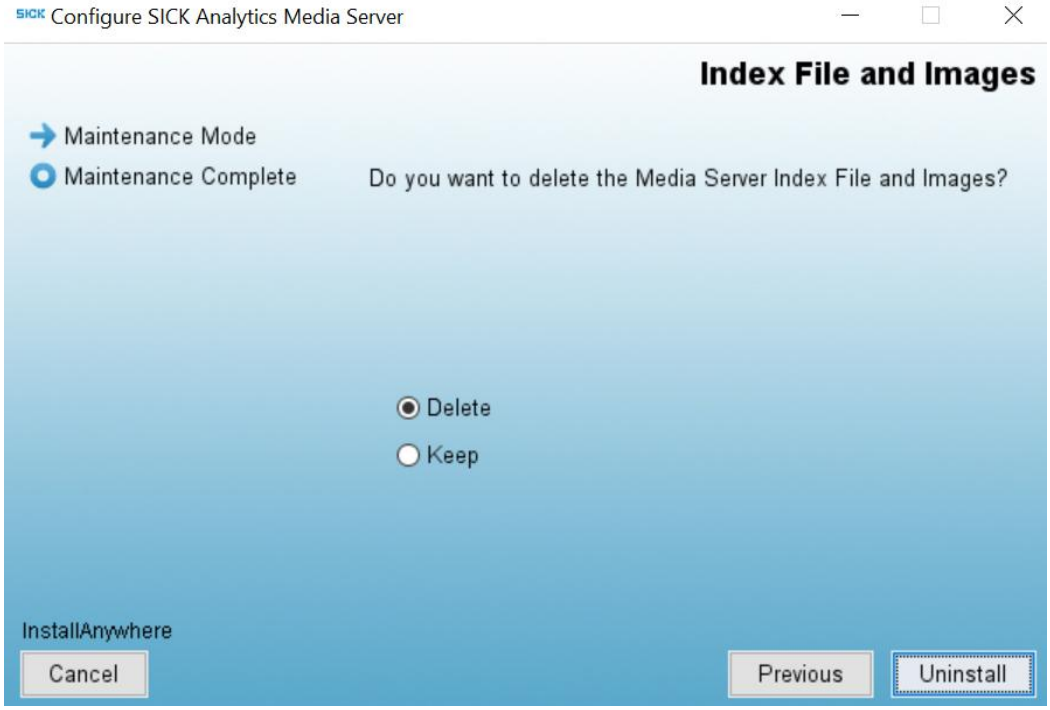


Figure 4.2:9: **Uninstallation In-progress**

11. If you are using the **patch uninstaller**, a new **Product Uninstallation** screen appears before finalizing the process:
    - If **Uninstall Product** is selected, the entire application will be removed.
    - If left unchecked, only the patch will be uninstalled while keeping the core application intact.
    - Click **Next** to proceed.

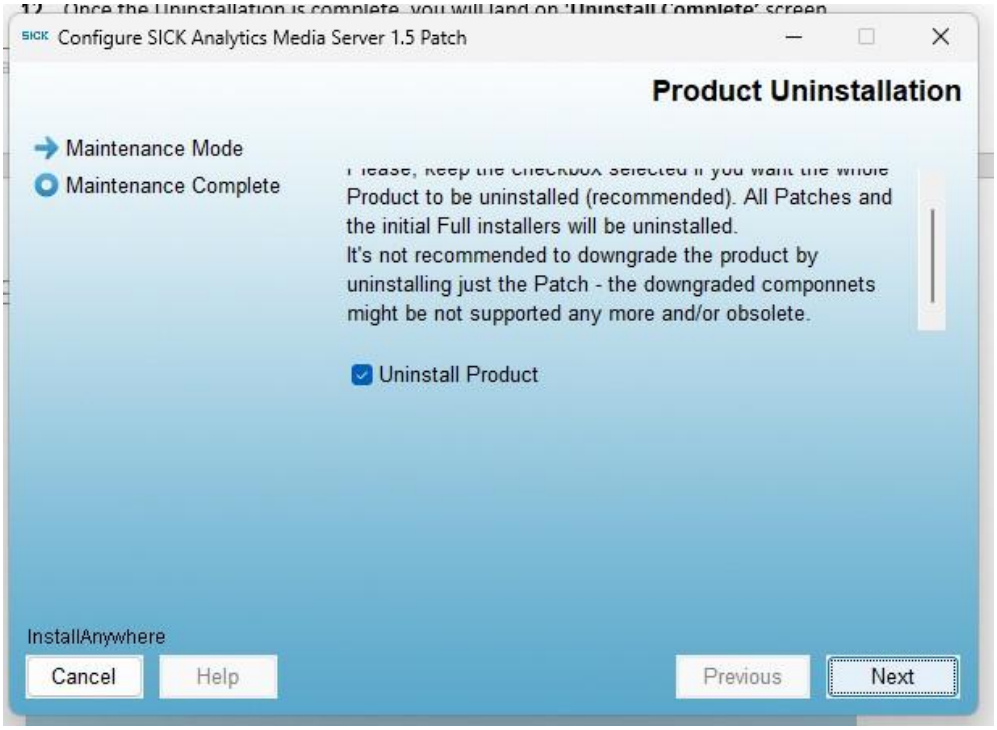


Figure 4.2:10: Product Uninstallation Screen

12. Once the uninstallation is complete, the **Uninstall Complete** screen appears:
    - Select **Yes, restart my system** to restart immediately.
    - Select **No, I will restart my system myself** if you prefer to restart later.
    - Click **Done** to exit the uninstallation process.

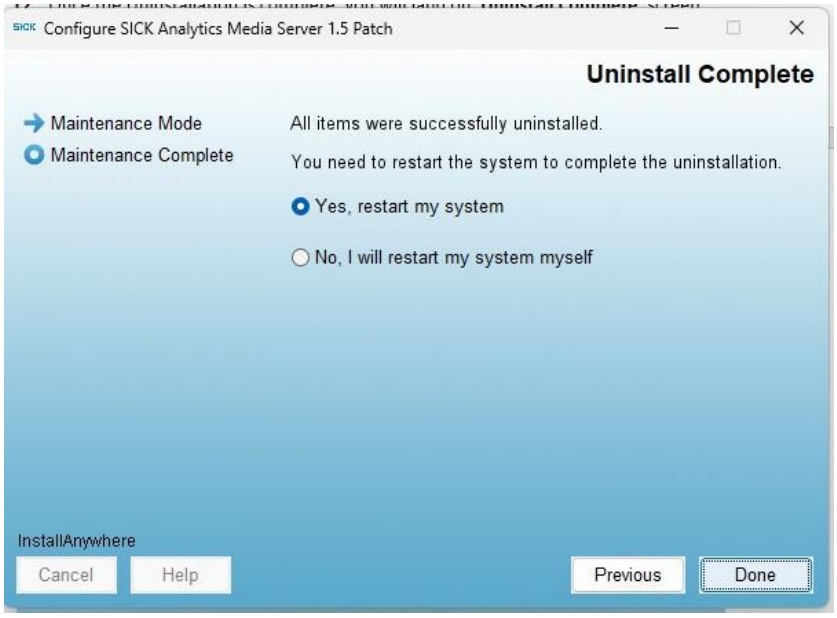


Figure 4.2:11: Uninstall Complete

Note:

- For Linux, uninstallation mode of Media Server can be opened on relaunching the installer. Please refer to section To launch the installer on Linux for steps to launch installer.

5 Using SICK Media Server

SICK Analytics Software applications may use various media capturing devices to analyze/ enhance the performance of the system. Media Server is used to store these captured media files locally or at a remote location as per the user requirement. The Media Server can be configured from Analytics Software or from Media Server GUI.

5.1 Launching SICK Media Server

The SICK Media server Dashboard can be accessed from supported web browsers. You can access Media server Dashboard from the host PC, or any device PC given that the host PC and the Device PC are on the same network. As Media Server has support for secured connection, application can also launch through HTTPS port.
Launching the Media Server application through HTTP/HTTPS port.

Launch Method	Description
From host PC	Media server can be accessed using *URLs http://localhost:{HTTP port} or https://localhost:{HTTPS port}* Example: *http://localhost:*8084 *https://localhost:*443
From Device PC	Media server can be accessed using URL http:// {IP address}: {HTTP port} or https://{IP address}:{HTTPS port} Example: *http://10.102.11.197:*8084 *https://10.102.11.197:*443

Table 4: Launch Methods

Note: *HTTP/HTTPS port run on 8084 and 443 by default. To launch the application on https, the same must be enabled from License. In case there is no License applied, application will be accessible on HTTP and HTTPS (HTTPS requires a valid certificate) both, however, only License & Registration tab will be visible.*

5.2 Login

When you launch the **SICK Media Server**, the login screen is displayed. Users can authenticate using either **OIDC (Single Sign-On)** or **database credentials**, depending on the authentication configuration.

Login Options

The login page provides the following options:

Login via MS OIDC

- Allows users to log in using corporate credentials through an **OpenID Connect (OIDC) Identity Provider**, such as **Microsoft Entra ID**.
- Selecting this option redirects the user to the configured identity provider for authentication.

Figure 3.2:1: Login Screen – MS OIDC Authentication

Login as Database User

- Allows users to log in using locally stored **Media Server credentials**.

Credentials

Username: `<Enter your username>`
Password: `<Enter your password>`

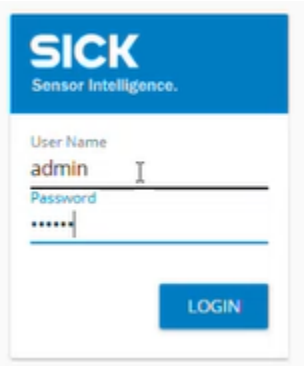


Figure 3.2:2: Login Screen – Database User Authentication

Note: *Media Server can be configured from Media Server GUI after logging into the application using User's credentials (username & password). You can add a new user or update existing user credentials from sick-bip-is.cfg file. Refer to* Manage Media Server User *for details.*

5.3 Applying license

Logging into the application will take you to the '**License & Registration'** page if the License is missing, invalid or expired. You will be able to access application components only if a valid license is already present or on applying a new valid license.
Refer to License and Registration for more details.

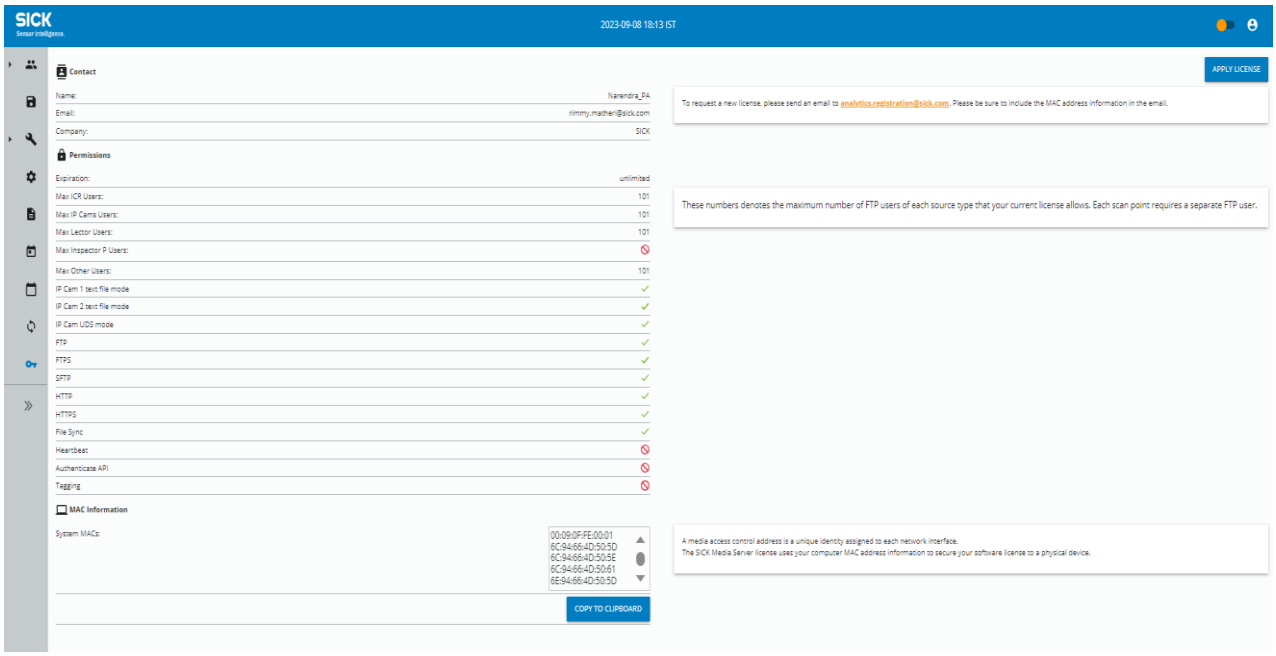


Figure 5.3:1: After Applying Valid License

Note: *Only License and Registration tab will be loaded before applying valid license. Application components can only be accessed after applying valid license file.*

6 Dashboard

SICK Media Server Dashboard gives you access to different components of the application. You can use these components to configure your Media Server.

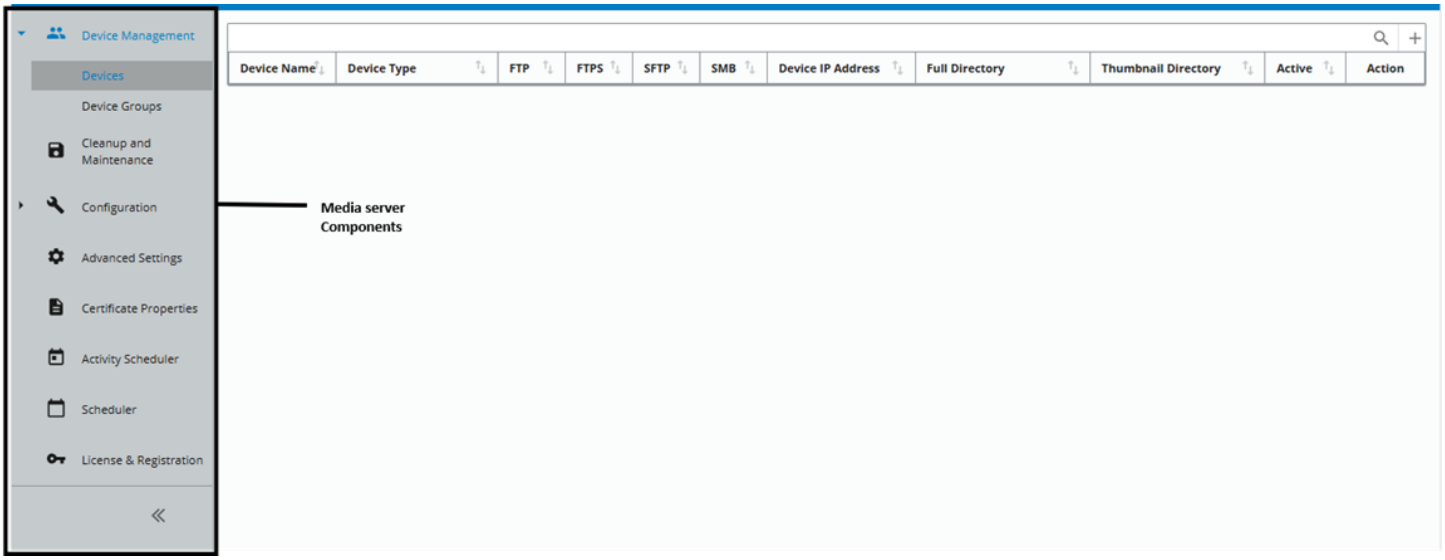


Figure 5.3:1: Media Server Window

Here is the list of components of the Media Server:

Selection	Description
Device Management Screen a. Devices b. Device Groups	This section allow user to Add/Edit/delete the FTP/FTPS/SFTP/SMB devices and device groups.
Cleanup and Maintenance Screen	This tab allow user to configure cleanup process settings for media files
Configuration a. Primary Server b. File Sync	• This section provides licensed protocol information of the Media Server. Protocols FTP/FTPS/SFTP/File Sync can be configured from this section. • File sync helps in archival of media files to the remote server. This feature is useful in situations where the Media server connected to image capturing devices has limited/low disc space.

Selection	Description
Advanced Settings	Consists of three sections i.e., Database, Barcode Counter, API Users Configuration Heartbeat and Properties Configuration. Database (Edit or Recover MySQL Configuration): provides details about the configured MySQL database. Barcode Counter stores metadata information about the cumulative code count matching the configured rule. Information such as: UID, 1Z/PTN Tracking Number, Timestamp, UPS Code Count, Image File path/r/n; will be stored by reading the incoming xml files for the camera API Users section allow user to configure API control access for users. Heartbeat section allows user to configure Heartbeat properties. This section also allows you to enable/disable publishing Heartbeat message to Facility View.
Certificate Properties	Displays the status and properties of the currently applied certificate.
Activity Scheduler	Activity Scheduler feature helps user to schedule an activity covering the schedule downtime with respect to the activity.
Scheduler	User can schedule Media Server Activities for specified intervals. These intervals can be configured using scheduler page and called as schedules.
Sync Status	This tab enables to track the Live status of the activity
License and registration	This section displays the currently applied License and permissions. You can also apply/update new license from this section.

Table 5: Components of Media Server

7 Device Management

Device Management is used create and maintain the devices & device groups.

7.1 Device

Media files are saved in the storage location as per device name and time of storage. Media capturing devices of SICK auto-identification systems are identified by the Media Server as their devices. Each media capturing device has an option to configure a username and password, which is added to the Media Server as a Device. It is required to configure these settings for media capturing devices of SICK auto-identification systems so that the associated media files can be saved in proper location.

Note:

- Only licensed protocols are displayed as configurable/supported protocols for the devices.
- Starting with Media Server 1.6, FTP can be disabled directly from the Media Server UI without requiring a new license.
- HTTP can be disabled through license configuration, configuration file, or directly from the Media Server UI by navigating to **Advanced Settings → Properties Configuration**. .
- The option to enable or disable HTTP from the UI is available only when the application is accessed over HTTPS.
- When HTTP is disabled, the HTTP port field will not be displayed.
- For detailed steps on how to enable or disable protocols, refer to Section Enable/Disable Protocols.
- It is recommended to use secure alternatives such as SFTP and HTTPS for encrypted communication. For further assistancehttps://supportportal.sick.com/.

.

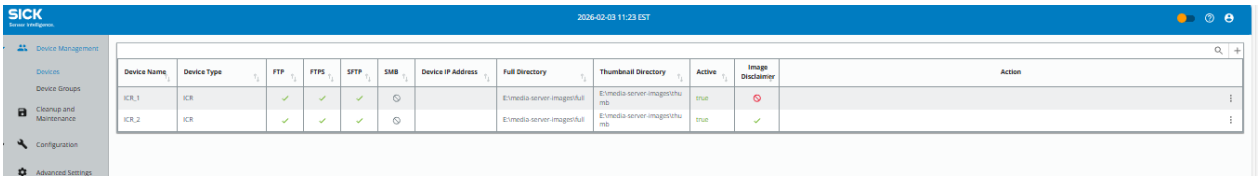


Figure 7.1:1: Device Table

All the configured FTP/FTPS/SFTP device in the Media Server are available in a tabular format under the tab Device Management. This table provides detailed information of the configured FTP/FTPS/SFTP device:

Selection	Description
Username	Provide Username
Device Type	Configured Device type for the device
FTP	Enabled if the FTP protocol is licensed and the device can accept files over FTP.
FTPS	Enabled if the FTPS protocol is licensed and the device can accept files over FTPS.
SFTP	Enabled if the SFTP protocol is licensed and the device can accept files over SFTP.
SMB	Enabled if ICR890-4 device is added.
Device IP Address	IP address of the device. This is an optional field for all devices except ICR890-4 device. For ICR890-4, application displays SMB Server IP Address field which is a required field.
Full Directory	Displays location of Full directory where full size images are stored
Thumbnail Directory	Displays location of Thumbnail directory where thumbnail images are stored
Active	This field gives info of the device state which is dependent on the uploaded license file. Active device can accept data over the supported protocols. Deactivated device accepts data over the time; however, images will not be retrieved from deactivated devices.

Selection	Description
Action	This field displays the ellipsis. Clicking on the ellipsis provides Edit and Delete options for the device.
Image Disclaimer	Indicates whether the image disclaimer is enabled for the device.

Table 6: Configured Device Details

7.1.1 Add Device

A new device can be configured in the application from **Add Device** window. Various types of media capturing devices can be configured as devices: ICR, Lector, IPCam – 1 txt file mode, IPCam – 2 txt file mode, Event Cam, Inspector-P and Other Sources.

Device	Description
Lector	It captures multiple images and generates xml on trigger
ICR	It captures thumb and full-size images. It generates xml on trigger.
IP Cam-1 txt file mode	This device is used for IP Camera's which support software triggers for image renaming. Supported modes: - One txt file - Renaming Mode - UDS Mode
IP Cam-2 txt file mode	This device is used for IP Camera's which support hardware triggers for image renaming.
Event Cam	This device is used for Event camera's which captures me-dia on a trigger
Inspector-P	This device is used for Inspector-P Devices which captures media on a trigger
SEC	Captures JPEG images upon a trigger using SEC 100 devices for package identification in logistics, compatible with Package Analytics for tracking,

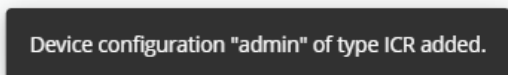
	sorting, and auditing. Requires licensing via Media Server or Package Analytics.

Table 7: Devices and its Description

Refer to Appendix C about IP cam for more details.
You can create devices in Media server application based on the devices available in Analytics / SICK auto-identification systems.

To add FTP, FTPS, SFTP device:

1. Navigate to Device Management screen by clicking on Device Management tab  in the left navigation panel.
2. Click on the **+** icon at the top right corner.
3. The **Add Client Device** window will open.
4. Select **Server** option.
5. Select Protocol/s (At least one protocol selection is required).
6. Select a **Device Type** under Device Settings.
7. Enter Login credential i.e., **Username** and **Password**
8. Enter **IP Address** for the device. This field is optional.
9. Select **Enable Image Disclaimer**, if the image disclaimer must be applied to images generated by this device.
   ***Note**: Configure the disclaimer content in Advanced Settings → Properties Configuration. For more information about configuring the image disclaimer, see Section 10.3, Image Disclaimer.*
10. The disclaimer content can be configured in Advanced Settings → Properties Configuration.
11. Click on '**Save**' button.
12. A new device will be added, and a success snack bar message will be displayed.



13. If there is an error while adding the device, application will display a snack bar message that an error has occurred.

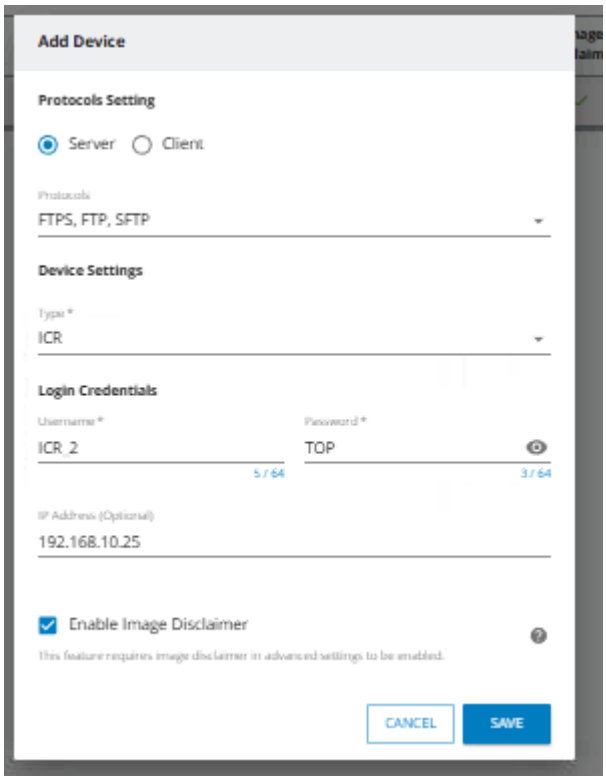


Figure 7.1:2: Add Device

Note: *At least one transfer protocol should be selected for a device. Devices with specific device type cannot be added more than the allowed no. from the License. Example: If the License allow 5 ICR's, then you can only add up to 5 ICR type device. It is suggested to use one device per Camera. Using multiple cameras to send images to a single device can cause redundancy/image loss due to overwriting.*

To add a SMB Device:

1. Navigate to Device Management screen by clicking on Device Management tab in the left navigation pane.
2. Click on the **+** icon at the top right corner.
3. The **Add Device** window will open.
4. Select **Device** option.
5. By default, Protocol is selected as **SMB** under Protocols dropdown
6. By default, **Device Type** is selected as **ICR890-4** under Device Settings.
7. Enter Login credential i.e., **Username** and **Password**
8. Enter SMB Server IP Address.
9. Full/Thumb Directory location will be populated based on the Username. Example: image_ssd/<Username>.
10. **Save** button will be enabled once all the fields are filled in with valid values. Click on '**Save'** button.

11. A new SMB device will be added, and a success snack bar message will be displayed.

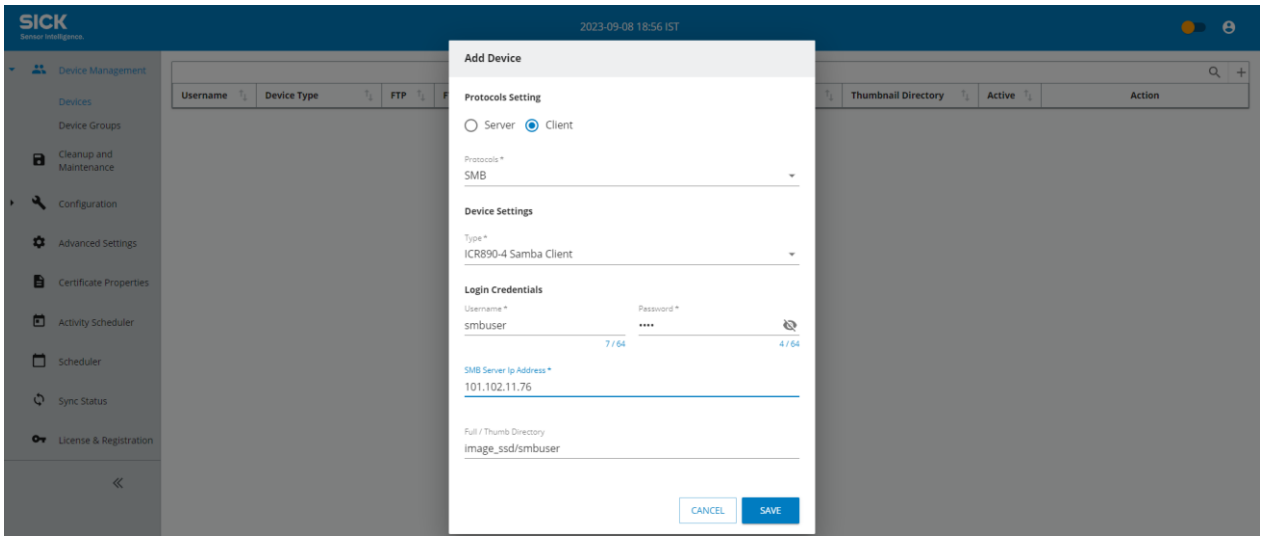


Figure 7.1:3: Add SMB Device

7.1.2 Points to consider before configuring ICR890-4 device

- **Shared Folder Requirement**
  - The ICR890-4 camera must have a shared folder named **"image_ssd"**.
- **Username-Based Subfolder**
  - Inside the "image_ssd" folder, create a subfolder named after the username used to access the ICR890-4 device via the Samba protocol.
  - Example: If the username is "smbuser", the folder structure should be:
    - **image_ssd/smbuser**
- **Timestamp Folder Structure**
  - The folder structure under the username must follow a timestamp-based hierarchy:
    - **Syntax**: `image_ssd/username/yyyy/mm/dd/hh/image.ext`
    - **Example**: `image_ssd/smbuser/2021/02/23/06/02-20210223-023212-00000090.jpg`
- **Time Synchronization**
  - Ensure that the ICR890-4 dashboard and MSC (Management System Console) are synchronized to maintain consistency in timestamped files.
- **Username Requirement**
  - The username for accessing the ICR890-4 device must be unique to ensure proper folder organization and access control.

7.1.3 File retrieval with ICR890-4 Device using Samba Protocol

- **Single Media Retrieval (All File Types: jpg, jpeg, png, bmp, html, xml, ply, etc.)**
  - If the file is retrieved successfully, the Media Service (MS) will return the requested file data in its native format.
  - If there is any failure during retrieval:
    - For image files (jpg, jpeg, png, bmp), MS will return an error response image (in one of the supported image formats) containing the requested filename and detailed error information.
    - For all other file types (e.g., html, xml, ply, etc.), MS will return an HTML error response page specifying the error code and relevant error details.

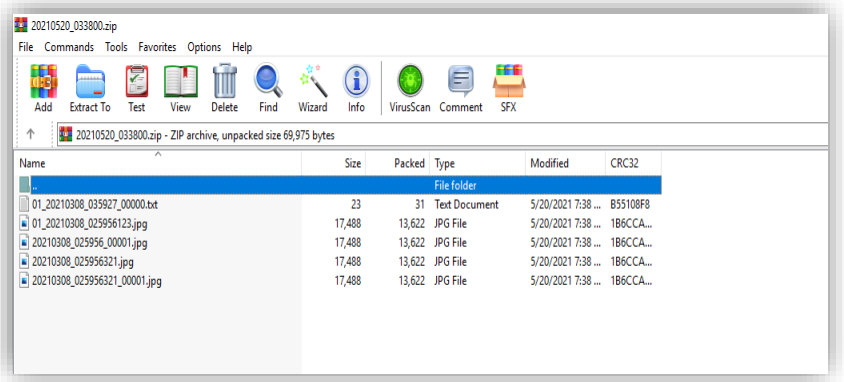


Figure 7.1:4: Files Retrieved

- **Multiple Media Retrieval (Image File Types: jpg, jpeg, png, bmp)**
  - If all the files are retrieved successfully, MS will add all the file data into a zip file and return the zip folder.
  - If some files were retrieved successfully while others failed, MS will add only the successfully retrieved file data and return the zip folder.

7.1.4 Edit Device

The Devices can be edited as per the user requirement from this window. Edit Device window can be accessed from edit Device option available under menu icon ⋮ corresponding to each configured device.
To edit a Device:

1. Navigate to Device Management screen by clicking on Device Management tab in the left navigation pane.
2. Click on the menu icon ⋮ for the device you would like to edit.

3. **Edit Device** and **Delete Device** options are available under this menu.

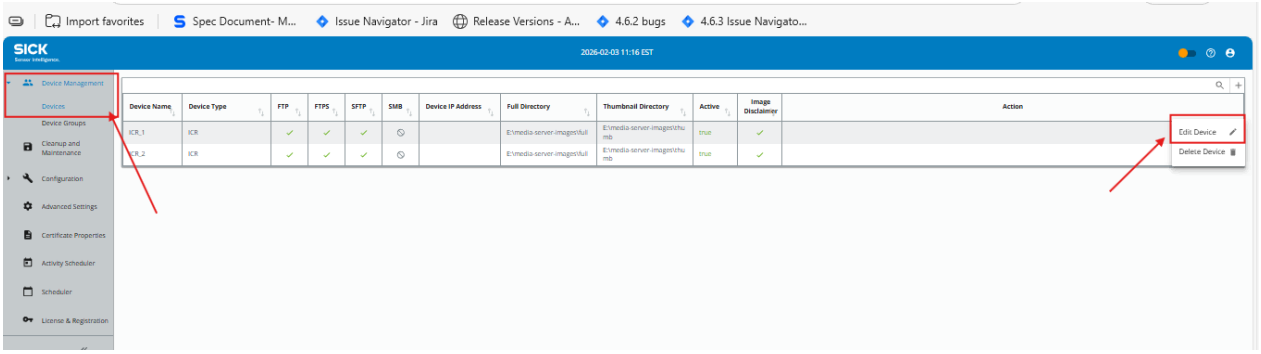


Figure 7.1:5: Device Screen

4. Click on **Edit Device** option.
5. On **Edit Device** make necessary changes and click on **Save** button.
6. The selected device will be updated, and a success snack bar message will be displayed. If there is an error while editing the device, application will display a snack bar message that an error has occurred.

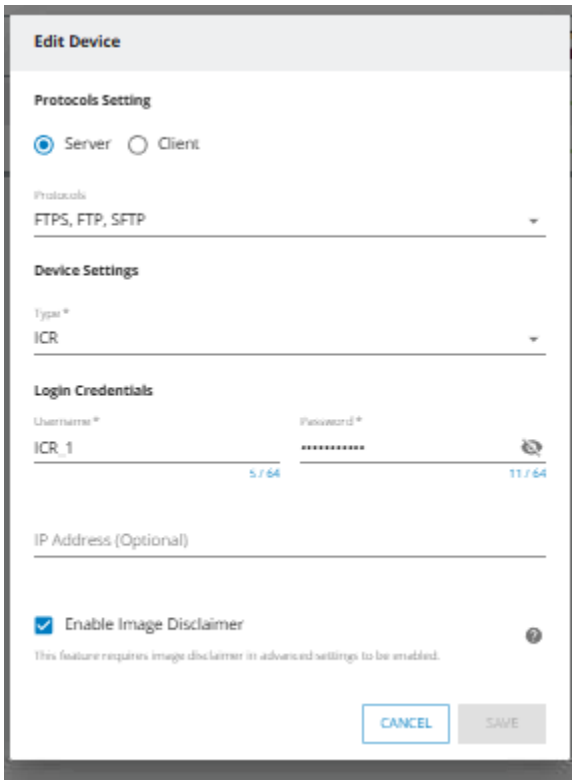


Figure 7.1:6: Edit Device Window

Note: *At least one transfer protocol should be selected for a device.*

7.1.5 Delete Device

The Device can be deleted by clicking on the **Delete Device** option under the menu icon ⋮.

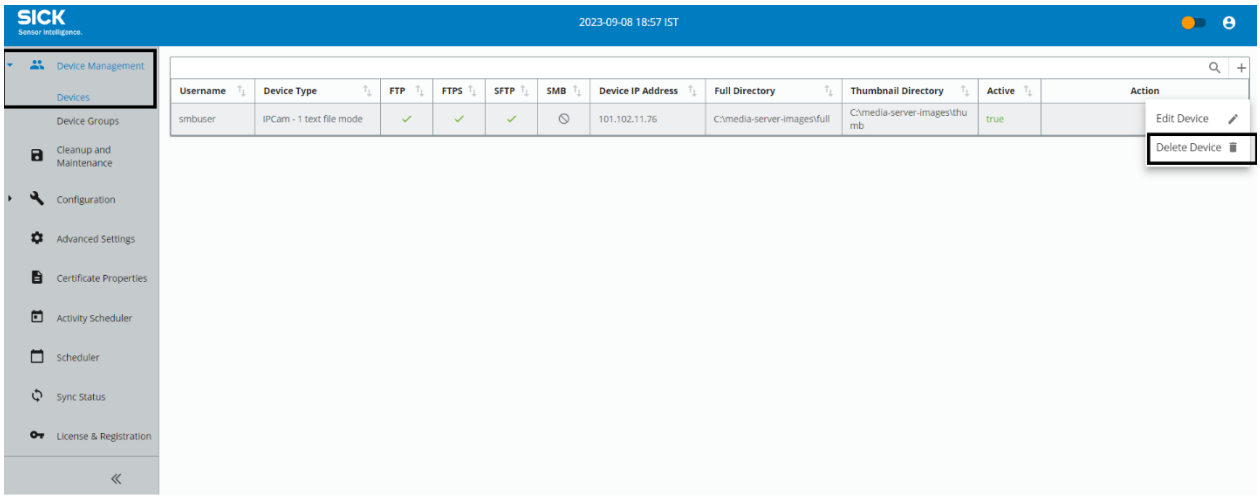
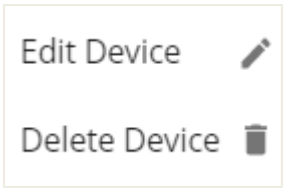


Figure 7.1:7: Delete Device Option

To delete a device:

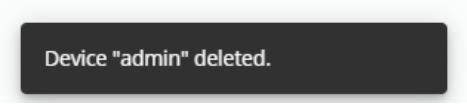
1. Navigate to Device Management screen by clicking on Device Management tab in the left navigation pane.
2. Click on the menu icon ⋮ for the device you would like to delete.
3. **Edit Device** and **Delete Device** options are available under this menu.



4. Click on **Delete Device** to delete the selected Device. On successful deletion, a snack bar message will be displayed, as shown below.

Note: *The images of the deleted devices are not deleted from the file location; however, you will not be able to extract images of a deleted device.*

There is no confirmation/undo message for delete device. Once deleted, user would need to add device again.



7.2 Device Group

To create a '**Device Group'**, follow below steps:

1. Select '**Device Groups'** tab under '**Device management'** in the left navigation pane.
2. From the '**Device Groups'** screen, click on '+**Add Group'** on the top right corner of the screen.

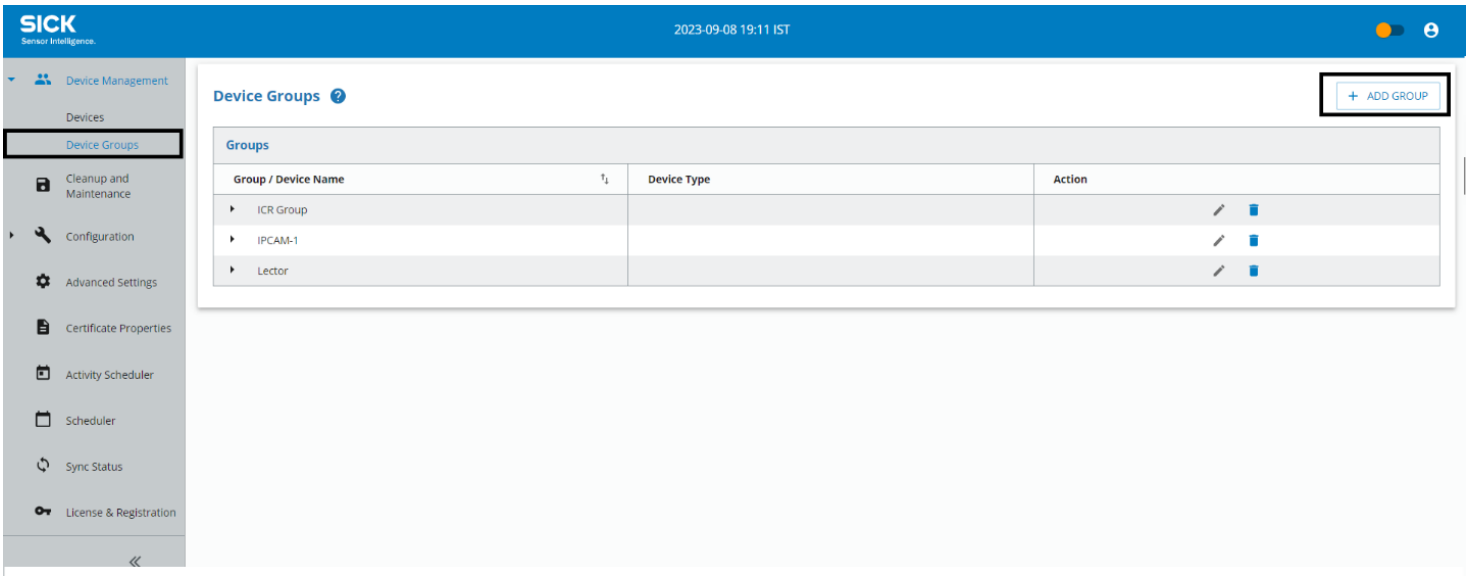


Figure 7.2:1: Device Groups Screen

3. '**Add Group'** window appears with following fields:
   - **Group Name**: Provide group name.
   - **Groups**: Select the groups from the drop-down.
   - **Devices**: Select devices from the drop-down.
   - Click on **'Save'** button.

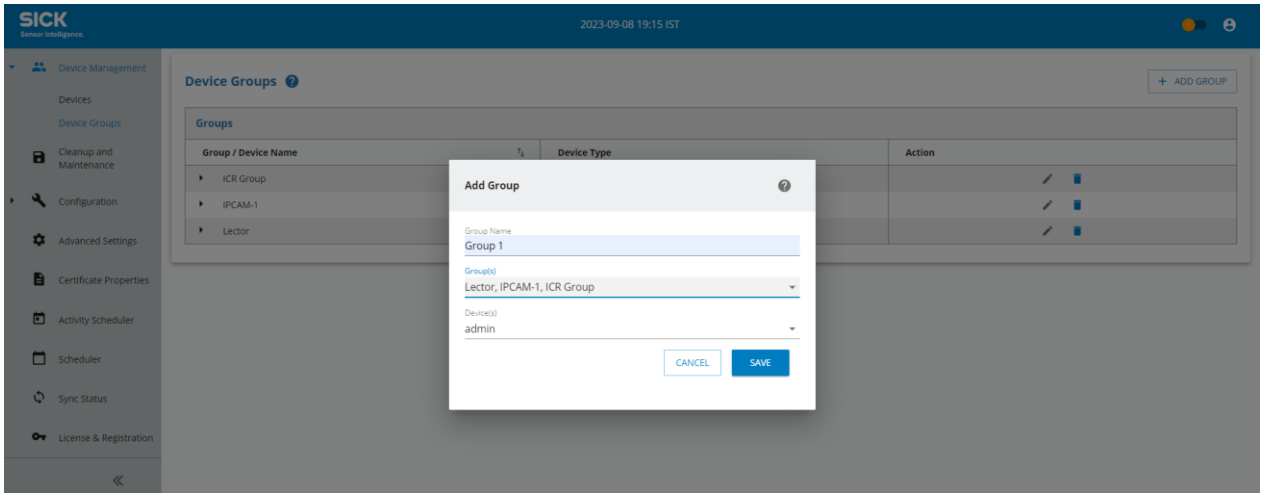


Figure 7.2:2: Add Group Window

4. The added group is displayed in the Device Groups table.

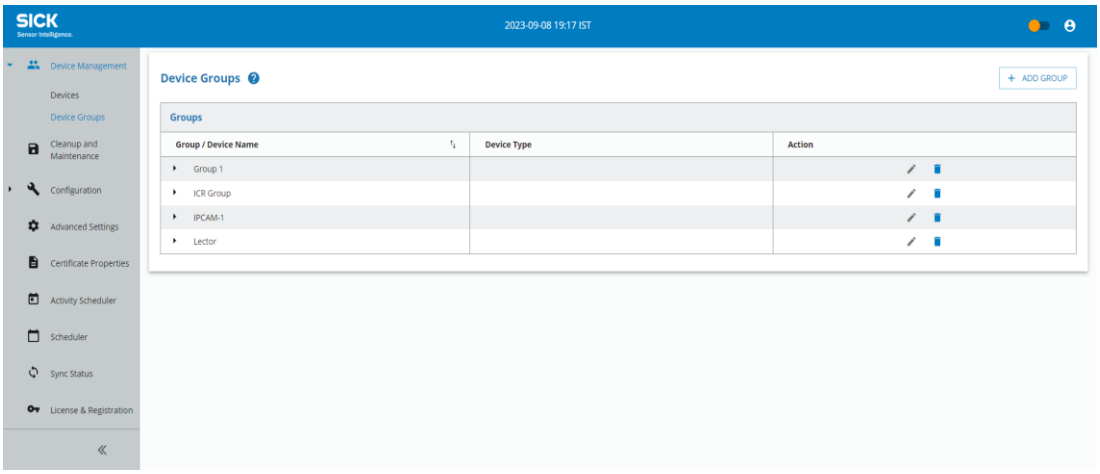


Figure 7.2:3: Added Group in Device Group Screen

7.3 Sorting the Table Columns

By default, the Device table displays the devices based on the order they were added. You can sort devices listed in the table by clicking on Username, Device Type or Device IP Address column heading. Clicking on the column heading for the first time will sort the table in ascending order of the column selected.

- Click a column heading to sort by that value. Click the heading again to toggle between ascending and descending sort order for the selected heading.

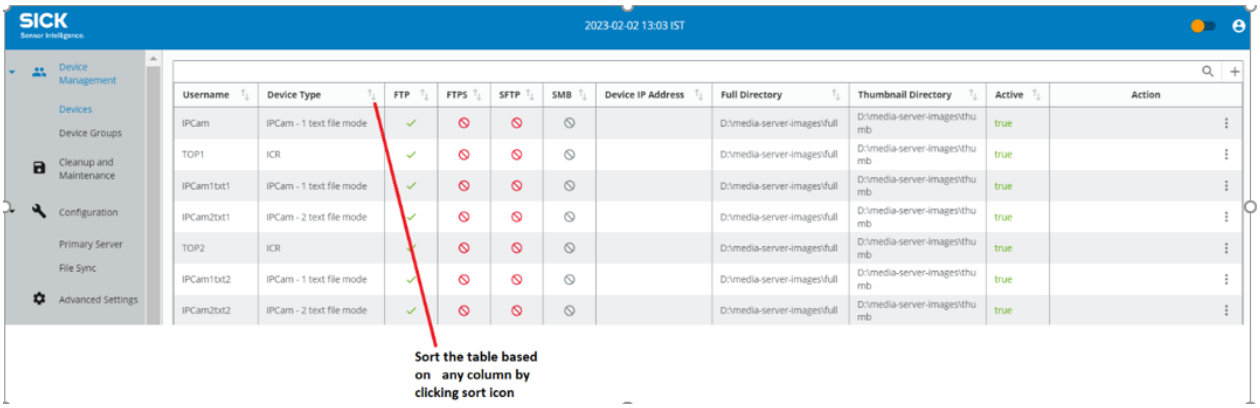


Figure 7.3:1: Sorting based on Device Type

8 User Profile

This option provides information about the currently logged in user. Click on profile icon at the top right corner. Application will display a greeting message **Welcome <<username>>** and a Logout option.
Click on the **Logout** option to Log out of the application.

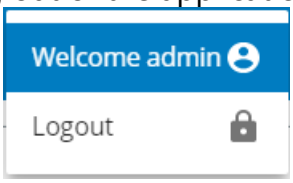


Figure 7.3:1: User Profile

Note: *Media Server can be configured from Media Server GUI using User's credentials (username & password). These are the pre-defined Users (Admin, Operator, API) for media server and all users have same privileges.*

9 Cleanup and Maintenance

The SICK Media Server provides tools for managing storage locations, cleaning up media files, and maintaining optimal disk space. This section covers cleanup processes, storage considerations, and important maintenance mechanisms.

The server storage has limited capacity. If the storage fills up, the Media Server will stop saving media files received from MSC or Cameras. To prevent data loss, older media files must be deleted automatically based on the cleanup settings.

9.1 Cleanup Methods

The following types of cleanup can be performed to manage storage effectively:

- **Size-based cleanup** – Automatically deletes files when the storage reaches a pre-defined threshold.
- **Age-out-based cleanup** – Removes older files based on their retention period.
- **Manual cleanup** – Allows users to manually delete files.
- **Rule-based cleanup** – Custom cleanup rules can be defined based on system policies.

Note: Cleanup operations will be **halted during database migration**. Please refer to **Error! Reference source not found.** for migration details.

9.2 Migration impact on cleanup

During database migration, cleanup operations and certain configurations are disabled to ensure data integrity.

- A banner message appears in the user interface (UI) stating **"Data migration in progress. Cleanup halted."**
- Cleanup processes, including size-based, age-out, rule-based, and manual cleanup, do not run while migration is in progress.
- Configuration changes to devices, server name, storage locations, properties, and protocols are disabled.
- If storage fills up during migration, older migrated records are deleted using the **first in, first out (FIFO)** method.

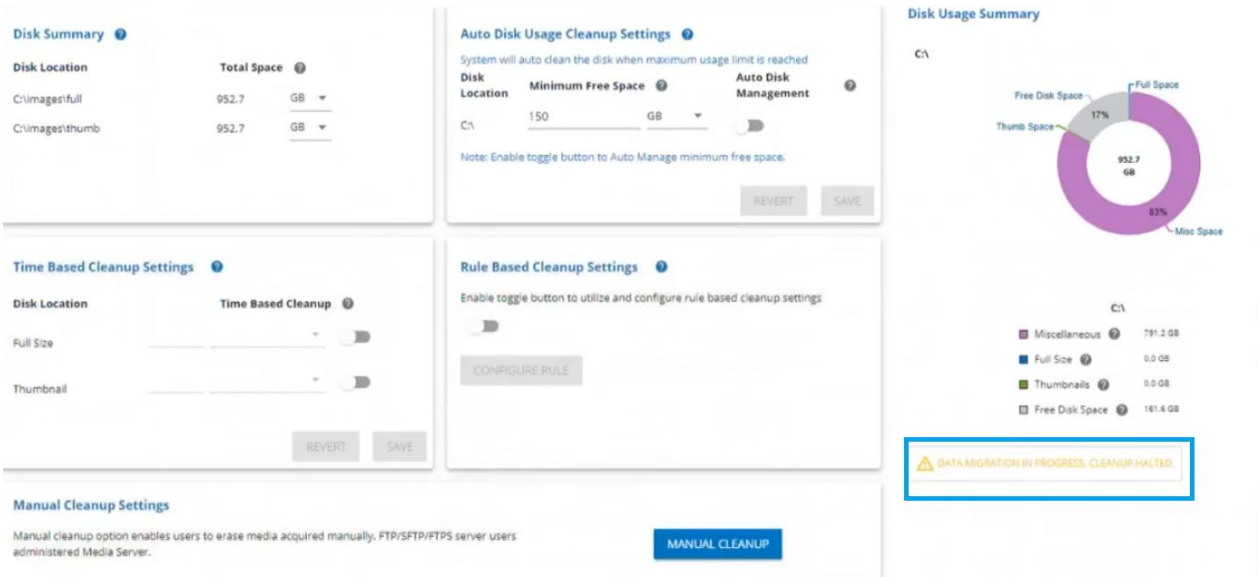


Figure 9.2:1: Cleanup and Maintenance UI during migration

9.3 Media server Name and Storage Location

The name of the server, full-size and thumbnails folder location can be configured using Edit Media Server window.

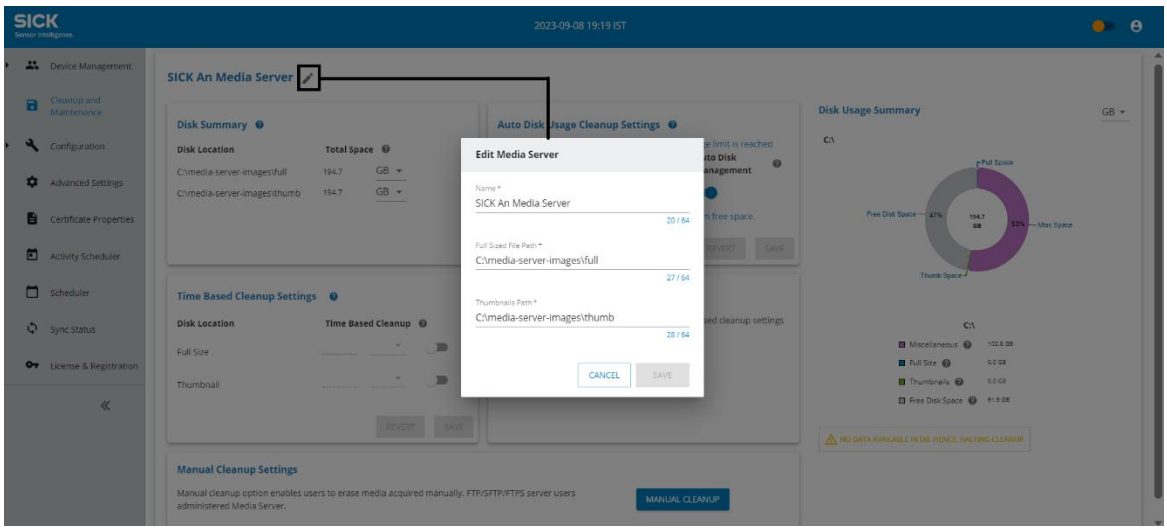


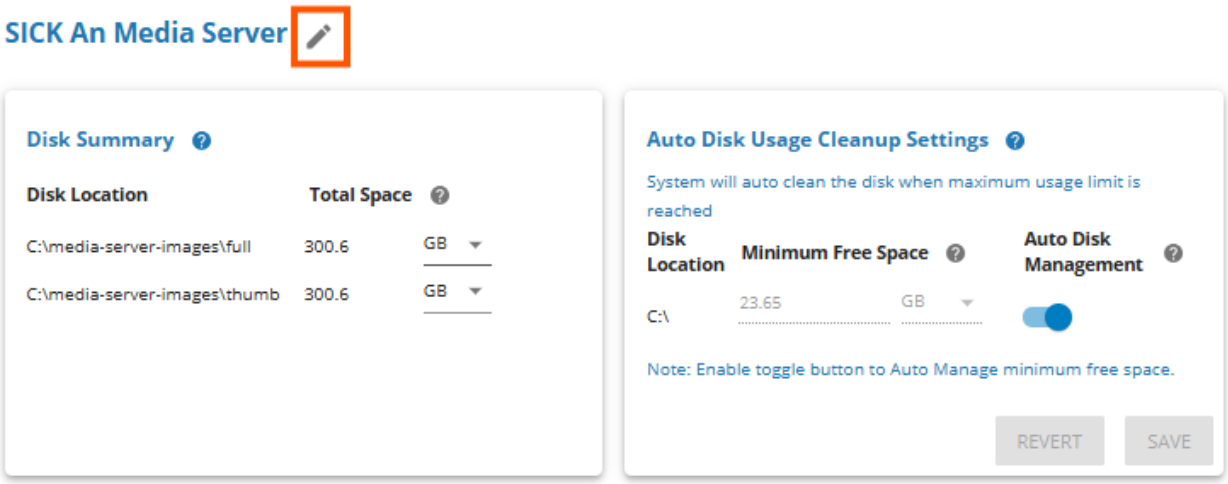
Figure 9.3:1: Edit Media Server

***Note**: Media acquired by Media Server will be saved in the full size or thumbnail location set in Edit Media Server section.*

To set/Update name, full-size and thumbnail location:

1. Launch and login to Media Server application.
2. Navigate to Cleanup and maintenance screen by clicking Cleanup and Maintenance option from the left navigation pane.

3. Click on pencil icon to open Edit Media Server Window



4. In **Edit Media server** window make changes:
   (a) Name: to set/update Media server name.
   (b) Full Sized File Path: to set/update location where full-sized files will be saved.
   (c) Thumbnail Path: to set/update location where thumbnail files will be saved.

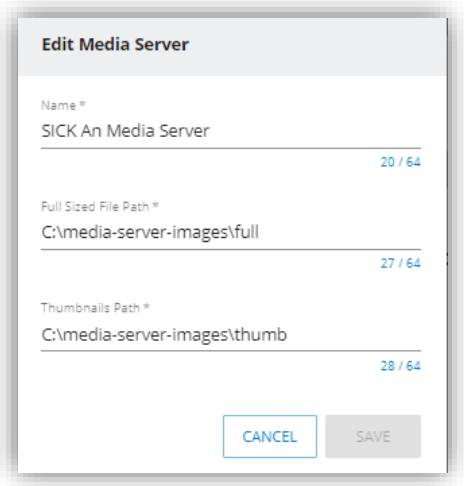


Figure 9.3:2: Edit Media Server

5. Click on **Save** Button to confirm the changes.

9.4 Size Based Cleanup

Size based cleanup (also known as Storage based cleanup and Usage based cleanup) clears out the media files as per the minimum free space configured under Auto Disk Usage Cleanup Setting. The cleanup operation is performed if the set Usage based criteria is fulfilled.

Note: *Size based cleanup cannot be disabled as this is the primary cleanup mechanism.*

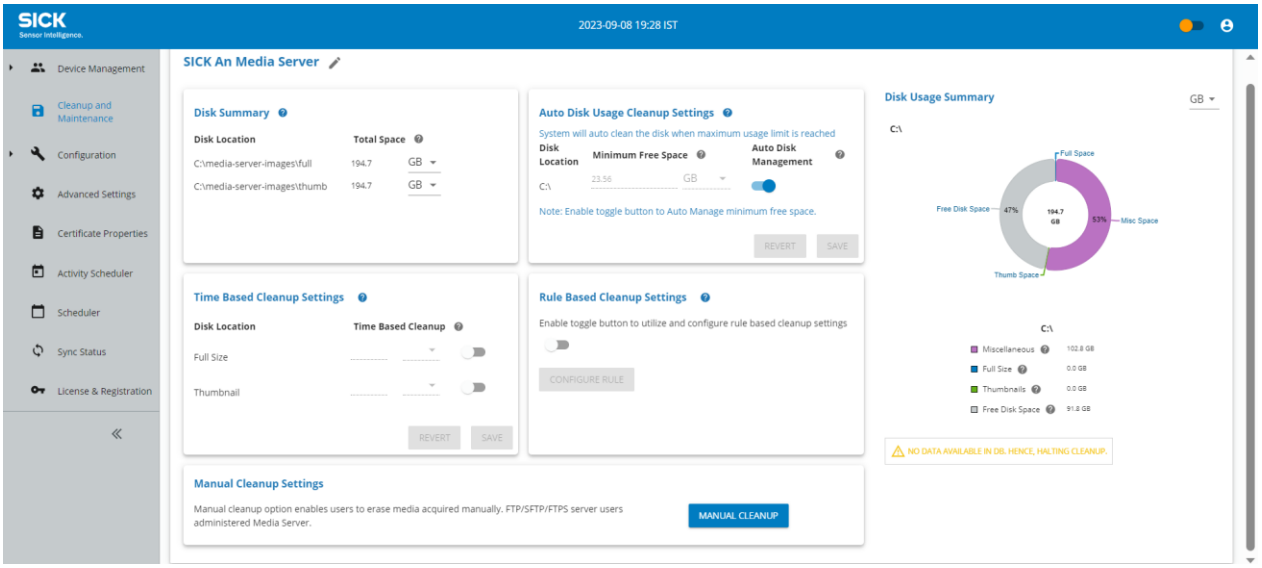


Figure 9.4:1: Size Based Cleanup

Size based cleanup is maintained for individual drives as per the size cleanup settings configured. The number of drives that are visible under this section is based on the path set for full size and thumbnail images. If full size and thumbnail location is set in the same drive, single drive is displayed in size cleanup setting. This drive can be configured for size-based cleanup.

Note: *Please refer* *Media Server Name and Storage Location* *for details on how to set/update full size and thumbnail location.*

If full size and thumbnail location is set in different drives, two different drives are displayed in size cleanup setting. These drives can be configured for size-based cleanup individually.

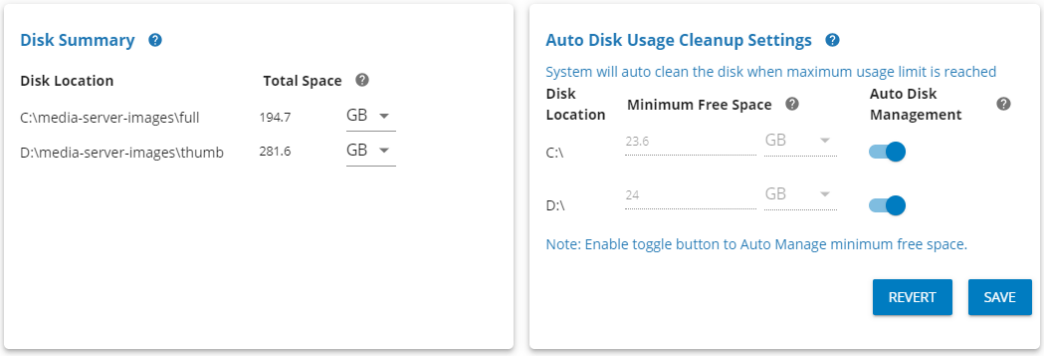


Figure 9.4:2: Auto Disk Usage Cleanup Setting

Note:

- Maximum aggressive and Aggressive cleanup are safety mechanism to avoid overflow of disk space.
- User will observe Warning messages displayed in the UI under Disk Usage Summary if Maximum aggressive or Aggressive cleanup is being performed by Media Server. Please refer to Disk Usage Summary or the detailed message displayed during these cleanups.
- Please refer to Appendix B for detailed information on Regular Buffer, Additional Buffer, Maximum Aggressive cleanup, Regular cleanup, and Aggressive cleanup.

Note: *You might not see the Media server files utilizing the maximum disk space due to internally configured Regular Buffer and Additional Buffer. Media server files are deleted based on FIFO (First in First out) if any of this buffer space is hit.*

9.4.1 Size Based Cleanup modes

Size based cleanup can be configured in two modes: Auto and Custom

9.4.1.1 Custom Size Based Cleanup

To configure this type of cleanup, disable the toggle button under Auto disk management for the drive that needs to have custom free space settings. This setting will come in handy if it is required to reserve some free space in the drive that is being used by other applications for their proper functioning.

Note: *It is recommended to use custom size-based cleanup for the drives that do not have operating system (OS) installed but has some other important application installed. Available space in this drive can be customized based on the requirement.*

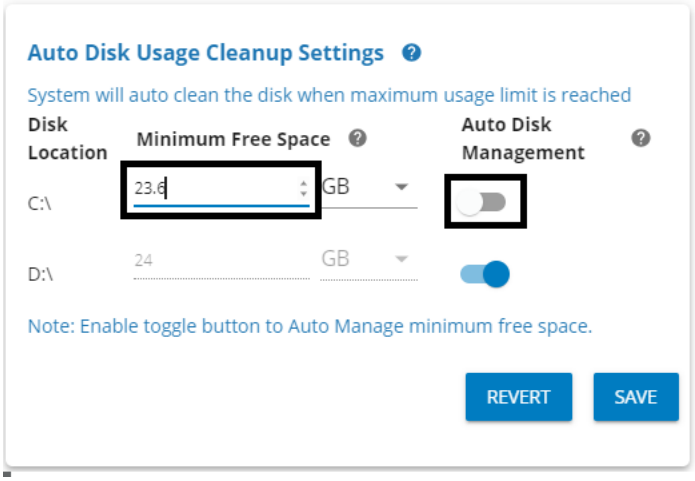


Figure 9.4:3: Custom Size Based Cleanup

9.4.1.2 Auto Size Based Cleanup

To configure this type of cleanup, enable the toggle button under Auto disk management for the drive that needs to be auto managed for size-based cleanup. Media Server will set minimum free space as 1Gb and will try to utilize maximum disk space for Media Server files. This setting is recommended for the disk location that is only storing media server images and requires maximum utilization of the space.

> ***Note:*** *It is recommended to use Auto size-based cleanup for the drives that have operating system (OS). This will assign 1.5 times the total RAM by default as the minimum free space. Use Custom size-based cleanup to increase the reserved space for this drive.*

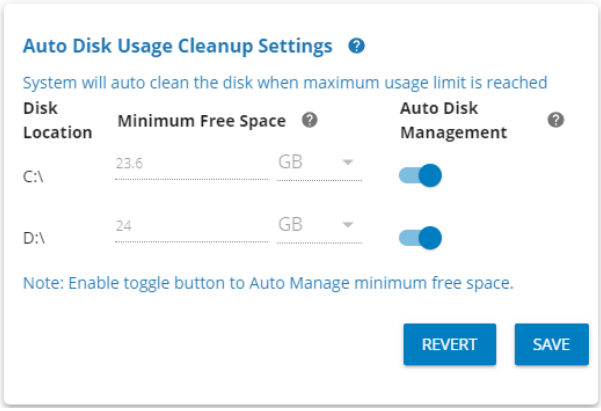


Figure 9.4:4: Auto Size Based Cleanup

9.4.2 Important points to consider before configuring clean-up rules

- **Auto Disk Management**
  - Enable **Auto Disk Management** for maximum disk space utilization.
  - When enabled, Media Server reserves 1.5 times the RAM of the machine as the minimum free space on the operating system (OS) disk.
  - To reserve more than 1 GB of free space**,** disable Auto Disk Management and manually enter the reserved space.
    - This setting is recommended for drives containing other important software**.**
- **Recommended Storage Setup**
  - It is recommended to use a dedicated drive exclusively for storing Media Server files.
  - Separate buffers are maintained for each drive type.
- **Cleanup Operations**
  - Age-out based cleanup **is required if the** storage location **for full-size or thumbnail images has changed.**
  - Size-based cleanup **applies** only to the current drive**.**
    - **Example:** If the storage location is changed from **C:** to **D:**, size-based cleanup will only apply to **D:**.

- **Historical data** in **C:** will remain and must be cleared using **Age-out based cleanup**.

- **Minimum Free Space Allocation**
  - When **Auto Disk Management** is enabled:
    - For OS Disk: **Minimum free space is set to** 1.5 times the RAM**.**
    - For Non-OS Disk: **Minimum free space is set to** 1 GB**.**
  - **Custom Size-based cleanup** should be used for drives storing images and other important software.
    - This allows increasing the **minimum free space beyond 1 GB** for software to function properly.
- Storage Cleanup Configuration
  - Storage-based cleanup settings are **configurable via the configuration file**.
  - Refer to **Configuration File** for detailed parameter settings.

9.4.3 Set up Size Based Clean-up

1. Launch and login to Media Server application.
2. Navigate to Cleanup and maintenance screen by clicking Cleanup and Maintenance option  from the left navigation pane.

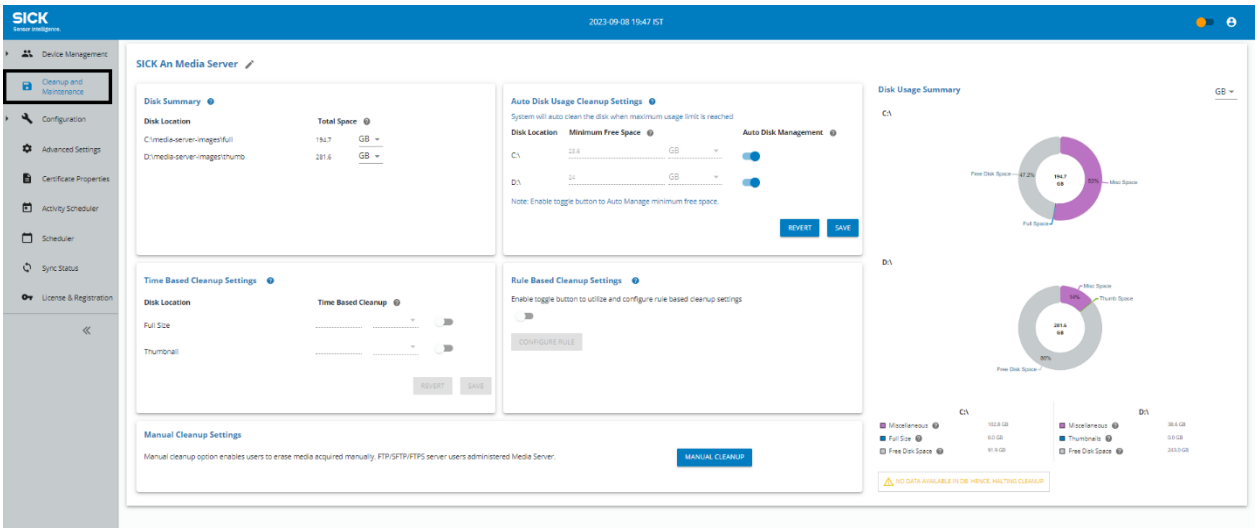
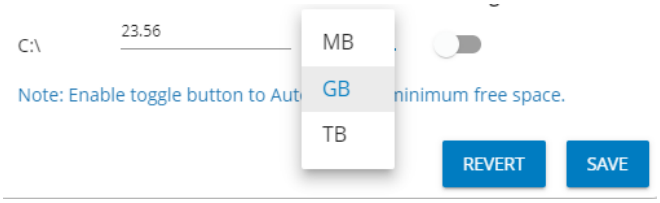


Figure 9.4:5: Cleanup and Maintenance

3. Navigate to Size Cleanup Settings section and enable the toggle under Auto Disk Management to enable auto cleanup with max disk utilization by Media Server
4. If you want to customize the reserved free space in the disk, disable the Auto Disk Management toggle button and follow the mentioned steps:
   (a) Navigate to section below Minimum Free Space

(b) Select MB/GB/TB by clicking on the dropdown icon

(c) In the text field, enter or increase/decrease the value for minimum free space that should be reserved in the storage disk.



5. Click on **SAVE** button to save the changes.

9.5 Time Based Cleanup

Time Base cleanup is used for deleting the stored media files based on the desired retention period. These intervals can be configured according to the days/ hours of images needed. The media files get automatically deleted from the storage drive when the files are aged beyond the configured retention period.

The data stored in full and thumb folders gets deleted based on the configured retention period. For example, if the Time-Based cleanup setting duration is set to 10 Hours, images older than 10 hours will be cleared from the folder location on each cleanup cycle. Media Server will try to maintain images that are at least 10 hours old (given that images are not cleaned based on size-based cleanup)

Time based cleanup is not a primary cleanup mechanism and can be enabled/disabled using toggle buttons available next to the storage location of full-size or thumbnail image under Time Based Cleanup section of UI.

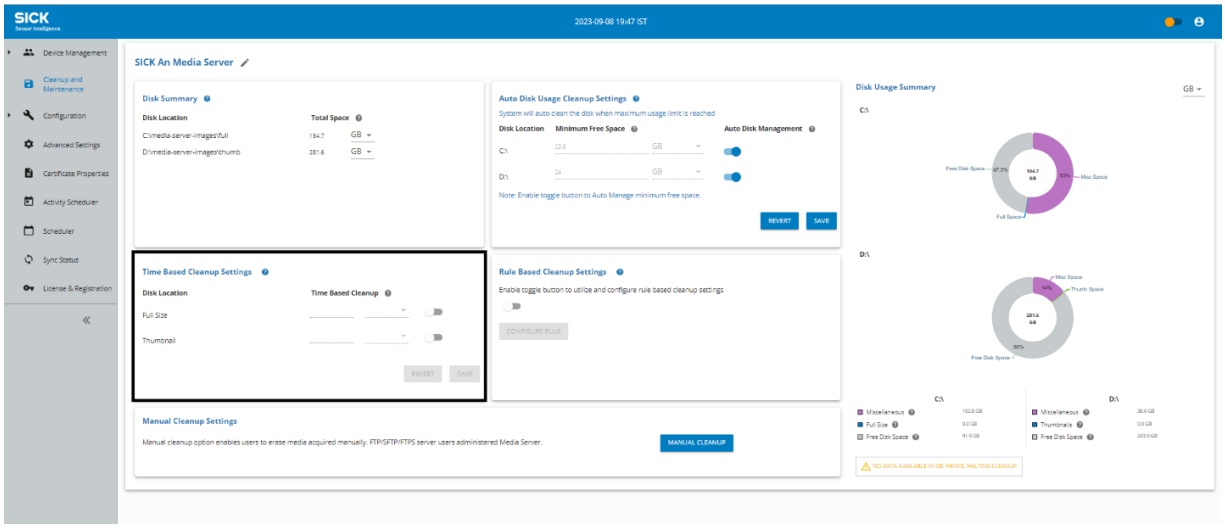
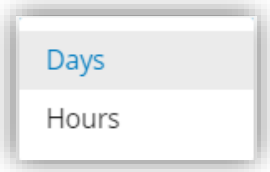


Figure 9.5:1: Time Based Cleanup

9.5.1 Set-up Time Based Clean-up

1. Launch and login to Media Server application.

2. Navigate to Cleanup and maintenance screen by clicking Cleanup and Maintenance option from the left navigation pane.
3. Navigate to Time Based Cleanup Settings section and enable the toggle button next to full size or thumbnail location.
4. Select Days or Hours option by clicking the dropdown icon for Full Size Files and Thumbnail.



5. In the text field, enter or increase/decrease the value for no. of days/hours, the file should be retained.

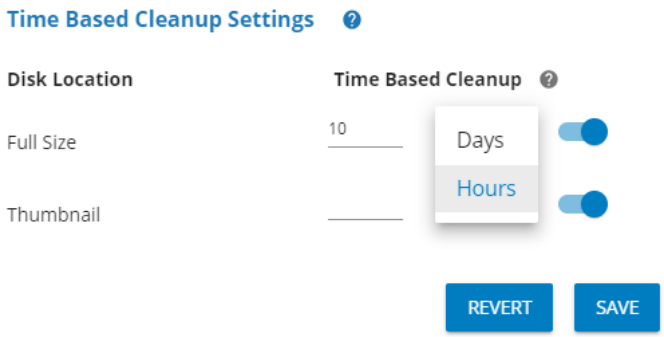


Figure 9.5:2: File Storage duration

6. After the changes are done, **SAVE** button is enabled.
7. Click on SAVE button to save the changes.
8.

9.6 Manual Cleanup

Manual cleanup clears all the media files from the storage drive based on the selected File type. This type of cleanup can be performed based on file type. This is the most efficient way to clear out media files from storage completely.

Caution: *Manual cleanup once started cannot be stopped. Please be very careful while using this functionality.*

9.6.1 Initiate Manual Cleanup

1. Launch and login to Media Server application.
2. Navigate to **Cleanup and maintenance** screen by clicking Cleanup and Maintenance option from the left navigation pane.
3. Click on **Manual Cleanup** button MANUAL CLEANUP

4. Pop-up window with **Full size** and **Thumbnails** option with checkboxes will appear.
5. When the **Full size** and **Thumbnails** options are selected then **Selective Clean** option checkbox appears respectively.

***Note**: Selective Cleanup is used to clean up a specific set of files for the selected time window. If the user selects only full size or thumbnail cleanup, then specific clean up starts when 'Clean' button is clicked.*

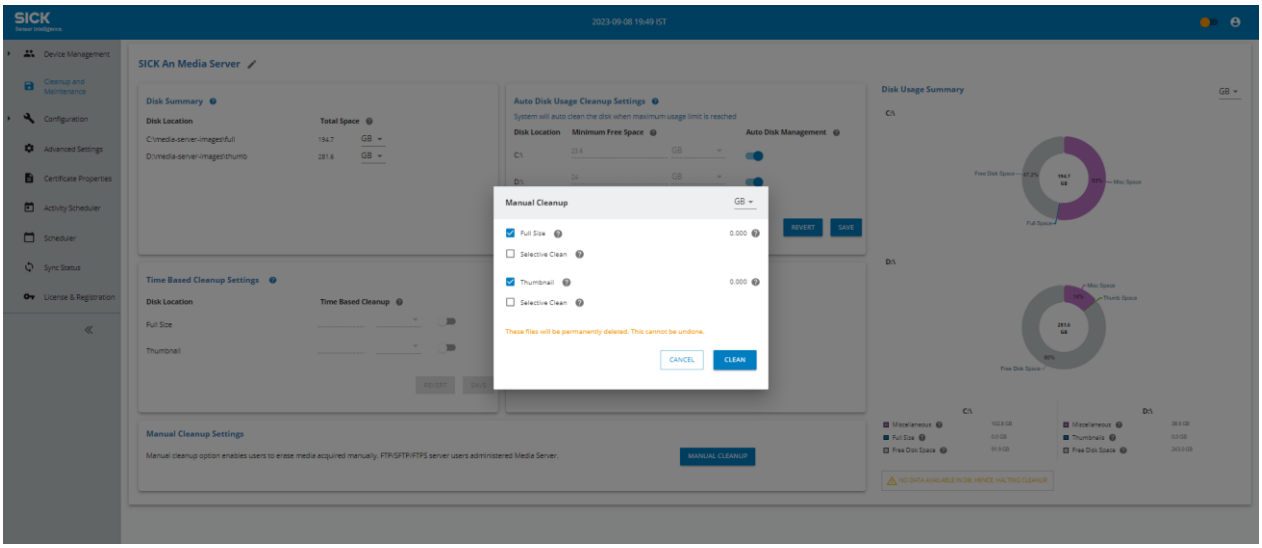
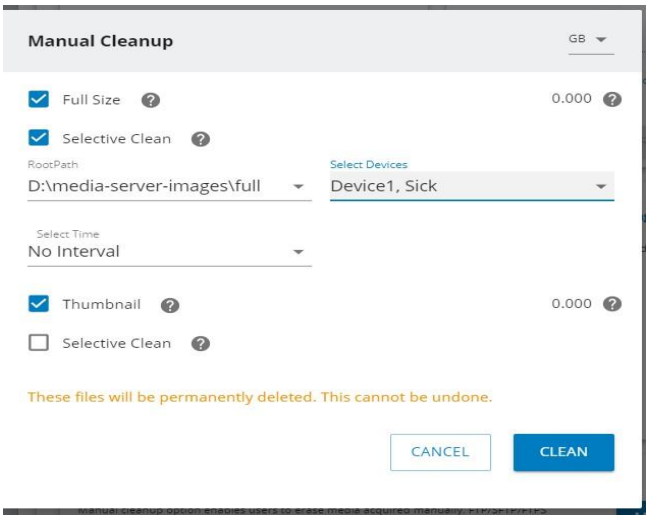


Figure 9.6:1: Manual Cleanup

6. Click the **Selective Clean** checkbox for which the Manual Cleanup needs to be done.
7. When the user clicks on **Selective Clean** checkbox, following fields appear:
   - **Root Path**: Select the root path of the file that contains the images to be cleaned from the drop-down.
   - **Select Devices**: Select the devices from the drop-down list.
   - **Select Time**: User can select from three options that are no interval, time interval and End Time for cleanup.

   i. When user selects **No interval**, it does not display any interval to select. It cleans all the images for selected root path and users

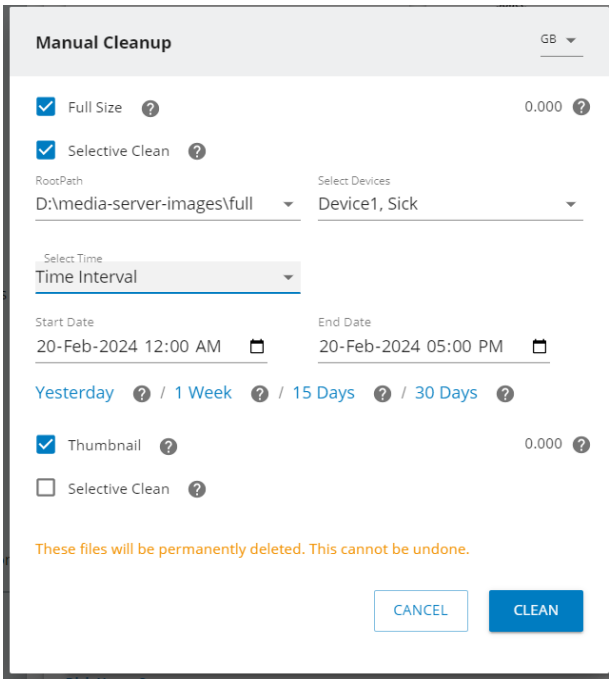


ii. When the user selects Time interval, the Start Date and End Date fields appear.
   - **Start Date:** Select the date and time when cleanup must begin.
   - **End Date:** Select the date and time when cleanup must stop.

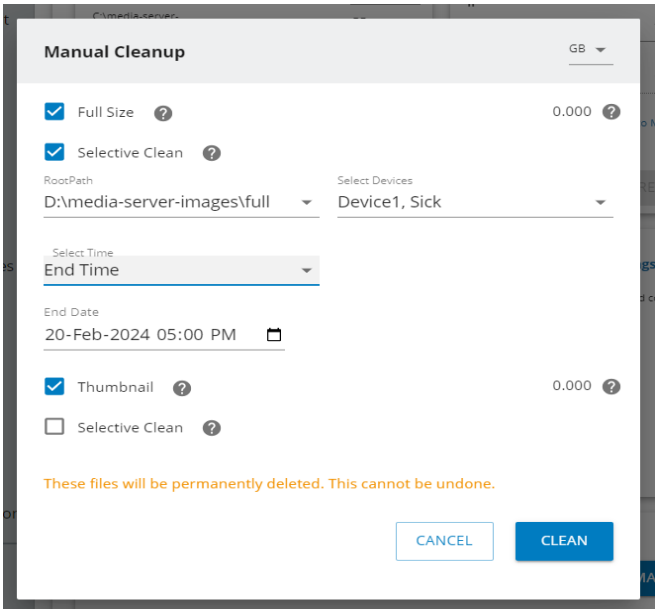
   Note: Images available for the selected device(s) and root path within the mentioned time interval will be cleaned.

   Note: *Images available for the selected device(s) and root path within the mentioned time interval will be cleaned.*

iii. When user selects **Time interval**, it displays to Start Date and End Date fields to select i.e., **Start Date**: Select the date and time when cleanup must begin and **End Date**: Select the date and time when cleanup must stop.



iv. When End Interval is selected then End Date field appears, select the end date and time when cleanup must stop. It deletes the media for the selected rootpath and devices till the send time selected



8. Click on '**Clean'** button.

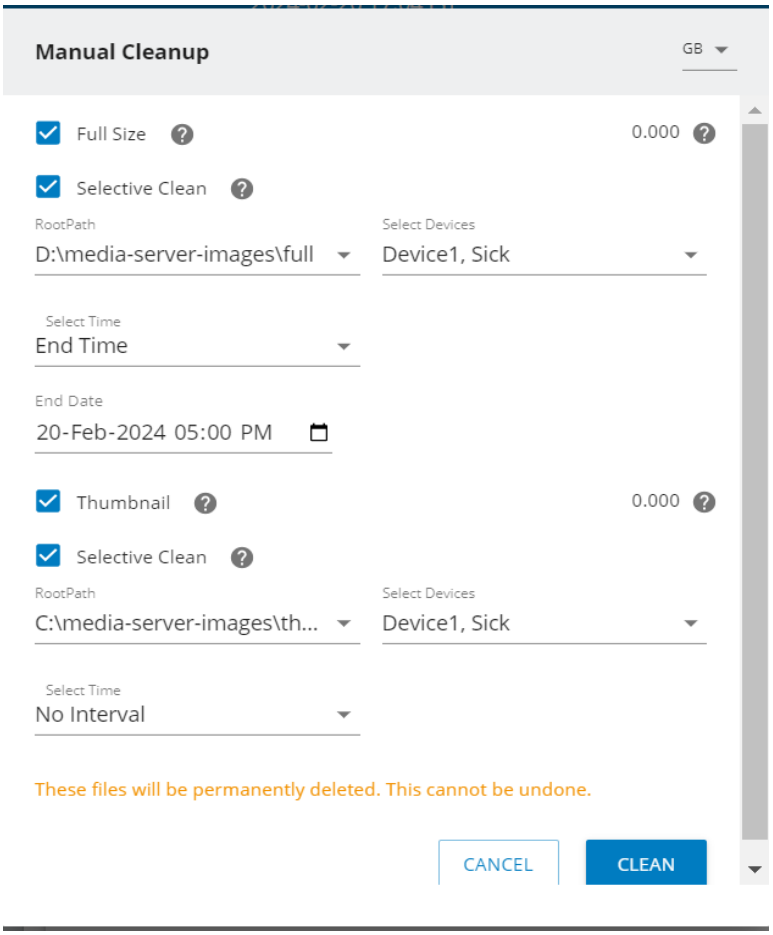


Figure 9.6:2: Selective Cleanup

9. Snack Bar messages ('Background process to purge selected files have started' and 'successfully validated the request, initiating manual cleanup process') will appear.
10. Manual cleanup will be processed in background. This will take time if lot of images are to be cleaned.

Note: *It is suggested to restart Media server after manual cleanup has been completed.*

9.7 Rule-Based Cleanup

Rule-based cleanup automatically removes media files based on predefined rules. Users can configure cleanup rules for specific devices or device groups to manage storage efficiently.

Note: *Rule-based cleanup is supported only in single-drive mode.*

- **Max Count**: Limits the total number of media files stored. When the limit is reached, the system deletes the oldest files.
    - **Example**: If set to 10,000 files for a single device, the system retains only the most recent 10,000 files, deleting older ones when new files are added.

For a device group, the 10,000-file limit is distributed across all devices in the group, with the allocation varying dynamically based on system logic (e.g., not necessarily 3,333 files per device for a group of three devices).

- **Max Space**: Limits the total allocated storage space. When the limit is exceeded, the system removes the oldest files.
    - **Example**: If set to 2 TB for a single device, the system ensures storage does not exceed 2 TB, deleting older files as needed. For a device group, the 2 TB limit is distributed across all devices in the group, with the allocation varying dynamically.

9.7.1 Configuring Rule-Based Cleanup

1. Open **Cleanup and Maintenance** from the left-side menu.
2. Click **Configure Rule** under **Rule-Based Cleanup Settings**.

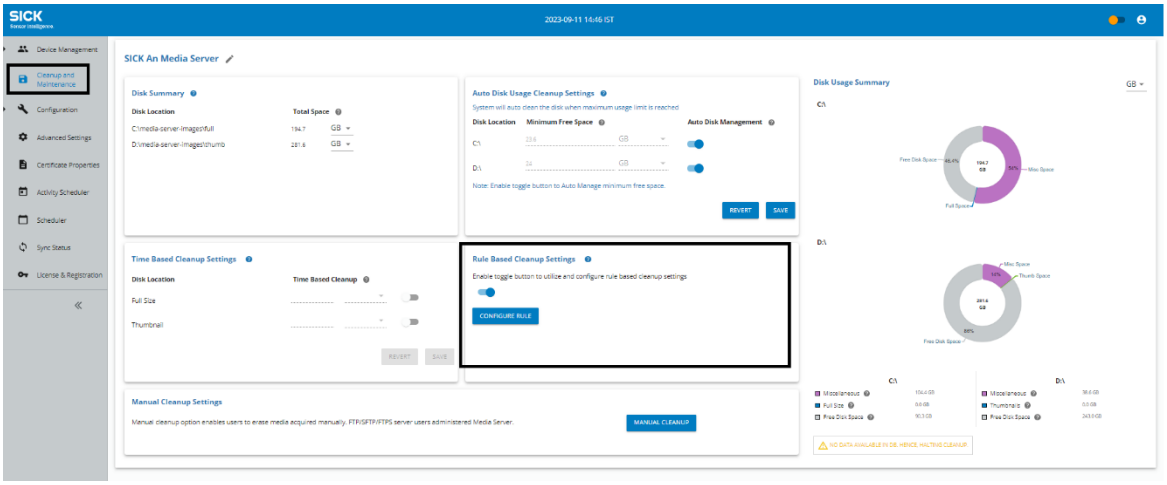


Figure 9.7:1: Rule-Based Cleanup Settings

3. Click **+ Add Rule** in the upper-right corner.

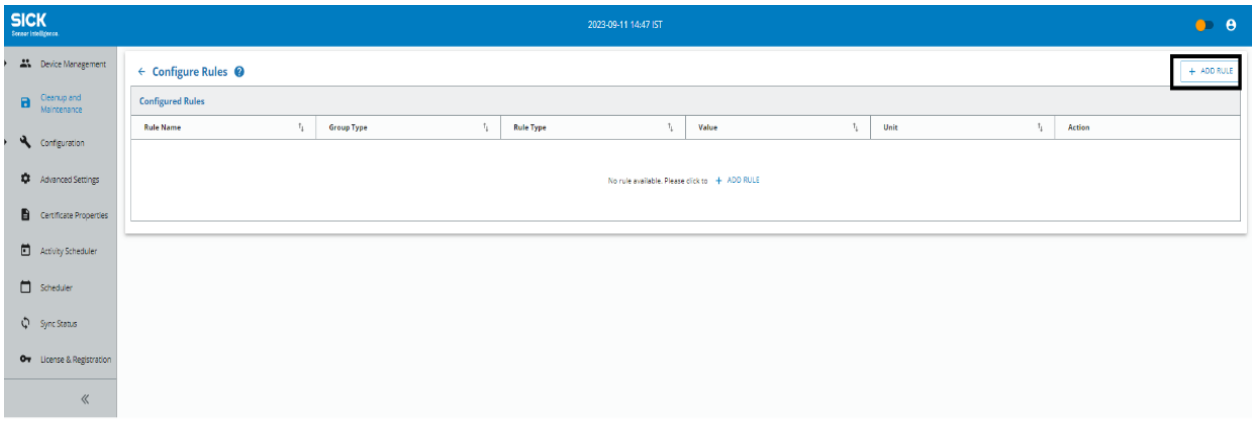


Figure 9.7:2: Add Rule

4. In the **Add Rule** dialog box, complete the following fields:
   - **Rule Name**: Enter a name for the rule.
   - **Device(s)**: Select one or more devices.
   - **Group(s)**: Select one or more device groups.
   - **Rule Type**: Select **Max Count** or **Max Space**.
   - **Value**: Enter the numeric limit.
   - **Unit**: If **Max Space** is selected, choose MB, GB, or TB.

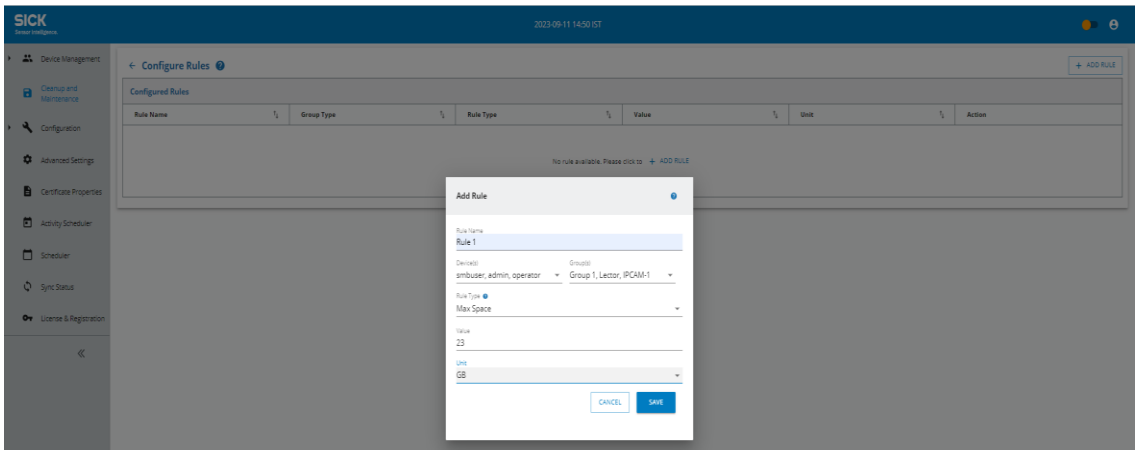


Figure 9.7:3: Add Rule Dialog Box

5. Click **Save**.

Note*: *Changing the **Minimum Free Space** setting may invalidate a **Max Space** rule. No warning is displayed if the configured rule exceeds available space.

6. The configured rule appears in the **Configure Rules** list.

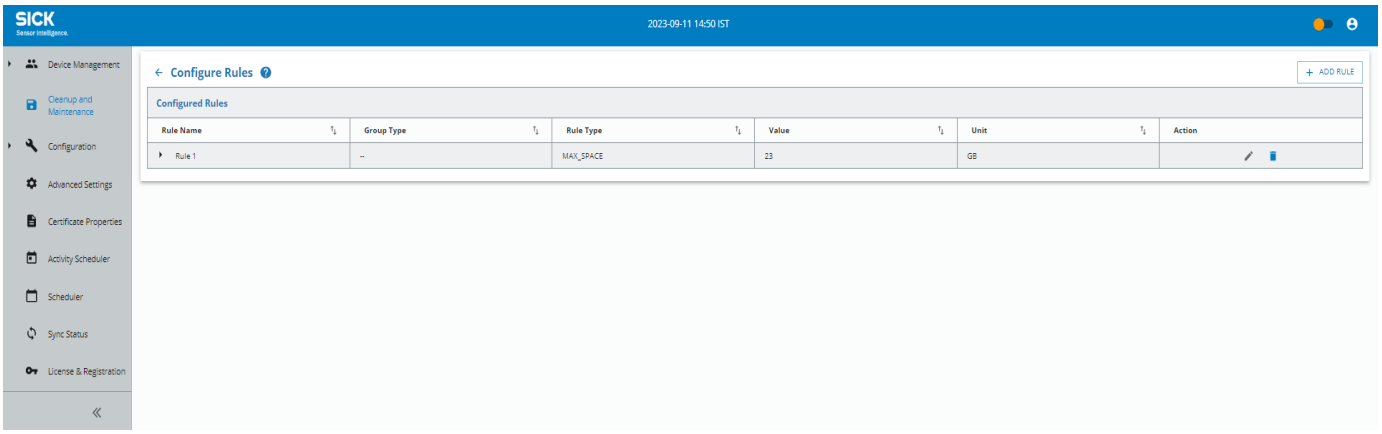


Figure 9.7:4: Configured Rule

9.7.2 Edit Rule

User can edit the configured rule by clicking on the edit icon.

1. When the user clicks on edit icon of the configured rule, **Edit Rule** dialog box appears with configured rules.

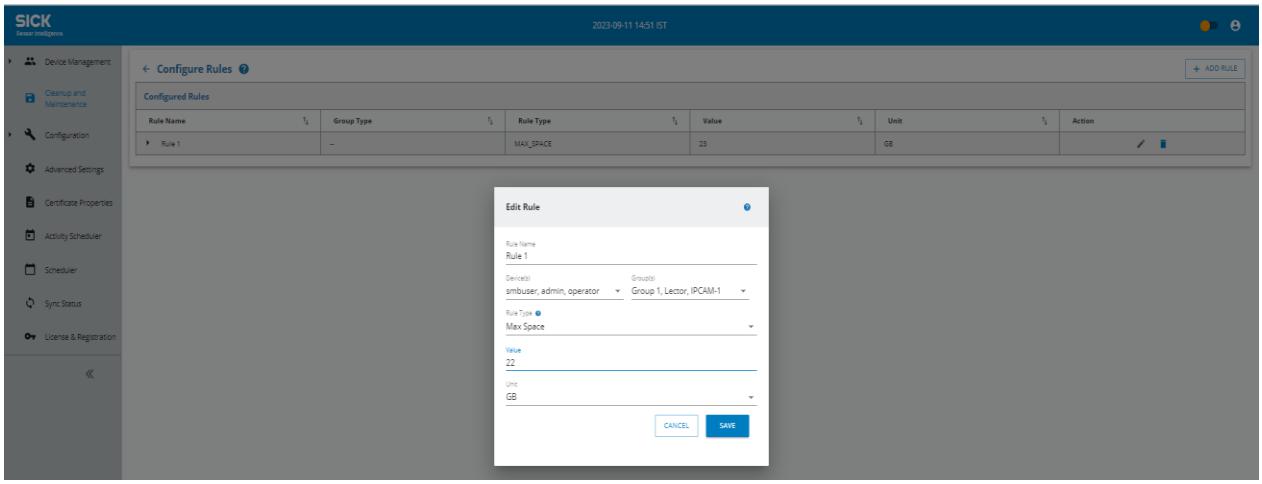


Figure 9.7:5: Edit Rule

2. User can update the changes and click on '**Save**' button.

9.7.3 Delete Rule

User can delete the configured rule by clicking on the delete ' ' icon.

1. When the user clicks on delete ' 'icon of the configured rule, **delete** confirmation dialog box appears with confirmation message '**Are you sure you want to delete this rule**?' with **Yes** and **No** buttons.
2. Click on '**Yes**' to confirm the deletion and '**No**' to cancel the deletion.

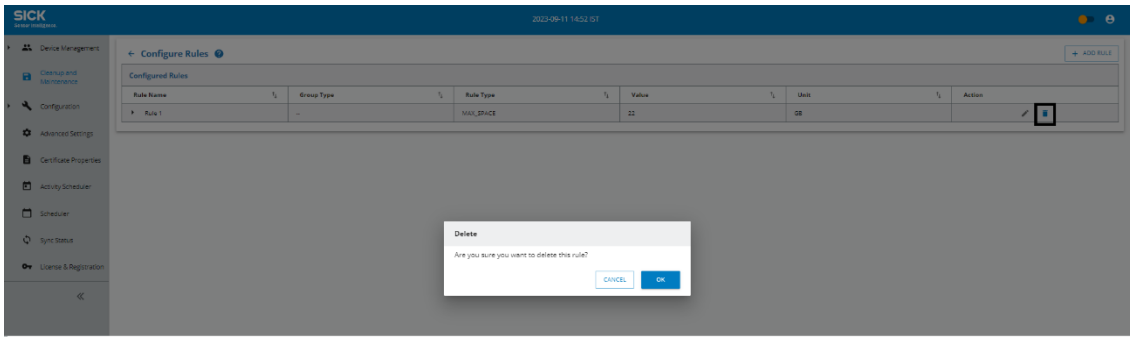


Figure 9.7:6: Delete Confirmation Box

9.8 Disk Usage Summary

Disk Usage Summary represents disk utilization in percentage for full size images, thumbnail images, miscellaneous data and available free space. The respective space utilization details of the above-mentioned fields (in MB/GB/TB) in the disk can be seen in tabular format below the disk indicator.

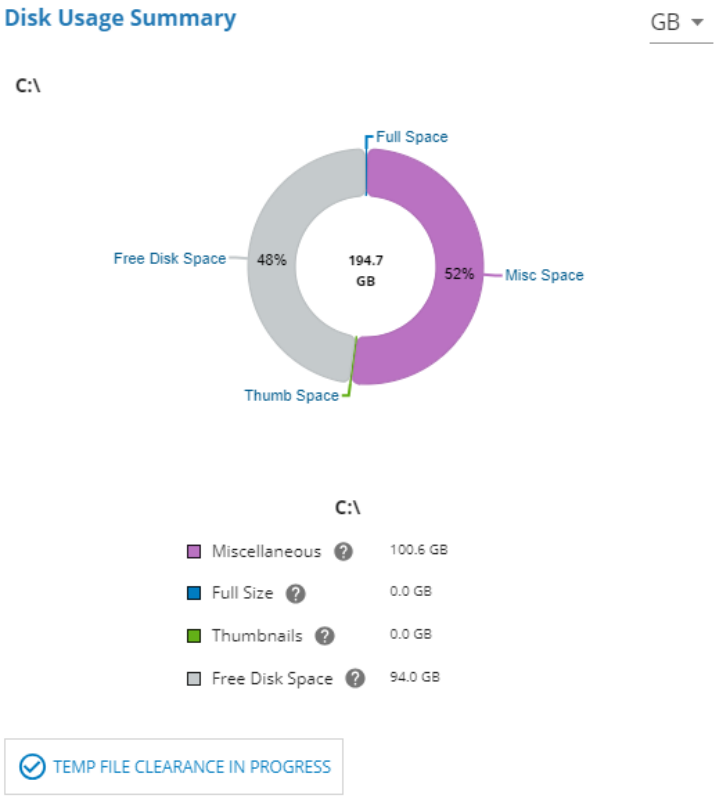


Figure 9.8:1: Disk Usage Summary

Indicator uses four colors to represent data of different file types.

Legend	Description
 Full Size	Blue indicator is used to display the disk space occupied by full size media
 Thumbnails	Green Indicator is used to display disk space occupied by thumbnail media
 Miscellaneous	Purple Indicator is used to display disk space occupied by the system applications and content that are not associated with Media Server
Free Disk Space	Grey Indicator is the total available space in the drive configured to store full size/thumbnail media

Table 8: Different Colors for Different Files

9.8.1 Disk Usage Display Modes

Disk Usage summary is displayed based on the storage location set for thumb and full location. If both full size and thumbnail storage locations are configured on the same drive, a single donut chart is displayed under Disk Usage Summary with details of full-size usage, thumbnail usage, miscellaneous usage and available free space within the drive.

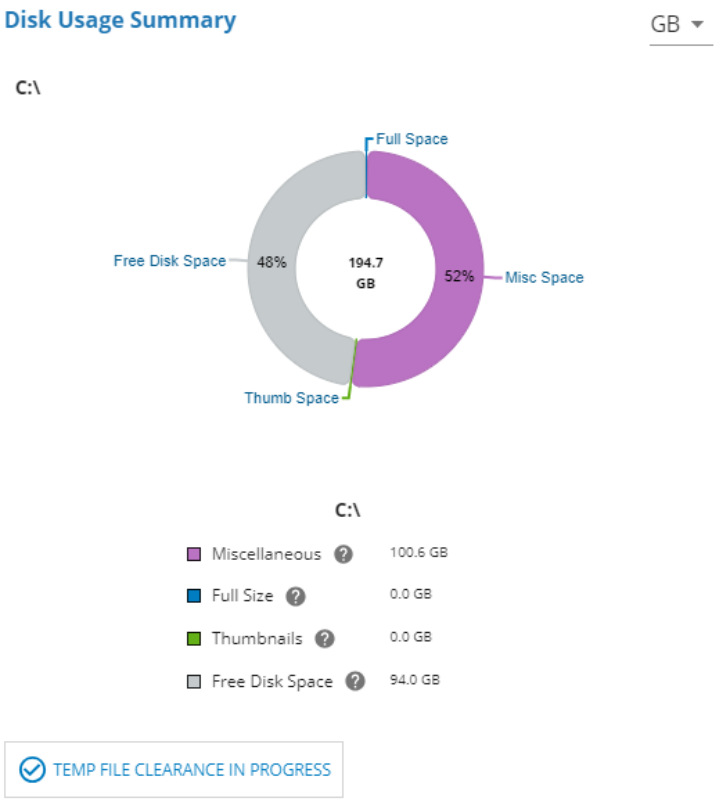


Figure 9.8:2: Disc Usage Summary

If full size and thumbnail storage locations are configured on different drives, two different donut charts are displayed under disk usage summary, one for each location, each doughnut representing the disk utilization with details of full-size usage/thumbnail usage, miscellaneous usage and available free space for each drive.

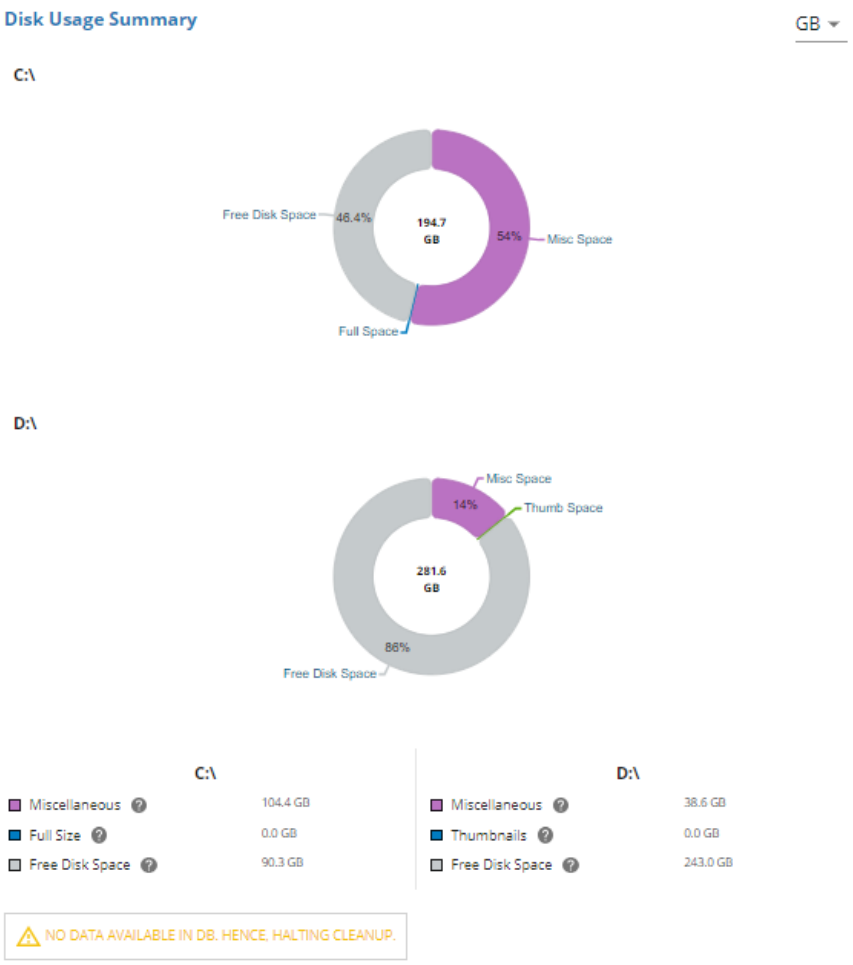


Figure 9.8:3: Two drive Disk Usage Summary mode

9.8.2 Cleanup Health Indicators

Cleanup health information is displayed in the form of messages below the disk indicator with the detailed information on cleanup activity that is happening in the background.

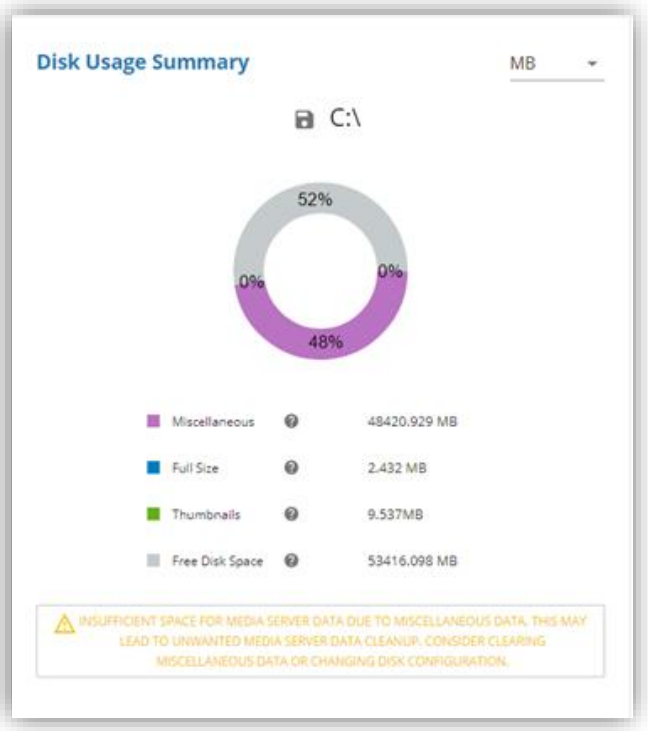


Figure 9.8:4: Warning message displayed in Yellow Font

Here is the list of messages that will appear and action (if required) that needs to be performed:

Note: *Message in* ***blue*** *are regular messages indicating normal operation of Media server. Messages in* ***orange*** *are warning messages and might require action to rectify them.*

Messages	Action required/ Background Activity
Cleanup health OK	No Operation/Normal operation of cleanup is happening in the background
Checking and Purging Empty/Unwanted Directories	When Media server is performing purge operation on empty/unwanted directories

Messages	Action required/ Background Activity
Cleaning full size records older than <timestamp>	When Age out based Cleanup for full-size images is in-progress
Cleaning thumbnail records older than <timestamp>	When Age out based Cleanup for thumbnail images is in-progress
Cleaning xml records	When xml files are being cleared out from MS
Cleaning xml records Aggressively	When xml files are being cleared out in aggressive cleanup Please refer to Appendix B for detailed information on aggressive cleanup
Regular size out cleanup in progress as buffer space being used for Single drive.	When regular Size based cleanup is happening, and thumbnail and full-size images are configured to be saved in same drive Please refer to Appendix B for detailed information on this type of cleanup
Regular size out cleanup in progress as buffer space being used for Full drive.	When regular Size based cleanup is happening for images stored in full-size drive, given that thumbnail and full

Messages	Action required/ Background Activity
	images are being stored in different drive Please refer to Appendix B for detailed information on this type of cleanup
Regular size-out cleanup is in progress as buffer space is being used for the thumb drive.	When regular Size based cleanup is happening for images stored in thumb drive, given that thumbnail and full images are being stored in different drive Please refer to Appendix B for detailed information on this type of cleanup Regular size-based cleanup is in progress for images stored in the thumb drive, considering that thumbnail and full-size images are stored in separate drives. See Appendix B for more details on this type of cleanup.
Gathering Disk information	The Media Server reads through the database to correct its full-size and thumbnail details in cache or when updating its database. Cleanup is halted during this interval and will resume once recalculation is complete.

Messages	Action required/ Background Activity
Data Migration in progress. Cleanup halted.	Regular Cleanup activity will be halted if Data migration is in progress
Inventory in progress. Cleanup halted.	Inventorying is a process to re-build database where it re-trieves Image data from File Location and store its details in. When inventorying process is happening in the background. Cleanup is halted during this interval and will resume once the inventorying has been completed
Inventory will be halted. Aggressive Cleanup resumed	When inventorying has been completed, aggressive cleanup is resumed
Active DB/connection: MySQL is down. Cleanup halted	If MySQL is set as database, and MySQL service is non-re-sponsive. Cleanup is halted un-til MySQL DB is back online. **Action:** Check MySQL instance by launch the services form search Module in the machine and bring back MySQL server online by starting MySQL ser-vice
Miscellaneous data Occupying/Occu-pied reserved disk space. Data acquisi-tion by Media Server might be	If the miscellaneous data in the drive saving both full size and thumbnail images is occupying

Messages	Action required/ Background Activity
hampered. Please consider changing disk configuration.	more space than the minimum free space set for cleanup. **Action:** Cleaning up miscellaneous data or switch to a drive with more disk space.
Miscellaneous data Occupying/Occupied reserved space on full size disk. Data acquisition by Media Server might be hampered. Please consider changing disk configuration.	If the miscellaneous data of the drive saving full size images is more than the minimum free space set for cleanup. **Action:** Cleanup miscellaneous data or switch to a drive with more disk space
Miscellaneous data Occupying/Occupied reserved space on thumbnail disk. Data acquisition by Media Server might be hampered. Please consider changing disk configuration.	If the miscellaneous data of the drive saving thumbnail images is more than the minimum free space set for cleanup. **Action:** Cleanup miscellaneous data or switch to a drive with more disk space
Maximum aggressive size out Cleanup in Progress as Disk used space reached minimum free space	High acquisition throughput causing Maximum aggressive Size based cleanup for disk space maintenance. This process will start deleting a lot of images from drive storing both full size and thumbnail images **(Maximum aggressive Cleanup).** Please refer to Appendix B for detailed information on this type of cleanup

Messages	Action required/ Background Activity
Maximum aggressive size out Cleanup in Progress as full-size Disk used space reached minimum free space	High acquisition throughput causing Maximum aggressive Size based cleanup for disk space maintenance. This process will start deleting a lot of images from drive storing full size images **(Maximum aggressive Cleanup).** Please refer to Appendix B for detailed information on this type of cleanup
Maximum aggressive size out Cleanup in Progress as thumbnail Disk used space reached minimum free space	High acquisition throughput causing Maximum aggressive Size Based cleanup for disk space maintenance. This process will start deleting a lot of images from drive storing thumbnail images **(Maximum aggressive Cleanup).** Please refer to Appendix B for detailed information on this type of cleanup
Aggressive size out Cleanup in Progress as Disk used space reached additional buffer space.	High acquisition throughput causing normal maintenance of disk space. This will delete data from drive storing both full size and thumbnail images **(Aggressive Cleanup).** Please refer to Appendix B for detailed information on this type of cleanup

Messages	Action required/ Background Activity
Aggressive size out Cleanup in Progress as full-size Disk used space reached additional buffer space.	High acquisition throughput causing normal maintenance of disk space. This will delete data from drive storing full size images **(Aggressive Cleanup).** Please refer to Appendix B for detailed information on this type of cleanup
Aggressive size out Cleanup in Progress as thumbnail Disk used space reached additional buffer space.	High acquisition throughput causing normal maintenance of disk space. This will delete data from drive storing thumbnail images **(Aggressive Cleanup).** Please refer to Appendix B for detailed information on this type of cleanup
Insufficient space on disk for proper functioning of cleanup. Maximum Aggressive cleanup will be performed once disk usage reaches minimum free space. Consider changing the disk configuration.	The configured disk to acquire both full size and thumbnail image does not have enough space available to store images properly and maintain disk space. This will cause all the images available to be cleaned up on regular interval. **Action:** Switch to a drive with more disk space
Insufficient space on full size disk for proper functioning of cleanup. Maximum Aggressive cleanup will be performed once disk usage reaches minimum free space. Consider changing the disk configuration.	The configured disk to acquire full size image does not have enough space available to store images properly and maintain disk space. This will

Messages	Action required/ Background Activity
	cause complete image cleanup on regular interval. **Action:** Switch to a drive with more disk space
Insufficient space on thumbnail disk for proper functioning of cleanup. Maximum Aggressive cleanup will be performed once disk usage reaches minimum free space. Consider changing the disk configuration.	The configured disk to acquire thumbnail image does not have enough space available to store images properly and maintain disk space. This will cause complete image cleanup on regular interval. **Action:** Switch to a drive with more disk space
Insufficient space for Media server data due to Miscellaneous data. This may lead to unwanted media server data cleanup. Consider clearing miscellaneous data or changing disk configuration.	The configured disk to acquire both full size and thumbnail images does not have enough space available to store images properly and maintain disk space, as the miscellaneous data has grown over the time. **Action:** Cleanup miscellaneous data.
Insufficient space for Media server full size data due to Miscellaneous data. This may lead to unwanted media server data cleanup. Consider clearing miscellaneous data or changing disk configuration.	The configured disk to acquire full size images does not have enough space available to store images properly and maintain disk space as the miscellaneous data has grown over the time. **Action:** Cleanup miscellaneous data.

Messages	Action required/ Background Activity
Insufficient space for Media server thumbnail data due to Miscellaneous data. This may lead to unwanted media server data cleanup. Consider clearing miscellaneous data or changing disk configuration.	The configured disk to acquire thumbnail images does not have enough space available to store images properly and maintain disk space as the miscellaneous data has grown over the time. **Action:** Cleanup miscellaneous data.
No Data available in DB. Hence, Halting Cleanup.	If the DB is empty, cleanup operation will be halted. Once Data is acquired by Media server, the cleanup process will resume
Data not being stored as minimum free limit reached. No Data available in DB. Hence, Halting Cleanup.	When Minimum free space is reached and there is no data available in the DB. **Action**: Clear out space in the drive or change the drive for new data to be stored.
Max Aggressive cleanup going on. File size will be rectified after the cleanup.	On Starting Media server, if the first recalculation does not complete due to Maximum aggressive cleanup. Once Maximum aggressive cleanup is complete, the recalculation will resume and set the correct File size.

Messages	Action required/ Background Activity
Configuration File Drive low on disk space. Can't save any changes to file. Clear space to save changes to file.	If the space of the Drive/s in which the files;sick-bip-is.cfg, ScheduleConfig.cfg and Clean-upRuleConfig.cfg are present, is less than 500 MB, changes will not be saved to the files. To start saving the space must be more than 500MB. **Action:** Do Not configure the Media storage drive and DB Drive to be same as these files and clear out unwanted data from the drive.
Data Drive has reached Minimum Free Space.	If the configuration files (Files mentioned in the above sce-nario) drive is the same as the data drive, this message will be displayed along with the above message
Media Server is working on rectifying the Miscellaneous Data size	If the Miscellaneous Data size is not displayed properly, it will be rectified in a subsequent Recalculation cycle. This is dis-played when Media server has single drive for both full and thumb data.
Media Server is working on rectifying the Miscellaneous Data size for both drives.	If the Miscellaneous Data size is not displayed properly, it will be rectified in a subsequent Recalculation cycle. This is dis-played when Media server has two separate drives for full and

Messages	Action required/ Background Activity
	thumb data and the error happens on both the drives
Media Server is working on rectifying the Miscellaneous Data size for full drive.	If the Miscellaneous Data size is not displayed properly, it will be rectified in a subsequent Recalculation cycle. This is displayed when Media server has two separate drives for full and thumb data and the error happens only for full drive.
Media Server is working on rectifying the Miscellaneous Data size for thumb drive.	If the Miscellaneous Data size is not displayed properly, it will be rectified in a subsequent Recalculation cycle. This is displayed when Media server has two separate drives for full and thumb data and the error happens only for thumb drive.
Cleanup waiting for DB Maintenance thread to be up.	Cleanup is Halted until the Maintenance DB thread has started.
Tagged Deletion Started.	Deletion of data marked to be deleted by tagging feature starts.
Tagged Files deleted.	Deletion of data marked to be deleted by tagging feature Finishes.

Messages	Action required/ Background Activity
Device: <device Name> Cleaning xml records	When xml files are being cleared out from MS for a particular device
Device: <device Name> Cleaning xml records Aggressively	When xml files are being cleared out in aggressive cleanup for a particular device
Aggressive Xml records deletion Completed	When aggressive xml deletion is complete
Device: <device Name> Aggressive Xml records deletion Completed	When aggressive xml deletion is complete for a particular device
Xml records deletion Completed	When xml deletion is complete
Cleaning Synced records	When Synced records are being deleted
Synced Files deleted.	When Synced deletion is complete
Miscellaneous data Occupying/Occupied reserved disk space for rules. Rules may not be able to utilize the max space allocated to it. Please consider changing rule configuration.	When Miscellaneous data occupies the space allocated for a device/group by a rule. **Action**: Change the rule configuration or clear out unwanted data to reduce miscellaneous space utilization

Messages	Action required/ Background Activity
Rule allocations exceeds the maximum limit. Current Available Disk Space (Total Disk Space - Minimum Free Space): <usable space> Current Total Allocation: <Total allocated space> Please consider changing rule configuration.	When the allocated space by a rule is more than the disk available space. **Action:** Change the rule configuration.
Both Full and Thumb path changed. Wait for next cleanup cycle	When both the full and thumb paths are changed during a cleanup cycle. The current cleanup cycle is terminated, and cleanup will resume in the next cycle.
Thumb path changed. Wait for next cleanup cycle	When both the thumb path is changed during a cleanup cycle. The current cleanup cycle is terminated, and cleanup will resume in the next cycle.
Full path changed. Wait for next cleanup cycle	When both the full path is changed during a cleanup cycle. The current cleanup cycle is terminated, and cleanup will resume in the next cycle.
Active DB:<DB type> Modification in progress.	Halted Cleanup When DB columns are being modified (which happens at the start of the media server). Cleanup is halted during this modification.
Active DB:<DB type> modification complete.	Cleanup resumed. Once above-mentioned operation is complete

Messages	Action required/ Background Activity
File size recalculation in progress. Cleanup halted.	When Recalculation is in progress.
Manual Cleanup in progress. Regular cleanup cycle halted	When Manual cleanup is initiated
Tag Details Table being cleared.	Tag details table records are being cleared after records from file index table are deleted.
Checking and Removing Purged records from DB	When removing records of Purged data from DB.
Drive: <drive mode> <device/group> Started count based cleanup	Count based cleanup for a given device or group
Drive: <drive mode> <device/group> Rulebased Regular size out cleanup in progress as buffer space being used by the device/group	Rule based size out cleanup in progress for a device or group
Drive: <drive mode> <device/group> Rule based Maximum aggressive cleanup in progress as device/group completely utilized the space allocated	Rule Based maximum aggressive cleanup for a device or group when device/group utilizes allocated space by the rule.
Partition limit reached for MySQL. Purging old data and dropping respective partition	MySQL has a 340-day data retention limit due to subpartitions. This message appears when purging data as it reaches day 339.

Messages	Action required/ Background Activity
No Data for Current Full/Thumb drive available. However, Unwanted tagdetails Cleanup in progress.	No data in Full/Thumb tables, but unwanted data still exists in tagdetails table, so cleanup continues.
No Data for Current Full/Thumb drive available. However, Continue with Unmigrated Data Cleanup.	No data in Full/Thumb tables, but unmigrated data in the old structure is being cleaned up.
System is running low on memory. Total available RAM:	The system has low available physical memory (RAM), which might impact cleanup or media server operation.
Cleanup cycle Started	Indicates the start of the regular cleanup cycle.
Unmigrated Data Cleanup in progress.	Indicates cleanup of old data structures post migration.
Temp file Clearance in progress	Temporary files (e.g., from IP-Cams) are being cleared from the /tmp directory.

Figure 9.8:5: List of Messages in Application

10 Configuration

This Section provides high level information of licensed protocols in media server such as binding IPs for FTP/FTPS/SFTP servers, configured FTP/FTPS/SFTP port/s used to store media files. Also allows user to Enable/Disable transfer protocols using checkboxes.

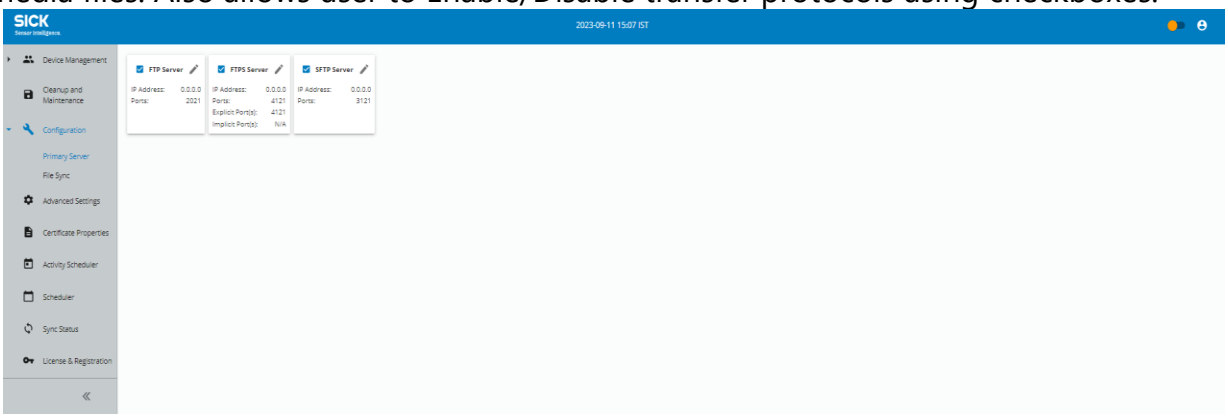


Figure 9.8:1: Configuration

This configuration will appear as below when certificates are offline, invalid, or expired. Secure protocols such as SFTP, FTPS, and FileSync will display a warning icon in this case. These protocols will not function unless a valid certificate is present. File Sync is disabled due to a certificate error. Please rectify the issue to continue**.**

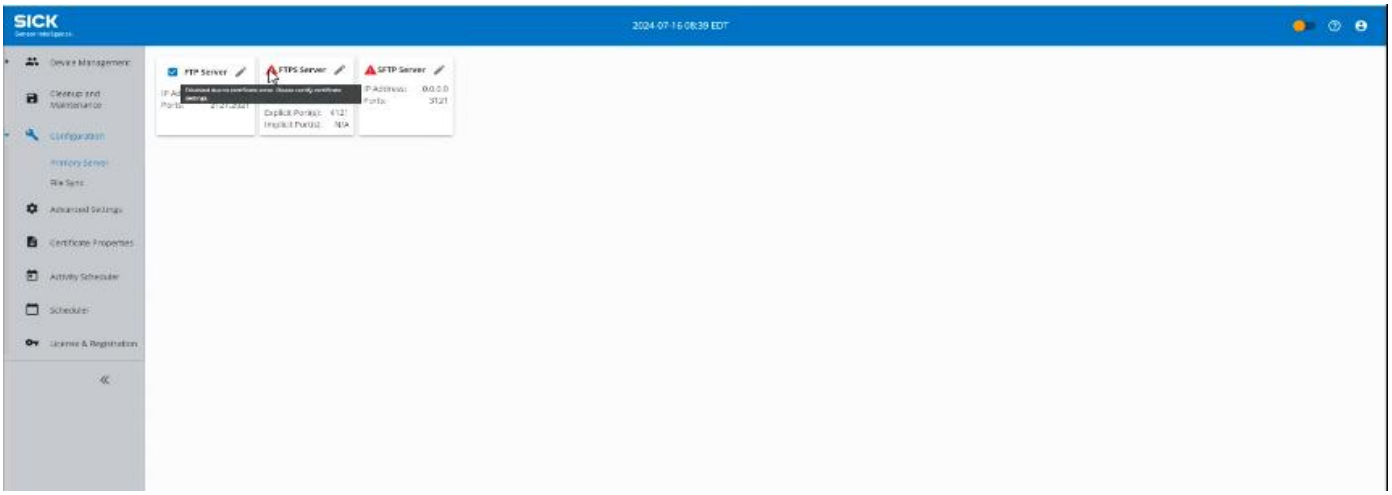


Figure 9.8:2: Primary Server

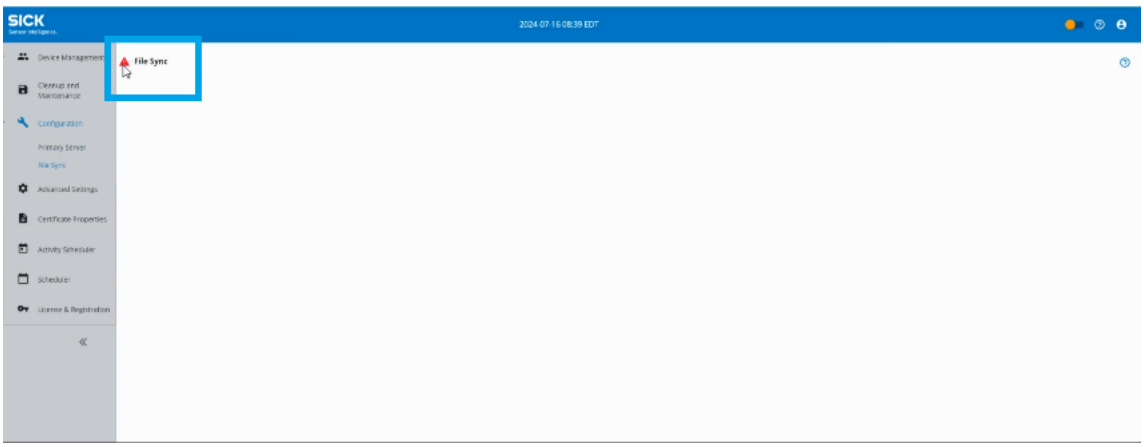


Figure 9.8: File Sync

10.1 Enable/Disable Protocols

You can enable/disable the licensed protocol by selecting/deselecting the checkboxes.

or by modifying the configuration file (**sick-bip-is.cfg**). Starting with **Media Server 1.6**, unsecured protocols (HTTP, FTP) can be disabled without requiring a new license, enhancing security and flexibility.

- **FTP**: Uncheck the FTP checkbox in the Device Management UI to disable. This change takes effect immediately.
- **HTTP**: Set **enabled=false** in the **[HTTPD]** section of **sick-bip-is.cfg** and restart the **Media Server**.
- **HTTPS:** Set enabled=false in the **[HTTPSD]** section of sick-bip-is.cfg and restart the Media Server.
- **FTPS, SFTP**: Enable or disable via UI checkboxes or configuration settings, depending on the license and device setup.

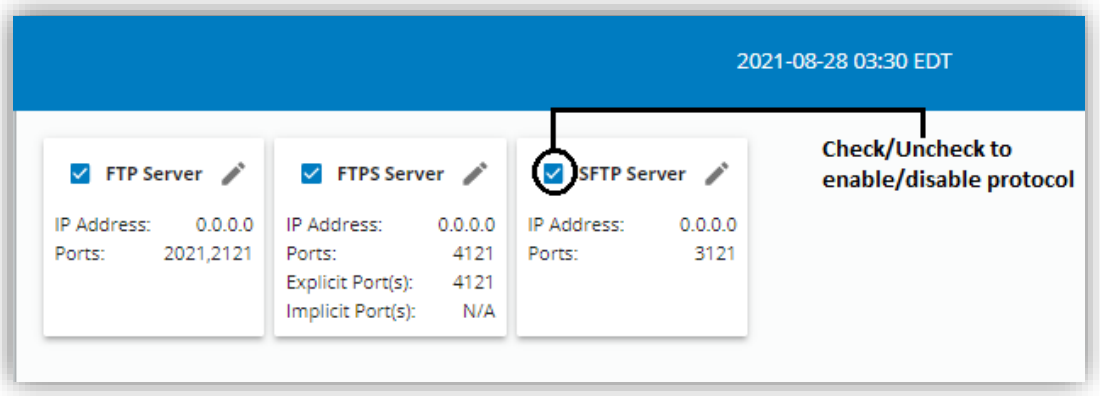


Figure 10.1:1: Enable/Disable Protocol Server Window

Note:

- *A protocol is only visible if licensed.*
- ***FTP** and **HTTP** are unsecured protocols. It is recommended to use their secure alternatives, **FTPS** and **HTTPS**, for encrypted communication. For further assistance, contact the support team at https://supportportal.sick.com/.*
- *Starting with **Media Server 1.6**, HTTP and FTP can be disabled without a new license, unlike previous versions where a new license was required.*

Important:

- Changes to **HTTP** protocol settings using the UI can be performed only when the Media Server is accessed over **HTTPS**. If accessed over HTTP, this option cannot be modified.
- When HTTP is disabled, ensure that HTTPS is properly configured and accessible to avoid loss of access to the Media Server UI.

Application displays a snack bar message if the selected protocol server is enabled/disabled successfully.
If there is an error while enabling the protocol, an **alert** message will be displayed.

***Note:** On start of media server, FTPS server will run with implicit and explicit mode both. The Port assignment will be based on formula Round off-to-floor i.e., number of ports divided by 2 goes to EXPLICIT mode, rest goes to IMPLICIT. Example:*

FTPS Port Configuration	EXPLICIT	IMPLICIT
4121	4121	NA
4121, 4020	4121	4020
4121, 4020, 4343	4121	4020, 4343
4121, 4020, 4343, 4545	4121, 4020	4343, 4545

Table 9: FTPS Port Configuration

If the following ports are configured: 4121,4020,4343,4545; and 4020 is invalid (due to port range or conflicting port) and FTPS server does not start in this port, then 4121 will start as Explicit and 4343, 4545 will start as implicit.

In case the ports are changed later from "4121,4020,4343" to "4121,4020,4343,4545" then 4020 which was previously running as implicit will now be explicit after change.

10.2 Edit Protocols Server

Click on the edit icon next to the server. You can update the IP Address and Ports from Edit <<Servername>> Server window. The ports selected can only be within the port range defined for a protocol. Use this window to bind the local IP to the server and configure the ports where the server (FTP/FTPS/SFTP) should run.

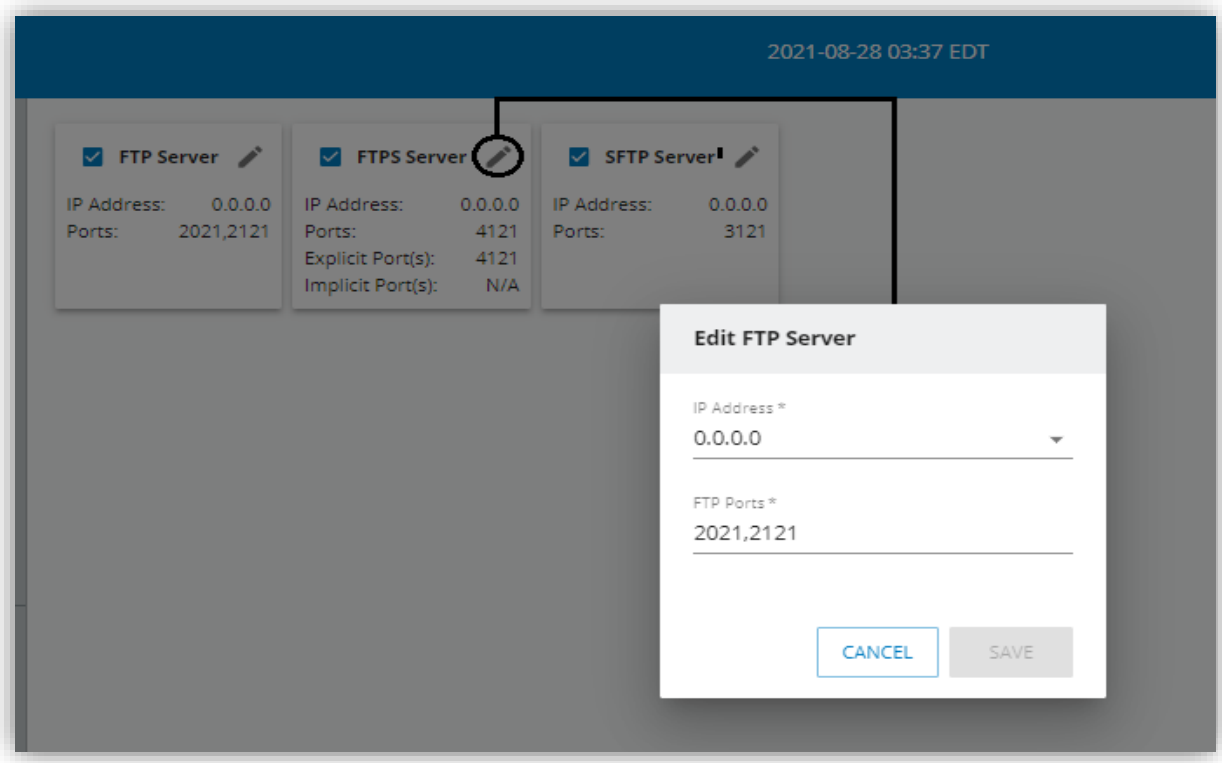


Figure 10.2:1: Edit Protocol Server Window

Note: *Ports of a protocol should not conflict with ports used by any other protocol. Example: FTP port(s) should not conflict with HTTP/HTTPS/SFTP/FTPS/UDS port(s)/File Sync. Ports already used by other system activities are not allowed to be added.*

To run multiple FTP/SFTP/FTPS servers, use comma separated port numbers. For example, to run multiple FTP Servers on the same IP address configure the port number as 2021, 2121.

10.3 File Sync

File sync helps in archival of media files to the remote server. This feature is useful in situations where the Media server connected to image capturing devices has limited/low disc space. Disc maintenance of Media server cleans the acquired files to overcome disk overflow. As the connected media server is low on disc space, the acquired image is

likely to be clean up quickly. To retain these files for a longer duration, we can sync/archive these acquired files in a Media server with bigger storage.
File sync synchronizes the files between two media servers. File Sync (FS) service comprises of two components, namely FS server and FS device. File Sync (FS) server acquires images sent from FS device. File archival interval/duration is controlled by the schedules assigned to the File Sync activity which can be extracted from downtime (Shift Data) published by the connected analytics product or customized as per user preference. Refer to Scheduler.
The incoming files that are getting stored in the Full Folder (the storage folder for Full size images) of the media server is saved in same folder structure of the remote Media Server post archival. Similarly, the incoming files that are getting stored in the Thumb Folder (the storage folder for Thumbnail images) of the media server will be synced-up with the Thumb Folder of the remote media server. Files are archived in the same folder structure as its source. Example: If Image 01_20230203_211104_000001.jpg is available in location <<root location>>/TOP/2023/02/03/21 folder, after archival it will be available in same location in the Sync Server.
If the user requested file is not available in the connected media server, it finds the requested file in the backup server (Note this will only happen if the file sync is properly configured). File sync feature also gives access to the archived media in sync server. Therefore, any media requested will be searched in both server/client before showing error.

> ***Note:*** *The sub-folders name within the Full and Thumb folder depends upon the day and hour of the file received. Analytics solution run on shift management basis and there is an interval between these shifts which is known as Downtime.*

10.3.1 File Sync Mode

- Server
- Client
- Server and Client

Server: When the user checks the '**File Sync'** checkbox and selects the **'Server'** radio button, file sync starts in this mode in the Media Server. Media Server with this mode can archive media received from Media Server configured as Client. It does not display anything when Server radio button is selected, as there is nothing to configure on the UI for file sync server.

Note: *Server related information is pre-configured in sick-bip-is.cfg.*

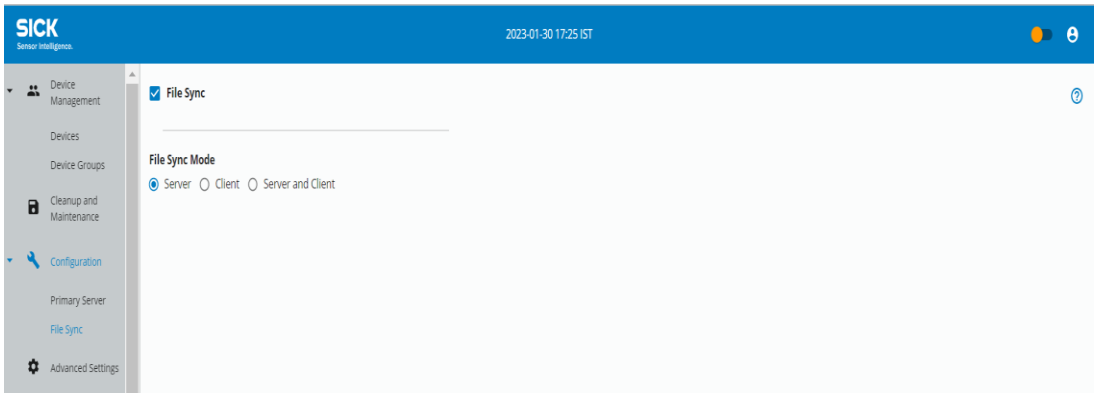


Figure 10.3:1: Server File Sync Mode

Note: *Files are archived from client to the server in File Sync mode.*

Client: Media server selected as client can archive its files to the media server selected as Server. To select the Client mode, check the '**File Sync'** checkbox then file sync mode options appear. Select **'Client'** radio button then following fields appear:

- **Server Address**: IP address of the Media Server running in File Sync server mode. This field is empty by default.
- **Ports:** Port where file sync server is running. Default port is 2020.
- **Username:** Authentication username (Default: sick)
- **Password:** Authentication password
- **Set Bandwidth:** (Custom/Max available) Choose custom to restrict the archival speed. Choose Max available to utilize max archival speed.
- **Bandwidth value**: Provide the bandwidth value.
- **Bandwidth Unit:** Provide the bandwidth unit from the drop-down which has units like image per minute/per second/mbps/kbps.

Note: *If user selects the Bandwidth Unit as 'kbps' / 'image per minute' then it does not display correctly in sync status plot chart as limitation of plotter chart is that it does not support these units hence it will show other values within the drop down on sync status. Thus, it is preferred that user select image per second / mbps.*

- **Test button:** It is used to test the connection with the target Sync server and verify the correct network before saving the details.
- **Save button**: It saves the client details for file archival. This button is enabled after testing is done.

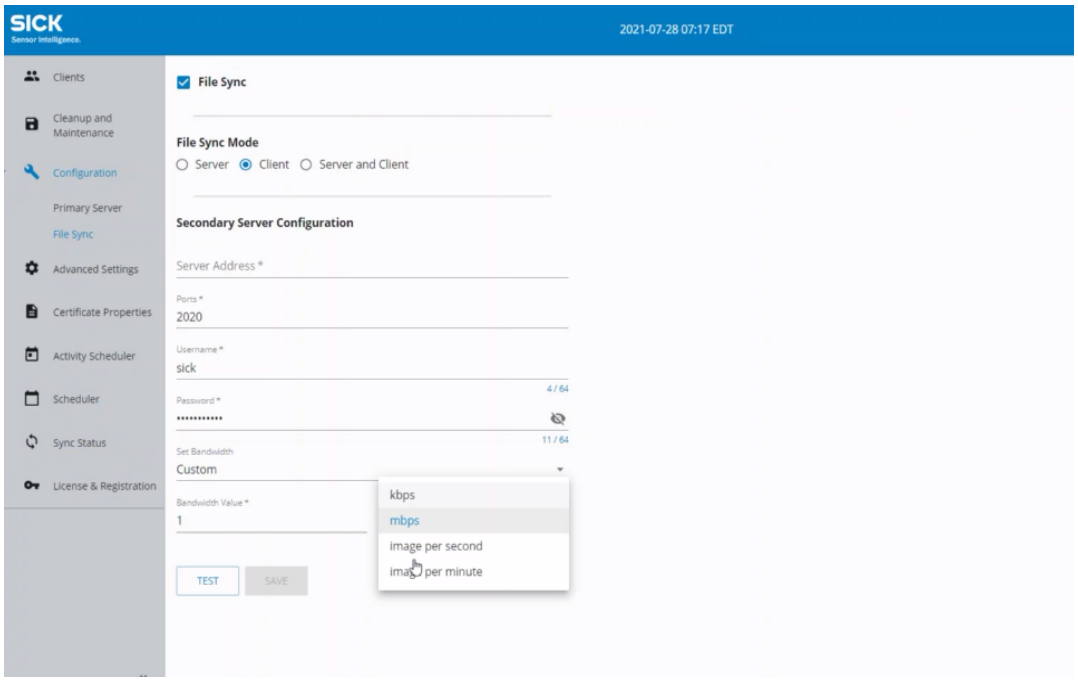


Figure 10.3:2: Client File Sync Configuration

Server and Client: When Server and client is selected, it runs as both file sync server and client. To configure this mode, check the '**File Sync'** checkbox then file sync mode options appear. Select '**Server and Client'** radio button then following fields appear as shown in Figure 10.3:3: Server and .

- **Server Address**: IP address of the Media Server running in File Sync server mode. This field is empty by default.
- **Ports**: Port where file sync server is running. Default port is 2020.
- **Username**: Authentication username (Default: sick)
- **Password:** Authentication password
- **Set Bandwidth** (Custom/Max available) Choose custom to restrict the archival speed. Choose Max available to utilize max archival speed.
- **Bandwidth value**: Provide the bandwidth value.
- **Bandwidth Unit:** Select the bandwidth unit from the drop-down which has units like image per minute/per second/mbps/kbps.
- **Test button:** It is used to test the connection with the target Sync server and verify the correct network before saving the details.

- **Save button**: Saves the client details for future reference and file archival. This button is enabled after testing is complete.

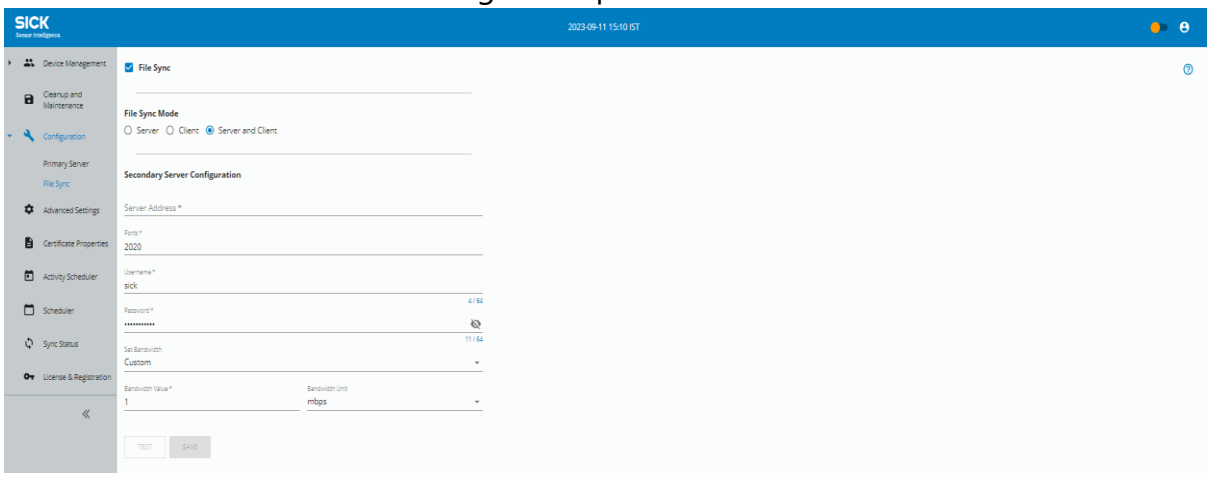


Figure 10.3:3: Server and Client

10.3.2 Types of File Sync Set-up

There are two types of file sync:

- Uni-directional
- Bi-directional

10.3.2.1 Uni-directional File Sync

Using Unidirectional setup, sends of images from one media server to another. Here one Media Server is selected as File Sync Server and another as File Sync Client. This is a one-way flow. It is the preferred configuration to utilize max space of both servers with unique image sets.

Please refer File Sync Mode on how to configure server and client mode.

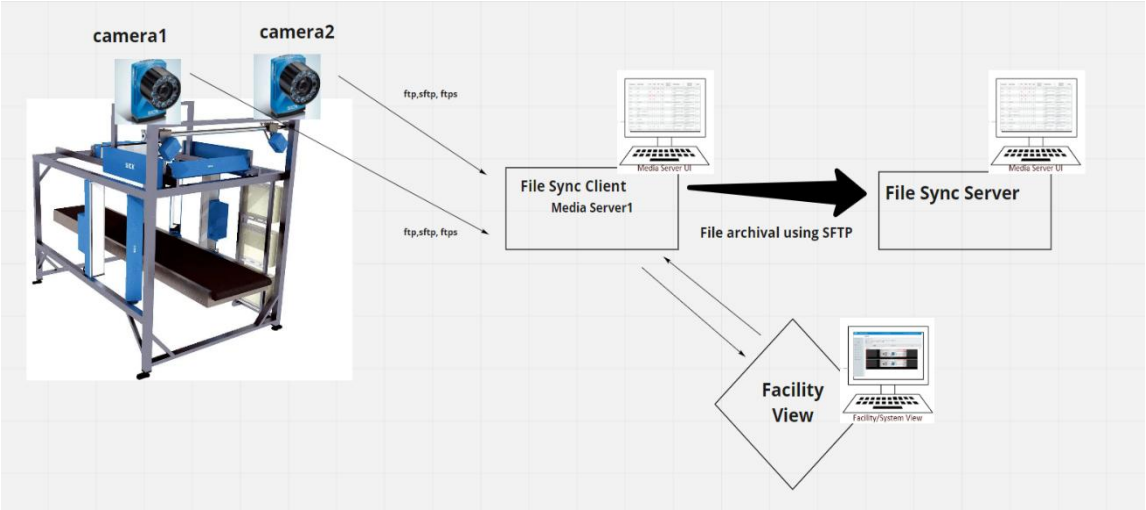


Figure 10.3:4: Uni-directional File Sync

10.3.2.2 Bi-directional File Sync

Bi-directional is a setup where both Media Servers are selected as server and client under file sync. Here both media servers act as File sync client and server. FS client of both MS is pointing to FS server of the other MS. When either of the media servers acquire images from image capturing devices, they archive the files to the other Media Server. Refer to File Sync Mode.

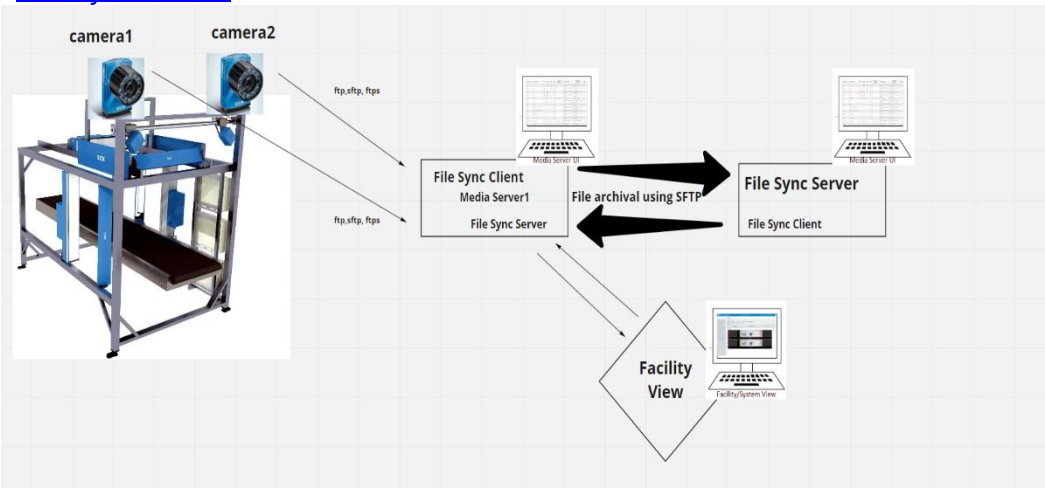


Figure 10.3:5: Bi-directional File Sync

11 Configure Media Server

11.1Overview

The Media Server can be hosted on the same hardware as other SICK Analytics products or as a standalone system, depending on your architecture requirements.
All user access to the Media Server is through the Media Server dashboard, which is available in the SICK Analytics application installed at your facility.
Use the Media Server Configuration section in LA to configure the Media Server. You can also edit existing Media Servers or remove them from LA using this section.

***Note**: You must be logged in with the necessary permissions in Facility View to add, edit, or remove a Media Server. If you do not have sufficient permissions, the Media Server page does not display these options.*

11.2 Configuring a New Media Server

To configure a new Media Server in Facility View, follow these steps:

1. **Access the Configuration Menu**
   - Navigate to the **Configuration** menu on the left navigation pane.
   - Click **Media Server Configuration**, or expand the **Configuration** menu and select **Media Servers**.

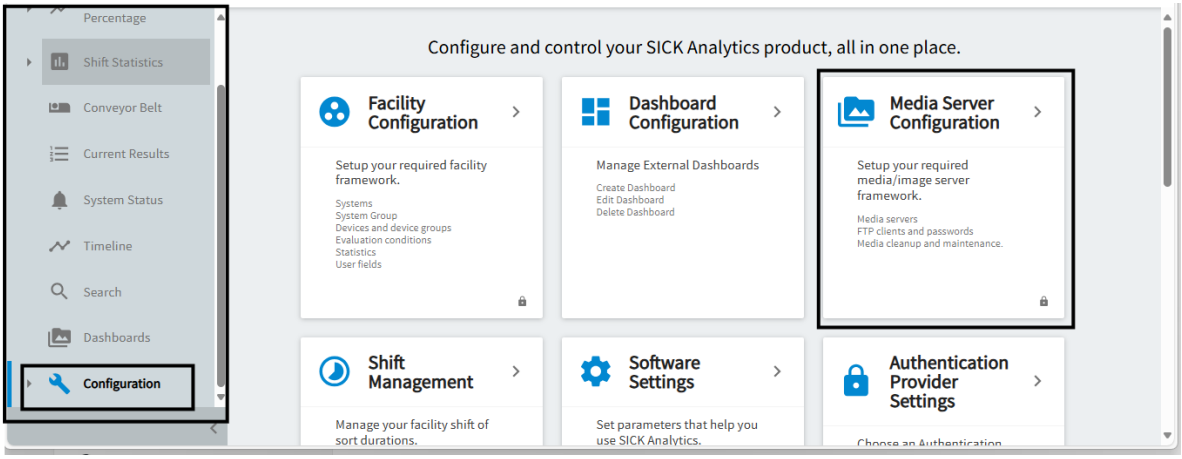


Figure 11.2:1: Navigation to Media Server Configuration

2. **Add a New Media Server**
   - On the **Media Servers** page, click the **Add (+)** icon at the top-right corner to open the **Add Media Server** form.

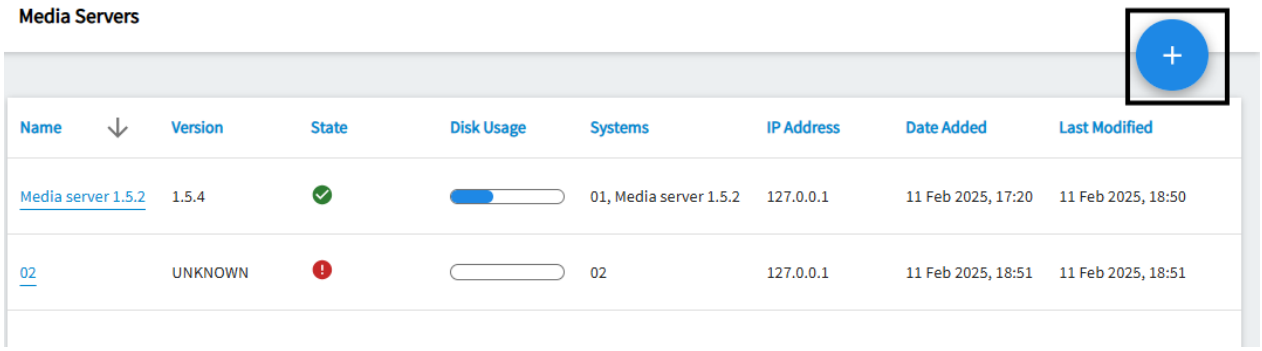


Figure 11.2:2: Media Servers Page - Adding a New Media Server

3. **Provide Basic Details**
   - Enter a **unique name** for the Media Server.

- Specify the **IP Address** where the Media Server is running.

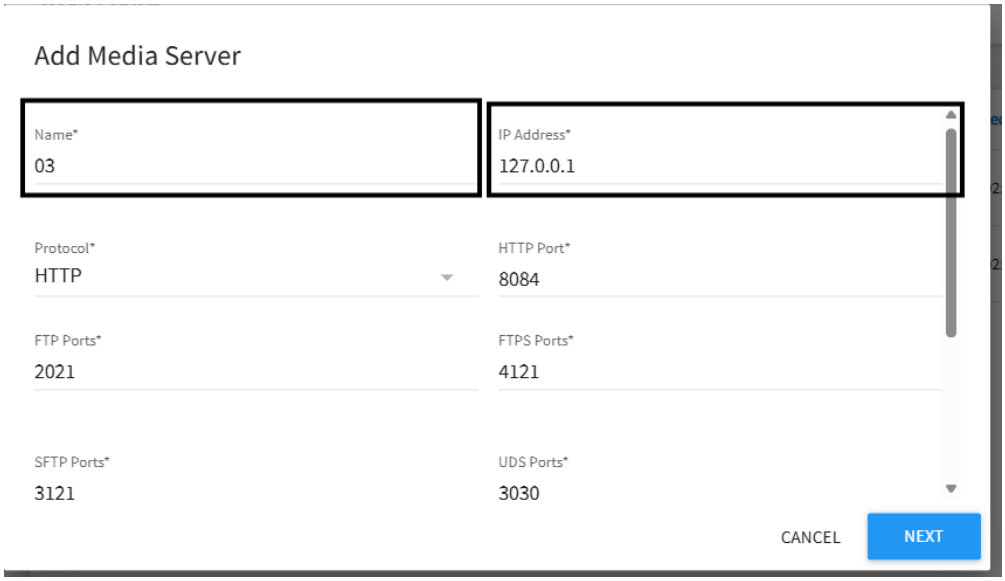


Figure 11.2:3: Add Media Server Form - Basic Details

4. **Select Protocol**
   - Choose the protocol:
     - **HTTP** (default)
     - **HTTPS** (requires specifying an **HTTPS Port**).

Note:

- Starting with Media Server 1.6, FTP can be disabled directly from the Media Server UI without requiring a new license. HTTP can be disabled through license configuration, configuration file, or directly from the Media Server UI by navigating to **Advanced Settings →** Properties Configuration. FTP and HTTP are unsecured protocols. The option to enable or disable HTTP from the UI is available only when the application is accessed over HTTPS. When HTTP is disabled, the HTTP port field will not be displayed. For detailed steps on how to enable or disable protocols, refer to Section ENABLE/DISABLE PROTOCOLS.
- It is recommended to use secure alternatives such as **SFTP** and **HTTPS** for encrypted communication. For further assistance with disabling these protocols or transitioning to secure alternatives, contact the support team at: https://supportportal.sick.com/

- FTP and HTTP are unsecured protocols. Starting with Media Server 1.6, FTP can be disabled directly from the Media Server UI without requiring a new license.
- HTTP can be disabled through license configuration, configuration file, or directly from the Media Server UI by navigating to **Advanced Settings → Properties Configuration**.
- The option to enable or disable HTTP from the UI is available only when the application is accessed over HTTPS.
- When HTTP is disabled, the HTTP port field will not be displayed.
- For detailed steps on how to enable or disable protocols, refer to Section ENABLE/DISABLE PROTOCOLS.
- It is recommended to use secure alternatives such as **SFTP** and **HTTPS** for encrypted communication. For further assistance, contact: https://supportportal.sick.com/

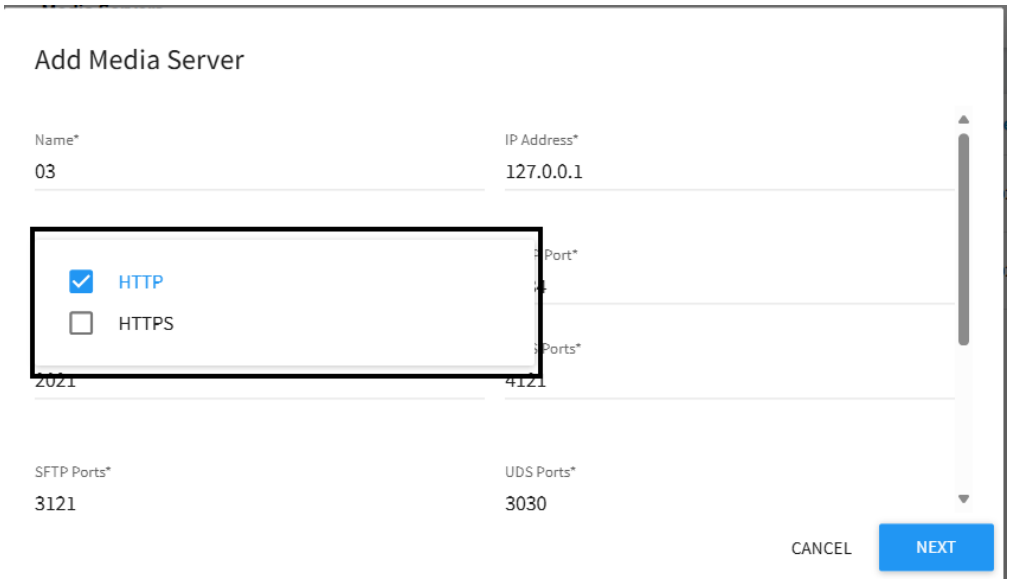


Figure 11.2:4: Select Protocol

5. **Configure Ports**
   - Enter the **HTTP Port**. A green validation message confirms if the port is valid.
   - Configure **File Transfer Ports**:
     - **FTP Port**
     - **FTPS Port**
     - **SFTP Port**

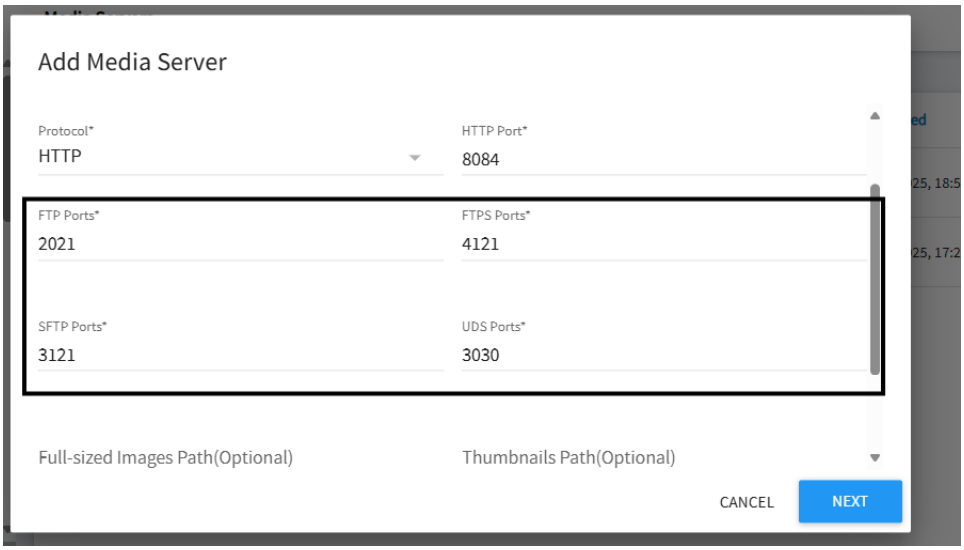


Figure 11.2:5: Media Server Ports Configuration

6. **Set Additional Communication Ports**
   - Specify the **UDS Port**, if required.

7. **Specify Image Storage Directories (Optional)**
   - Provide paths for:
     - **Full-sized Images Path**
     - **Thumbnails Path**

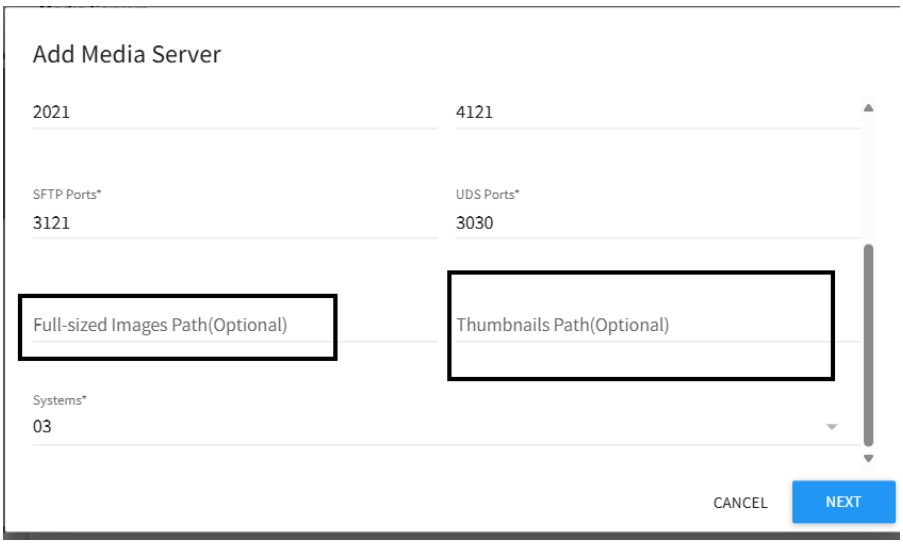


Figure 11.2:6: Image Storage Directories

8. **Assign Systems**
    - Select systems from the dropdown:
        - Choose **"All Systems"** or select specific systems from the list.

Figure 11.2:7: System Selection

9. **Select Imaging Devices**
    - After selecting the system(s), the **Add Media Server** screen updates to display available imaging devices.

        - Check the boxes next to the imaging devices you want to assign as FTP users for the Media Server.
        - You can select **all devices** or choose specific ones.
        - Click **SAVE** to finalize the selection or **BACK** to return to the previous step.

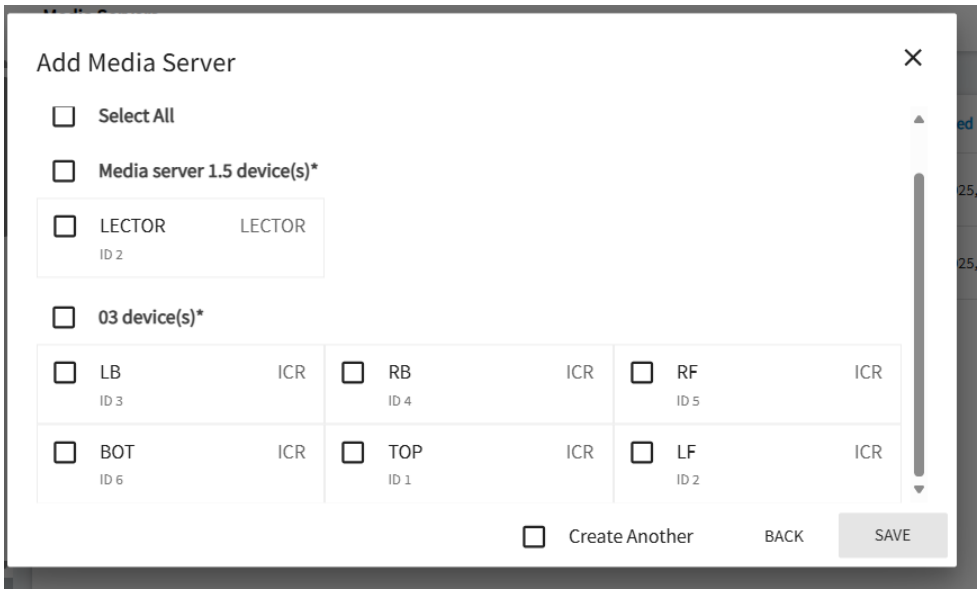


Figure 11.2:8: Select Imaging Devices

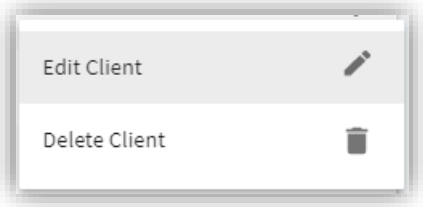
Note:

- *Ensure the Device Username and Password match the credentials of the FTP device configured on the Media Server.*
- *For example, if a device named "TOP" exists in Facility View with the username/password Top/123, the same credentials must be configured in the Media Server application.*
- *If a device is not configured properly, clicking **SAVE** will display an error message: "DEVICE(S) <DEVICENAME> IS (ARE) NOT CONFIGURED PROPERLY. PROPER CONNECTION SETTINGS ARE REQUIRED FOR THE IMAGE SERVER.*

11.3 How to configure devices with FTPS and SFTP with Facility View

Currently Facility View version 4.4 and lower versions does not support direct creation of SFTP/FTPS devices. To create SFTP/FTPS device, you need to first create FTP device in Media Server application and then edit FTP device to SFTP/FTPS device.
To add FTPS/SFTP device for Facility view:

1. Create FTP device in Facility View.
2. Launch and login to Media Server with user having add device permission.
3. Navigate to device tab.
4. Click on the vertical ellipsis ⋮ for the FTP device you would like to update.
5. This will display Edit device and Delete device options.



6. Click on **Edit Device** option to open the Edit Delete window.
7. Select the protocol as **FTPS** or **SFTP.**

Note:

- FTP and HTTP are unsecured protocols. Starting with Media Server 1.6, FTP can be disabled directly from the Media Server UI without requiring a new license.
- HTTP can be disabled through license configuration, configuration file, or directly from the Media Server UI by navigating to **Advanced Settings** → **Properties Configuration**.
- The option to enable or disable HTTP from the UI is available only when the application is accessed over HTTPS.
- When HTTP is disabled, the HTTP port field will not be displayed.
- For detailed steps on how to enable or disable protocols, refer to Section ENABLE/DISABLE PROTOCOLS.
- It is recommended to use secure alternatives such as **SFTP** and **HTTPS** for encrypted communication. For further assistance with disabling these protocols or transitioning to secure alternatives, contact the support team at: https://supportportal.sick.com/
- Starting with Package Analytics version 4.6 and later, when devices are created and integrated with the Media Server, both **FTPS** and **SFTP** are enabled by default. This is a change from earlier Package Analytics versions, where only FTP was enabled by default.

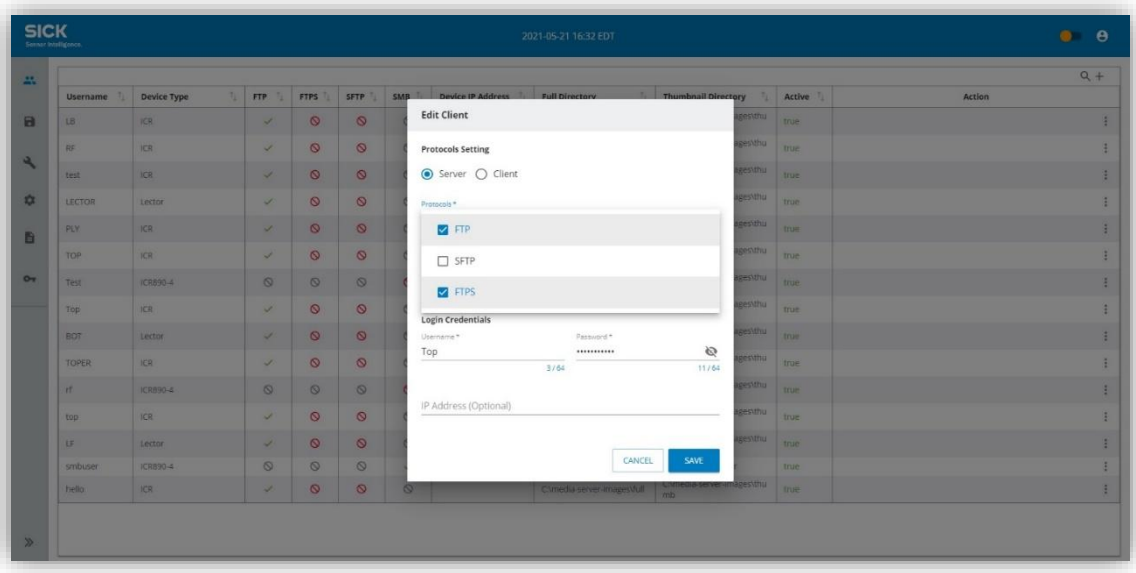


Figure 11.3:1: Edit Protocol

Note: *Starting with Package Analytics version 4.6 and later, when devices are created and integrated with the Media Server, both FTPS and SFTP are enabled by default. This is a change from earlier PA versions, where only FTP was enabled by default.*

8. Click the '**Save**' button.
9. The selected device will be updated, and a success snack bar message will be displayed. If there is an error while editing the device, application will display a snack bar message that an error has occurred.

12 Advanced Settings

This tab includes six sections: **Database**, **API Configuration**, **Heartbeat**, **Properties Configuration**, **Image Disclaimer**, and **Barcode Counter**.

- The **Database** section allows the user to configure MySQL connection properties.
- The **API Configuration** section allows you to set API access control values.
- The **Heartbeat** section allows you to configure publishing details for Media Server heartbeat messages.
- The **Properties Configuration** section allows you to configure the **HTTP Port**, **HTTPS Port**, and the path where image logs are saved. It also allows you to configure customized FTP data ports for image acquisition in FTP passive mode.
- The **Image Disclaimer** section allows you to configure a disclaimer message that is printed on images generated by selected devices.
- The **Barcode Counter** stores metadata information about the cumulative code count matching the configured rule. Information such as: **UID**, **1Z/PTN Tracking Number**, **Timestamp**, **UPS Code Count**, and **Image File path** will be stored by reading the incoming XML files for the camera.

Note: *SQLite DB is deprecated in MS 1.5. Patching will migrate the data to MySQL DB.*

- *SQLite to MySQL migration: 7 million records take 17 minutes.*
- *MySQL to MySQL migration: 108 million records take 5 hours and 17 minutes.*

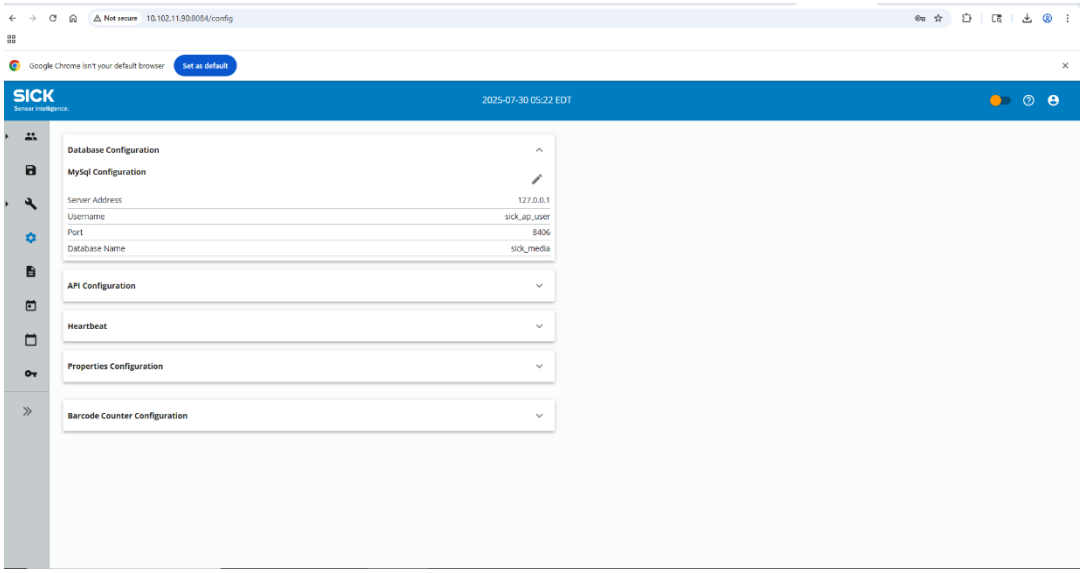


Figure 11.3:1: Advanced Settings Screen

12.1 Edit or Recover MySQL Configuration

You can edit the current MySQL database settings by navigating to the **Advanced Settings** tab and clicking on the **Edit** icon.

1. Navigate to **Advanced Settings** tab.
2. Click on the edit icon .
3. This will display **Edit MySQL Config** window.

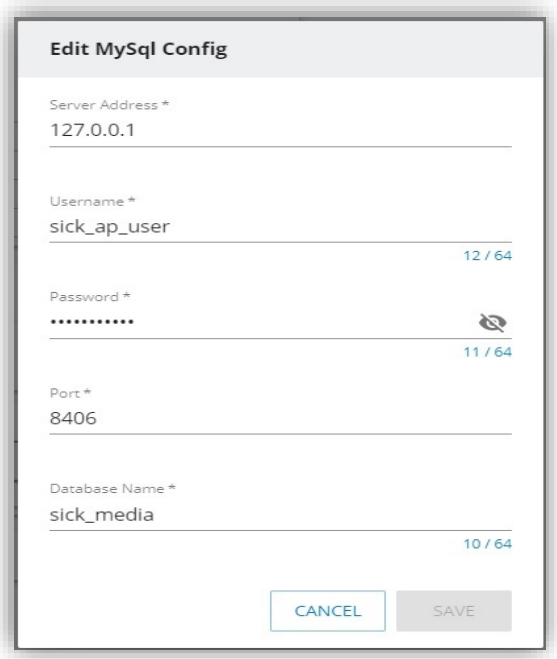


Figure 12.1:1: Edit MySQL Config Window

4. All fields on **Edit MySQL Config** window are mandatory. Username and Password will be set to default Analytics Username/Password if Analytics MySQL is running.
5. Update the **Server Address** if MySQL is running on a different machine.
6. Update **Port** (8406 is the default port for MySQL Server installed with Analytics) and **Database Name**.
7. Click on '**Save'** button.
8. If all provided details are correct and the connection is successful, the configuration file will be updated with latest changes and the popup window will disappear.
9. Navigate to windows services app by clicking on windows search icon and search for Services OR via Task Manager.

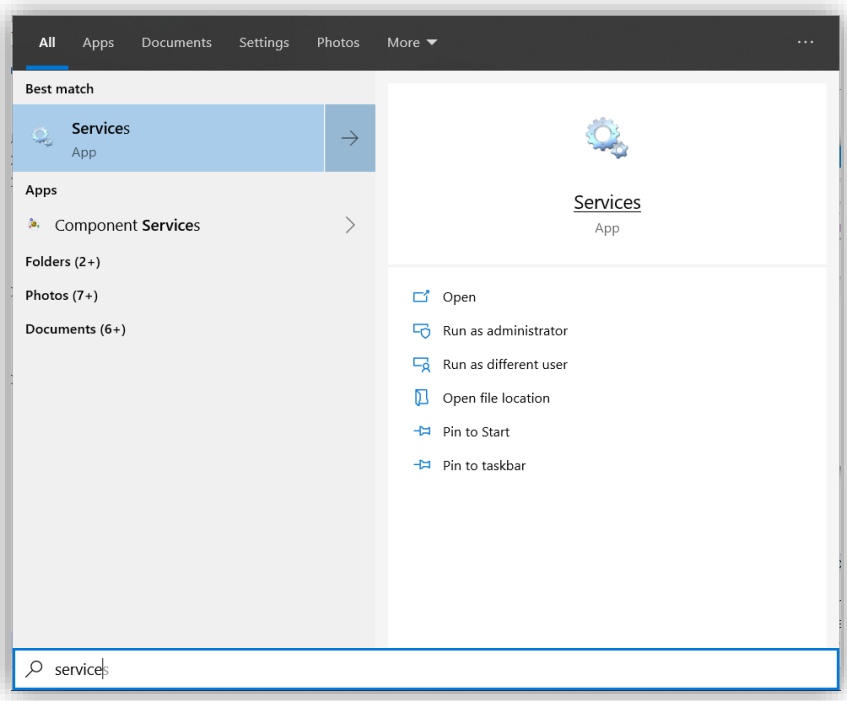


Figure 12.1:2: Windows Service Search

10. Click on services. This will open the windows services screen.
11. Locate SICK A Media Server Service.

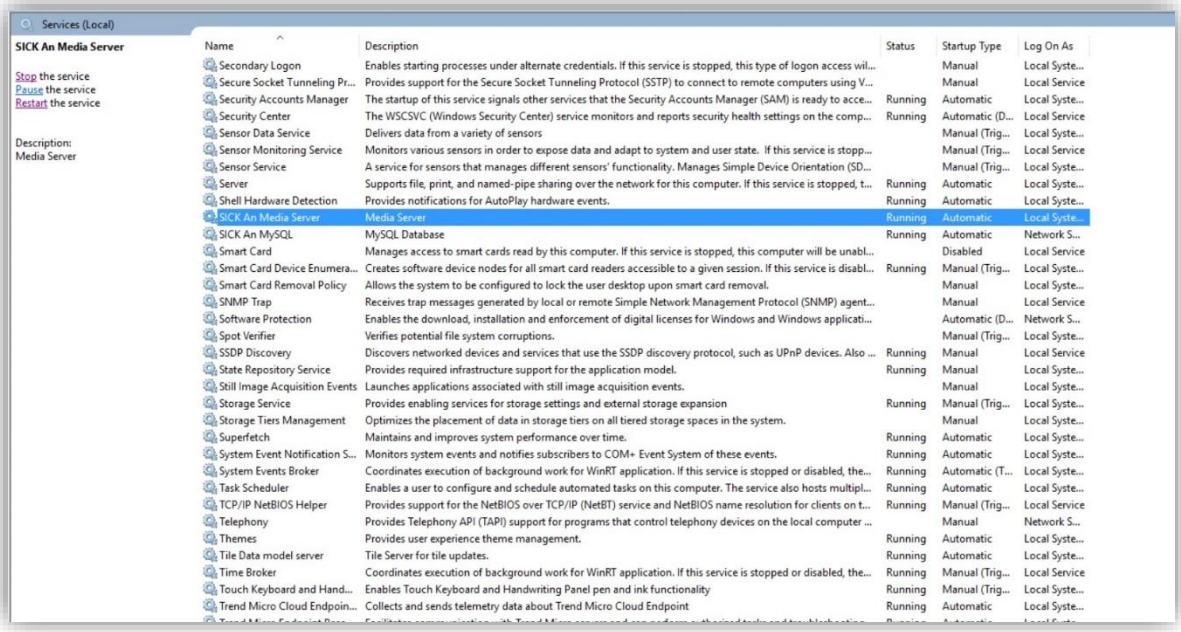


Figure 12.1:3: Media Server Service Screen

12. Restart Media Server Service by right clicking on SICK A Media Server Service and selecting restart option.

13. The changes will not be updated in configuration file and will throw error message saying "Could not establish database connection" unless you provide the valid details.

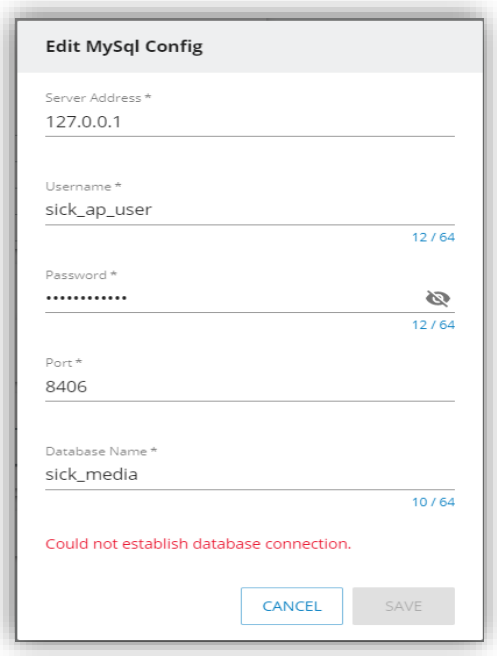


Figure 12.1:4: Could Not Establish Connection

Setting	Description
Server Address	The MySQL Server address.
Username	Username of the MySQL server used for authentication.
Password	The password of the MySQL server used for authentication.
Ports	MySQL server Port number.
Database Name	Name of the database schema to which Media Server connects

Table 10: Configuration Settings

After successfully updating configuration settings, the media server must be restarted for the selected database connection to take place. A banner will appear on top of the UI notifying:

If a connection issue is encountered during starting/restarting the Media Server, **the system will only display the "Configure DB" section instead of the full UI**. To restore functionality, follow these steps:

1. Open the **Media Server UI**.
2. Navigate to **Advanced Settings → Configure DB**.
3. Enter the correct **MySQL Server Address, Port, Username, and Password**.
4. Click **Save** and restart the **Media Server**.
5. If the issue persists, verify the MySQL service is running on the configured server.

12.2 Points to Note While Upgrading to Media Server 1.5 or Higher

- **Important Notes While Patching:**
  - MS 1.5 has deprecated SQLite DB.
  - Upon patching MS 1.5, all data in SQLite DB will be migrated to MySQL.
  - MS 1.5 restructures MySQL DB for performance improvements, making patching a time-consuming process.
  - When upgrading from Media Server 1.4 or any earlier version to 1.5 or 1.6, only 339 days' worth of data will be retained. Any data older than 339 days will be automatically purged during the migration process.
- **Migration Timelines:**
  - SQLite to MySQL migration (36 million records, 69 days): 1.5–2 hours.
  - MySQL to MySQL migration (108 million records, 35 days): 5.5–6 hours.
- **Storage Requirements:**
  - 50GB free space required on the MySQL DB drive for 100 million records.
  - 20GB free space required for 10 million records.
- **Performance & Restrictions During Migration:**
  - Older images may not be visible in PA until fully migrated.

- Image acquisition continues but may be slower.
- Downtime is recommended to avoid slow performance.
- Configuration changes (e.g., client creation, updates) are not allowed during migration to prevent data loss.
- Clean-up processes are halted during migration.
- If the image storage drive runs out of space, MS will aggressively clean up migrated records (FIFO method).

Database Migration Process:

- Migration initiates automatically when patching MS 1.5.
- If the previous version used SQLite, all records migrate to MySQL.
- It is recommended to perform this migration during downtime.
- Refer to Section Edit or Recover MySQL Configuration for detailed migration steps.

MySQL Connection and Configuration:

- Media Server requires MySQL to function.
- If Analytics MySQL Server is external, users will be prompted to enter MySQL details on MS login.

Editing MySQL Configuration:

1. Go to **Advanced Settings > Database.**
2. Click **Edit** in the Database Container.
3. Update:
    - Server Address (IP where MySQL is installed).
    - Port (default: 8406).
    - Valid MySQL credentials with CRUD (Create, Read, Update, Delete) permissions.
4. Click Save to apply changes.
5. Restart Media Server Services for changes to take effect.

Migration Performance Considerations:

- Migration time depends on disk IOPS (Read & Write speed).

During Migration:

- Image acquisition and retrieval may slow down due to high disk activity.
- clean-up processes are halted.
- Ensure sufficient disk space to prevent data loss.

- **Post-Migration Considerations:**
  - Disk storage visibility:
    - "Disk Storage" for Full and Thumb storage is not visible in UI during migration.
    - Inventorying process rebuilds the database.
- **Important Warnings:**
  - Do not restart Media Server before inventorying is complete.
  - If interrupted, inventorying will not resume, and images may not be retrievable.
  - Contact SICK Analytics Support for assistance.
  - No image loss is expected, but MS may drop images if server load is too high.
  - MS 1.6 requires MySQL 8.4.5. Ensure MySQL is upgraded before migration.
  -

12.3 Image Disclaimer

The **Image Disclaimer** feature allows you to configure a disclaimer message that is printed on images generated by selected devices. This helps display legal, informational, or operational messages directly on image outputs.

12.3.1 Fields

- **Enable image disclaimer** – Enables or disables the image disclaimer feature.
- **Disclaimer Message** – Specifies the text printed on images.
- **Select Devices** – Select the devices to which the disclaimer applies.

12.3.2 To configure the image disclaimer

1. Navigate to **Advanced Settings** → **Properties Configuration**.
2. Select **Enable image disclaimer**.
3. Enter the disclaimer text in **Disclaimer Message**.
4. Select the required devices.
5. Click **Save**.

The disclaimer is applied only to newly acquired images.

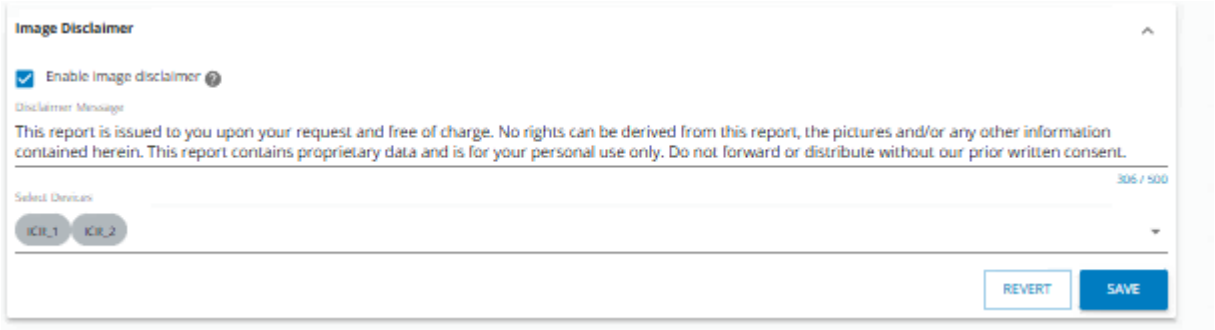


Figure 10.3:1: Image Disclaimer Configuration

12.4 API Configuration

The **API Configuration** section consists of two configurations:

1. **Default API Configuration**
2. **User API Configuration**

These settings define how frequently an API can be accessed within a specific time interval. API rate limits prevent excessive API requests, optimize resource usage, and ensure system stability.

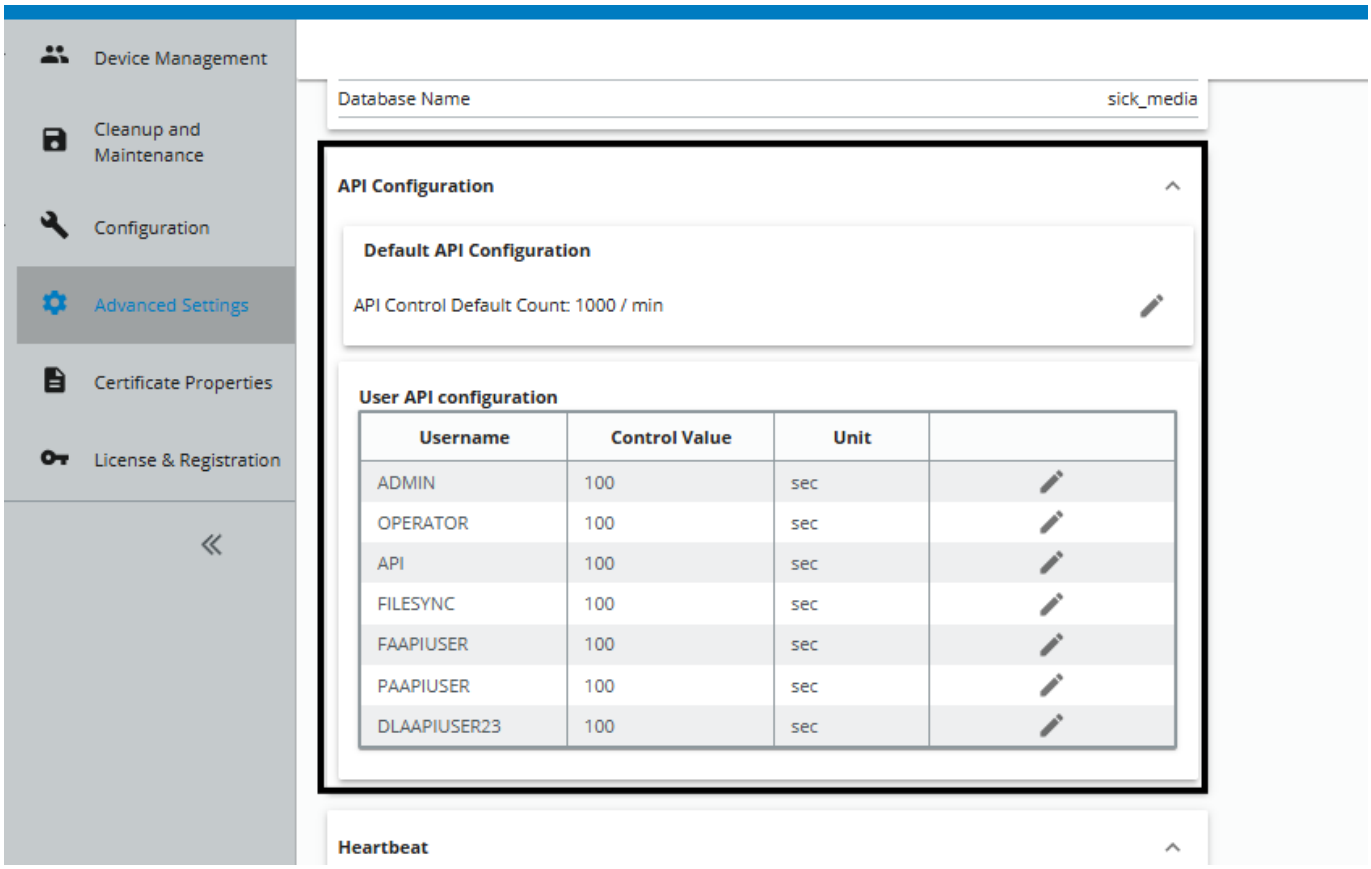
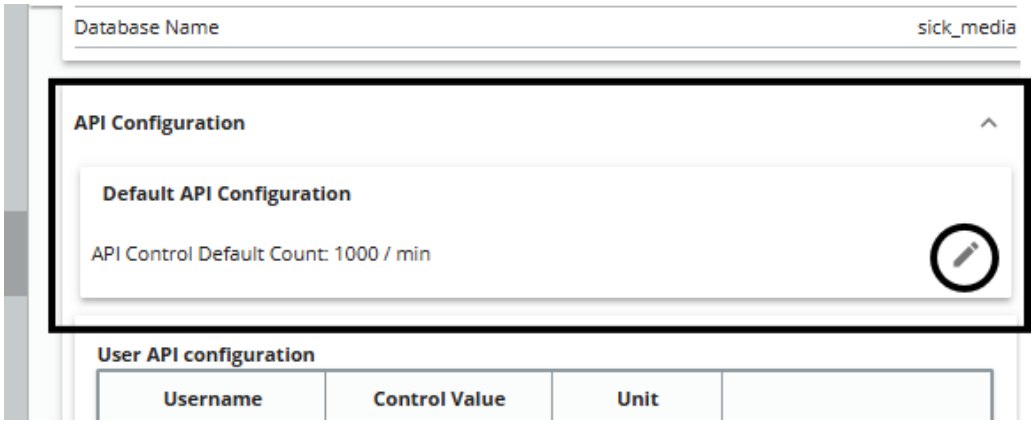


Figure 12.4:1: API Configuration Screen

12.4.1.1 Default API Configuration

The **Default API Configuration** sets a **global API rate limit** that applies to users unless a specific user configuration overrides it.



To edit the Default API Configuration:

1. Navigate to the **Advanced Settings** tab.

2. Click the **edit icon** next to **Default API Configuration**.
3. The **Edit Default API** window appears.
4. Modify the **Control Value** (number of API requests allowed per selected time unit).
5. Select the **Unit** from the dropdown (**seconds, minutes, hours, or days**).
6. Click **Save**.

For example, if the **Control Value** is set to **500** and the **Unit** is set to **"hour"**, then the API can be accessed **500 times per hour**.

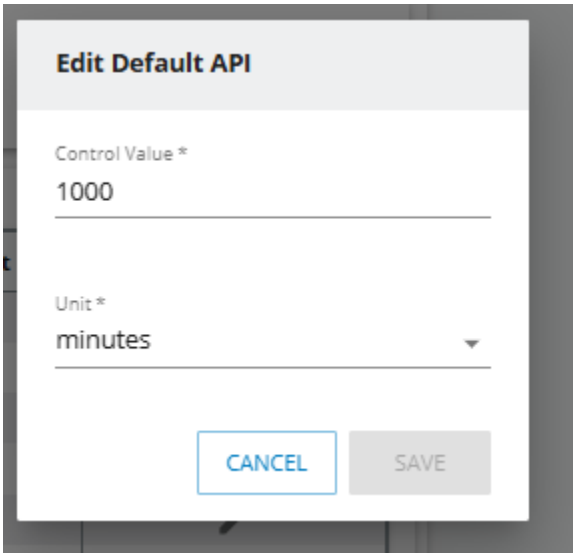


Figure 12.4:2: Edit Default API Window

12.4.1.2 User API Configuration

The **User API Configuration** allows administrators to **assign custom API rate limits per user**. If configured, these limits override the **Default API Configuration** for that specific user.
User API Configuration Table

The **User API Configuration table** displays the following fields:

- **Username**: The login username of the API user. (THIS FIELD IS NON-EDITABLE.)
- **Control Value**: The maximum number of API requests allowed within the selected time unit.
- **Unit**: The time unit for API requests (**seconds, minutes, hours, or days**).

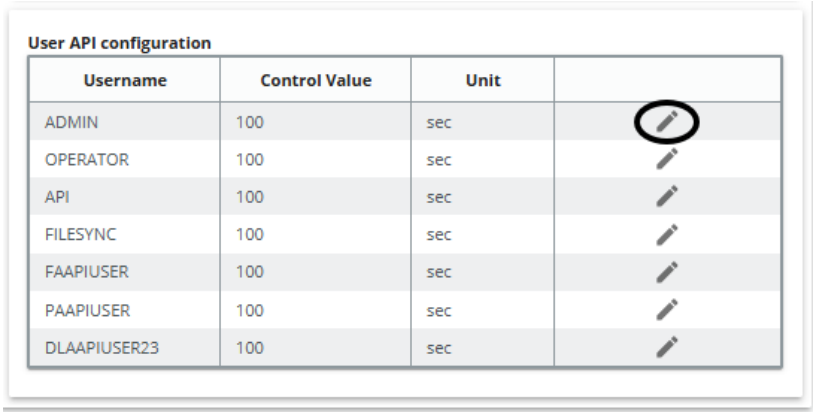


Figure 12.4:3: **User API Configuration Screen**

To edit a user's API configuration:

1. Navigate to the **Advanced Settings** tab.
2. Locate the **User API Configuration** table.
3. Click the **edit icon** next to the username.
4. The **Edit User API** window appears.
5. Modify the **Control Value** (number of API calls allowed per time unit).
6. Select the appropriate **Unit** from the dropdown (**seconds, minutes, hours, or days**).
7. Click **Save** to apply the changes.

For example, if the **Control Value** is set to **100** and the **Unit** is set to **seconds**, then the user can access the API **100 times per second**.

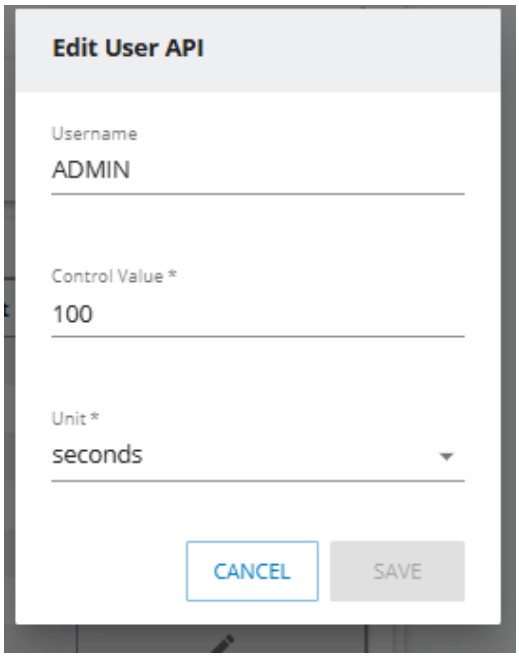


Figure 12.4:4: Edit User API Configuration Window

12.5 Heartbeat

Heartbeat is an alert mechanism to provide MS alert/heartbeat to Analytics Software. Heartbeat is used to inform the user that Media Server is reaching the threshold configured for the application and system stats in configuration file. Heartbeat section allows user to enable publishing heartbeat messages to the Facility server when the image drop reaches a threshold or High CPU Utilization, and High memory usage reaches the configured threshold. These settings are configured in the sick-bip-is.cfg config file. This is a licensed feature and can be enabled/disabled from UI.

The heartbeat properties provide the information of current configuration of the Heartbeat messages. You can edit/update the properties by clicking on edit icon.

Note: *This is an upcoming feature for future releases.*

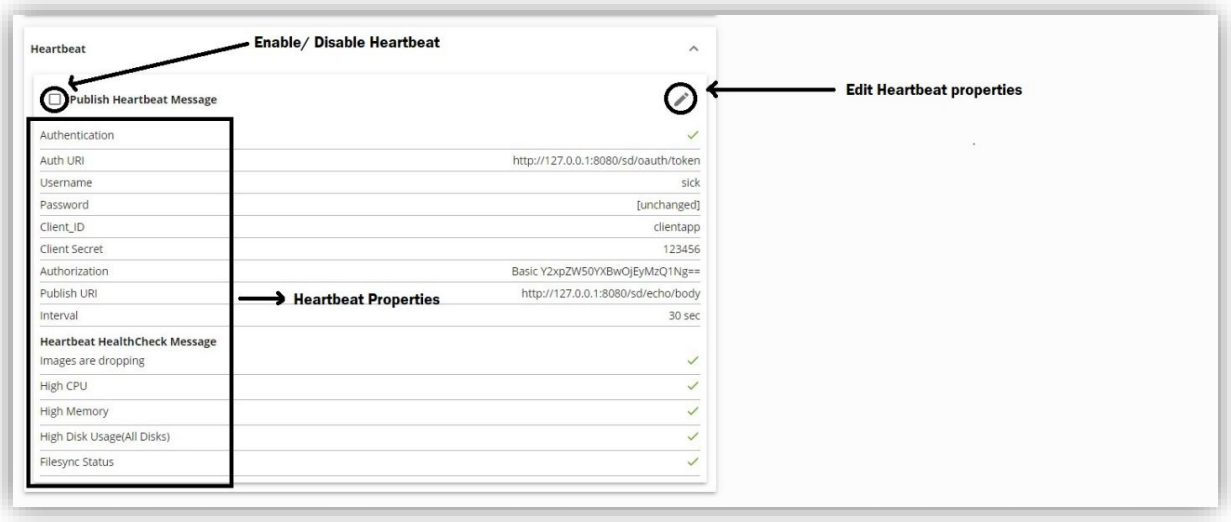


Figure 12.5:1: Heartbeat configuration

Setting	Description
Authentication	Indicates if authentication is required to publish heartbeat message.
Auth URI	The authentication URI which returns the access_token used for authorizing publish operation (if authentication is required by the facility server).
Username	Username of the Facility server used for authentication.
Password	Password of the Facility server used for authentication.
Device_ID	Device ID is the ID which is sent along with the authentication request.
Device Secret	Device Secret is the random ID sent along with the authentication request.

Setting	Description
Authorization	Authorization code sent as part of the authentication request header.
Publish URI	The URI using which the heartbeat message is published to the facility server.
Interval	Time interval for sending the heartbeat message. Allowed units are sec/min.
Images are dropping	Shows heartbeat health-check messaging is enabled/disabled for image drop feature.
High CPU	Shows heartbeat health-check messaging is enabled/disabled for CPU usage feature.
High Memory	Shows heartbeat health-check messaging is enabled/disabled for memory usage feature.
High Disk Usage(All Disks)	Shows heartbeat health-check messaging is enabled/disabled for disk usage feature.
Threshold	A threshold is required to be defined to generate a warning for the heartbeat messages whenever there is High Disk Usage, High CPU and Memory Usage or images being dropped. You can configure the threshold from the config file.

Table 11: Heartbeat Configuration Settings

12.5.1 Heartbeat Warnings:

Based on the threshold settings and Health check messages options for Heartbeat messages, following warnings will be sent to the Facility Application:

- **High Disk Usage**: If the Disk Usage have crossed the defined threshold
- **High CPU Usage**: If the CPU Usage have crossed the defined threshold

- **High Memory Usage:** If the Memory Usage have crossed the defined threshold
- **Image drop**: If the Image drop count have crossed the defined threshold

Also, If the active database is MySQL and if it is down, a warning messages will be sent to the Facility server whenever data is being pushed to the database.
On starting/restarting the Media Server if Media Server is unable to connect to MySQL, heartbeat warning message will be sent to the Facility server stating active database has been switched to SQLITE.

12.5.2 Enable/Disable Authentication for Heartbeat Messages:

You can enable/disable authentication from the Edit Heartbeat Settings popup window. If authentication is disabled, the **Edit Heartbeat Settings** window will hide all authentication related properties (i.e., Auth URI, Username, Password, Device_ID, Device Secret and Authorization) which are not required. Only Publish URI, Interval and Heartbeat Health Check options will be available as shown in the image below.
To enable/disable Authentication for Heartbeat messages:

1. Navigate to **Advanced Settings** tab.
2. Click on the edit icon present in front of **Publish Heartbeat Message** checkbox.
3. This will display **Edit Heartbeat Settings** window.

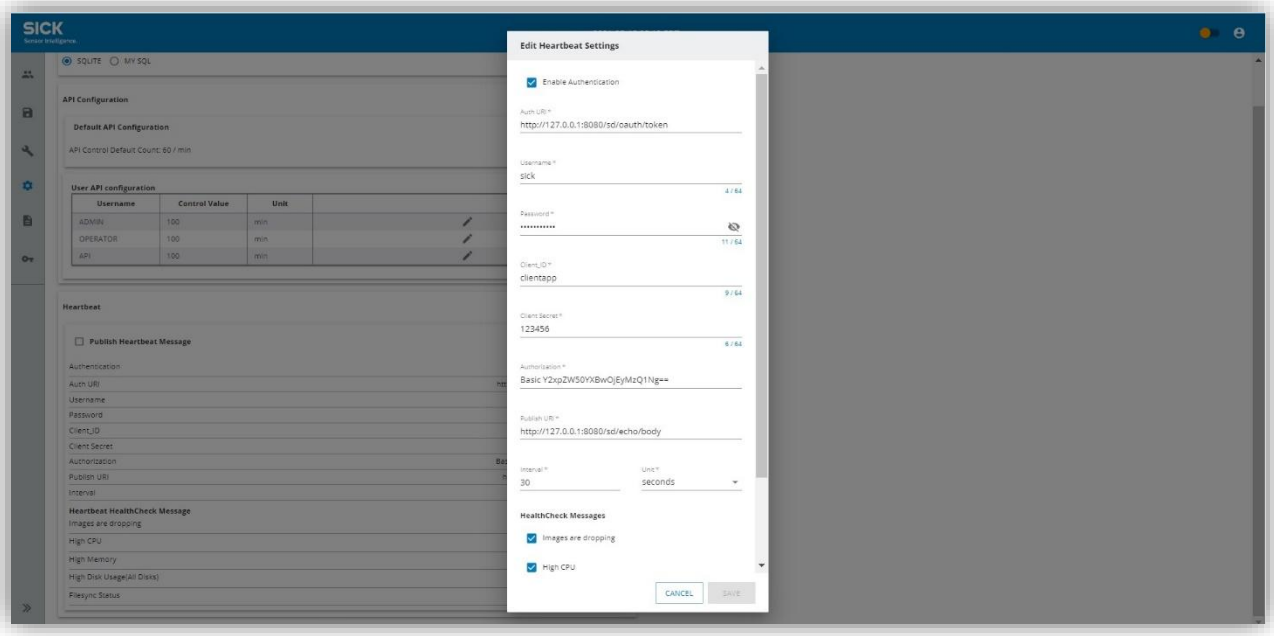


Figure 12.5:2: Edit Heartbeat Settings Window when Authentication is Enabled

4. If authentication is enabled, i.e., Enable Authentication checkbox is selected, window will display all the authentication related fields and these fields are marked as required/mandatory fields.
5. Enter all the mandatory fields and click on SAVE button.
6. Click the SAVE button to save the changes and enable the authentication.
7. To disable the authentication, deselect Enable Authentication checkbox. All the authentication related fields will be removed. Click the SAVE button to save the changes.

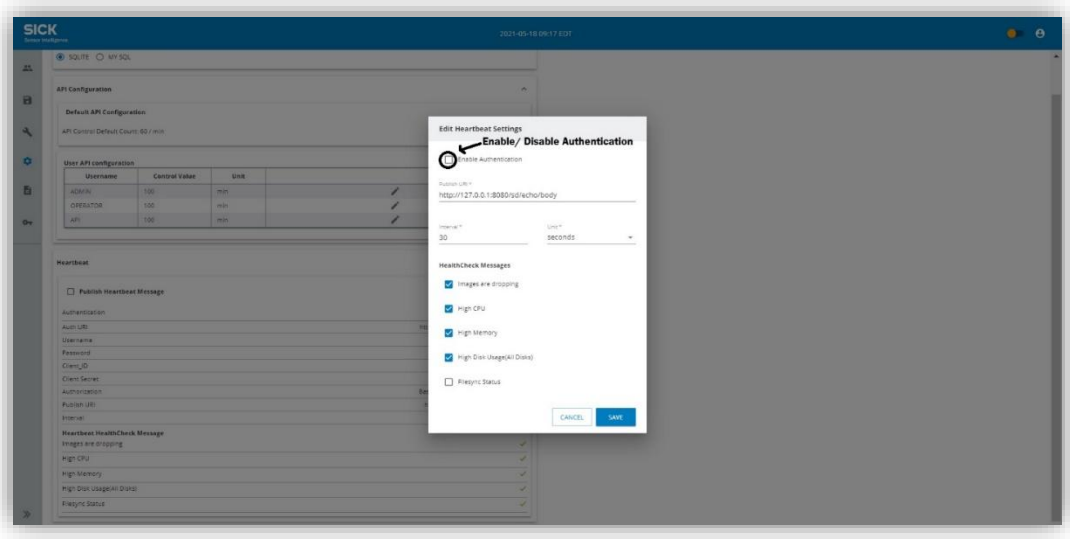


Figure 12.5:3: Edit Heartbeat Settings window when Authentication is disabled

12.6 Properties Configuration

The Properties Configuration section allows users to configure key Media Server settings related to network access, secure communication, FTP data transfer, and log storage.

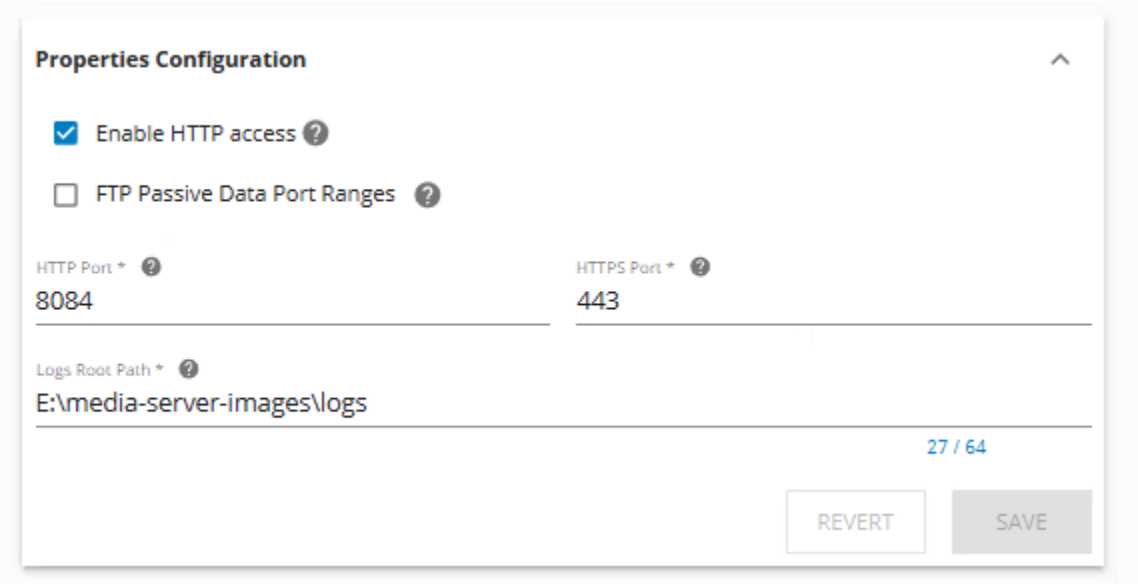


Figure 10.5:1: Properties Configuration

12.6.1 Fields

- **Enable HTTP Access**

  Allows users to enable or disable HTTP (non-secure) access to the Media Server.

  - When enabled, the Media Server can be accessed using the configured HTTP port.
  - When disabled, HTTP access is blocked and only HTTPS access is allowed.
  - **Important:** This setting can be modified only when accessing the Media Server using **HTTPS**. If the Media Server is accessed over HTTP, this option cannot be changed.

- **FTP Passive Data Port Ranges**

  Controls how ports are allocated for FTP passive mode data transfer.

  - When disabled, FTP uses random ports for data transfer.
  - When enabled, FTP uses only the configured port range.

- **HTTP Port**

  Specifies the port used for HTTP access to the Media Server.

  - This field is applicable only when **HTTP Access** is enabled.
  - **HTTPS Port**
    The **HTTPS Port** field specifies the port used for secure, encrypted access to the Media Server.

- **Logs Root Path**

  The **Logs Root Path** field specifies the directory where image logs and system logs are stored.

  Example: E:\media-server-images\logs

12.6.2 To Configure Properties

1. Enable or disable **HTTP Access** as required.
2. Enable **FTP Passive Data Port Ranges** if controlled FTP port usage is required.
3. Enter the **HTTP Port** and **HTTPS Port** values.
4. Specify the **Logs Root Path**.
5. Click **Save** to apply the changes.
6. Click **Revert** to discard unsaved changes.

***Note**: When "**FTP Passive Data Port Range**" is enabled, ensure that the FTP data port range configured should have enough ports in its range to support the feature. It is suggested to have port range equivalent to the camera's configured X20 times to acquire images using passive mode to avoid slowness in acquisition.*

12.7 Configure the Barcode Counter Feature in Media Server

Use the Barcode Counter feature in Media Server to track, validate, and extract barcode details from XML files based on user-defined rules. By specifying barcode types and regular expressions, you control which barcodes are processed or ignored during image analysis.

For advanced configuration, such as setting barcode processing priorities, see Configuring Barcode Counter Using sick-bip-is.cfg.

To Set Up the Barcode Counter in Media Server:

1. **Navigate to the Barcode Counter Configuration**

- Open the Media Server Web UI in your browser.
- In the left pane, click **Advanced Settings**.
- Scroll to find **Barcode Counter Configuration**.

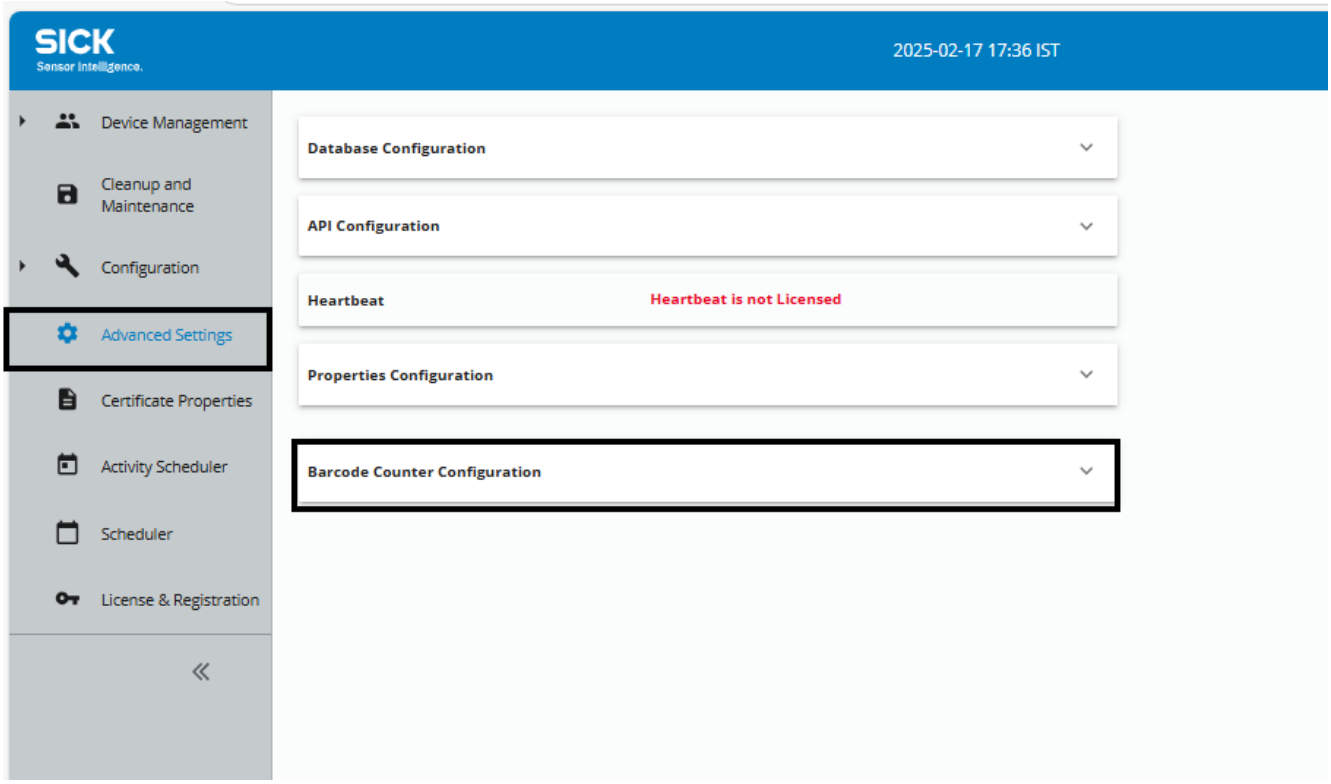


Figure 10.6.1: Navigating to the Barcode Counter Configuration

2. **Open the Barcode Counter Configuration Panel**

- Click **Barcode Counter Configuration** to expand the panel.
- Note: The panel opens with the **Barcode Counter** toggle **Off**, no rules defined, and the **Save** button disabled.

Figure 10.6.2: Initial Barcode Counter Configuration Panel

3. **Enable the Barcode Counter**

- In the **Barcode Counter Configuration** panel, locate the **Barcode Counter** toggle.
- Click the toggle to turn it **On** (it appears blue when enabled).
- OPTIONAL: Hover over any **?** (help icon) for tooltips about settings.

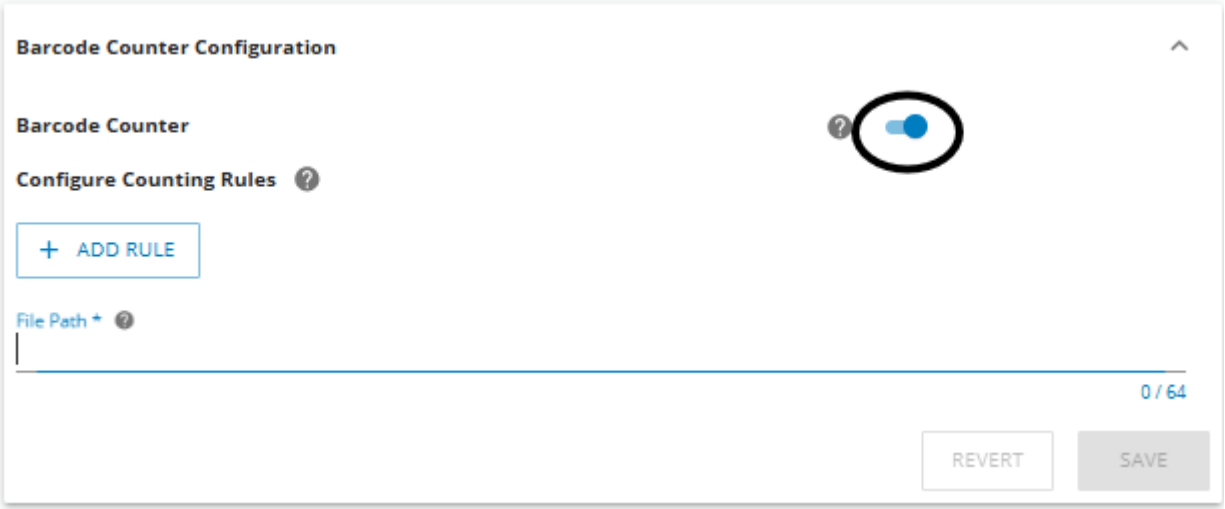


Figure 10.6.3: Enabling the Barcode Counter (Toggle Highlighted)

4. **Add Barcode Counting Rules**

- Click **+ ADD RULE**
- In **Barcode Type**, enter the barcode type (e.g., `C128`, `PDF417`, `EAN128`, `MAXI`).
- In **Barcode Pattern (Regex)**, enter a regular expression to filter accepted barcodes (e.g., `^1Z.*`).
- OPTIONAL: Add additional rules by repeating these steps.
- To delete a rule, click the icon next to it (highlighted in Figure 10.6.6).

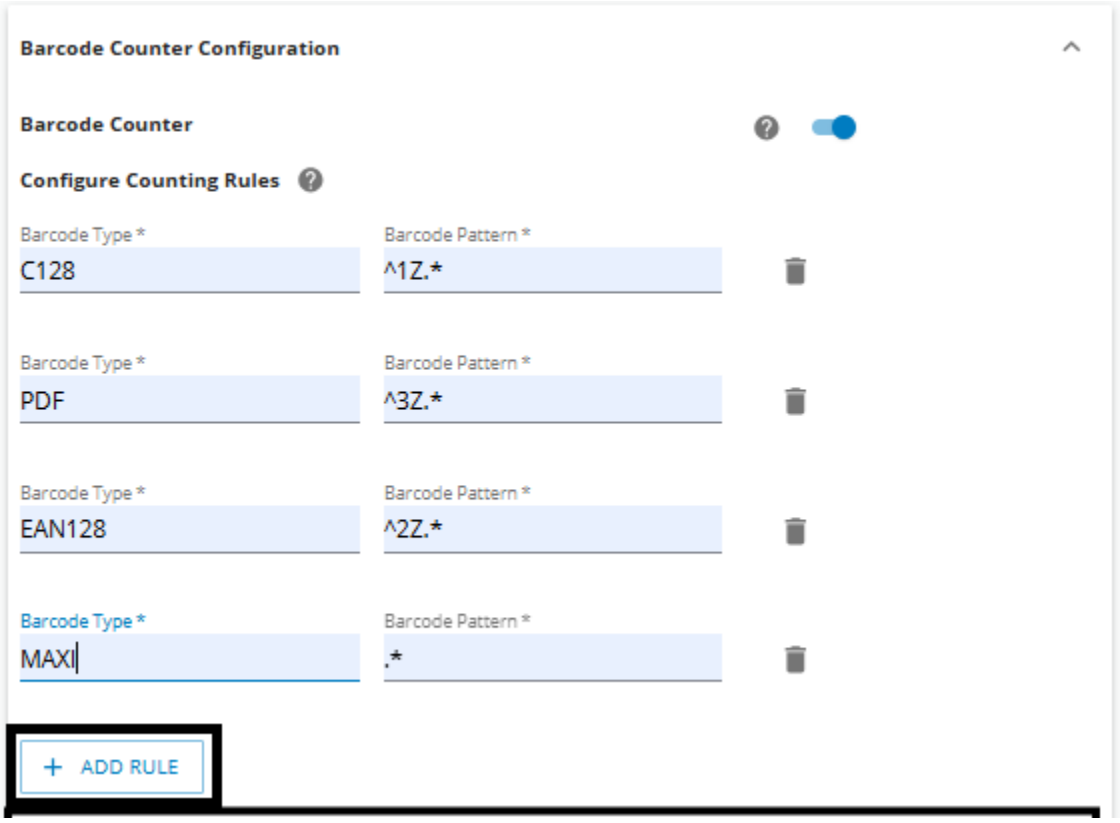


Figure 10.6.4: Adding a Barcode Rule

Example Rules:

Barcode Type	Barcode Pattern (Regex)	Processing Outcome
C128	`^1Z.*`	Accepts barcodes starting with 1Z (e.g., UPS tracking numbers).
PDF417	`^3Z.*`	Accepts barcodes starting with 3Z (e.g., FedEx tracking numbers).
EAN128	`^2Z.*`	Accepts barcodes starting with 2Z (e.g., warehouse tracking).

Barcode Type	Barcode Pattern (Regex)	Processing Outcome
MAXI	`.*`	Accepts all barcodes (catch-all rule).

Table 10.6.1: Example Barcode Rules

Important: Setting Barcode Processing:

- If a package contains multiple barcodes, you can define the processing priority in the `sick-bip-is.cfg` file. The system first attempts to process the highest-priority barcode. If that barcode is not present, it moves on to the next priority, ensuring the most relevant barcode is used.

```
[BARCODE_COMBINATION_PRIORITY]
1=C128; ^1z.*
2=C128; ^1Z.*
```

Example:

- If a package has multiple barcodes, the system first checks for `C128;^1z.*`.
- If `C128;^1z.*` is not present, it moves to the next priority, `C128;^1Z.*`.
- You can define multiple barcode priorities based on your system's needs.

For more details, refer to Configuring Barcode Counter Using sick-bip-is.cfg.

5. **Specify the File Storage Path**

- In the **File Path** text box, enter the directory for storing barcode counter files (e.g., `E:\media-server-images\DataAcqImgDir`).

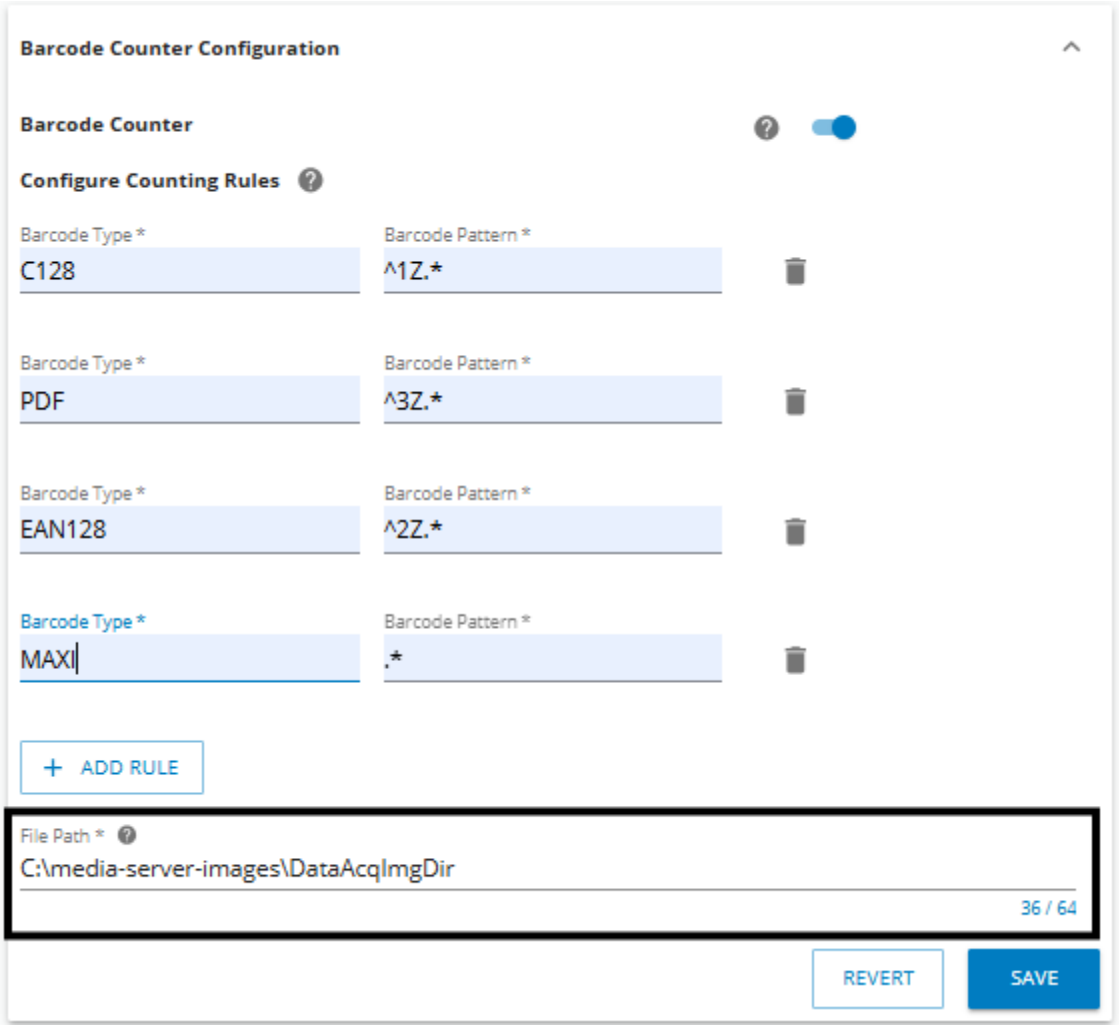


Figure 10.6.5: Specifying the File Path

6. **Save or Revert Changes**

- Verify that:
  - The **Barcode Counter** toggle is **On**.
  - At least one rule is defined.
  - A valid file path is entered.
- Click **SAVE** to apply changes.
- To discard unsaved changes, click **REVERT** to restore previous settings.

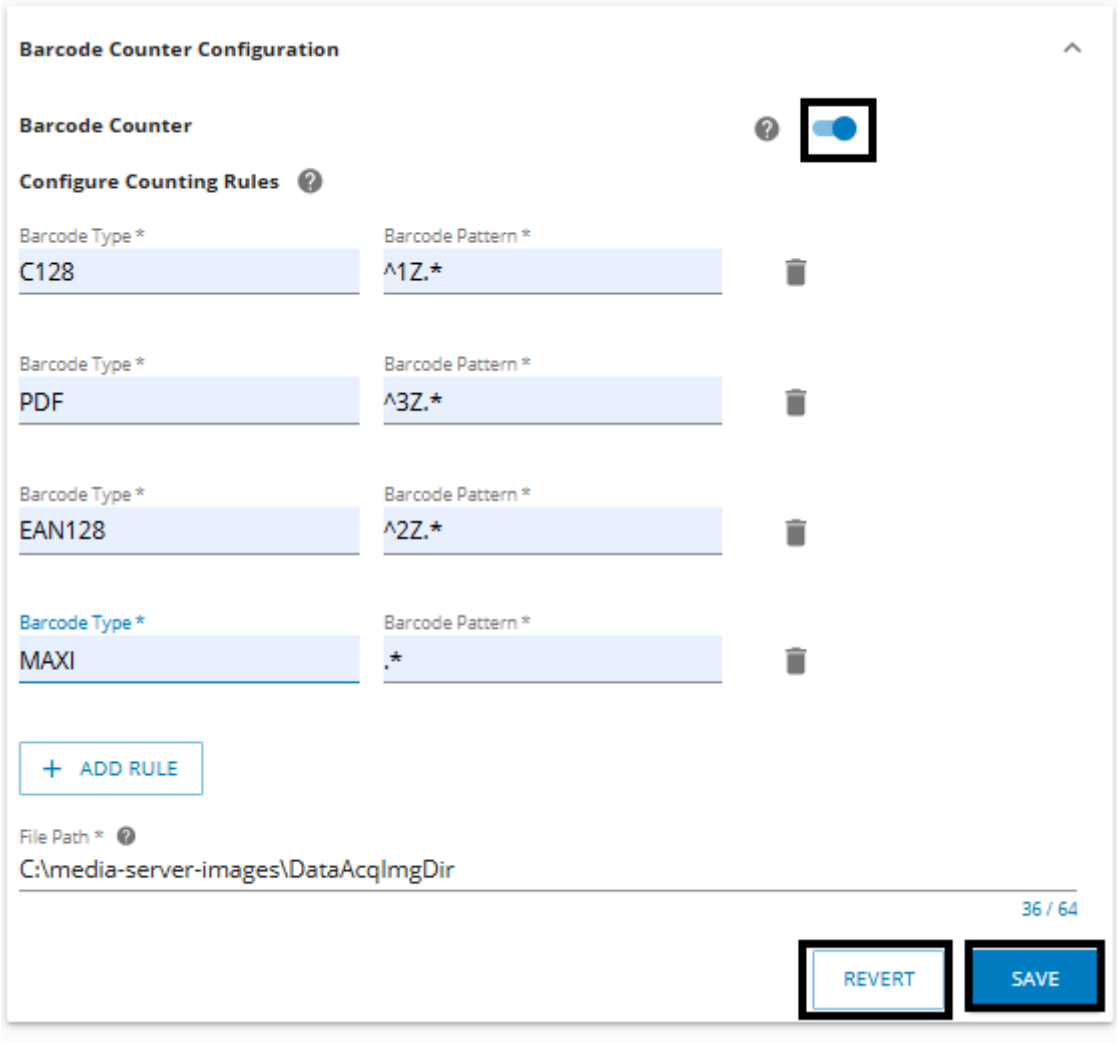


Figure 10.6.6: Saving the Configuration (SAVE and REVERT Buttons Highlighted)

7. **Verify the Generated Barcode Counter File**

- Once the **Barcode Counter** feature is enabled and you have processed at least one **valid XML** file, Media Server creates a log or data file in the configured storage path. To confirm:

- Open the folder you specified in **File Path** (for example, `C:\media-server-images\DataAcqImgDir`).

- Look for a file named **DataAcqImgDir_YYYYMMDD** or similar (the actual name may include a timestamp or date).

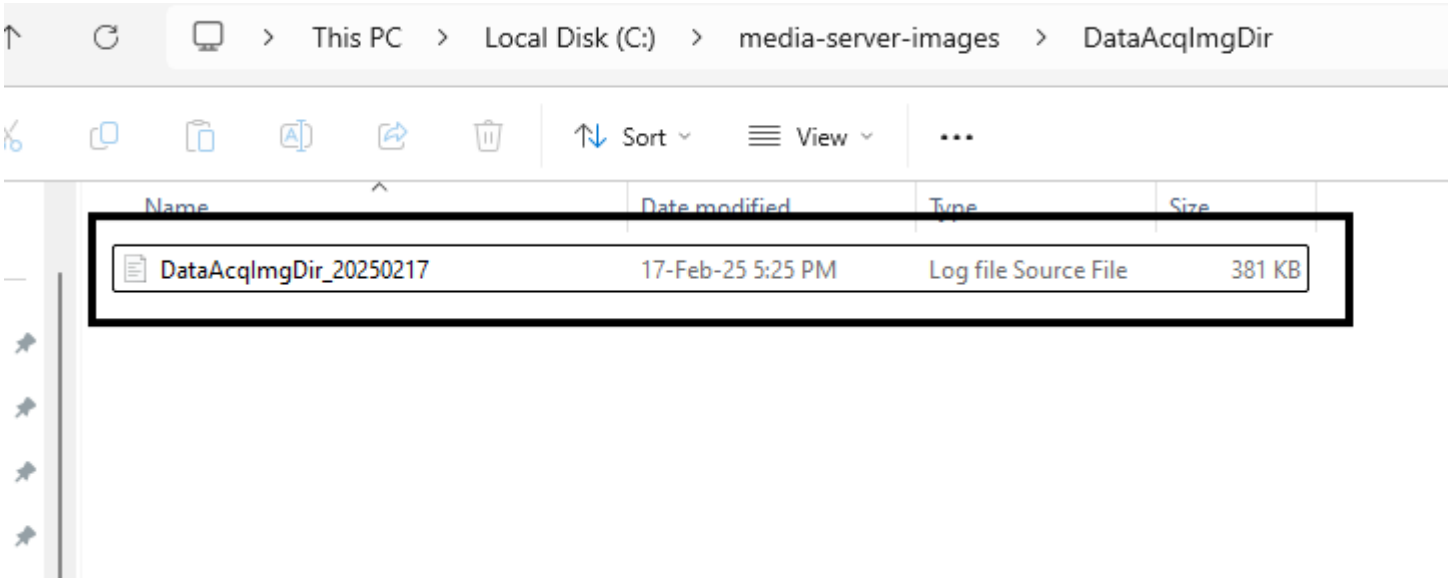


Figure 10.6:6: Example of a Generated Barcode Counter File

- After verifying the presence of the generated barcode counter file, you can open it to inspect barcode details extracted from processed XML files. The file is a comma-separated value (CSV) log. A sample portion might look like this:

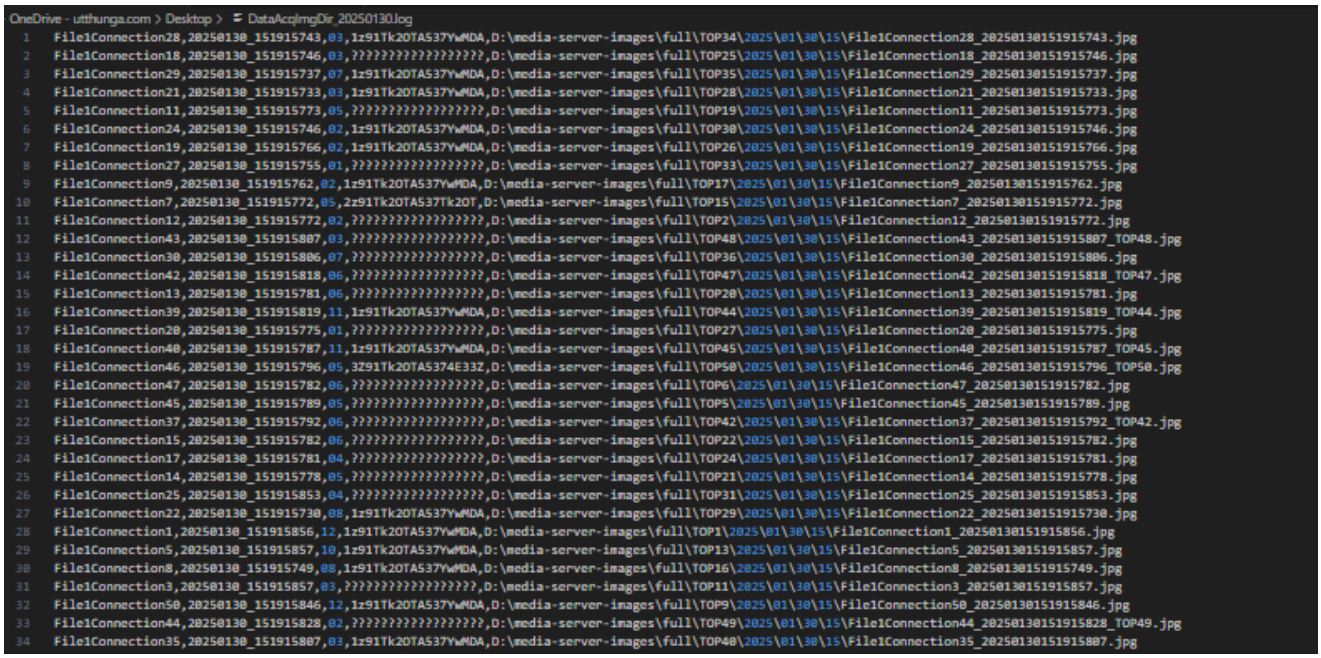


Figure 10.6:7: Example of a Generated Barcode Counter Log Snippet

Note:

For more details about how this data file is structured and what each field represents, refer to the Barcode Data File section.

- Media Server creates the associated barcode counter file only after it receives the first valid XML file once the feature is enabled.

- The system does not allow duplicate or ambiguous rules. Each rule must have a unique type-and-regex combination.

12.8 Barcode Data File

The Barcode Data File logs details extracted from processed XML files, including unique identifiers, barcode counts, timestamps, and associated image paths. It supports accurate barcode tracking, system debugging, and verification of processed data. The file is a structured, comma-separated value (CSV) log, prioritizing barcode details based on predefined rules.

Field	Description
Unique ID	A unique identifier for the record.
Timestamp	The date and time when the barcode details were processed (e.g., YYYYMMDD_HHMMSSFFF).
Barcode Count	The number of barcodes identified in the processed XML file.
Barcode Value	The decoded value of the barcode (e.g., a tracking number).
Image File Path	The full path to the image file associated with the barcode details extracted from the XML file.

Sample Entry

```
UniqueID,Timestamp,BarcodeCount,BarcodeValue,ImageFilePath
File1Connection19,20250130_151915766,2,1z91Tk2OTA537YwMDA,D:\media-server-im-
ages\full\TOP26\2025\01\30\15\File1Connection19_20250130151915766.jpg
```

Where:

- **File1Connection19** is the Unique ID.
- **20250130_151915766** is the timestamp.
- **2** is the barcode count (number of barcodes identified).
- **1z91Tk2OTA537YwMDA** is the barcode value (e.g., a tracking number).
- **D:\media-server-images\full...** is the image file path.

Unrecognized Barcode Records

When barcode details do not meet the configured rules (e.g., a rule is set for a MAXI type barcode or the length is to be checked and the tracking ID or barcode value does not meet the configured

length), the barcode value is recorded as "????????????????", indicating an unrecognized barcode record.

Example of an unrecognized barcode record:

```
UniqueID,Timestamp,BarcodeCount,BarcodeValue,ImageFilePath
File1Connection18,20250130_151915746,1,????????????????,D:\media-server-images\full\TOP25\2025\01\30\15\File1Connection18_20250130151915746.jpg
```

Note:

If the barcode type and value do not match any configured rules, the entry is not included in the output file unless specifically configured to include such cases.

13 Activity Scheduler

Activity Scheduler feature helps user to schedule an activity covering the schedule downtime with respect to the activity. List of activities that can be scheduled are:

- File Sync
- Tagged Deletion
- Tagging

Note: *These three will be available for scheduling if they are enabled from license. Tagged deletion and tagging will be available if tagging feature is licensed.*

Creating a schedule can be done from Scheduler page as well as Activity scheduler using 'Create New Schedule' link from Activity scheduler page or by clicking '+ 'icon on top right of Scheduler page.

There are two types of Schedules:

- Downtime Schedule
- Customized Schedule

Downtime Schedule are pushed from connected Analytics software. These are the gaps between the active shifts of Analytics software. The user must select at least one schedule to enable the Save button under Activity Scheduler i.e., if the activity scheduler has no activity scheduled, then save button will not activate for assignment.

Note: *User can only assign or un-assign downtime schedules via activity scheduler, but user cannot edit or delete the downtime schedules which exist.*

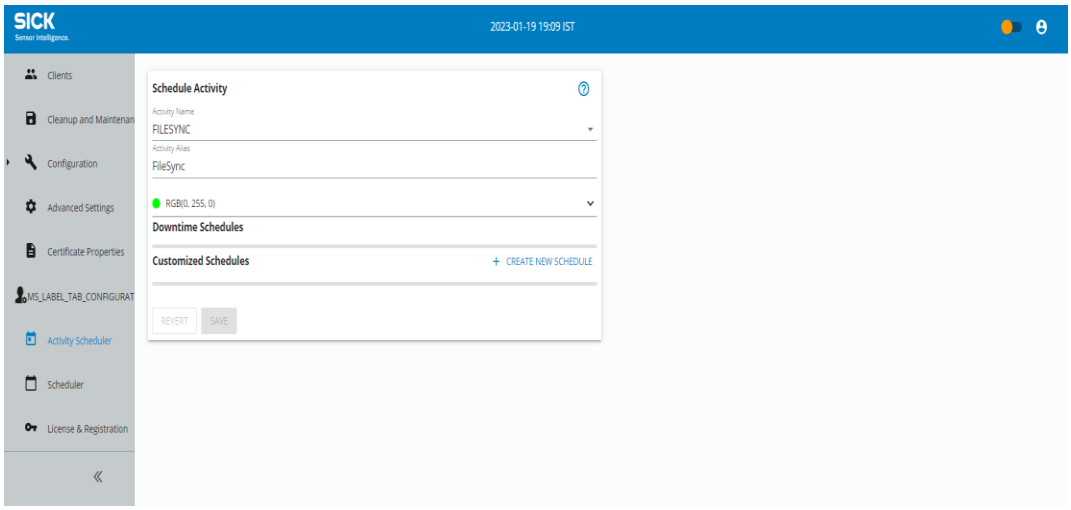


Figure 12.8:1: Activity Scheduler

Customized Schedules:

These are the schedules which user customizes according to the requirement with respect to current or future date and time. Refer to section 12.1 Create Schedule.

14 Scheduler

User can schedule Media Server Activities for specified intervals. These intervals can be configured using scheduler page and called as schedules.

14.1Create Schedule

To create a schedule, select **Scheduler** tab from the menu list on the left side of the screen. Click on "⊕" icon on right side of the screen.

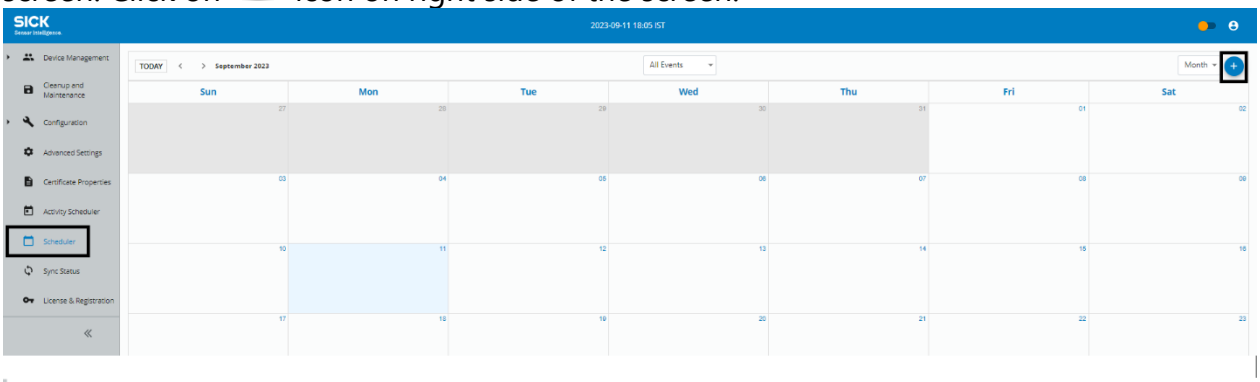


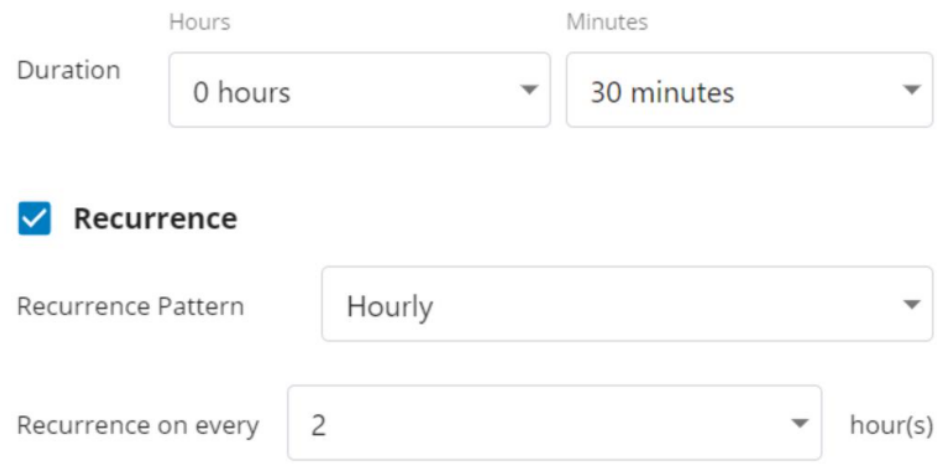
Figure 14.1:1: Scheduler Tab

A '**Create Schedule**' window appears with following fields:

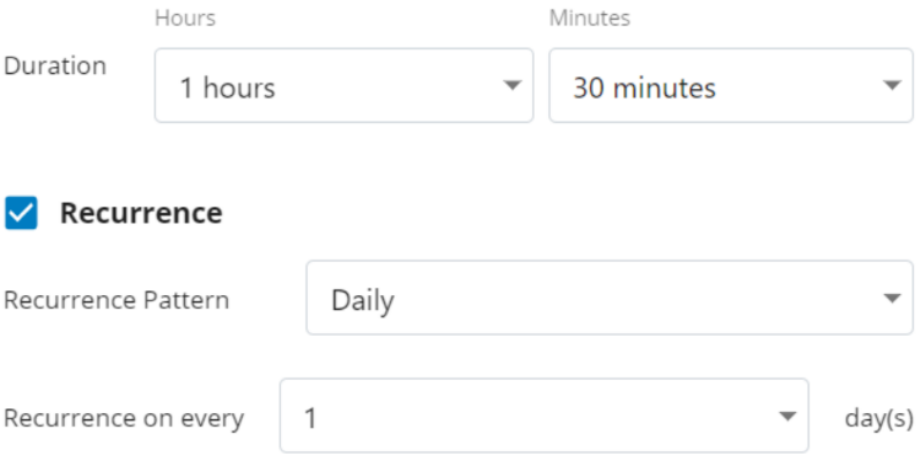
- **Schedule Name**: Provide a name for the schedule.
- **Date & Time**: Select the start date and start time by clicking on the calendar icon ' '.
- **Duration**: Select the hours and minutes from the drop-down. This is the duration for which the schedule will run.
- **Recurrence**: User can check the recurrence checkbox to repeat the schedule.
    - **Recurrence Pattern**: Select the recurrence pattern (When the scheduled activity must repeat) from the drop-down like daily, weekly, monthly, or yearly.

14.2 Working of Recurrence pattern:

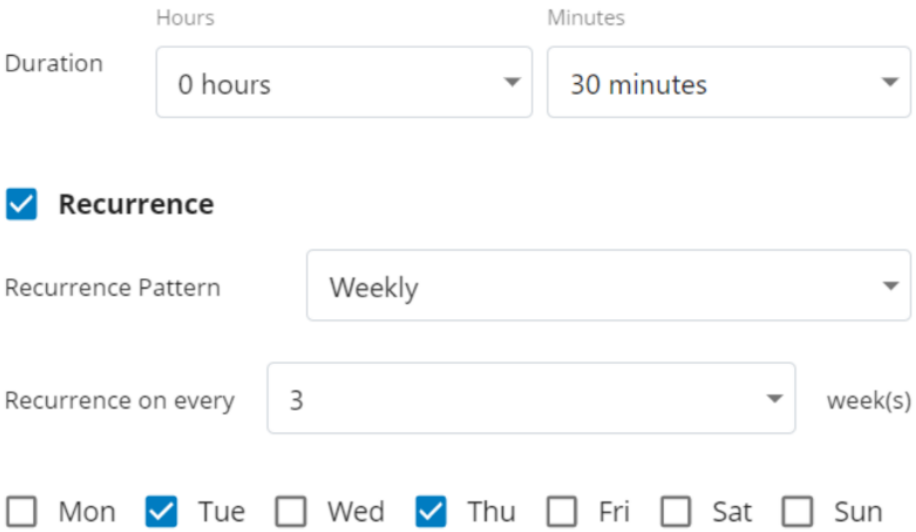
I. **Hourly:** The assigned activity with this schedule will run for the given duration in intervals of 'x' hours. For example, as shown in below image the assigned Activity for this schedule will run for 30 mins every 2 hours from the time the schedule starts.



II. **Daily:** The assigned activity with this schedule will run for the given duration in intervals of 'x' day. For example, as shown in below image, the assigned activity for this schedule will run for 1 hour and 30 mins every day when it is scheduled to start of the schedule.

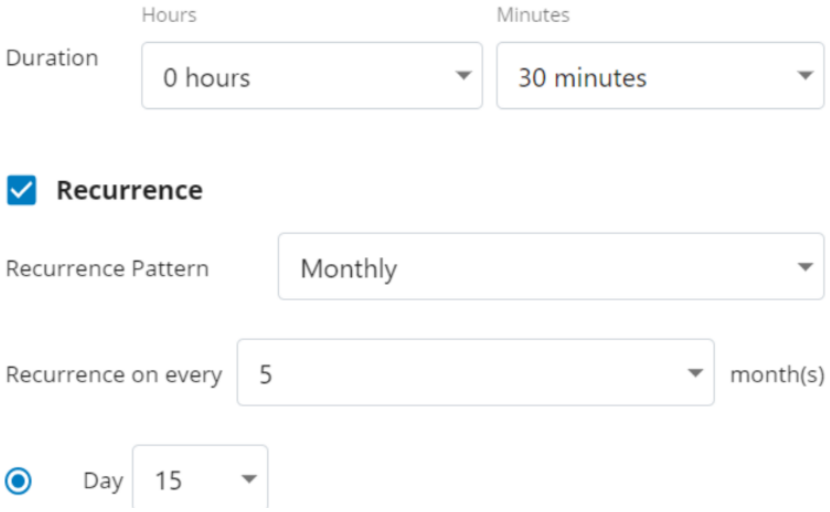


III. **Weekly:** The assigned activity with this schedule will run for the given duration for the selected days of the week in intervals of 'x' week. For example, as shown in below image, the assigned activity for this schedule will run for 30 mins on Tuesday and Thursday every 3 weeks from the start date and time of the schedule.

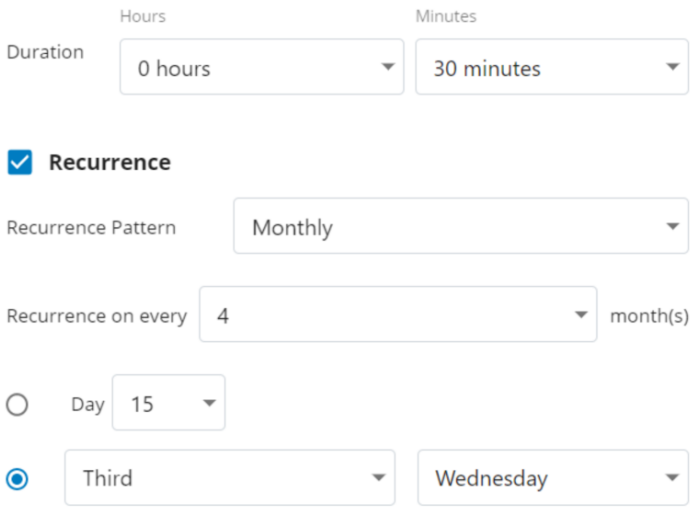


IV. **Monthly**: There are two ways to configure a monthly schedule

a. **By Date**: The assigned activity with this schedule will run for the given duration on the selected date of a month in intervals of 'x' months. In case the month in the activity is supposed to run does not have the said date (For example: Feb does not have 30), that month will be skipped. For example, as shown in below image, the assigned activity for this schedule will run for 30 mins, on the fifteenth day of a month every 5th month from the start date and time of the schedule.

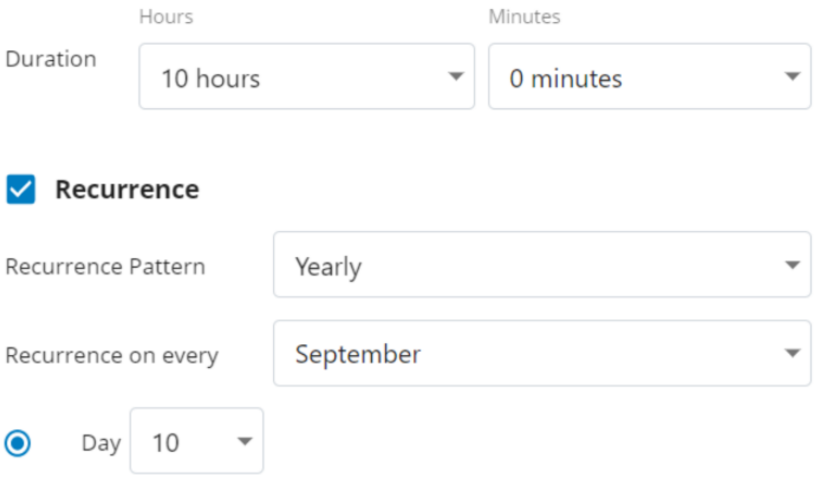


b. **By Day**: The assigned activity with this schedule will run for the given duration on the selected day of a month in intervals of 'x' months. For example, as shown in below image, the assigned activity for this schedule will run for 30 mins, on third Wednesday of a month, every 4th month from the start date and time of the schedule.

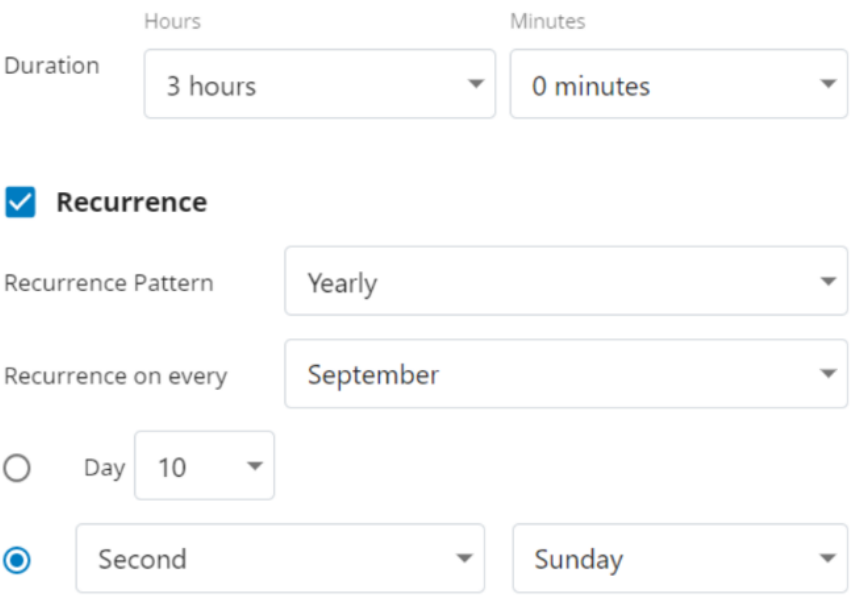


V. **Yearly**: There are two ways to configure a yearly schedule

a. **By Date**: The assigned activity with this schedule will run for the given duration on the selected date of the selected month every year. For example, as shown in below image, the assigned activity for this schedule will run for 10 hours on 10th of September every year from the start date and time of the schedule.



b. **By Day**: The assigned activity with this schedule will run for the given duration on a selected day of the selected month every year. For example, as shown in below image, the assigned activity for this schedule will run for 30 mins on the second Sunday of September every year from the start date and time of the schedule.



- **Recurrence on Every**: Select the number from the drop-down to recur the schedule for selected recurrence pattern.
- **Ending**: User can select either of these three options:
  - **No End Date**: Click on '**No End Date'** radio button if there is no end date of recurrence.
  - **Ending on**: Select a date from the calendar icon ' ' to stop the recurrence.
  - **After**: User can recur the schedule after a specific number of executions by providing a number in the text box.

Click the '**Save**' button.

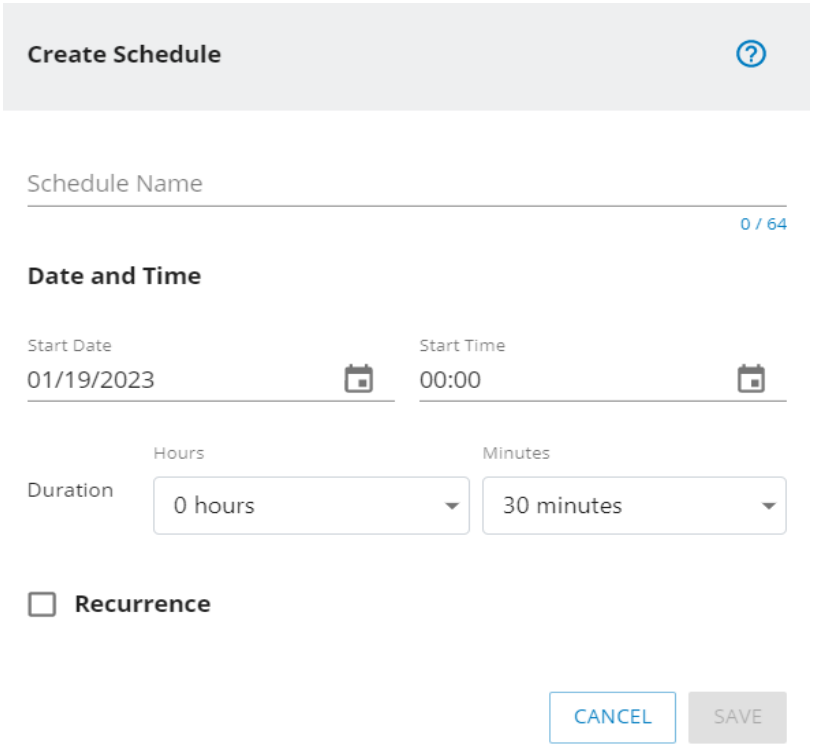


Figure 14.2:1: Create Schedule

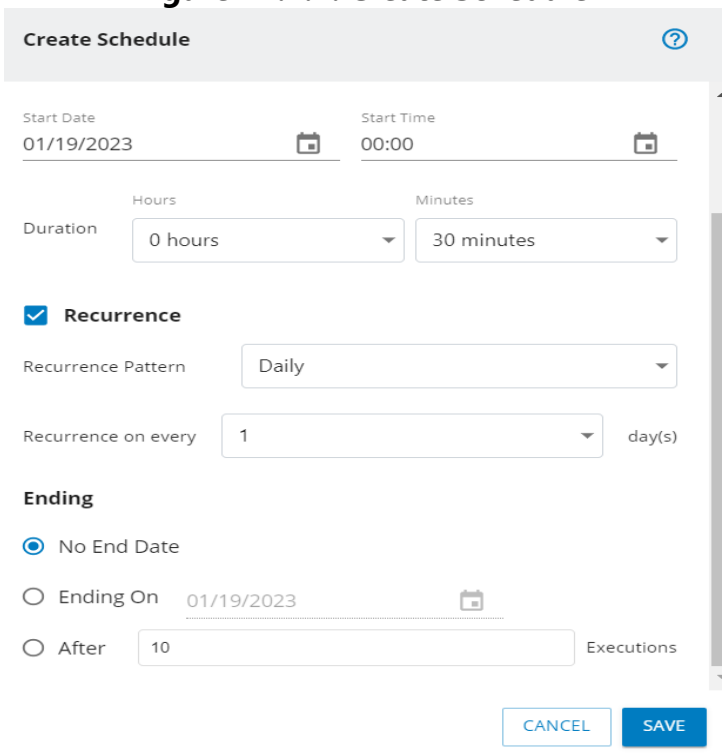


Figure 14.2:2: Recurrence Schedule

Once the schedule is created, it appears in the calendar as shown in below Figure 14.2:1: Create Schedule. User can click on schedule name to edit or delete the schedule.

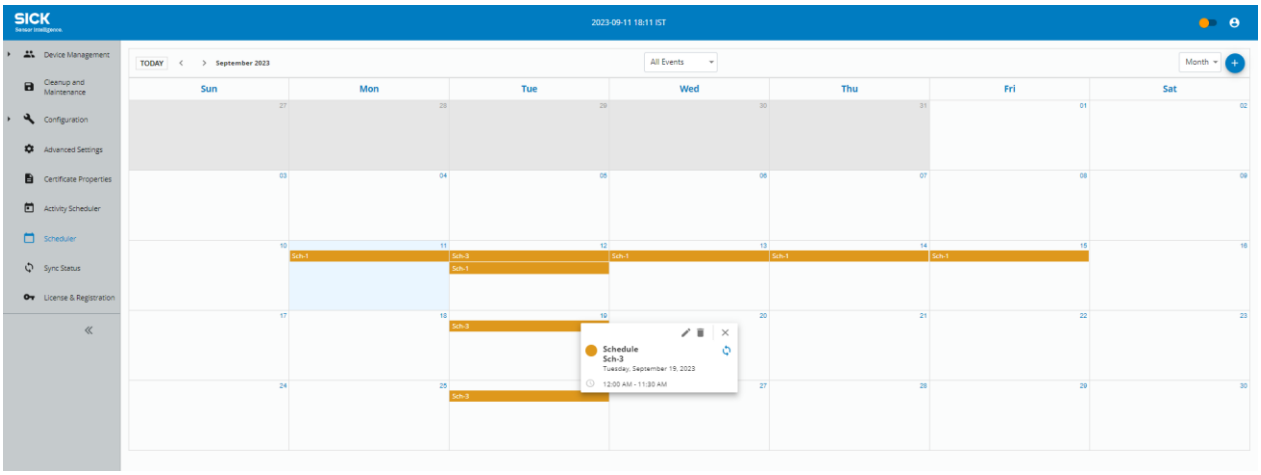


Figure 14.2:3: Created Schedule

14.3 Edit Schedule

When clicked on edit icon ' ', **Edit Schedule** Window appears. Update the changes and click on '**Save**' button.

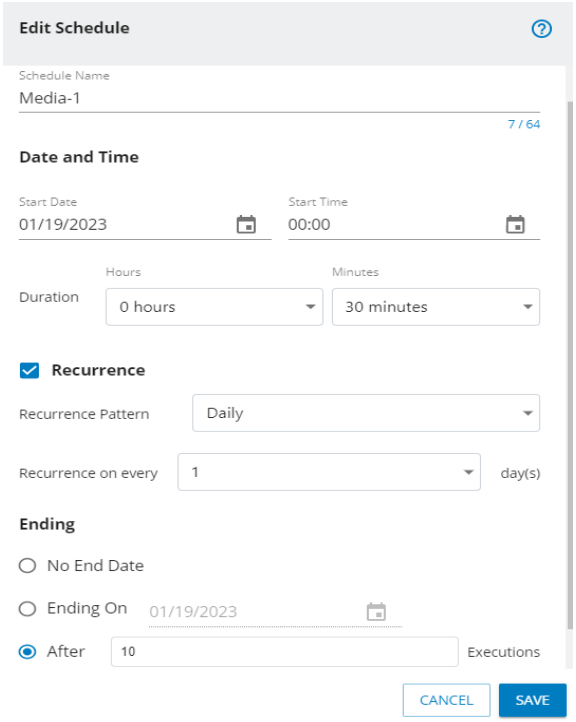


Figure 14.3:1: Edit Schedule

14.4 Delete Schedule

When clicked on delete icon ' ', a confirmation dialog box appears "**Are you sure you want to delete this schedule?"** as shown in Figure 14.4:1: Delete Confirmation**.** Click **'Ok'** to delete the schedule or **'Cancel'** to withdraw the deletion**.**

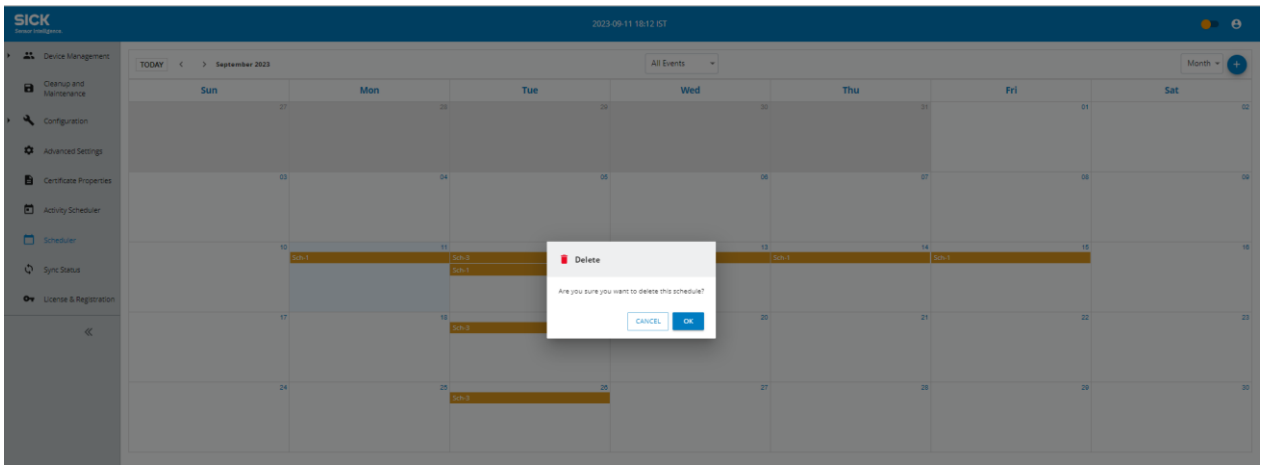


Figure 14.4:1: Delete Confirmation

14.5 Filtering Scheduler

User can filter the schedule by Event types. To filter by event, user can click on drop-down on top center of the screen which has three options '**All Events'**, '**Activity View**' or '**Schedule View'.**

- When **All Events** is selected, it displays all the schedules.
- When **Activity View** is selected, it displays the active schedules in the color defined for the activity in Activity scheduler Page.
- When **Schedule View** is selected, it displays list of all the schedules created.

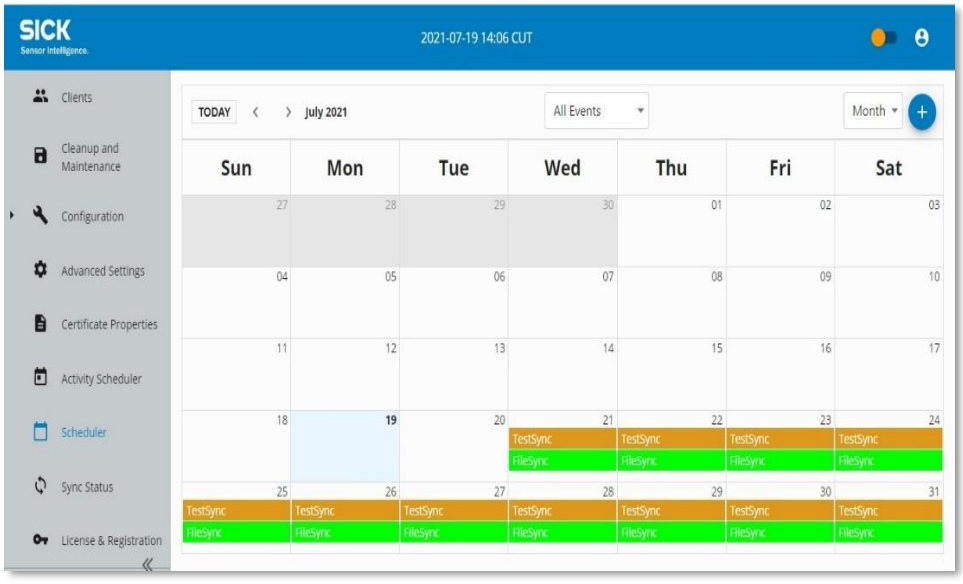


Figure 14.5:1: All Events Filter

User has calendar view for scheduler page. This can be done by clicking on the drop-down at the top right corner of the screen. There are three view options that are Day, Week, Month.

Note: *User can schedule multiple activities and activity schedules for same time frame.*

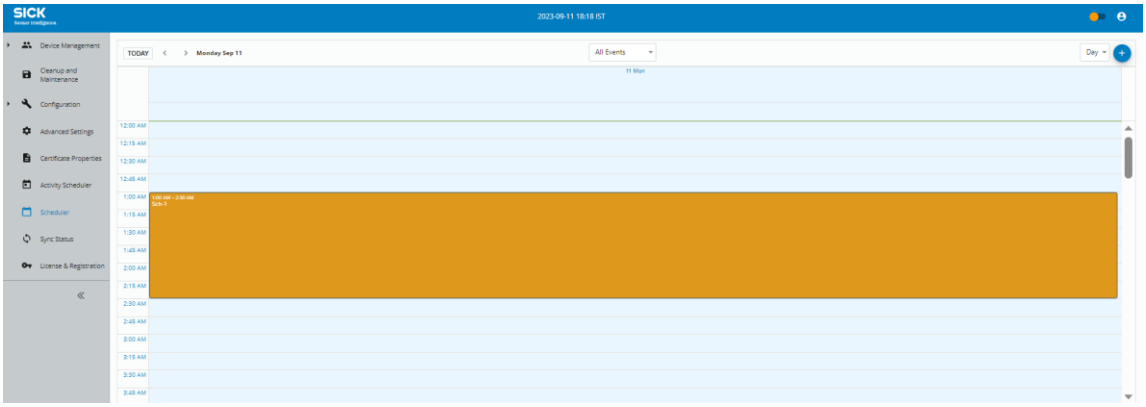


Figure 14.5:2: Time Based Filter

15 Tagging

Tagging Features is used to classify the acquired images by media server using the Neural network models into various categories based on their classifications and confidence score.

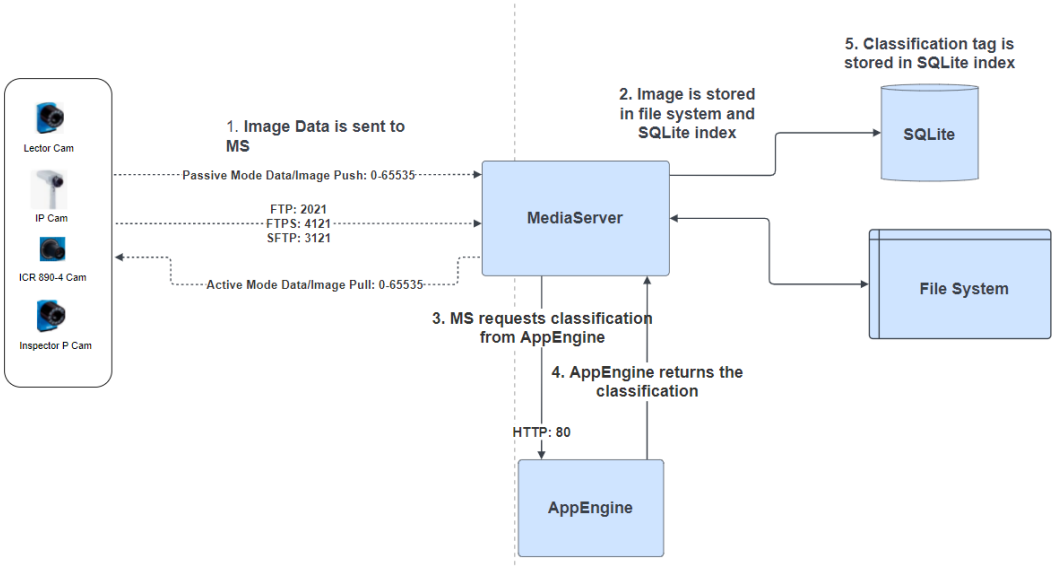


Figure 14.5:1: Network Diagram of Tagging

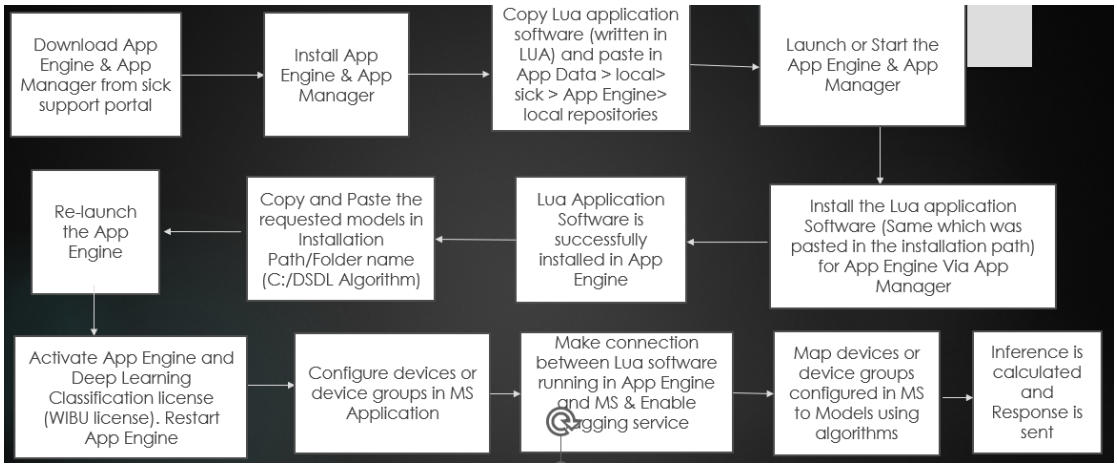


Figure 14.5:2: Tagging Workflow

15.1 Prerequisites

1 Download App Engine and App Manager from sick support portal https://supportportal.sick.com/
2 Procure Lua Application Software from Sick team
3 Procure Algorithm Models from Sick team

Note: *Configuration of App Engine & App Manager for Windows must be done in the same machine where the media server is installed.*

15.2 Installation of App Manager

1 Unzip the Sick App Manager Installer file “SICK-AppManager-1.5.6-installation-file-(Windows, -64-bit)”

2 Click the App Manager Application file. Refer to Figure 15.2:1: App Manager Application File

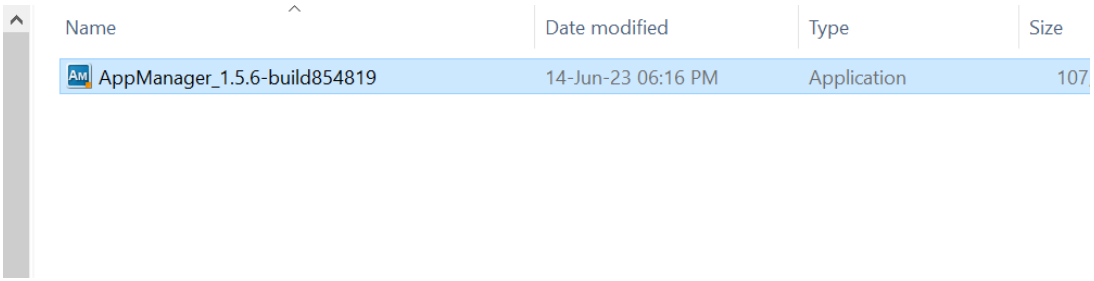


Figure 15.2:1: App Manager Application File

3 Sick App Manager Setup Wizard window appears. Click the **Next** button

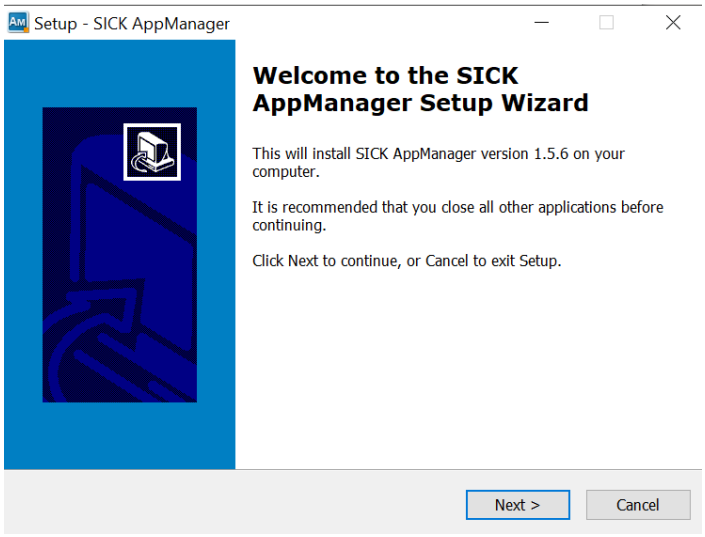


Figure 15.2:2: App Manager Setup Wizard

4 License Agreement Window appears. Select “**I accept the agreement**” radio button then click the **Next** button

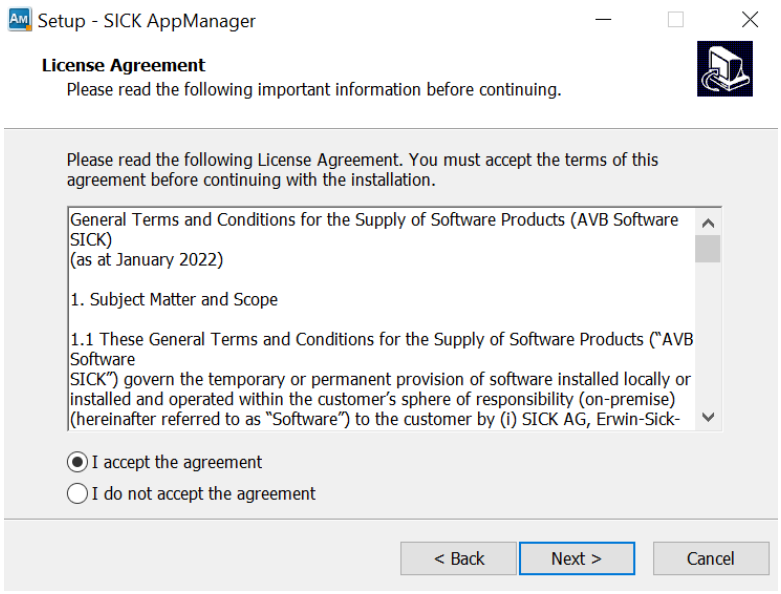


Figure 15.2:3: License Agreement

5 Select Destination location window appears. Browse the location for App manager to be installed by clicking the **Browse** button then click the **Next** button

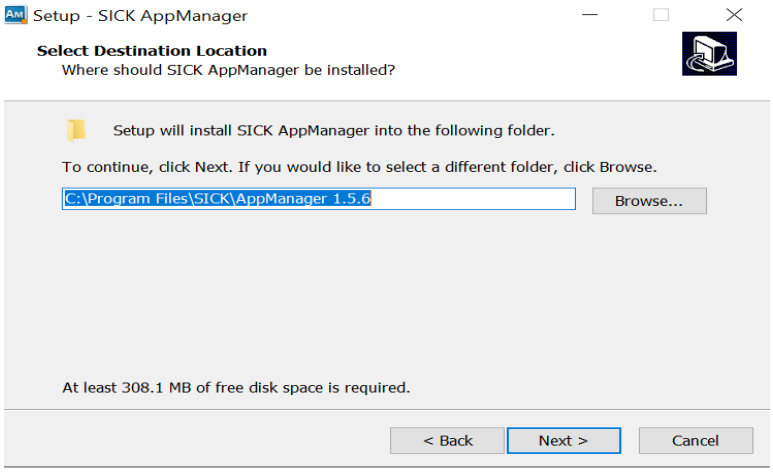


Figure 15.2:4: Destination Location

6 Select Start Menu Folder window appears. Click the **Next** button

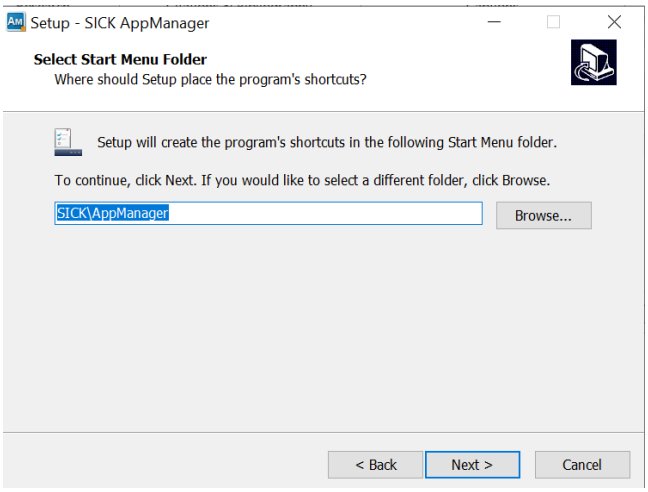


Figure 15.2:5: Start Menu Folder

7 Select Additional Tasks Window appears. Check the **Create desktop icon** check-box then click the **Next** button

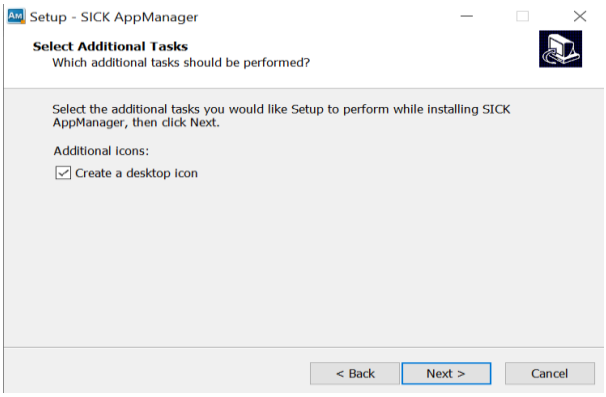


Figure 15.2:6: Select Additional Tasks

8 Ready to Install window appears. Verify all the settings and click the **Install** button

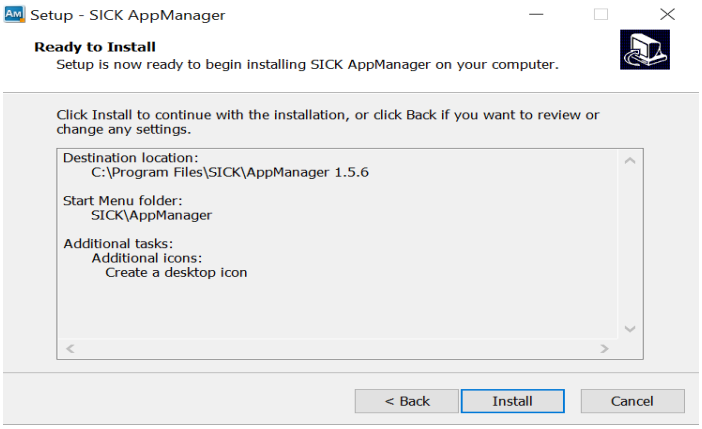


Figure 15.2:7: Ready to Install

9 Click the **Finish** button to complete the installation

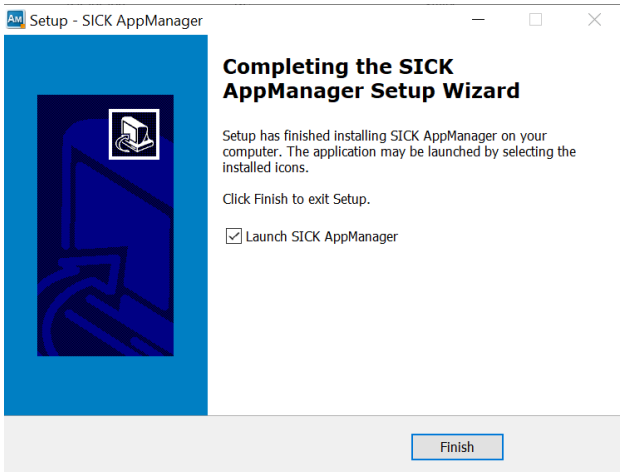


Figure 15.2:8: Complete Installation

10 App Manager is successfully installed

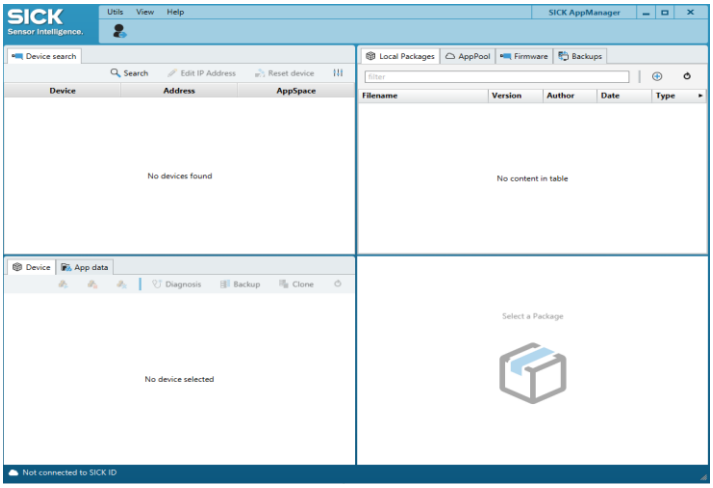


Figure 15.2:9: App Manager

15.3 Installation of App Engine

1 Unzip the Sick App Engine installer “SickAppEngine_1.4.0_Windows_x86_64_Release”

2 Click the App Engine Application file. Refer to Figure 15.3:1: App Engine Application File

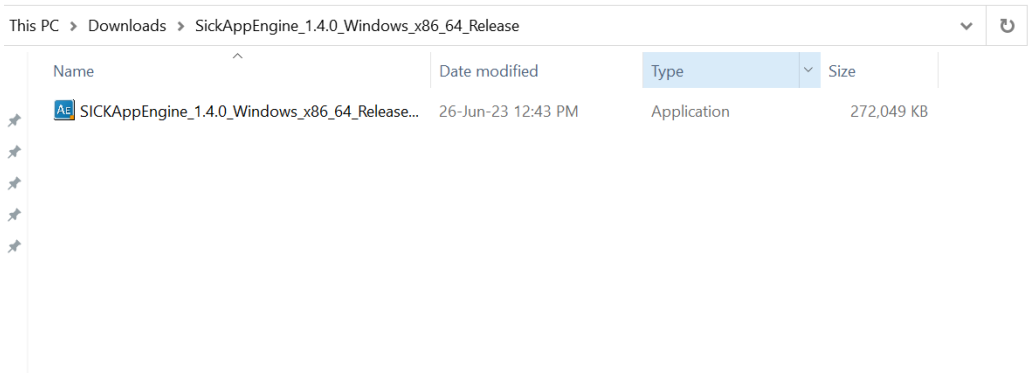


Figure 15.3:1: App Engine Application File

3 Sick App Engine Setup Wizard window appears. Click the **Next** button

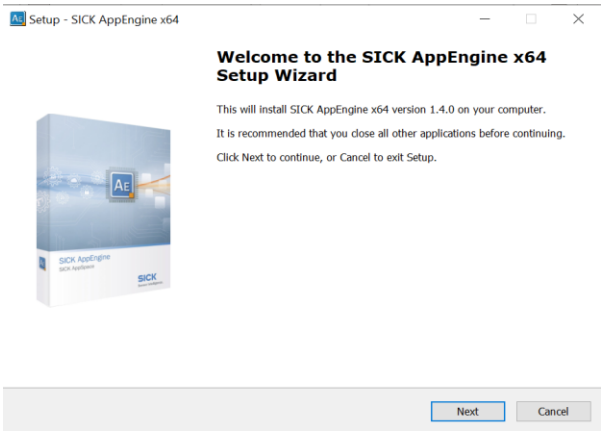


Figure 15.3:2: App Engine Setup Wizard

4 License Agreement Window appears. Select "**I accept agreement**" radio button then click the **Next** button

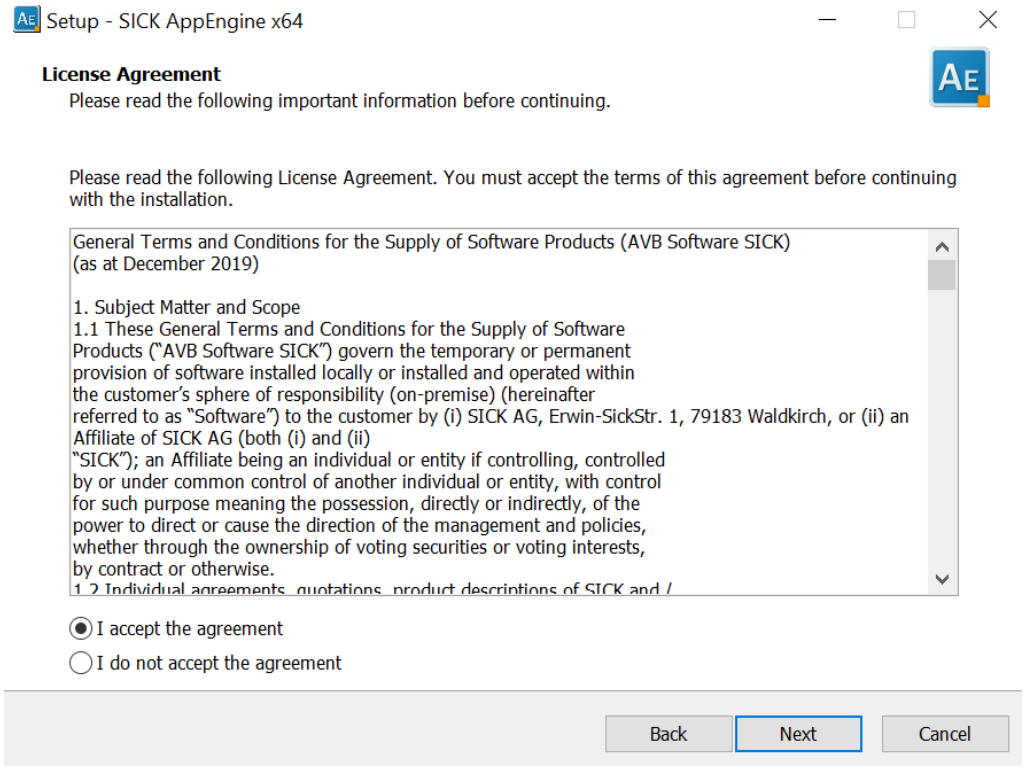


Figure 15.3:3: License Agreement Window

5 Select Destination location window appears. Browse the location for App manager to be installed by clicking the **Browse** button then click the **Next** button

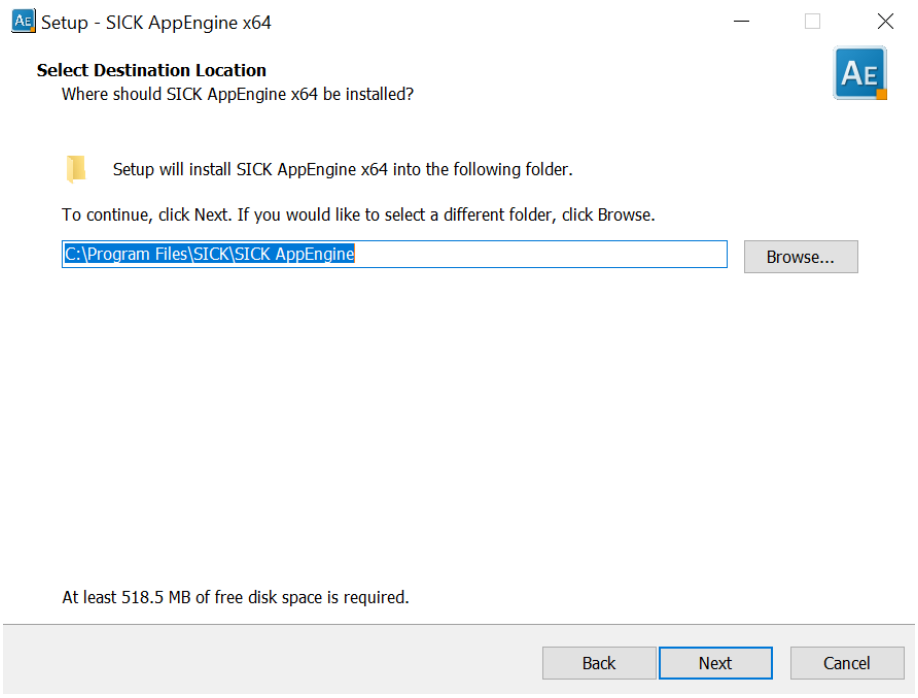


Figure 15.3:4: Destination Location Window

6 Ready to Install window appears. Verify all the settings and click the **Install** button

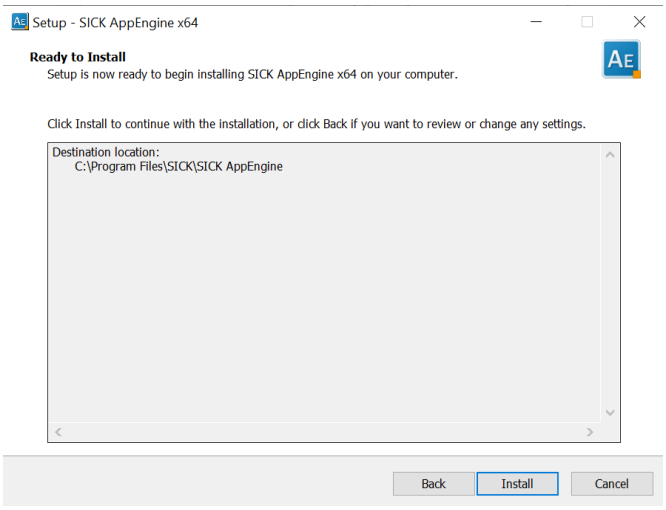


Figure 15.3:5: Ready to Install

7 Click the **Finish** button to complete the installation

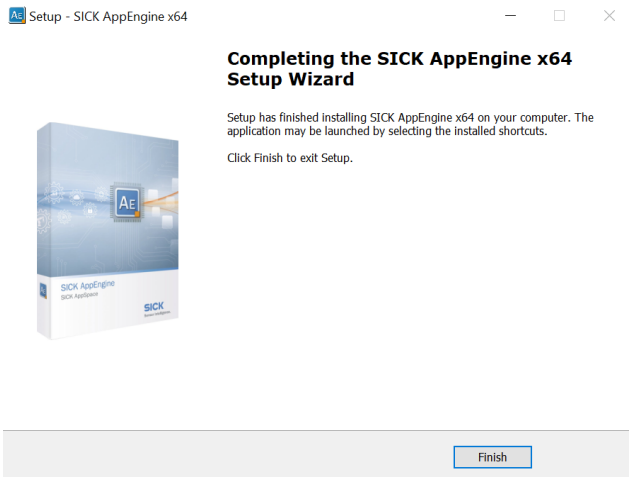


Figure 15.3:6: Installation Complete

8 Navigate to install location and double click on AppEngine.exe icon to launch App Engine

9 App Engine is successfully installed

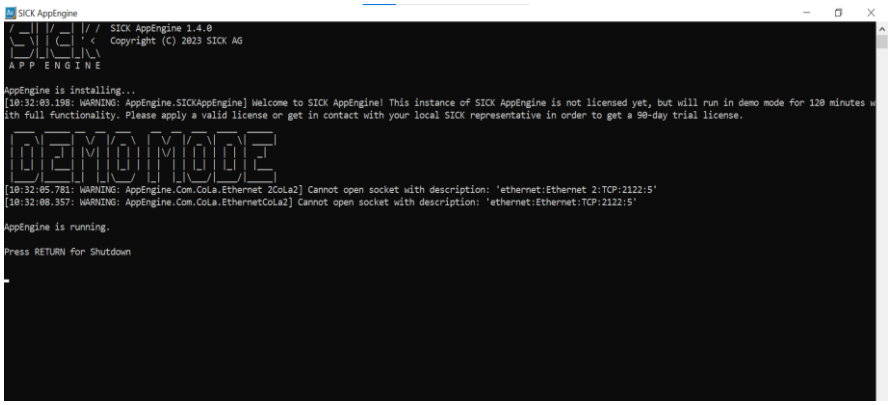


Figure 15.3:7: App Engine

Note: *User needs to start the App Engine manually by double-clicking on the app or manually create a service as it does not run as a service.*

15.4 Tagging Procedure

1 Copy and paste the Lua application software procured from Sick in below path:
   I. C://Users/ {User}/App Data > local> sick > App Engine> local repositories
2 Launch App Engine and then App Manager applications
3 Select App Engine in the App manager application under the detected devices
4 Select Lua application under local packages
5 Click the Install button

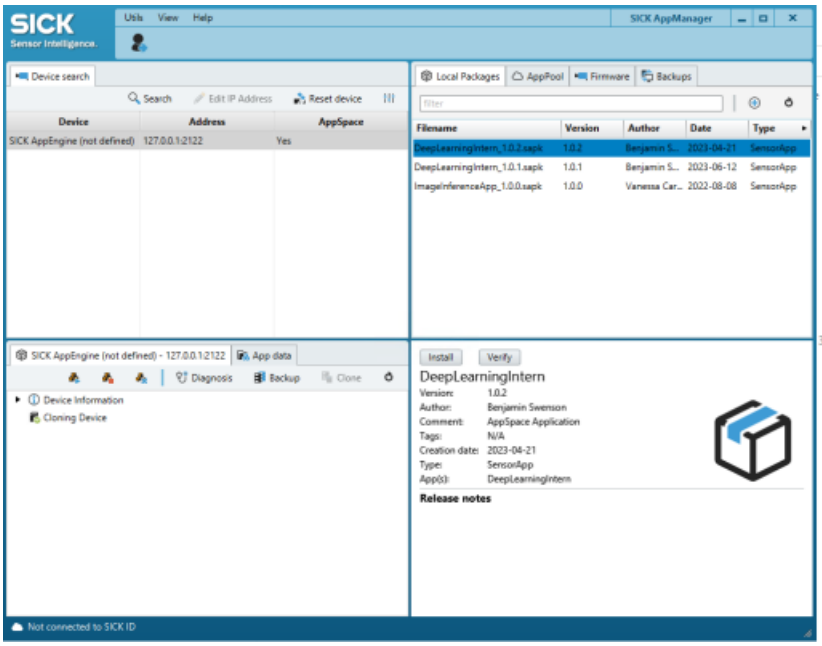


Figure 15.4:1: Lua application

6 Validation success message appears. Click **Ok**

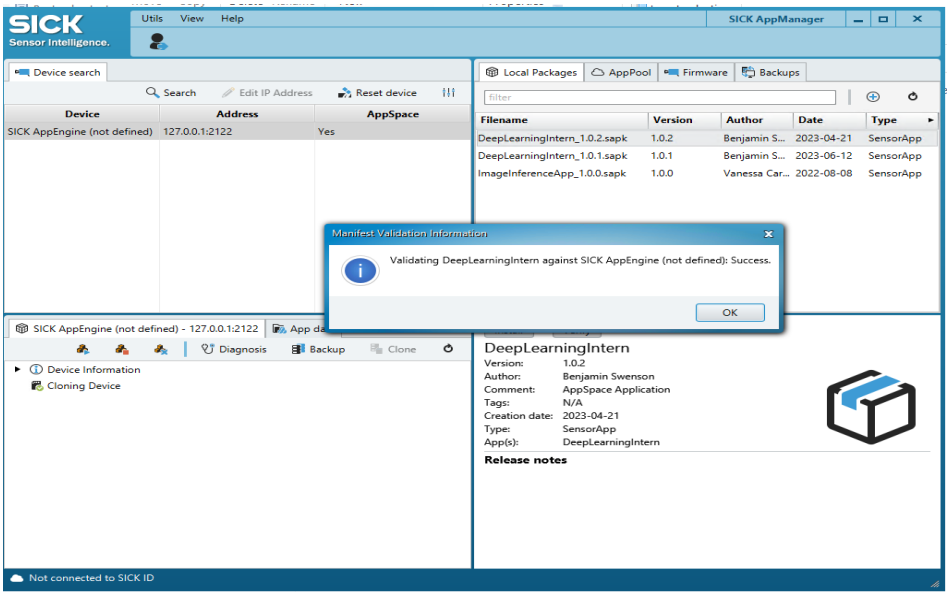


Figure 15.4:2: Validation Success Message

7 A confirmation dialog box appears. Click the **Ok** button to continue

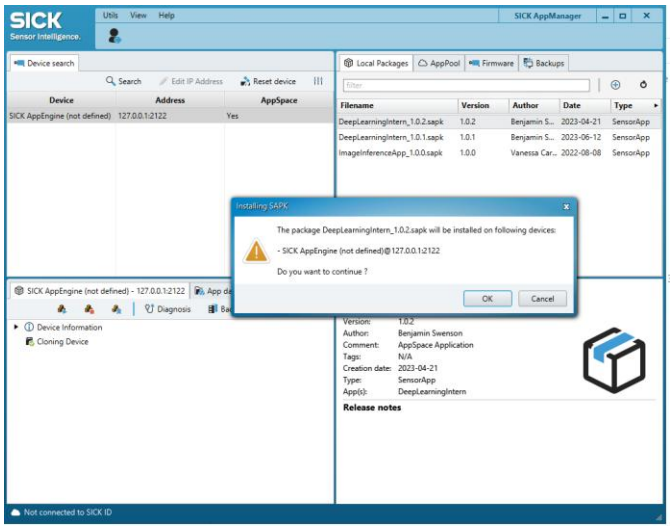


Figure 15.4:3: Installing SAPK Confirmation

8 Installation of Lua application on App Engine starts

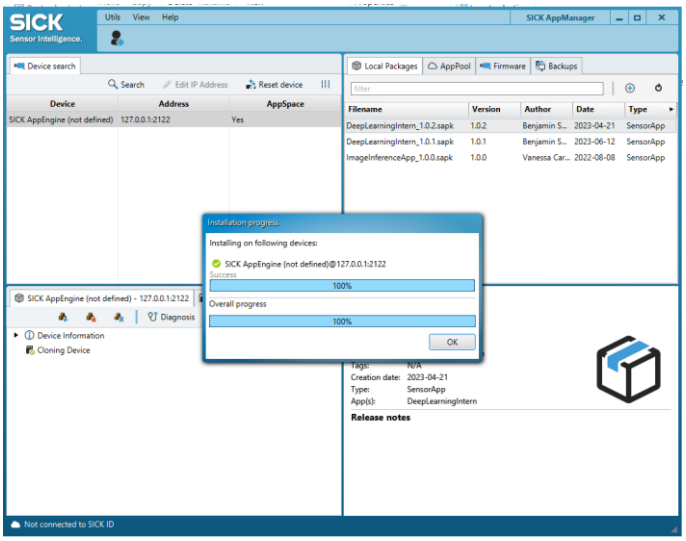


Figure 15.4:4: Installing Software in App Engine

9 Lua application successfully installed on App Engine

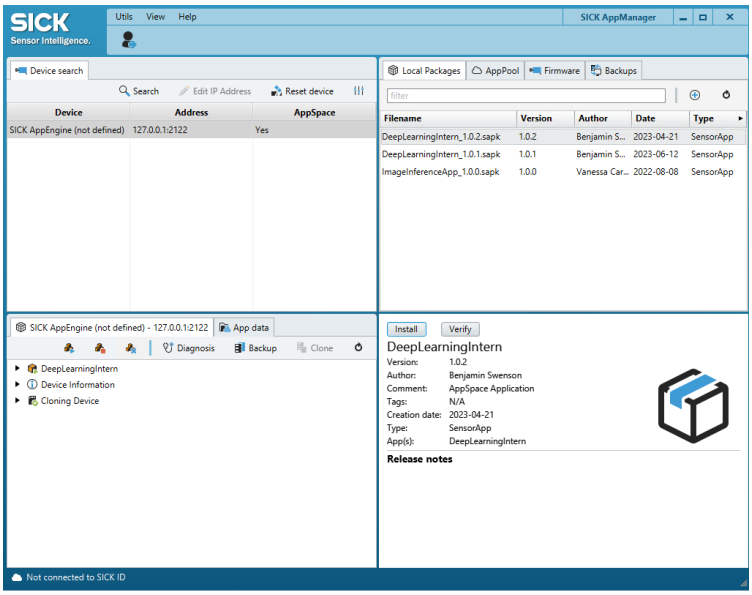


Figure 15.4:5: Application Successfully Installed on App Engine

10 Copy and paste the procured models in below path:

I. C:/DSDL Algorithm

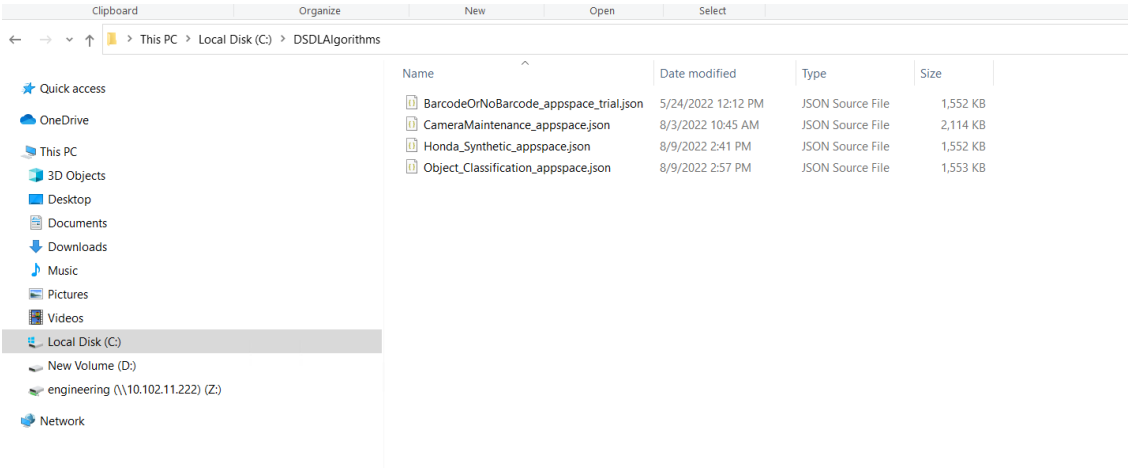


Figure 15.4:6: Models

11 Close App Engine application and start it again

12 Activate App Engine and Deep Learning Classification License (WIBU License). Refer to Sick Support Portal link https://supportportal.sick.com/tutorial/sick-appengine-getting-started/ for activating WIBU license

13 Login to Sick Media Server application portal with authorized credentials

14 Configure Device or Device groups. Refer to Device and Device Group.

15 Create connection between Lua application running in App Engine and Media Server using following steps:

I. Stop Media Server Services

II. Set ENABLED=true under TAGGING_SERVICES in sick_bip-is.cfg file to enable tagging feature

III. If App Engine is running in different machine or port, navigate to IMAGE_INFERENCE_APP and set HTTP_IP as IP where App Engine is running and HTTP_PORT as the port in which App Engine is running

```
[TAGGING_SERVICE]
ENABLED=false

[IMAGE_INFERENCE_APP]
;This indicates if image inference app has https support.By Default this will be false.
HTTPS_SUPPORT=false

;The HTTPS IP Address where the AppEngine Image Inference App is running
HTTPS_IP=

;The HTTPS Port where the AppEngine Image Inference App is running
HTTPS_PORT=

;The HTTP IP Address where the AppEngine Image Inference App is running
HTTP_IP=127.0.0.1

;The HTTP Port where the AppEngine Image Inference App is running
HTTP_PORT=80

;API to get Algorithms from AppEngine
ALGORITHM_API=/api/crown/DeepLearningIntern/getAlgos

;API to get the inferences from AppEngine
INFERENCE_API=/api/crown/DeepLearningIntern/multiModelInference

[TAGGING_INTERVALS]
; The Image Tagging is done in batches of this specified interval. The minimum value can be 1H and maximum 30D. By default it will be 1D.
BATCH_INTERVAL=1D

; The Image Tagging calculates the timestamp of the oldest untagged imgage for each User
; It refreshes this timestamp value at THIS interval so it doesnt miss anything. By default it will be 1H.
OLDEST_TS_INTERVAL=1H
```

Figure 15.4:7: Enabling Tagging Service

Note: *App engine does not provide HTTPS support. Therefore, update IP/Port as per the location where app engine is running.*

16 Map device or device groups configured in media server to models using algorithms under ALGORITHM_MAPPING section

Note*: In current version UI support to map device/group with algorithms is not available. Hence, this mapping needs to be done manually.*

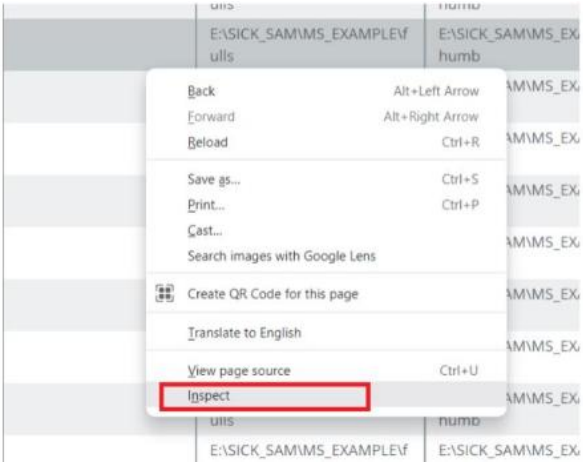
```
[GROUPS]
{f2b62cdd-b864-11ed-8d4b-003064456da5}=IPCam 1txt Group
OutOfSync:{673e3f19-2ada-11ed-939c-003064456da5},{676464cd-2ada-11ed-939c-003064456da5},{678a8a77-2ada-11ed-939c-003064456da5},{67b0b035-2ada-11ed-939c-003064456da5},{684ba955-2ada
-11ed-bfb7-003064456da5},{686d0a5f-2ada-11ed-bb9c-003064456da5},{688e6b5f-2ada-11ed-bb9c-003064456da5}
{2e3ae220-b865-11ed-becd-003064456da5}=ICR
Group:{65f9fe8b-2ada-11ed-b1ac-003064456da5},{6648ac4d-2ada-11ed-b1ac-003064456da5},{667f8295-2ada-11ed-b1ac-003064456da5},{66b8bb0f-2ada-11ed-a089-003064456da5},{66dee0cd-2ada-11e
d-a089-003064456da5},{6705069f-2ada-11ed-a089-003064456da5},{672b2c35-2ada-11ed-939c-003064456da5}
{4620ef74-b865-11ed-85da-003064456da5}=IPCam 1txt Group
regular:{660d0fcb-2ada-11ed-b1ac-003064456da5},{66359973-2ada-11ed-b1ac-003064456da5},{666ed20b-2ada-11ed-b1ac-003064456da5},{66a80a99-2ada-11ed-a089-003064456da5},{66cbcde9-2ada-1
1ed-a089-003064456da5},{66f1f3b1-2ada-11ed-a089-003064456da5},{6718196f-2ada-11ed-a089-003064456da5}
{57746257-b865-11ed-920d-003064456da5}=IPCam 2txt Group:{65046bc9-2ada-11ed-9d85-003064456da5},{652a917d-2ada-11ed-9d85-003064456da5},{6563ca15-2ada-11ed-8436-003064456da5}
{df8ecce5-beb4-11ed-a6cd-003064456da5}=ICR Group Size Based:{64d98161-2ada-11ed-9d85-003064456da5},{65151c49-2ada-11ed-9d85-003064456da5}
{f7018917-beb4-11ed-9436-003064456da5}=ICR Group Size Based Common:{6705069f-2ada-11ed-a089-003064456da5},{672b2c35-2ada-11ed-939c-003064456da5}
{0eb48d2f-beb5-11ed-a0ec-003064456da5}=IPCam 1 txt Group Size Based:{64eef695-2ada-11ed-9d85-003064456da5},{653da457-2ada-11ed-9d85-003064456da5}
{358ea13d-beb5-11ed-8bea-003064456da5}=IPCam 1 txt Group Size Based Common:{66f1f3b1-2ada-11ed-a089-003064456da5},{6718196f-2ada-11ed-a089-003064456da5}
{131cb7f3-e047-11ed-b574-003064456da5}=ICR Inference
Group:{679d9d5b-2ada-11ed-939c-003064456da5},{67c887b9-2ada-11ed-bfb7-003064456da5},{67eead81-2ada-11ed-bfb7-003064456da5},{6814d123-2ada-11ed-bfb7-003064456da5}
{3dcb6b6b-e047-11ed-a895-003064456da5}=Inspector Group:{26c9bc96-e047-11ed-b7fe-003064456da5},{2d197b2c-e047-11ed-91a2-003064456da5},{33379fad-e047-11ed-b3e8-003064456da5}
{ab7a4641-c431-11ed-8557-003064456da5}=Other
Group:{26c9bc96-e047-11ed-b7fe-003064456da5},{2d197b2c-e047-11ed-91a2-003064456da5},{33379fad-e047-11ed-b3e8-003064456da5},{43d344ec-d061-11ed-a5d5-003064456da5},{648d35ef-2ada-11e
d-99b0-003064456da5},{649de683-2ada-11ed-99b0-003064456da5},{64b35ba3-2ada-11ed-99b0-003064456da5},{64c66e7d-2ada-11ed-9d85-003064456da5},{659d02a3-2ada-11ed-8436-003064456da5},{67
9d9d5b-2ada-11ed-939c-003064456da5},{67c887b9-2ada-11ed-bfb7-003064456da5},{67eead81-2ada-11ed-bfb7-003064456da5},{6801c051-2ada-11ed-bfb7-003064456da5},{6814d123-2ada-11ed-bfb7-00
3064456da5},{6827e60f-2ada-11ed-bfb7-003064456da5},{68f4f0af-2ada-11ed-9992-003064456da5},{6918b413-2ada-11ed-9992-003064456da5}

;This section provides the available ruletypes and corresponding priority
[RULE_TYPES]
MAX_COUNT=1
MAX_SPACE=2

[ALGORITHM_MAPPING]
{131cb7f3-e047-11ed-b574-003064456da5}=BarcodeOrNoBarcode_appspace.json,Object_Classification_appspace.json
{3dcb6b6b-e047-11ed-a895-003064456da5}=CameraMaintenance_appspace.json,Honda_Synthetic_appspace.json

[ACTION_CRITERIA]
{131cb7f3-e047-11ed-b574-003064456da5}=[DELETE,Box,LT,60];[DELETE,No Crack,NEQ,100];[DELETE,Polybag,NBET,96,100];[DELETE,Bin,BET,0,60];[DELETE,Forever Bag,LTE,59]
{3dcb6b6b-e047-11ed-a895-003064456da5}=[DELETE,Box,LT,60];[DELETE,No Crack,NEQ,100];[DELETE,Polybag,NBET,96,100];[DELETE,Bin,BET,0,60];[DELETE,Forever Bag,LTE,59]
```

Figure 15.4:8: Mapping Algorithms to Device/Device Groups

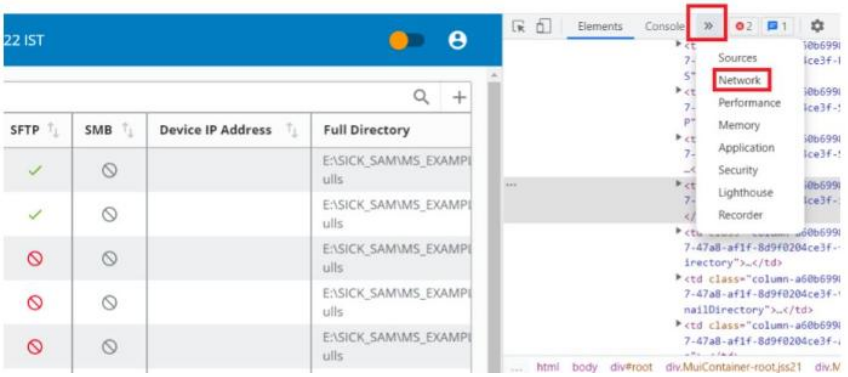
17 Steps to be followed for Algorithm Mapping are shown below:

I. Login to Media server application

II. Right click on the logged in page and select "**inspect"** from the options

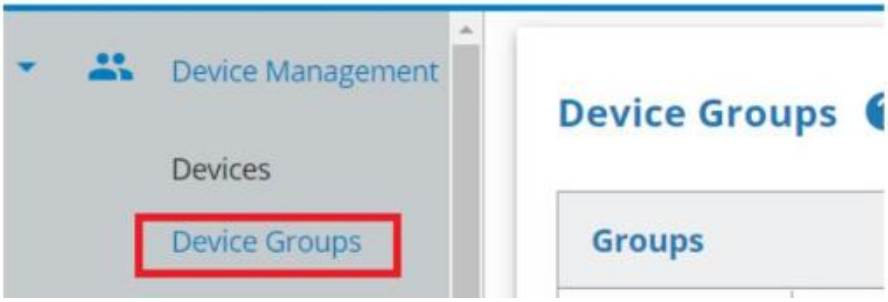


III. A Panel will open on the right side. Select the "**>>**" symbol and click "**Network**" from the options



IV. To get the UIDs of the devices/groups follow the below steps:

a. Select "**Devices Groups**" from the UI



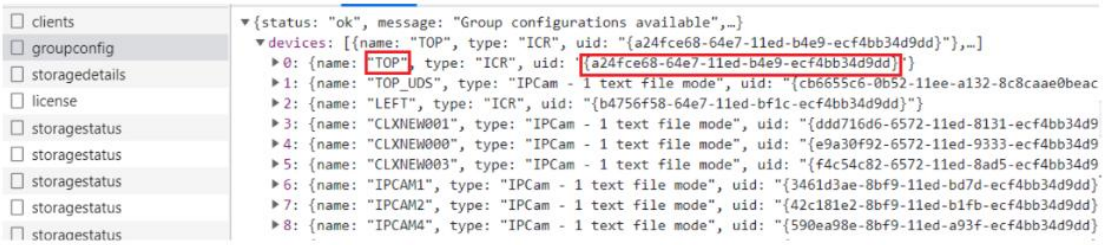
b. In the network tab, click on "**groupconfig"**

c. Select "**Preview**"

d. To get UIDs for devices select "**devices**"

e. The UID for a given device can be chosen from the list by selecting "devices"

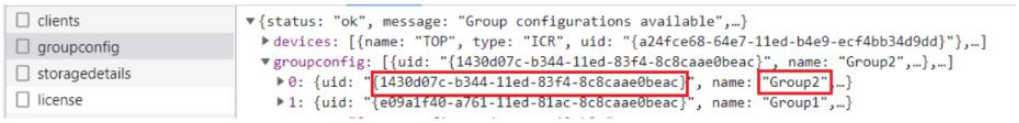
15. For Example: The UID for the device "TOP" is {a24fce68-64e7-11ed-b4e9-ecf4bb34d9dd}



f. To get the UIDs for groups select" groupconfig"

g. The UID for a given group can be chosen from the list by selecting "groupconfig"

16. For Example: The UID for the group "Group2" is {1430d07c-b344-11ed-83f4-8c8caae0beac}.



18 To get the algorithm names go to the folder "**C:/DSDL Algorithm** " where the models are saved as mentioned in section 13.4 step 10

19 Once the UID and algorithm details are available add the mapping in the **sick-bip-is.cfg** file under a section "**ALGORITHM_MAPPING**". One or more algorithms can be mapped to a device/group. The UID of device/group is the key (the left-hand value) and the algorithm/s is the value(or the right-hand value). Multiple algorithms for the same device/group are delimited by comma ",". Below is an example:

```
[ALGORITHM_MAPPING]
{131cb7f3-e047-11ed-b574-003064456da5}=BarcodeOrNoBarcode_appspace.json,Object_Classification_appspace.json
{3dcb6b6b-e047-11ed-a895-003064456da5}=CameraMaintenance_appspace.json,Honda_Synthetic_appspace.json
```

20 Inference is calculated and response is sent

16 Certificate Properties

Media Server uses certificate for secured (FTPS/SFTP/HTTPS/File Sync) file transfer. **Certificate** tab displays currently used certificate properties and status. This tab will not be available if there are no secured protocols (FTPS/SFTP/HTTPS/File Sync) licensed.

Note:

- *All the secured file transfer servers will be stopped if the certificate is not configured or is invalid or expired. Default certificate will be installed with Media Server 1.5.*
- *MS patching will update the certificate if the previous install has default sick certificate.*

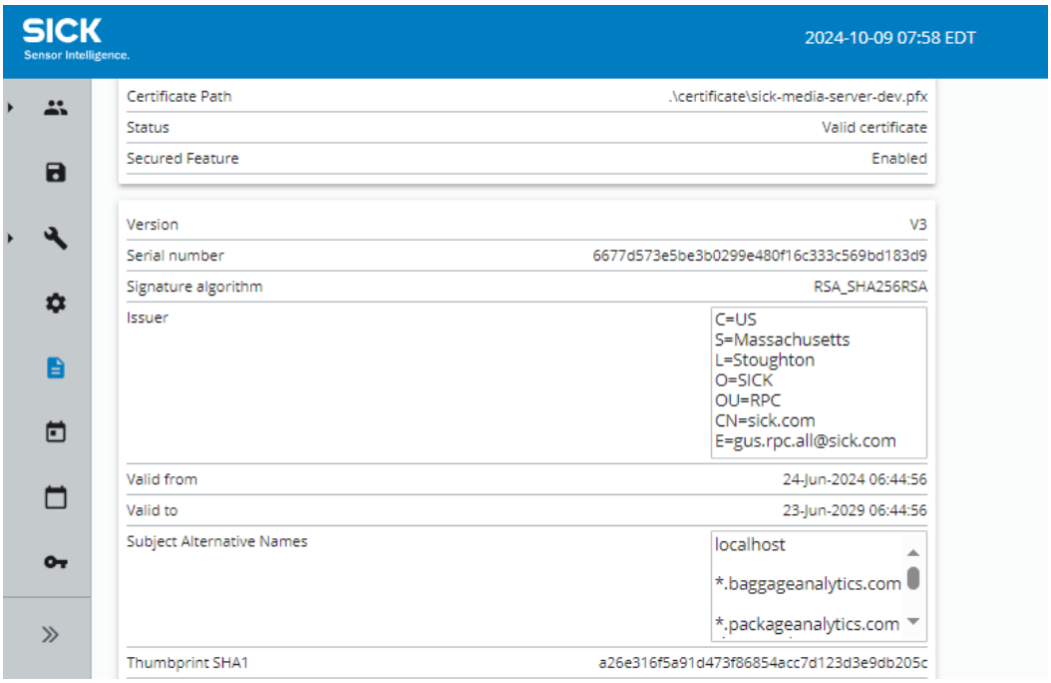


Figure 15.4:1: Certificate Properties Tab

User can manually configure certificate properties from configuration file. From configuration file update certificate path and the encrypted password under [CERTIFICATE] section.

If the format is PEM, then below shown path will be the configuration:

```
;PEM Certificate File Path
;path for public key
CERTIFICATE_KEY=C:\Program Files\SICK\Analytics Solutions\MediaServer\Windows x64\certificate\server.crt

;PEM private Key File Path
PRIVATE_KEY=C:\Program Files\SICK\Analytics Solutions\MediaServer\Windows x64\certificate\server.key
```

If the format is PFX, then below shown path will be the configuration:


```
[CERTIFICATE]
;PFX Certificate File Path
CERT_PATH=C:\MS\Windows x64\sick-media-server-dev.pfx

;PFX Certificate password
CERT_PASSWORD=XJ3YcRNe54st9vEHrfnUM6l01brd7aFse+3nUNFZYHB2iLv0QluSiu0jS7Zd3+aa0BSAaSyMh4y7IHZ4zeJD9Q==
```

Figure 15.4:2: Setting certificate path and password in configuration file

Note: *Media server only supports pfx/p12 and pem type of certificates.*

Setting	Description
Certificate Path	Indicates the path of the currently used certificate
Status	Status indicates whether the certificate is Valid/In-valid/Expired.
Secured Feature	Secured feature has to enable by default.
Version	Current version of the certificate.
Serial number	Serial number of the certificate.
Signature algorithm	Algorithm used to sign certificate public key.
Issuer	Provides details about the issuer.
Valid from	The date from which the certificate is valid.
Valid to	The date when certificate will expire.
Subject Alternative Names	SAN denotes multiple host names that are pro-tected by the certificate for security.
Thumbprint SHA1	A hexadecimal string generated using Secure Hash Algorithm 1, to identify a certificate uniquely.

Setting	Description
Thumbprint SHA256	A hexadecimal string generated using Secure Hash Algorithm 1, to identify a certificate uniquely.
Thumbprint MD5	A hexadecimal string generated using Message-Digest Algorithm-5, to identify a certificate uniquely.
Fingerprint	Fingerprint is the hash function of certificate in X509 binary format.

Table 12: Certificate Settings

Conditions due to which the Certificate becomes invalid:

1. In case incorrect path / password is entered, the certificate properties will not be available, and Status displayed with an invalid error message.

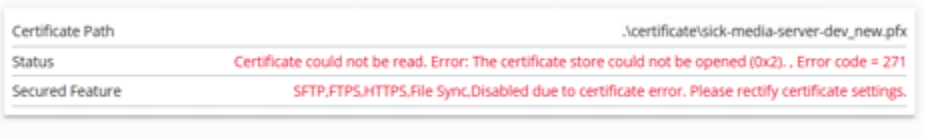


Figure 15.4:3: Certificate Properties Tab with Invalid Certificate Error

2. If the certificate is expired, available properties will be displayed along with the status message “Certificate expired” in red.

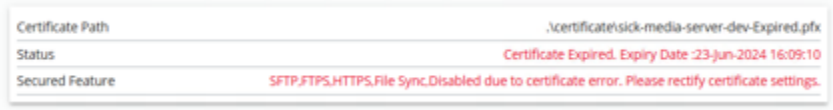


Figure 15.4:4: Certificate Properties Tab with expired Certificate Error

Note: *The secured features (FTPS/SFTP /HTTPS/File sync) will be supported only if the certificate is valid and Certificate properties tab will be shown if any of the secured transfer protocols are licensed.*

3. If the certificate is a valid self-signed certificate, then available properties will be displayed along with the status message “Valid Certificate” and a warning in red stating: "**WARNING”**: This certificate is not a verified certificate and is a self-signed certificate. Usage of verified certificate is recommended over self-signed certificate."

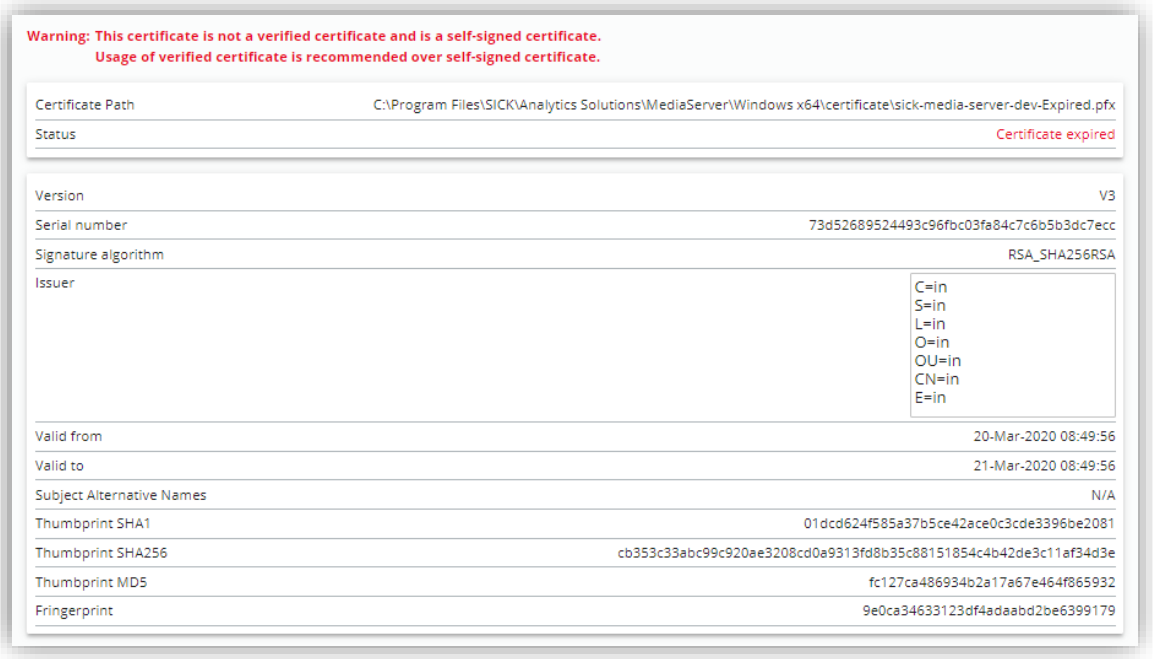


Figure 15.4:5: Self Signed Certificate Warning

4. Refer to Appendix A for instructions to create certificate with SAN.
5. If the secured features SFTP, FTPS, HTTPS, File Sync get disabled due to the certificate error. User should rectify the certificate Settings

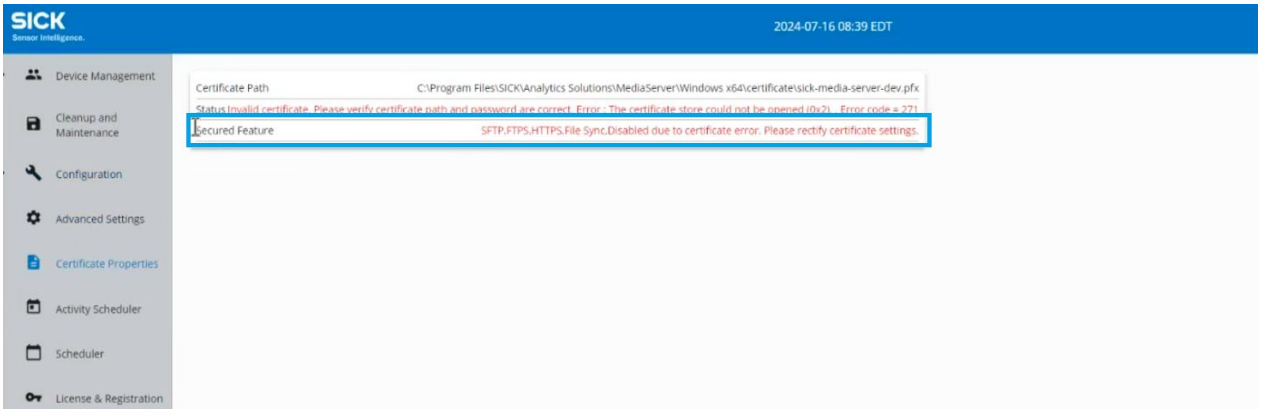


Figure 16-6: Secured Feature

16.1 Configuring Automatic Certificate Loading Using a Properties File

The Media Server can automatically load certificates from a folder using a properties file, simplifying management.

Configuration Steps:

1. Create a properties file (e.g., cert.properties) in a suitable folder.
2. Add the following parameters to the file:
   - certLocation: Path to the certificate file.
   - certificate_alias: Alias name of the certificate.
   - LimaKilo: Certificate password (plain or Base64-encoded).
   - group_email: (Optional) Email for certificate-related communication.

   Example:

   certLocation=C:/Certificates/uploadx/domain-cert.pem
   certificate_alias=domain-cert
   LimaKilo=^chQbddT.„/kR[jgR}/=Ea]qdM(x)TT
   group_email=admin@example.com

3. In the sick-bip-is.cfg file, under [CERTIFICATE], configure the following:
   - USE_CUSTOM_CERTIFICATE=true
   - CERT_CONFIG_PROPERTIES=*path to properties file*
   - PROPERTIES_CERT_PATH_FIELD=certLocation
   - PROPERTIES_PASSWORD_FIELD=LimaKilo
   - PROPERTIES_PASSWORD_ENCODED=false

   Example:

   [CERTIFICATE]
   USE_CUSTOM_CERTIFICATE=true
   CERT_CONFIG_PROPERTIES=C:\Certificates\cert.properties
   PROPERTIES_CERT_PATH_FIELD=certLocation
   PROPERTIES_PASSWORD_FIELD=LimaKilo
   PROPERTIES_PASSWORD_ENCODED=false

4. To store the password in Base64:
   - Encode the password using Base64.
   - Set PROPERTIES_PASSWORD_ENCODED=true.
   - Update the LimaKilo field with the encoded value.

   Example:

   ```
   [CERTIFICATE]
   USE_CUSTOM_CERTIFICATE=true
   CERT_CONFIG_PROPERTIES=C:\Certificates\cert.properties
   PROPERTIES_CERT_PATH_FIELD=certLocation
   PROPERTIES_PASSWORD_FIELD=LimaKilo
   PROPERTIES_PASSWORD_ENCODED=true

   certLocation=C:/Certificates/uploadx/domain-cert.pem
   certificate_alias=domain-cert
   ```



```
LimaKilo=<Base64-encoded-password>
group_email=admin@example.com
```

5. Save all changes and restart the Media Server.

On startup, the Media Server loads the certificate from the properties file for secure protocols.

17 Authentication Configuration

Use **Authentication Configuration** to select an authentication method and configure sign-in settings for the Media Server.

The system supports authentication using the **internal database** or through an external **OpenID Connect (OIDC) Identity Provider** such as Microsoft Entra ID.

OIDC authentication enables **Single Sign-On (SSO)**, allowing users to sign in using corporate credentials instead of local database credentials.

Only users with **administrator privileges** can access and configure authentication settings.

Accessing the Authentication Configuration Page

To access the **Authentication Configuration** page:

1. Log in to the application with **administrator privileges**.
2. From the **left navigation pane**, select **Authentication Configuration**.

The **Authentication Configuration** page is displayed.

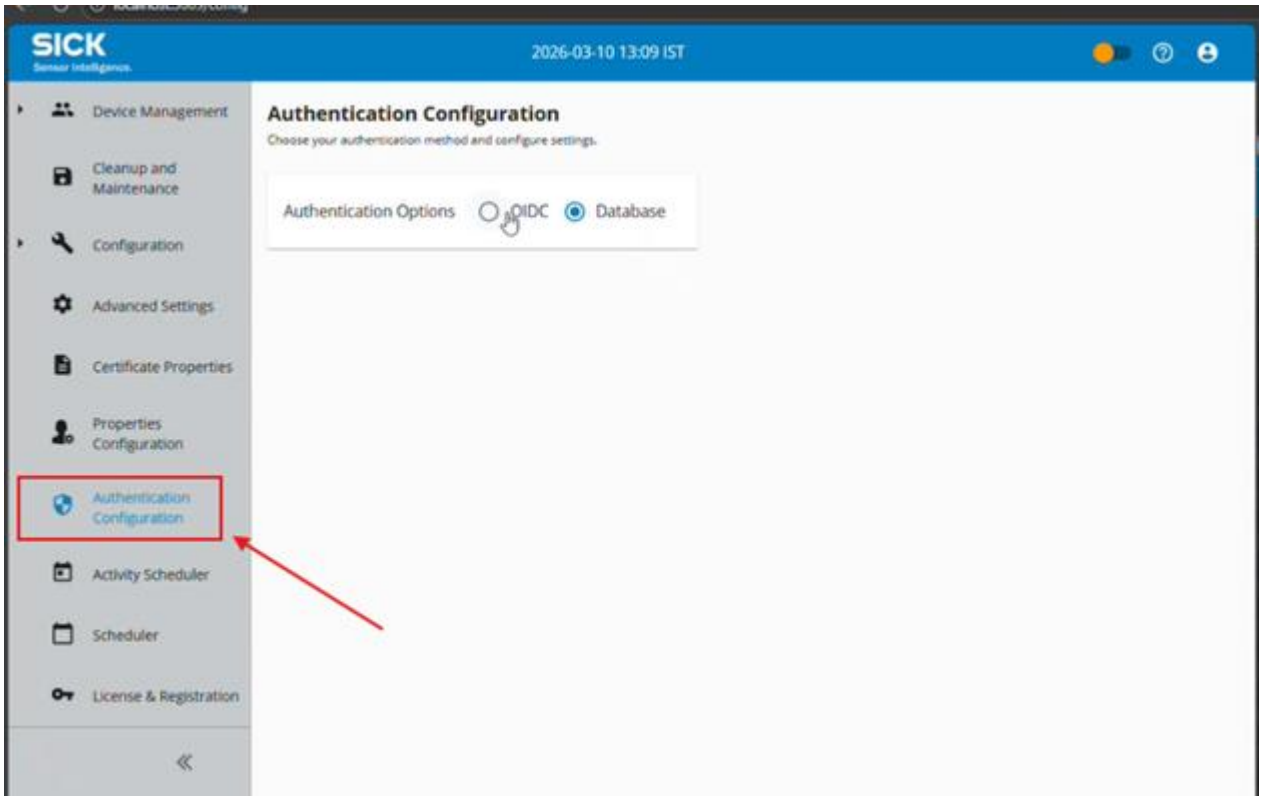


Figure 138: Accessing Authentication Configuration from the Navigation Menu

Authentication Options

The Media Server supports the following authentication methods.

Authentication Method	Description
OIDC	Enables authentication using an external Identity Provider (Single Sign-On) such as Microsoft Entra ID.
Database	Uses local Media Server user credentials stored in the database.

Select the required authentication method. The configuration fields for the selected authentication type are displayed.

Identity Provider Configuration (OIDC)

When **OIDC authentication** is selected, administrators must configure an **Identity Provider (IdP)**.

Multiple Identity Providers can be configured.

To add a new Identity Provider:

- Select the **Add (+)** icon.
- Enable **Active Provider** to activate the provider configuration.

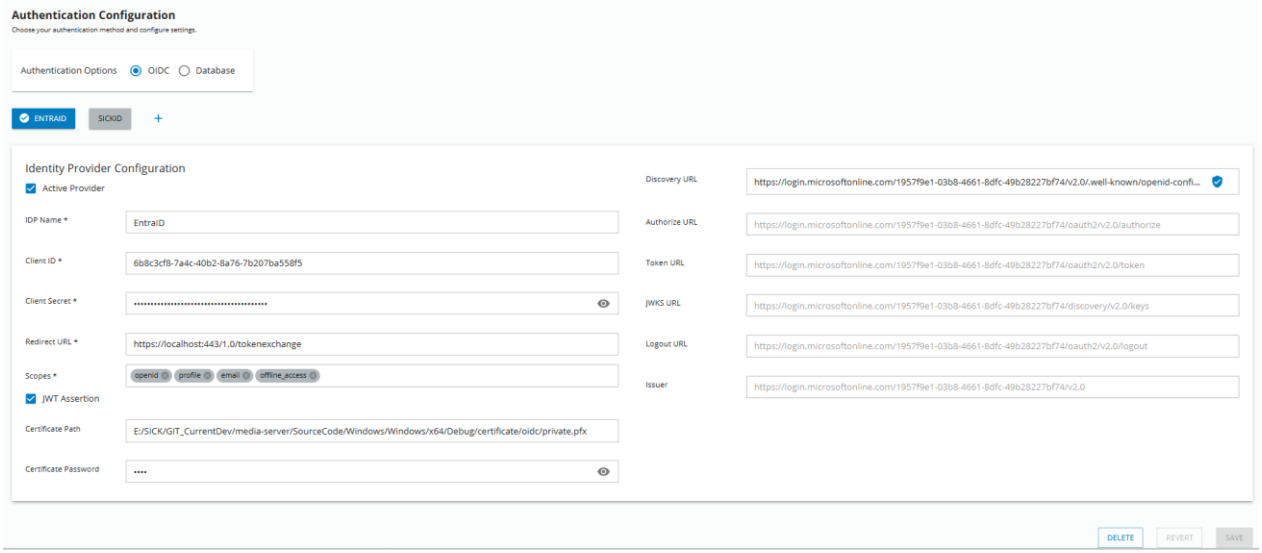


Figure 139: Authentication Configuration – OIDC Settings Page

Configuring an Identity Provider

To configure **OpenID Connect authentication**:

1. Select **OIDC** under **Authentication Options**.
2. Select the **Add (+)** icon to add a new Identity Provider.
3. Enable **Active Provider** to activate the configuration.
4. Enter the required configuration values:
    - **IDP Name**
    - **Client ID**
    - **Client Secret**
    - **Redirect URL**
    - **Scopes**
5. (Optional) Enable **JWT Assertion** and configure the certificate details.
6. Enter the **Discovery URL** and select **Verify**.

Note

The **Discovery URL** retrieves OpenID Connect metadata from the Identity Provider. This metadata includes authorization, token, and key endpoints required for authentication.

If validation succeeds, Media Server automatically populates the following endpoint fields:

- **Authorize URL**
- **Token URL**
- **JWKS URL**
- **Logout URL**
- **Issuer**

You can also enter these endpoint values manually. If you want to retain manually entered values, do not select **Verify**.

If the **Discovery URL** is invalid, verification fails and the endpoint values are not populated.

The **Redirect URL** is not automatically populated and must be entered manually.

Redirect URL Configuration

- When configuring the **Identity Provider (IdP)**, set the **Redirect URL** using the following format:

```
<protocol>://<media_server_IP>:<protocol_port>/1.0/tokenexchange
```

- In the **Redirect URL** field of the **Media Server configuration**, enter only the **Media Server IP address and port** used in the IdP configuration.

Example

```
https://192.168.1.2:443
```

The application automatically appends `/1.0/tokenexchange` to complete the redirect URL.

After verifying the configuration, select **Save**.

OpenID Configuration Fields

Field	Description
IDP Name	Display name of the Identity Provider shown on the login screen.
Client ID	Application Client ID obtained from the Identity Provider registration.
Client Secret	Secret key associated with the registered application.
Redirect URL	Callback URL where the Identity Provider redirects users after successful authentication.

Scopes	OIDC scopes requested during authentication such as openid, profile, email, and offline_access.
JWT Assertion	Enables certificate-based validation.
Certificate Path	Path to the certificate file used for JWT assertion.
Certificate Password	Password associated with the configured certificate.
Discovery URL	OIDC metadata endpoint used for automatic endpoint discovery.
Authorize URL	Authorization endpoint automatically populated after verification.
Token URL	Token endpoint automatically populated after verification.
JWKS URL	Endpoint used to retrieve keys for token signature validation.
Logout URL	Identity Provider logout endpoint.
Issuer	Expected token issuer value used for token validation.

Saving the Configuration

After completing the configuration:

1. Select **Save**.

2. A confirmation message is displayed indicating that the OIDC configuration is saved successfully.

3. A notification is displayed stating that the authentication configuration has been updated and the user will be logged out to apply the changes.

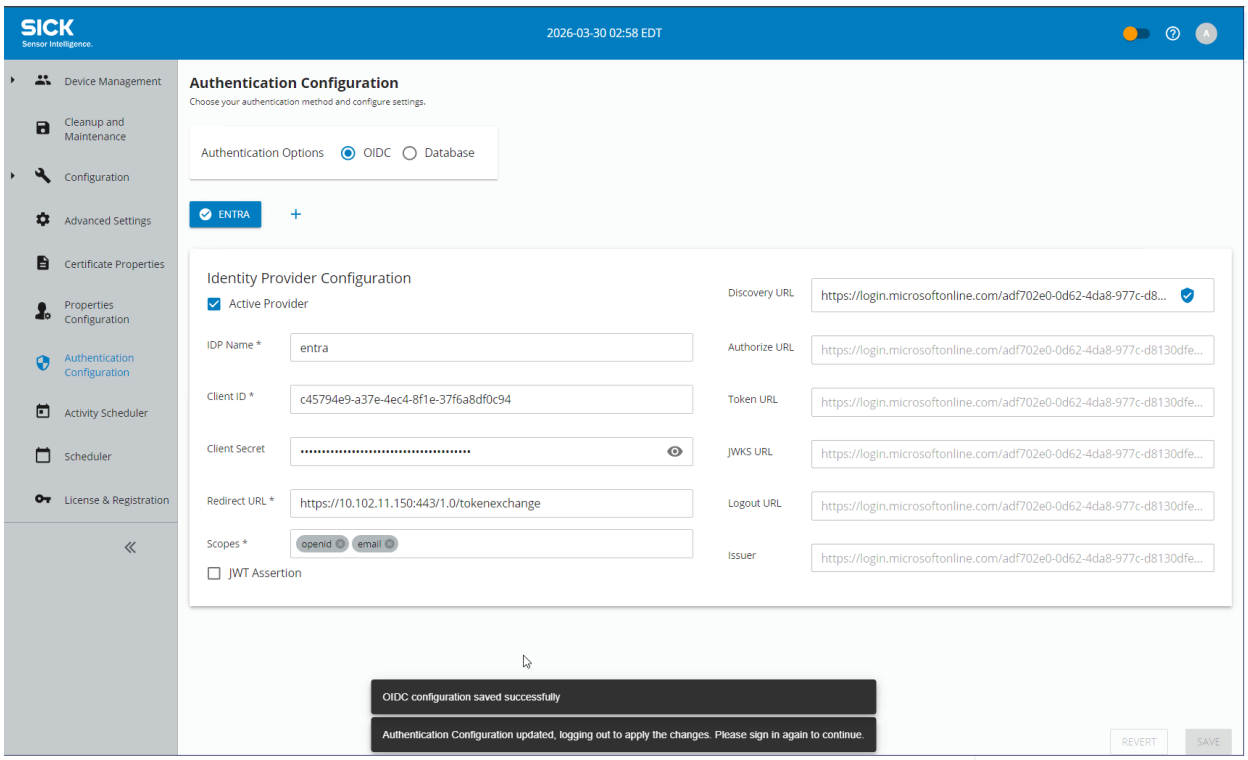


Figure : OIDC Configuration Save Notification and Logout Message

4. The system automatically logs out the current user session.
5. Log in again using the configured authentication method.
6. If prompted, restart the application services to apply the configuration.

Note

After saving the authentication configuration, the system displays a notification and automatically logs out the current user to apply the updated authentication settings.

Login Using OIDC Authentication

After **OIDC authentication** is enabled, the login page displays the **Login via MS OIDC** option.

Users can sign in using their **corporate credentials** by selecting **Login via MS OIDC**.

Users can also select **Login as Database User** to authenticate using **local database credentials**.

Database authentication remains available to ensure administrators can access the system if the external Identity Provider is unavailable.

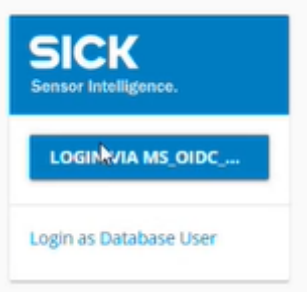


Figure 140: Login Screen – Login via MS OIDC

18 Sync Status

File Sync status is a feature which gives the in depth detailing of the synchronization process and displays a plot chart with very important aspects like:

Parameter	Description
Activity Name	Name of the activity to be scheduled.
Uploaded File Size	Actual file size (in GB) uploaded to the secondary server.
Remaining File Size	Actual file size (in GB) still to be synced to the secondary server.
Time Remaining	Time remaining for the completion of the sync activity.
Current Bandwidth	Speed at which the image transfer is happening from the client to the server.
Status	Displays the current status of the activity.
Information	Information about the sync activity. If nothing is shown, you do not have to provide a description.
Bandwidth Speed (Plot Chart)	Displays the current image transfer speed on a plot chart (from client to server).

File sync status will show how much our bandwidth is and how long it will take to synchronize the files.
The Plot Chart representation is where current bandwidth will be same as network upspeed.

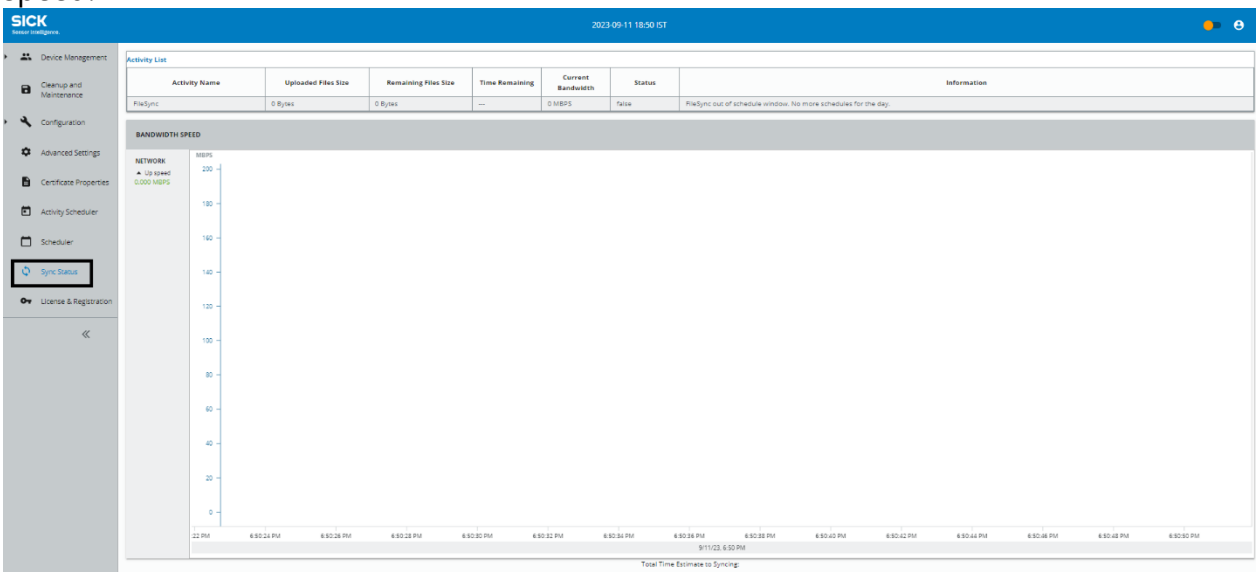


Figure 0:1: Sync Status

19 License and Registration

The License & Registration tab lets you view current SICK Media Server license information and permissions. You can also add a new license or update your permissions.

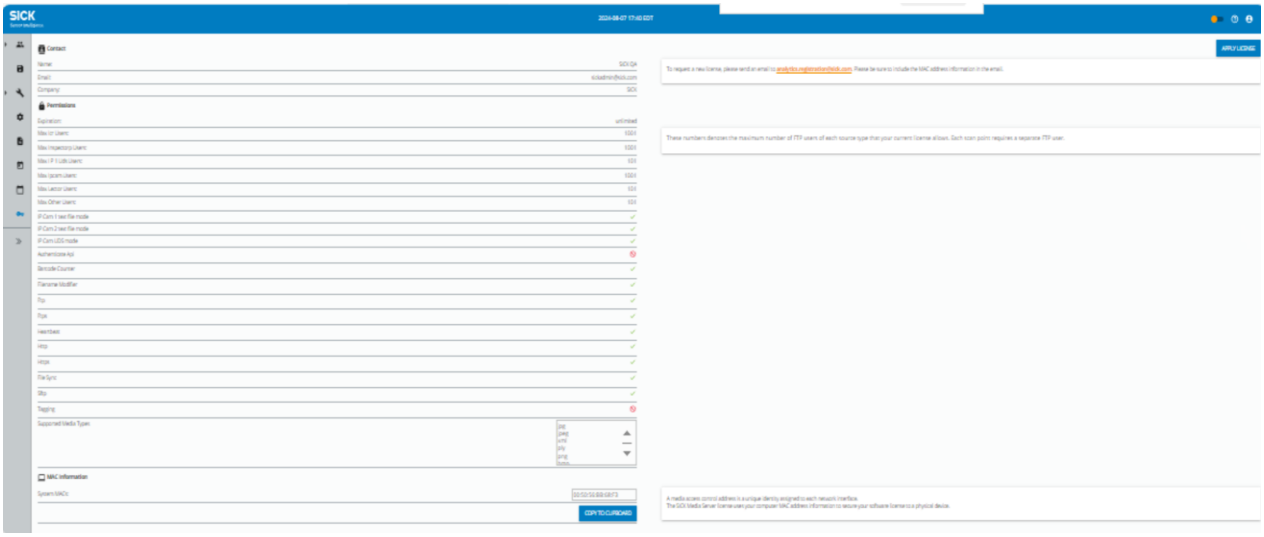


Figure 0:1: License and Registration

19.1Contact

Displays contact information for the SICK Media Server license.

Figure 19.1:1: Contact Information

19.2Schedule Tagging

User can also schedule the tagging activity, activity recurrence schedule using the Scheduler and Activity Scheduler feature in the Media Server application. Refer to Activity Scheduler and Scheduler.

19.3 Permissions

Describes software limitations and permissions for the currently installed license.

Figure 19.3:1: Permissions Section

Setting	Description
Expiration	Expiration date of the current software license. Expiration is based on the UTC time. After this date, Media Server will continue to acquire, store and clean media data in the background. However, you will no longer have access to change any configured settings in the software. Also, you will not be able to view/download media files in your application.
Max ICR Users	Maximum ICR users allowed in the application.
Max IP Cams Users	Maximum IP cam Users allowed in the application

Setting	Description
Max Lector Users	Maximum lector users allowed in the application
Max Other Users	Maximum users other than IPCam, Lector and ICR that are allowed in the application.
IP Cam 1 text file mode	Shows if IPCam 1 txt file mode is allowed to be configured in the application
IP Cam 2 text file mode	Shows if IPCam 2 txt file mode is allowed to be configured in the application
IP Cam UDS file mode	Shows if IPCam UDS file mode is allowed to be configured in the application
FTP/FTPS/SFTP/HTTP /HTTPS	Shows whether FTP/FTPS/SFTP/HTTP/HTTPS servers are Enabled/Disabled in the license.
Heartbeat	Shows whether HEARTBEAT functionality is configurable in the application.
File Sync	Shows if File sync feature is enabled or disabled
Authenticate API	Shows if APIs are accessible with or without authentication. If this feature is Disabled APIs can be accessed without authentication.
Tagging	Shows if tagging feature is enabled or disabled

Table 13: Software Limitations and Permissions Settings

19.4 MAC information

The system Media Access Controller (MAC) is a unique computer ID. MAC is used by SICK Media Server to secure your software license to a physical computer. Your new license request should include your system MAC.

Figure 19.4:1: Mac Information Section

19.5 Add or Update a Local License

You can apply a local license for Media Server from License & Registration page.

1. Click the '**Apply License'** Button.
2. In the **Apply License** window, browse and select the new valid license file, and then click **APPLY** button.

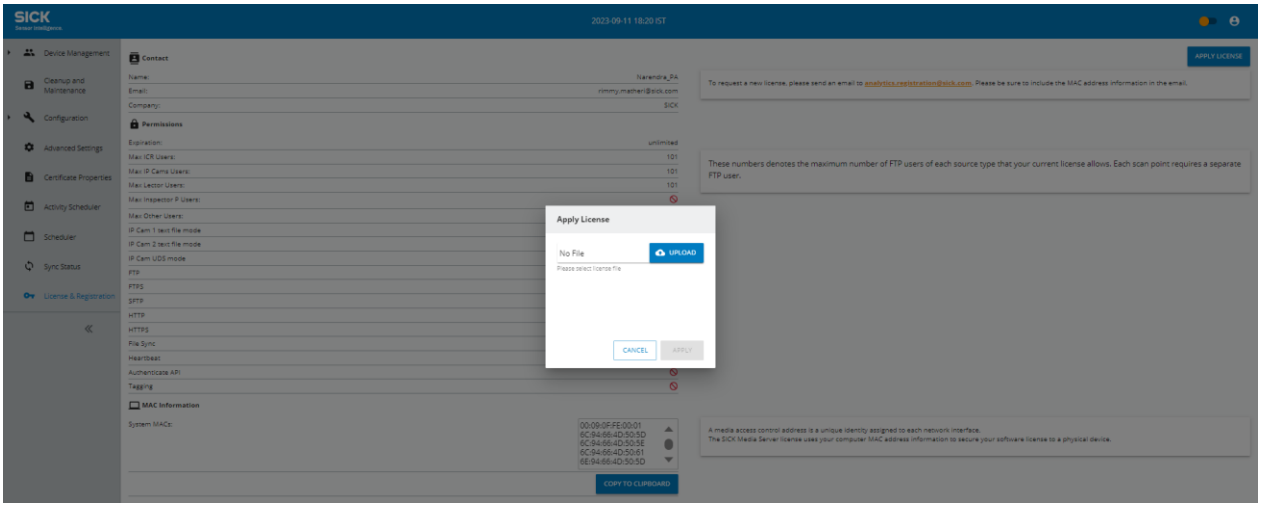


Figure 19.5:1: Apply License

On successful upload, application will display a successful snack bar message and the page will get reloaded.

In case of any issue/error, an error in the snack bar message will be displayed.

> ***Note:*** *If a trusted license is already applied, a new local license cannot be added. The trusted license needs to be removed first to apply a local license.*

19.6 Add or Update a Trusted License

Trusted License can be applied when the Media Server is connected to analytics application.

Steps to apply a trusted License:

- Trusted License property is set to true on Analytics application.
- License with Media Server features enabled has been applied to Analytics application
- Media server is added/configured on Analytics application.

Once the above settings/configurations have been done, trusted license will automatically get applied to Media Server.
License updated in Analytics application via **License & Registration** tab gets automatically added to configured Facility Media Servers.

20 Media Server Application Theme

Media Server application supports Light mode theme and Dark mode theme. User can switch between these themes by clicking the toggle button at the top right corner.

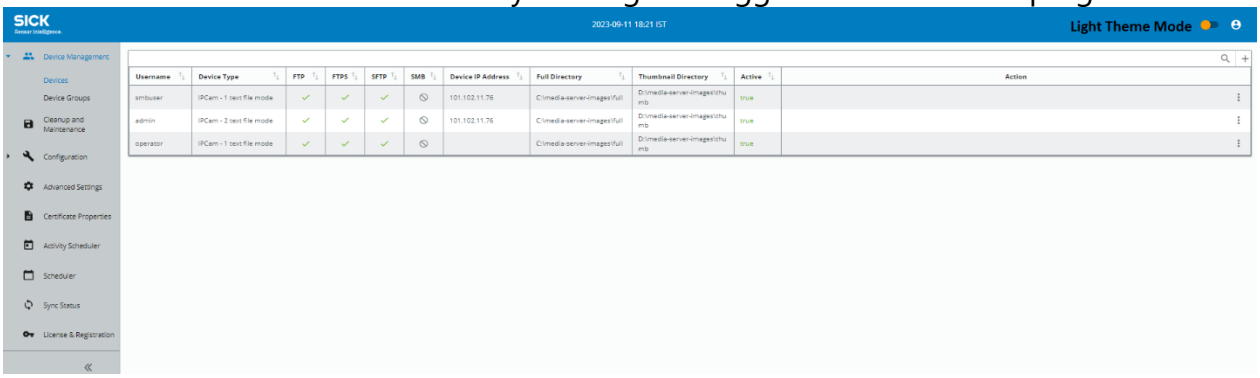


Figure 19.6:1: Light Theme Mode

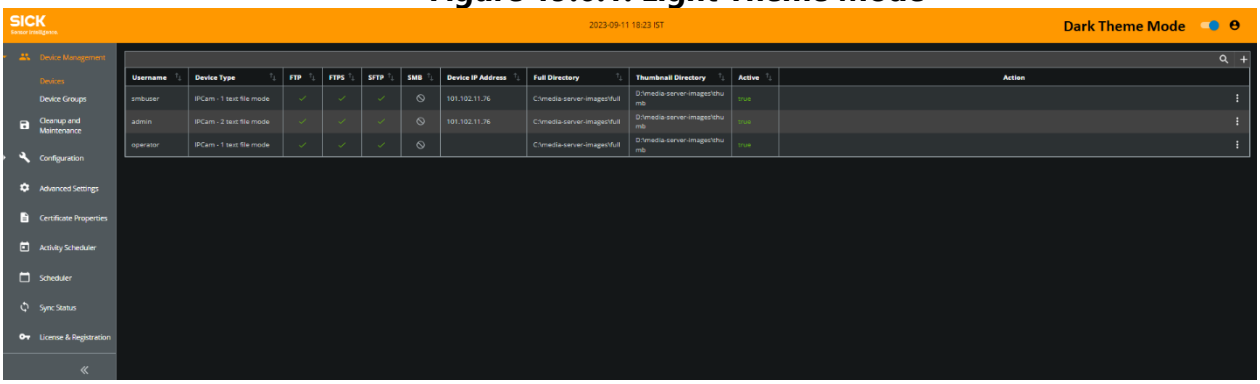


Figure 19.6:2: Dark Theme Mode

21 Manage Media Server User

Media server user can be managed (added/edited/deleted) by editing the **API_USERS** section in sick-bip-is.cfg file.

Figure 19.6:1:API_USERS Section

21.1 Add a Media Server User

You can add a media server user from the config file.

1. Open Encryption app (Encryption.exe) in command prompt.
2. The application will provide you two choices (1/2) to **Encrypt Application User Information** and to **Encrypt Password**.
3. Enter **1** to Encrypt Application User Information. You will be prompted you to provide User details.
4. Enter Username
5. Enter Password.
6. Enter API Count Value for API access control.
7. Enter API Count Unit when prompted.
8. Click on '**Enter'** button.
9. Encryption app will generate the encrypted Username and password as shown below.

Figure 21.1:1: Encrypt User Data

10. Copy the Encrypted User data value.
11. Open the config file in Text Editor.
12. Navigate to **API_USERS** section.
13. Add the Encrypted data under **API_USERS** section.

Figure 21.1:2: Add User Data to Config

14. Save.

15. Navigate to Windows services.

16. Search for SICK An Media Server service.

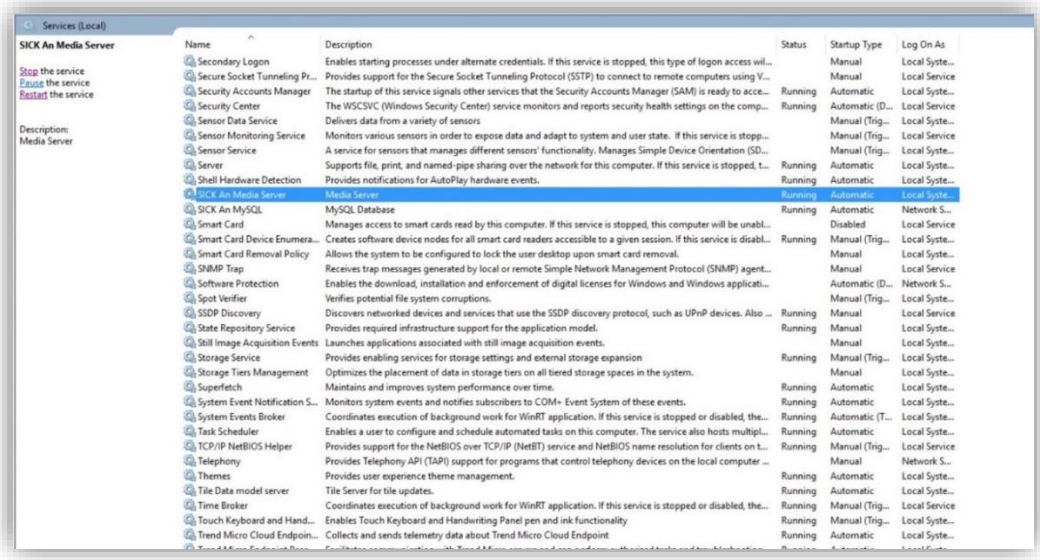


Figure 21.1:3: Media Server Service Screen

17. Restart Media Server Service by right clicking on SICK An Media Server Service and selecting restart option.

18. The newly created user will now be able to access the application. You can update or delete the API_USERS section to update/delete any of the users.

21.2 Update Password

You can update password for Certificates from the config file.

1. Open Encryption app (Encryption.exe) in command prompt.

2. The application will provide you two choices (1/2) to **Encrypt Application User Information** and to **Encrypt Password**.
3. Enter **2** to Encrypt Password. It will prompt you to provide password.
4. Enter Password.
5. Click on '**Enter**' button. The password will be encrypted.

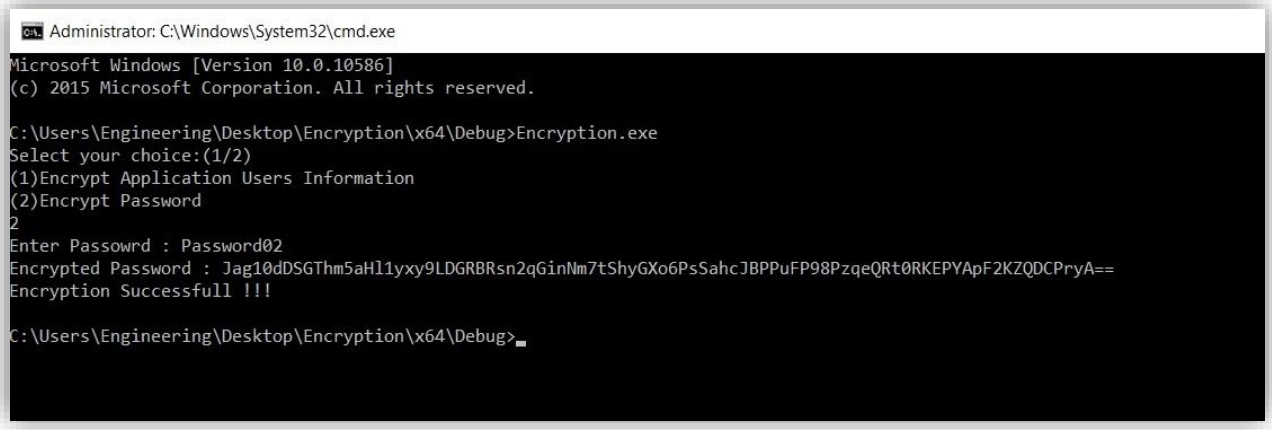


Figure 21.2:1: Encrypt Password

6. Copy the encrypted string.
7. Open the config file in Text Editor.
8. Navigate to the section for which you want to update the password.
9. Paste the encrypted password string.
10. Save.
11. Navigate to Windows services.
12. Search for SICK An Media Server service.
13. Restart Media Server Service by right clicking on SICK An Media Server Service and selecting restart option.
14. The updated password will take place on restarting the application server.

21.3 How to Add New Device

When a media capturing device is added in the analytics application that must be added in the media server application as well for viewing captured media files. User can add new devices to the application through a backend process. The added device type is reflected in the drop-down of '**Type**' in the '**Add Device**' dialog box in the Device screen.

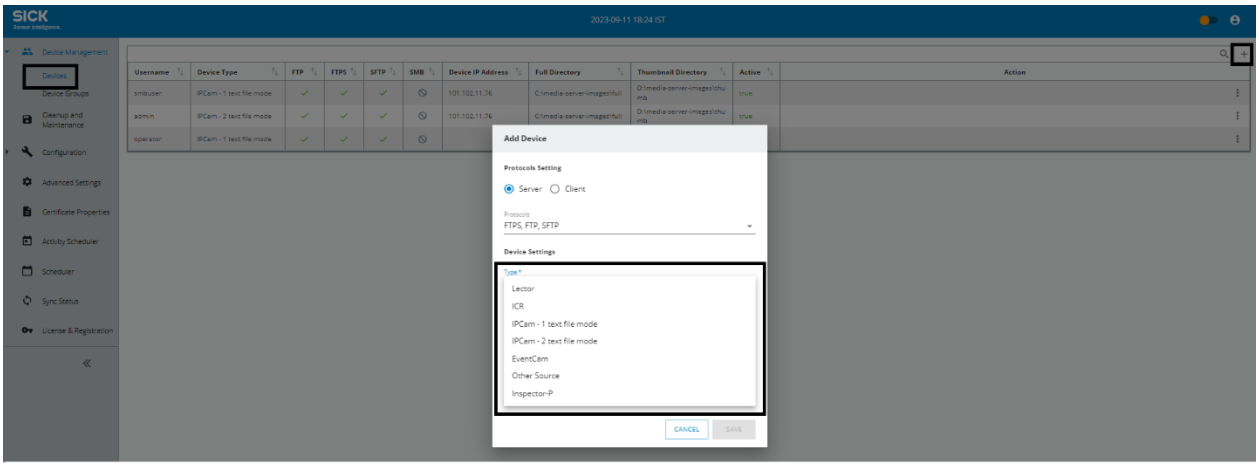


Figure 21.3:1: List of Devices under Type Field

Follow below procedure to add device to the media server application:

1. Open the config file '**sick-bip-is.cfg'** from the install files location where all the properties are stored through which media server application is running.
2. Navigate to the Devices section.
3. Provide the following parameters in one line as shown in Figure 21.3:2: Device Parameters:
    a. Device ID
    b. Device Family
    c. Device Type
    d. Device name

```
[DEVICE]
;The section includes unique Device ID as LHS and comma separated device details as RHS
;For example : <Device ID>=<Device Family>,<Device Type>,<Device Name>
;The Device should be unique.Also the device type cannot be duplicated under different device family.
;The Device Family cannot be added newly, supported Families are : TRACK_TRACE, IPCAM_1TEXTFILEMODE, IPCAM_2TEXTFILEMODE, OTHER_FTP, SAMBA_CLIENT
;The file processing will be based on the Device Family in which the Device is associated to
LECTOR=TRACK_TRACE,LECTOR,Lector
ICR=TRACK_TRACE,ICR,ICR
IP1TEXTFILE=IPCAM_1TEXTFILEMODE,IP1TEXTFILE,IPCam - 1 text file mode
IP2TEXTFILE=IPCAM_2TEXTFILEMODE,IP2TEXTFILE,IPCam - 2 text file mode
EVENTCAM=TRACK_TRACE,EVENTCAM,EventCam
OTHER=OTHER_FTP,OTHER,Other Source
ICR890-4=SAMBA_CLIENT,ICR890-4_SMBCLIENT,ICR890-4 Samba Client
INSPECTORP=TRACK_TRACE,INSPECTORP,Inspector-P
```

Figure 21.3:2: Device Parameters

Note: Device Family description:

- ***TRACK_TRACE:*** *The cameras in this family capture images and send them to the media server, where they are stored in the respective folder structure.*

- ***IPCAM_1TEXTFILEMODE****: The cameras in this family capture images and send them to the media server. The images are initially stored in a temporary folder for the given FTP user. A control file follows the image, containing naming details, and the image must be renamed accordingly. After receiving the file, the media server moves the image from the temporary folder to the appropriate folder structure and renames it based on the control file.*
- ***IPCAM_2TEXTFILEMODE****: The cameras in this family send a control file with sequence details for a given FTP user, followed by the captured image. The image is stored in a temporary folder for the given FTP user. Another control file follows, containing the naming details for the image. After receiving both files, the media server moves the image from the temporary folder to the appropriate folder structure and renames it based on the details provided in the two control files.*
- ***SAMBA_CLIENT****: Cameras in this family manage the storage of captured images. These cameras use the SAMBA server to serve requested images. Example: ICR890-4.*
- ***OTHER_FTP*** *This is a generic camera family that functions similarly to Track and Trace. However, the media server renames the received files for this family type based on its predefined naming convention.*

Note: *The use of other FTP types should be avoided.*

4. Save the file.
5. Request for license of the added device from the sick support team after adding the device in the file.
6. Open '**Services**' from start menu. Right-click on '**Sick An Media Server'** and restart the service.

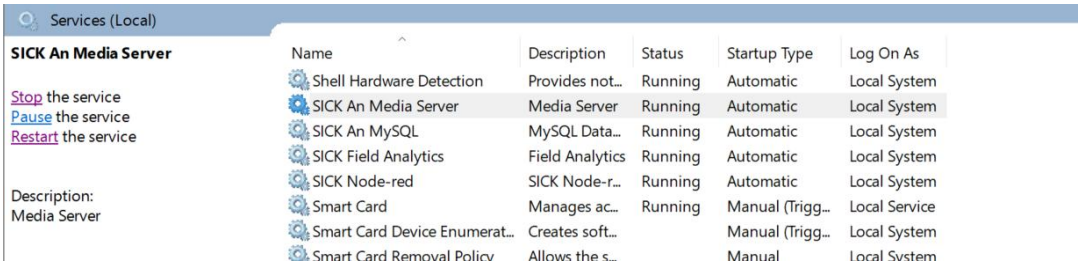


Figure 21.3:3: Running Sick An Media Server

7. Login to the Media server application then apply the license with new Configured Device type in the **License & Registration** tab in the application. Refer to License and Registration.
8. Navigate to **Devices** screen under Device Management tab in the left navigation panel.
9. Click on the '**+**' icon at the top right corner.

10. The Add Device window will open.
11. Select the server from the options under **Protocol Settings.**
12. Select the **Protocols** from the drop-down.
13. User can view the added device in the **Type** drop-down under **Device settings.**

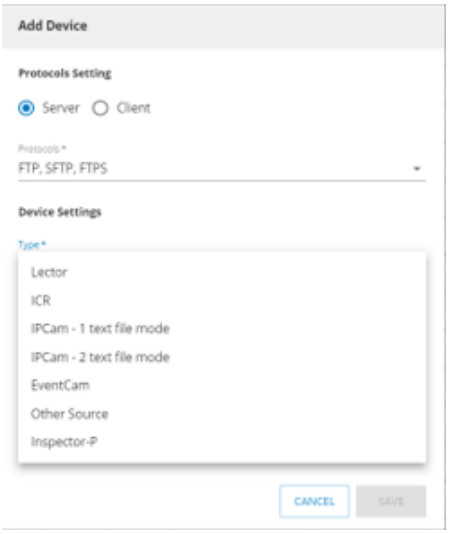


Figure 21.3:4: New Device added in Type Field

22 User Manual

1. To view the information related to User Manual, click the user manual icon on the home page as shown in below figure.

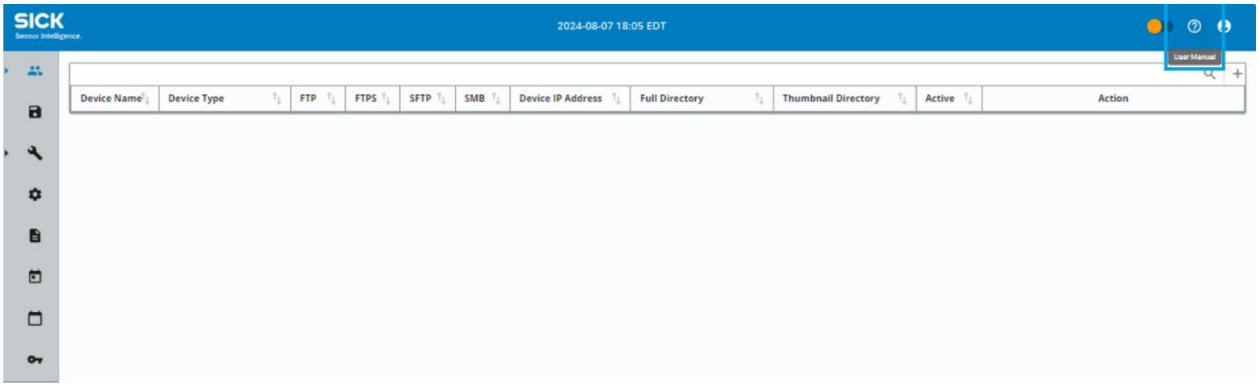


Figure 20-1: Home page

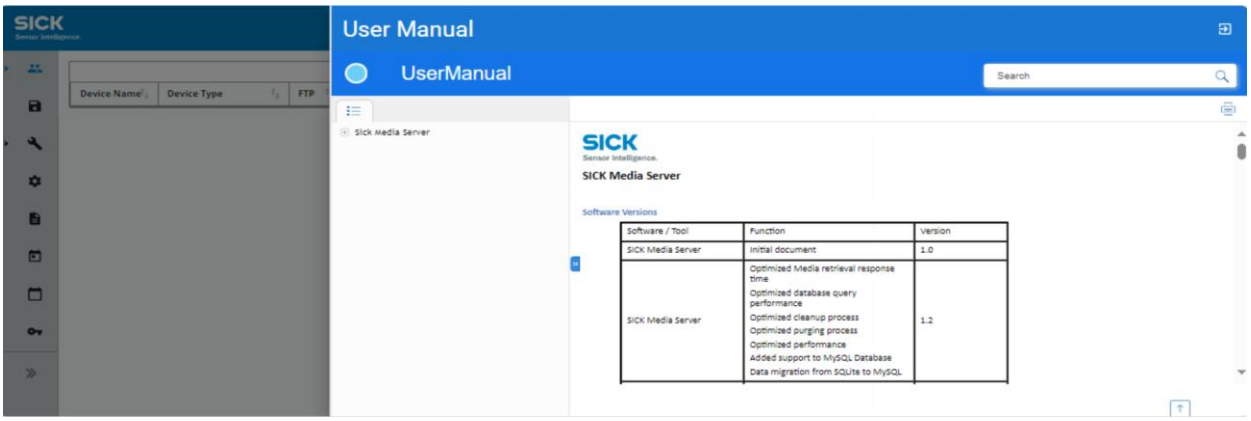


Figure 20-2: User Manual

2. In this Manual, user can get all the required information about the application usage, Installation procedures, how to login everything they can find in this Manual.
3. Also, in the left-hand side if we click on Sick Media Server you can see the Table of contents (TOC) for this Manual

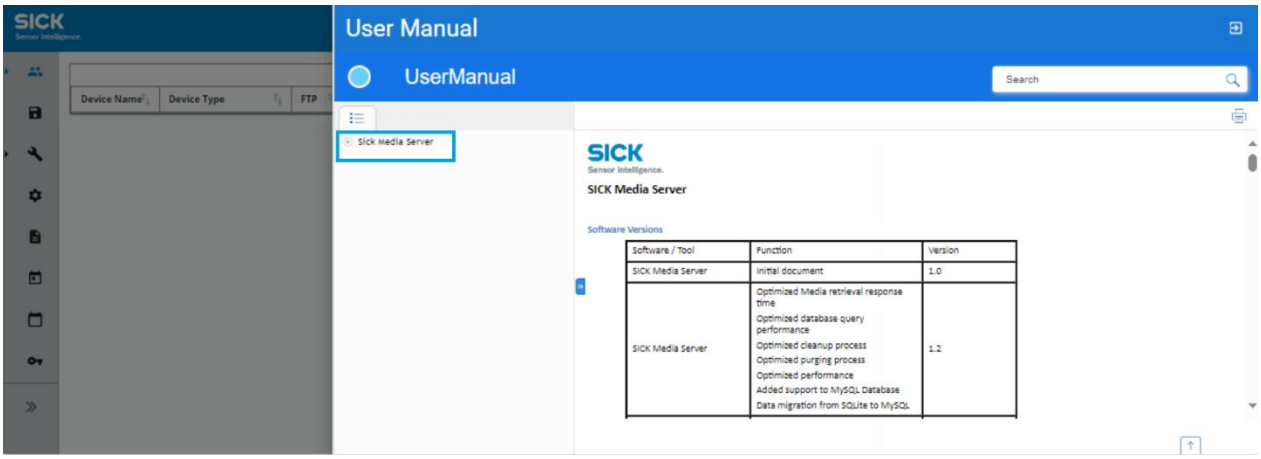


Figure 20-3: Table of Contents

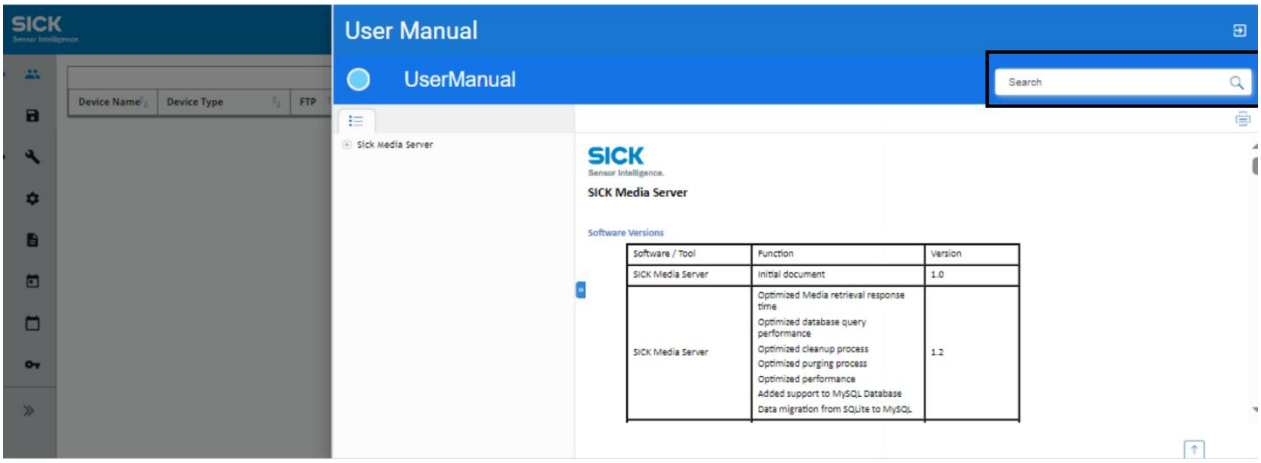


Figure 20-4: Search Tab

23 Configuration File

The **configuration file** stores settings that control the behavior of **SICK Media Server**. The UI allows limited modifications, so some configurations must be updated manually in the **configuration file**.

23.1 Location and Permissions

The configuration file must be stored in a **location with read/write access**.

- If **running as a service**, the application has **read/write access** under:
  - `C:\Program Files\`
  - `C:\Program Files (x86)\`
- If **running as a console application**, ensure it is **installed outside** Program Files.
  - Recommended location: `C:\SICK\`
- On **Linux**, the application **automatically** obtains **read/write** access.

Important: If modifying the startup file to run as a **non-root user**, ensure the user has **write permissions** to:

- Configuration file location
- License file location
- Log file location
- File index location
- Storage location for received media files

23.2 How to Modify Configuration Settings

To modify the **configuration file**, follow these steps:

1. **Stop** the Media Server services.
2. **Navigate** to the folder containing the **configuration file** (sick-bip-is.cfg).
3. **Open** the file in a text editor.
4. **Locate** the parameter you want to modify.
   - Example: To update the **maximum file size**, modify:

```
[STORAGE]
FILE_BUFFER_SIZE=15000000
```

5. **Save** the changes.
6. **Restart** the Media Server services.

***Note*:** *Restarting the services may take 1-2 minutes.*

23.3 Configuration File Structure

The configuration file is structured into sections. Each section starts with a header inside square brackets [ ], followed by its parameters.

Example Structure:

```
[GENERAL]
NAME=SICK Media Server
IndexFile=C:\media-server-images\files.idx
AUTH_CONN_TIMEOUT=60M
[THREAD POOL SIZE]
FTP_CONNECTION_MAX_THREADS=1000
REST_CONNECTION_MAX_THREADS=50
[FTPD]
BINDIP=0.0.0.0
PORT=2021
MAX_IDLE=30
ENABLED=true
```

Note: *Some parameters are hidden and used internally. Parameters starting with * indicate such entries. These parameters can be manually added to the configuration file if required.*

Tag	Key	Values	Description
[GENERAL]	NAME	SICK An Media Server	The name of the server for identification when remotely accessed.
	INDEXFILE	Index File Path	Fully qualified path to the files.idx index file.
	FileMetaCache	Numeric	Number of incoming files metadata maintained in cache memory
	RO	File path	Fully qualified path to the script that sets the

Tag	Key	Values	Description
			filesystem Read Only (UPS Linux Only)
	RW	File path	Fully qualified path to the script that sets the filesystem Read Write (UPS Linux Only)
	IPCAM_CONTROL-FILE_MAXLEN	Numeric	The max file size on in-coming files that will be checked if they are con-trol files for IP CAM mode transfers. De-fault value is 100
	IPCAM_SEQ_MASK	Numeric	The mask to apply to file postfixes to identify file sequence numbers.
	AUTH_CONN_TIMEOUT	Numeric	Connection timeout for ADMIN au-thenticated users. The unit can be Second S(seconds), M(minutes), H(hours),

Tag	Key	Values	Description
			D(Days). Default will be 60M
[THREAD POOL SIZE]	FTP_CONNECTION_MAX_THREADS	Numeric	Max number of threads that can be spawned for FTP connection
	REST_CONNECTION_MAX_THREADS	Numeric	Max number of threads that can be spawned for REST connection
[FTPD]	BINDIP	IP	Host system interface IP to bind the FTP server to “0.0.0.0”. Represents all interface IPs.
	PORT	Ports	A list of one or more comma separated ports that the FTP server listens to for incoming connections.
	MAX_IDLE	Numeric	Connection Max Idle time before

Tag	Key	Values	Description
			automatic disconnect
	Enabled	true/false	Indicates if the server/s are up
	MSC_SOCKET_POLLING_TIMEOUT	Duration in seconds, minutes, hour or days. Example: 5S	Ftp socket timeout value for MSC connections. The incoming control files from MSC can take time. This is the duration after which FTP connection with MSC will be timed out if control file is not received within mentioned interval
	SOCKET_POLLING_TIMEOUT	Duration in seconds, minutes, hour or days. Example: 1H	Ftp socket timeout value. The incoming images from camera can take time to transfer image bytes over time. This is the duration after which FTP connection with the camera will be timed out if image bytes

Tag	Key	Values	Description
			are not received within the mentioned interval
	WAIT_TO_SHUTDOWN	Duration in seconds, minutes, and hours	This Field indicates the maximum waiting time for FTP server to shut down. Beyond this FTP will be forcefully shutdown. Default will be 5S. Units can be S(seconds), M(minutes), H(hours), D(Days).
	FIREWALLED	Ports	This parameter decides if ports for data transfer needs to consider the ports within the port range. For ports to be considered from port range this parameter should be true. By default, it will be set to false.

Tag	Key	Values	Description
	DATA_PORT_WAIT_TIME	Duration in seconds, minutes, hours and days	This describes the time to wait to get the passive port when firewalled is true. Beyond this time the connection fails. It can be set in milli seconds (MS), seconds(S), minutes(M), hours(H), days(D). By default, it is 1M
[FTPSD]	BINDIP	0.0.0.0	Interface IP to bind FTPS server (0.0.0.0 for all interfaces)
	PORT	4121	Port to run FTPS server
	MAX_IDLE	30	Set connection max idle time in seconds
	ENABLED	true	Indicates if the server/s are up
	TLS_VERSION	1_3	Indicates the TLS_VERSION to be

Tag	Key	Values	Description
			used for FTPS. To set it to 1.3, set the parameter as 1_3. By default, it is 1.3. Any value apart from 1_3 or 1_2 will result in using 1.2. When set to 1.2, it will support a minimum TLS version of 1.2 and will also support higher versions.
	FIREWALLED	true/false	This parameter decides if ports for data transfer need to consider the ports within the configured port range. For ports to be considered from the port range, this parameter should be set to true. By default, it is false.
	CIPHERSUITES	Comma-separated list	Indicates which TLS cipher suites are blocked/allowed for

Tag	Key	Values	Description
			FTPS. A suite prefixed with "-" is blocked, while plain names are allowed suites. The value is a comma-separated list. By default, all ciphers are blocked and only a secure subset is allowed.
	TLS_CURVES	Comma-separated list	Indicates which elliptic curves are blocked/allowed for FTPS. A curve prefixed with "-" is blocked, while plain names are allowed curves. The value is a comma-separated list. By default, some curves such as secp521r1 and X448 are blocked.
[SFTPD]	BINDIP	IP	Host system interface IP to bind the SFTP server to “0.0.0.0”. Represents

Tag	Key	Values	Description
			all interface IPs.
	PORT	Ports	A list of one or more comma separated ports that the SFTP server listens to for incoming connections.
	MAX_IDLE	Numeric	Connection Max Idle time before automatic disconnect
	Enabled	true/false	Indicates if the server/s are up
[SFTP_LIB_CONFIG_PROPERTIES]	SSHKeyExchangeAlgorithms	Comma-separated list	Defines the key-exchange algorithms allowed for SFTP connections. The list is evaluated in order of preference.
	SSHEncryptionAlgorithms	Comma-separated list	Defines the symmetric encryption algorithms allowed for SFTP sessions.

Tag	Key	Values	Description
	SSHMacAlgorithms	Comma-separated list	Defines the MAC/integrity algorithms allowed for SFTP sessions.
	SSHPubKeyAuthSigAlgorithms	Comma-separated list	Defines the algorithms allowed for public-key authentication signatures.
	SSHPublicKeyAlgorithms	Comma-separated list	Defines which public key types are accepted by the SFTP server.
	LogLevel	Numeric	Controls the verbosity of the underlying SFTP library logging. Higher values produce more detailed logs.
	UseStrictKeyExchange	Numeric / Flag	Controls how strictly the SFTP server enforces the configured key-exchange algorithms. A higher value enforces stricter adherence to the

Tag	Key	Values	Description
			configured lists.
[PROTOCOLS]	FTP	FTP	FTP is supported if this Key/Value is available in the config file under [PROTOCOLS] section
	FTPS	FTPS	FTPS is supported if this Key/Value is available in the config file under [PROTOCOLS] section
	SFTP	SFTP	SFTP is supported if this Key/Value is available in the config file under [PROTOCOLS] section
	SMB	SMB	SMB is supported if this Key/Value is available in the config file under [PROTOCOLS] section
[PORT_RANGES]	FTP	Port range value for FTP. Example 20,21,1024-65535	The FTP Ports should be within the

Tag	Key	Values	Description
			specified FTP Port range. You can provide the Port range at the time of installation or can update it from the config file itself.
	FTPS	Port range value for FTPS control ports. Example 21,990,1024-65535	The FTPS control ports should be within the specified FTPS Port range. You can provide the Port range at the time of installation or can update it from the config file itself.
	SFTP	Port range value for SFTP. Example 1024-65535	The SFTP Ports should be within the specified SFTP Port range. You can provide the Port range at the time of installation or can update it from the config file itself.

Tag	Key	Values	Description
	FTP_DATA	Port range value for FTP data connections. Example 20,5000-10000	The FTP data ports used when FIRE-WALLED is true should be chosen from this range.
	FTPS_DATA	Port range value for FTPS data connections. Example 11000-16000	The FTPS data ports used when FIRE-WALLED is true should be chosen from this range.
[HTTPD]	BINDIP	0.0.0.0	Host system interface IP to bind the HTTP server to. ”0.0.0.0” represents all interface IPs.
	PORT	Port	The port on which the HTTP server will accept connections.
	ENABLED	true	Parameter to enable or dis-able HTTP. If true, the HTTP server will be up (provided it is licensed). De-fault is true.

Tag	Key	Values	Description
[HTTPSD]	BINDIP	IP	Host system interface IP to bind the HTTPS server to. ”0.0.0.0” represents all interface IPs.
	PORT	Port	The port on which the HTTPS server will accept connections.
	TLS_VERSION	1_2	Version of TLS to use. Set to 1_2 (default) or 1_3. Any other value defaults to 1_2.
	USE_TLS	true	Parameter to decide whether to use TLS. Default is true.
[HTTPD_COMMON]	FILES	html.zip	A zip file or a folder containing the HTML files used to serve out the admin interface. If a zip file is used, the extension .zip is expected. All other naming

Tag	Key	Values	Description
			patterns will be assumed to be folders. If no path is included, the file or folder is assumed to be in the same folder the Media Server is launched from.
	ROOTDOC	Index.html	The html document served out as the root URL (/). Include path relative to the FILES folder/zip file.
	MAX_ARCHIVE_FILE_COUNT	Numeric	The max number of files that can be returned in a zip archive from the media REST API. If more files are requested a 412 – Precondition Failed status is returned. Default value is 100 if not set.
	LOGIN_TIMEOUT	Numeric	Inactivity logout timer in seconds.

Tag	Key	Values	Description
	MAX_FIELD_LENGTH	Numeric	Max length of Name and Paths in the web UI and REST APIs
	MAX_PASSWD_LENGTH	Numeric	Max length for the FTP password field in the web UI and REST APIs
	MAX_USERNAME_LENGTH	Numeric	Max length of the FTP username field in the web UI and REST APIs.
[API_USERS]	{<USER KEY>}	<USERID>, <SHA-1 Password>>	This section holds list of encrypted username-passwords of the users that can access the MS UI. Default users: Admin, Operator, API
[HEARTBEAT]	AUTH_URI	URL	authentication URI which returns the access_token used for authorizing

Tag	Key	Values	Description
	USER_NAME	Username	Username of the facility server
	PASSWORD	SHA-1 Password	Encrypted password of the facility server user
	Client_ID	ID	Id sent along with the authentication request
	Client_SECRET	ID	Random Id sent along with the authentication request.
	AUTHORIZATION	ID	Authorization code sent as part of the authentication request header
	PUBLISH_URI	URL	The URI using which the heartbeat message is published to the facility server
	INTERVAL	Numeric	Time interval for sending the heartbeat message

Tag	Key	Values	Description
	UNIT	Time unit in Sec or Min	Unit of time interval which is either min or sec
	ENABLED	True/False	Boolean value to indicate if heartbeat messaging is up
	ENABLE_AUTH	True/False	Boolean value to indicate if authentication is required to publish heartbeat message
	RETRY_CONNECTION	Numeric	Value in minutes, indicating the interval of connection re-establishment if disconnected from the Facility server.
[HEARTBEAT_HEALTHCHECK]	IMAGE_DROP	True/False	Boolean value to set the image drop health check feature.
	IMGDRP_THRESHOLD	Numeric	Value beyond which if images drop a

Tag	Key	Values	Description
			warning is raised
	HIGH_CPU	True/False	Boolean value to set the CPU usage health check feature.
	CPU_THRESHOLD	Numeric	Value in percentage beyond which if the CPU usage surges a warning is raises.
	HIGH_MEM	True/False	Boolean value to set the memory usage health check feature.
	MEM_THRESHOLD	Numeric	Value in GB below which if the available memory drops a warning is raised.
	DISK_USAGE	True/False	Boolean value to set the disk usage health check feature.

Tag	Key	Values	Description
	DISK_THRESHOLD	Numeric	Value in GB below which if the available disk drops a warning is raised.
	FILESYNC_STATUS	True/False	Boolean value to set the file sync status health check feature.
	FILESYNC_THRESHOLD	Numeric	Boolean value to set the file sync status health check feature.
[UDSD]	BINDIP	IP	Host system interface IP to bind the UDS server to “0.0.0.0”. Represents all interface IPs.
	PORT	Port number	The port on which the UDS server will accept connections. Set to blank or comment out to disable UDS. Note: Server socket will only be

Tag	Key	Values	Description
			created if there is at least one FTP user defined as IP-CAM 1 text file.
	MAX_IDLE	Numeric	Connection Max Idle time before UDS Device automatic gets disconnected.
[STORAGE]	CLEANUP_INTERVAL	Numeric	Interval in seconds between file cleanup jobs - keep in mind a maximum of 5000 files will be scheduled per job if extended intervals are used
	FILE_BUFFER_SIZE	Numeric	File Buffer Size in Bytes - must be larger than the largest file size received on the ftp servers, or the file will be discarded.
	FILE_BUFFER_IDLELIFE	Numeric	File buffer idle life in milliseconds. The amount

Tag	Key	Values	Description
			of time buffers is idle before released.
	TEMPFILE_MAXAGE	Age in seconds, minutes, hour, or days. Example: 1H	Max age for the temporary files when using IPCam modes. One file in the temp location gets older than the indicated age they will be clean up. Time can be specified in seconds(S), minutes (M), hours (H) and days (D). The cleanup is performed together with the standard time-based cleanup and is running on the standard cleanup interval.
	FW_QUEUE_LIMIT	Numeric	File Writer Queue size limit
	VACUUM	True/false	Media Server will run Vacuum command on media server start. If this property is set as true.

Tag	Key	Values	Description
			After task completion, this property will be set as false. This will defragment the SQLite DB and its size will be reduced. By default, this will be false.
	RECAL_FILESIZE	True/false	File size will be re-calculated if this key is set to true. By default, this will be true.
	RECAL_FILESIZE_INTERVAL	Numeric	File size will be re-calculated in intervals based on this value which is in hour. By default, this will be 24.
	REGULAR_PURGE	True/false	If this is set "true" then all old directories will be purged. If set to "false" then only empty old directories will be purged. Default will be true.

Tag	Key	Values	Description
	PURGE_INTERVAL	In minutes. Example: 30M	Interval for Purging unwanted directories. This Value can be set for secs(S) or Mins(M) or hours(H) or Days(D). By default, it will be 30 mins.
	FOLDERS_TRAVERSE	Numeric	Number of folders to be traversed before halting. Default is 100
	TRAVERSE_HALT	Numeric	Number of seconds to halt while traversing through the folders. Default is 0
	AGEOUT_DEL_LIMIT	Numeric	Maximum number of files to be deleted in one cleanup cycle. Default will be 30000
	SMART_UDS	True/false	If this parameter is set to true, MS can support multiple UDS camera provided there is a one-to-one

Tag	Key	Values	Description
			link between the MSC. If set to false only one UDS camera per MS will be supported. This parameter is important if the control file does not have the "user id" tag
	CREATE_SQLITE_INDEXES	True/false	If this parameter is set to true SQLite indexes will be created if not created on MS startup. By default, the value will be true.
	CREATE_MYSQL_INDEXES	True/false	If this parameter is set to true MySQL indexes will be created if not created. By default, the value will be true.
	RATIO	X: Y	The time ratio used when calculating the amount of Thumbnail/Xml files vs Full sized media files

Tag	Key	Values	Description
			are removed during stor-age-based cleanup (Max usage, Min Free space). 1:2 indicates that for every 1 x time unit of Thumb-nails/Xml files, 2 x time units of Full-sized images are removed.
	THUMB	Folder path	Fully qualified path indicat-ing where the thumb-nails/xml files tree is stored.
	FULL	Folder path	Fully qualified path indicat-ing where the full-sized me-dia file tree is stored.
	THUMB_PROFILE	DEFAULT|THUMB|FULL	Indicates which profile is used to store time based cleanup set-ting for thumb-nails/Xml files. DE-FAULT is al-ways used if both THUMB and FULL

Tag	Key	Values	Description
			storage areas is located on the same disk device. If different disk devices are used, individual settings can be used.
	FULL_PROFILE	DEFAULT|THUMB|FULL	Indicates which profile is used to store time based cleanup setting for full sized files. DEFAULT is always used if both THUMB and FULL storage areas is located on the same disk device. If different disk devices are used, individual settings can be used.
	THUMB_ID_PATTERN	*.xml; *_3.*	A list of semicolons (;) separated file patterns to recognize as thumbnails. Default value is “*.xml; *_3.*”.
	THUMB_POSTFIX	_3	Postfix used by the smart

Tag	Key	Values	Description
			file match in the media REST API to match against, if no initial match is found.
	POSTFIX	_2,_3	Additional postfixes considered by the smart file-matching logic in the media REST API when resolving related files. Multiple postfixes are comma separated.
	REMOVE_SOURCE_EXTENSION	True/false	If true, a configured postfix or extension will be removed from incoming filenames for selected devices before indexing. By default, this is false.
	SOURCE_EXTENSION_TO_BE_REMOVED	_2	Comma-separated list of postfixes or extensions that should be removed from the incoming filename when

Tag	Key	Values	Description
			RE-MOVE_SOU RCE_EX-TENSION is true.
	REMOVE_EXTEN-SION_FROM_DEVICE	ICR	Comma-sep-arated list of device IDs for which the source exten-sion or postfix removal should be ap-plied.
	SQL_TO_MYSQL_ETL_B ATCH_SIZE	Numeric	Number of data to be re-trieved from File index for processing. Default will be 50000
	AFTER_ETL_BATCH_DE-LETE_RECORDS	True/false	Flag set whether SQLite rec-ords must be deleted after migrating rec-ords from SQLite to MySQL
	QUEUE_PRO-CESS_TIMEOUT	In seconds, minutes, hours or days. Example: 5M	If processing the DB queue during MS shutdown or switching DB takes more than the timeout value, it will

Tag	Key	Values	Description
			stop processing the queue and continue. The default value is 5 mins. It can be set in secs, mins, hours, or days.
	SIZEOUT_TIME_BUFFER	In seconds, minutes, hours or days. Example: 5M	This time value is to determine how much disk space is required to store data worth the time configured. By Default, the value will be 5 mins. We can set this value for any number mins(M) or hours(H) or days(D). This value will be considered if full and thumb drive are same.
	SIZEOUT_TIME_BUFFER_FULL	In seconds, minutes, hours or days. Example: 5M	This time value is to determine how much disk space is required to store data worth the time configured. By

Tag	Key	Values	Description
			Default, the value will be 5 mins. We can set this value for any number mins(M) or hours(H) or days(D). This value will be considered for full drive.
	SIZEOUT_TIME_BUFFER_THUMB	In seconds, minutes, hours or days. Example: 5M	This time value is to determine how much disk space is required to store data worth the time configured. By default, the value will be 5 mins. We can set this value for any number mins(M) or hours(H) or days(D). This value will be considered for thumb drive.
	AUTO_DISK_MGMT_FUL	True/False	Media server calculates the minimum free space automatically if this parameter is set to true. By default, it will be

Tag	Key	Values	Description
			true. This is for full drive. Also, this value will be considered if both full and thumb are in the same drive.
	AUTO_DISK_MGMT_THUMB	True/False	Media server calculates the minimum free space automatically if this parameter is set to true. By default, it will be true. This is for thumb drive.
	SIZEOUT_TIME_MAX_DEL	In seconds, minutes, hours or days. Example: 1D	This time value is to determine the maximum number of files to be fetched for deletion when the minimum free space is being used. This value by default is 1 day and can be set to any number of days. This value will be considered if full and thumb are in the same drive.

Tag	Key	Values	Description
	SIZEOUT_TIME_MAX_DEL_FULL	In seconds, minutes, hours or days. Example: 1D	This time value is to determine the maximum number of files to be fetched for deletion when the minimum free space is being used. This value by default is 1 day and can be set to any number of days. This value will be considered for full drive.
	SIZEOUT_TIME_MAX_DEL_THUMB	In seconds, minutes, hours or days. Example: 1D	This time value is to determine the maximum number of files to be fetched for deletion when the minimum free space is being used. This value by default is 1 day and can be set to any number of days. This value will be considered for thumb drive.
	NO_OF_MAX_DEL_AT-TEMPTS	Numeric	This Value determines number of

Tag	Key	Values	Description
			times to perform maximum aggressive cleanup until the used space is no more utilizing the minimum free space.
	SIZEOUT_NO_OF_FILES	Numeric	Number of files to be retrieved from DB for Size based cleanup in case there are no data being acquired. Default is 5000
	FW_TEMP_QUEUE_SIZE_LIMIT	Numeric	The size of the temp File writer queue to store data when minimum free space has reached. The size will be based on number of bytes. If it is set to zero, then by default it will be half of the total physical memory. It needs to be set properly to not exceed the total physical memory.

Tag	Key	Values	Description
	TIME BASED_CLEANUP_FULL	True/False	if set to true then Time Based cleanup for full size images will be performed. By default, this is set to false.
	TIME BASED _CLEANUP_THUMB	True/False	if set to true then Time Based cleanup for thumb size images will be performed. By default, this is set to false.
	ADDITIONAL_BUFFER_TIME	In seconds, minutes, hours or days. Example: 15M	Additional buffer time value. minimum and default will be 15mins. Max will be 1h. If the value is set below 15 mins or above 1H then the value will be reset to 15 mins. The additional buffer space size will be dependent on this parameter and the throughput. This parameter is for

Tag	Key	Values	Description
			single drive mode (full and thumb on the same drive).
	ADDI-TIONAL_BUFFER_TIME_FULL	In seconds, minutes, hours or days. Example: 15M	Additional buffer time value. mini-mum and de-fault will be 15mins. Max will be 1h. If the value is set below 15 mins or above 1H then the value will be reset to 15 mins. The ad-ditional buffer space size will be de-pendent on this parame-ter and the throughput. This parame-ter is for full drive
	ADDI-TIONAL_BUFFER_TIME_THUMB	In seconds, minutes, hours or days. Example: 15M	Additional buffer time value. mini-mum and de-fault will be 15mins. Max will be 1h. If the value is set below 15 mins or above 1H then the value will be reset to 15

Tag	Key	Values	Description
			mins. The additional buffer space size will be dependent on this parameter and the throughput. This parameter is for thumb drive.
	THROUGHPUT_VARIANCE_TOLERANCE	Numeric-Percentage Example: 50	This parameter is the tolerance which decides beyond what percentage of increase/decrease in median throughput should we retain the previous value i.e., if the previous throughput was 1 and the current throughput increased/decreased to 1.5/0.5 then 1 will be retained. This value is in percentage and should be integer. By default, it is 50
	PREV_THROUGHPUT_RETENTION_CYCLE	Numeric	This parameter is to decide up to how many

Tag	Key	Values	Description
			such consecutive cycles of surge/drop should we retain the previous median throughput value. If the surge/drop persists beyond these many cycles the median throughput will be set to the new value. By default, this is 2
	REG_SIZEOUT_MAX_FILES	Numeric	Maximum number of files to be deleted in a single regular Size based cleanup cycle. By default, it is 50000
	MIN_FREE_SPACE_MUL_FACTOR	Numeric	This parameter is the multiplication factor to set the minimum free space for an OS drive when auto disk management is enabled. The minimum free space for OS drive when auto disk management

Tag	Key	Values	Description
			is enabled will be set based on the product of this parameter and the total physical memory. By default, it will be 1.5. If the value is set to negative it will reset to 1.5. If the resultant product is greater than the total disk space, then minimum free space will be set as 1GB.
	AVOID_SIZEOUT_DEL_TIME	In seconds, minutes, hours or days. Example: 5M	Latest data for the time set in this parameter will not be deleted during Size based cleanup i.e., if 5M is set then latest records acquired in last 5 mins will not be deleted. By default, this value is set to 5 mins. It can be set to sec(S), min(M), Hour(H) and Days(D). This parameter is added so that

Tag	Key	Values	Description
			new data is not immediately deleted and to avoid the cache file size from going to negative. In case the minimum free space is reached 2 mins will be considered.
	AGGRESSIVE_BATCH_RETRIEVAL	Numeric	Records for Aggressive cleanup will be fetched in batches based on the value set in this parameter. By default, it will be 50000
	UPDATE_SQLITE_TABLE	True/False	If this parameter is set to true SQLite file index table will be updated with latest column changes. by default, the value will be true. Once the table is updated it will be set to false.
	UPDATE_MYSQL_TABLE	True/False	If this parameter is set to true MySQL

Tag	Key	Values	Description
			file index table will be updated with latest column changes. by default, the value will be true. Once the table is updated it will be set to false.
	RATIO_ENABLED	True/False	If this parameter is set to true Regular Size based cleanup will be ratio based. by default, it will be true.
	XML_BATCH_SIZE	Numeric	This parameter defines the maximum xml files to be deleted in a single batch. By default, it will be 30000
	XML_DELTIME_MODIFIER	In seconds, minutes, hours or days. Example: 10M	This parameter defines how much time to be deducted from the lowest timestamp of full/thumb file deleted. By default, it is 10 mins

Tag	Key	Values	Description
	*BUFFER_PATH	path	(Hidden): Sets path to location for temporary storage of IP-CAM files waiting for re-name com-mand. If not set, the stor-age location is set to a folder named “tmp”
	DELETE_SYNCED_FILE	True/False	Synced files will be de-leted if this parameter is true and there is no active File sync Sched-ule. By De-fault, this pa-rameter will be false
	SYNCED_DEL_LIMIT	Numeric	This is the max amount of data re-trieved for de-leting Synced files
	RULE_BASED_CLEANUP	True/False	If this param-eter is set to true rule-based cleanup will be performed

Tag	Key	Values	Description
	*TMP_FILE_IDX_SIZE	Numeric	The size of the list to store the temp file details. Default is 1000.
	*DEL_FLAG_LIMIT	Numeric	Maximum number of files marked for deletion by tagging to be deleted in one cleanup cycle. Default will be 30000
	*QUERY_BATCH_SIZE_TO_PROCESS	Numeric	Maximum Number of DB queries to be processed from the DB queue in one transaction. By default, it is 500
	*MYSQL_BATCH_RECALCULATION	True/False	If this parameter is true, MySQL Recalculation will be done in batches for each partition. By default, this is false.
	*RECALCULATION_BATCH_SIZE	Numeric	If recalculation is to be done in batches, this parameter

Tag	Key	Values	Description
			determines the size of the batch. By default, it is 50000
	*MYSQL_PARTITION_DELETION	True/False	This Parameter determines if the records to be deleted from DB for Rule based cleanup should be based on partition. By default, this is true.
	*MAX_FW_Q_COUNT	Numeric	Maximum File writer Queue size when Cleanup will be slowed down. By default, the value is 500
	*CLEANUP_SLOWDOWN_TIME	Numeric	Slowing down cleanup operation by introducing a time gap determined by this parameter when File writer Queue is high. This value is in milli seconds. By default, it is 100

Tag	Key	Values	Description
	*TMP_CLEAR_SLOW-DOWN_ TIME	Numeric	Slowing down control file clearance operation by introducing a time gap determined by this parameter when File writer Queue is high. This value is in milli seconds. By default, it is 300
	*NOT_FOUND_CLEANUP_THREAD_LIMIT	Numeric	Number of threads to be spawned for clearing the not Founds at a time. One thread belongs to one device. By default, it is 10.
	*FOUND_CTRL_FILE_COUNT	Numeric	If control files are found equal to or more than this parameter value, then files from temp folder for those users will be deleted based on an increased time. Default is 3.

Tag	Key	Values	Description
	*TAG_DEL_BATCH	Numeric	Batch size of data marked for deletion by tag action criteria to be deleted at a time. Default is 500.
	*SQLITE_BATCH_RE-CALCULATION	True/False	If this parameter is true, SQLite Recalculation will be done in batches for each partition. By default, this is true.
	*MIN_FREE_MEMORY_PERCENT	Numeric	This memory defines min free memory that should be available in the server. MS will not be able to use RAM for temp queue's if there is not enough memory available in the server. If the percentage of available memory is lesser than this value, then discard incoming images. Default is 10

Tag	Key	Values	Description
	*FW_NO_OF_PROCESSING_THREADS	Numeric	Maximum Threads to be spawned for each File Writer namely, full, thumb, xml and control file. Default is 100.
	*PARALLEL_FILE_PROCESSING	True/false	Process the files parallelly for all File writer Queue. By default, it is true.
	*ACQUISITION_SLOWDOWN_TIME	Numeric	SLowDown Acquisition when Max Aggressive cleanup is in progress. Value is in milli seconds. Default is 50.
*SLOWDOWN_ACQ_REG	True/false	If this is set to true, the acquisition will be slowed down when the file writer queue is high and control file clearance is going on. By default, this is false.	
*FW_QUEUE_COUNT_ACQ	Numeric	File writer Queue size when Acquisition will be slowed down. Default is 1000	

Tag	Key	Values	Description
*RE-STRICT_RULE_BASED_LINUX	True/false	If it is set to true, Rule based cleanup feature will be restricted in Linux. By default, it is true.	
*MYSQL_PARTI-TION_DELETION	True/false	If this flag set to true and the rule-based feature is enabled, the cleanup re-trieval/deletion will be per-formed based on partitions in MySQL. Default value is true.	
[PROFILE_DE-FAULT]	MIN_FREE	Numeric	This parame-ter is inter-nally used by Media Server for Size Based Cleanup
	MAX_STORE	Numeric	This setting is deprecated
	THUMB_MAXAGE	In days. Example: 99D	Max file age of thumb-nails/Xml files. 1D = 1 Day, 10H = 10 Hours.
	FULL_MAXAGE	In days. Example: 99D	Max file age of full-sized files. 1D = 1 Day, 10H = 10 Hours.
	MAX_HOURS	Numeric	Maximum number that can be used

Tag	Key	Values	Description
			to configure hours in Time Based rule.
[PRO-FILE_THUMB]	MIN_FREE	Numeric	This parameter is internally used by Media Server for Size Based Cleanup
	MAX_STORE	Numeric	This setting is deprecated
	THUMB_MAXAGE	In days. Example: 1D	Max file age of thumbnails/Xml files. 1D = 1 Day, 10H = 10 Hours.
	FULL_MAXAGE	In days. Example: 6H	Not used.
	AUTO_MIN_FREE_SPACE	In MB, GB and K Example: 1GB	This is minimum free space that will be set when auto disk management is enabled. By default, it will be 1GB. The units supported are KB, MB, and GB. If any other unit is provided it will be converted to GB.

Tag	Key	Values	Description
			If the value provided is greater than or equal to the total disk size, then it will be reset to 1GB.In case of single drive mode the value set in full will be considered. This is only for non-OS drives
	MAX_HOURS	Numeric	Maximum number that can be used to configure hours in Time Based rule.
	MAX_DAYS	Numeric	Maximum number that can be used to configure days in Time Based rule.
	RESERVED_SPACE	Numeric in Bytes	Minimal free space in bytes of total disk size used on the THUMB de-vice if custom settings size cleanup set-ting is used

Tag	Key	Values	Description
[PROFILE_FULL]	MIN_FREE	Numeric	This parameter is internally used by Media Server for Size Based Cleanup
	MAX_STORE	Numeric	This setting is deprecated
	THUMB_MAXAGE	In days. Example: 4D	Not used.
	FULL_MAXAGE	In days. Example: 12H	Max file age of full-sized files. 1D = 1 Day, 10H = 10 Hours.
	AUTO_MIN_FREE_SPACE	In MB, GB and K Example: 1GB	This is minimum free space that will be set when auto disk management is enabled. By default, it will be 1GB. The units supported are KB, MB, and GB. If any other unit is provided it will be converted to GB. If the value provided is greater than or equal to the total disk size, then it

Tag	Key	Values	Description
			will be reset to 1GB.In case of single drive mode the value set in full will be considered. This is only for non-OS drives
	MAX_HOURS	Numeric	Maximum number that can be used to configure hours in Time Based rule.
	MAX_DAYS	Numeric	Maximum number that can be used to configure days in Time Based rule.
	RESERVED_SPACE	Numeric in Bytes	Minimal free space in bytes of total disk size used on the FULL device if custom settings size cleanup setting is used
[CLEANUP_WARNING_MSG]	MISC_OCCUPY_RESERVED	Text Message	Miscellaneous data Occupying/Occupied reserved disk space. Data acquisition by

Tag	Key	Values	Description
			Media Server might be hampered. Please consider changing disk configuration.
	MISC_OCCUPY_RESERVED_FULL	Text Message	Miscellaneous data Occupying/Occupied reserved space on full size disk. Data acquisition by Media Server might be hampered. Please consider changing disk configuration.
	MISC_OCCUPY_RESERVED_THUMB	Text Message	Miscellaneous data Occupying/Occupied reserved space on thumbnail disk. Data acquisition by Media Server might be hampered. Please consider changing disk configuration.
	MAX_AGG_CLEAN	Text Message	Maximum aggressive Size based Cleanup in Progress as

Tag	Key	Values	Description
			Disk used space reached minimum free space
	MAX_AGG_CLEAN_FULL	Text Message	Maximum aggressive Size based Cleanup in Progress as full size Disk used space reached minimum free space
	MAX_AGG_CLEAN_THUMB	Text Message	Maximum aggressive Size based Cleanup in Progress as thumbnail Disk used space reached minimum free space
	AGG_CLEAN	Text Message	Aggressive Size based Cleanup in Progress as Disk used space reached additional buffer space.
	AGG_CLEAN_FULL	Text Message	Aggressive Size based Cleanup in Progress as

Tag	Key	Values	Description
			full size Disk used space reached additional buffer space.
	AGG_CLEAN_THUMB	Text Message	Aggressive Size based Cleanup in Progress as thumbnail Disk used space reached additional buffer space.
	NO_BUFFER_SINGLE	Text Message	Insufficient space on disk for proper functioning of cleanup. Maximum Aggressive cleanup will be performed once disk usage reaches minimum free space. Consider changing the disk configuration.
	NO_BUFFER_FULL	Text Message	Insufficient space on full size disk for proper functioning of cleanup. Maximum Aggressive cleanup will be performed once disk

Tag	Key	Values	Description
			usage reaches minimum free space. Consider changing the disk configuration.
	NO_BUFFER_THUMB	Text Message	Insufficient space on thumbnail disk for proper functioning of cleanup. Maximum Aggressive cleanup will be performed once disk usage reaches minimum free space. Consider changing the disk configuration.
	MISCELLANEOUS_OCCUPY_BUFFER	Text Message	Insufficient space for Media server data due to Miscellaneous data. This may lead to unwanted media server data cleanup. Consider clearing miscellaneous data or changing disk configuration.

Tag	Key	Values	Description
	MISCELLANEOUS_OCCUPY_BUFFER_FULL	Text Message	Insufficient space for Media server full size data due to Miscellaneous data. This may lead to unwanted media server data cleanup. Consider clearing miscellaneous data or changing disk configuration.
	MISCELLANEOUS_OCCUPY_BUFFER_THUMB	Text Message	Insufficient space for Media server thumbnail data due to Miscellaneous data. This may lead to unwanted media server data cleanup. Consider clearing miscellaneous data or changing disk configuration.
	MISCELLANEOUS_OCCUPYING_MIN_FREE_SPACE	Text Message	Warning message when used space crosses Minimum Free space due to Miscellaneous data in a

Tag	Key	Values	Description
			single drive mode
	MISCELLANEOUS_OC-CUPY-ING_MIN_FREE_SPACE_FULL	Text Message	Warning message when used space crosses Mini-mum Free space due to Miscellane-ous data for a full drive-in dual drive mode
	MISCELLANEOUS_OC-CUPY-ING_MIN_FREE_SPACE_THUMB	Text Messages	Warning message when used space crosses Mini-mum Free space due to Miscellane-ous data for a thumb drive in dual drive mode
MESSAGE_HEAD-ERS	ERROR_CODE	Code	Setting the header “Error Code:” in er-ror image. The corre-sponding er-ror code will be set be-sides the la-bel.
	FILENAME	Name	Setting the header “File-name:” in

Tag	Key	Values	Description
			error image. The corresponding file name will be set besides the label.
	PROBLEM_STATEMENT	Message	Setting the header “What Happened:” in error image. The corresponding error message will be set besides the label.
	PROBABLE_SOLUTION	Message	Setting the header “Try:” in error image. The probable solution will be set besides the label.
MESSAGES It has messages for each HTTP error code, which includes problem statement and probable solution. Example: For server connection failed error, assuming 10001 is the status code set in source code.	10001_PROBLEM	Message	Give the proper error message for the issue.
	10001_SOLUTION	Message	Provide a suitable solution for the issue occurred.

Tag	Key	Values	Description
[FTP_ADD_USERS] One record for each defined user.	{<USER KEY>}	<USERID>, <SHA-1 Password>,<ConnectionIP (option)>,<DeviceType>	Deprecated. Plain text users to get imported - if import fails, reason gets added as last entry on each item. These setting is best maintained via the admin interface.
[CLIENTS]	{<Device KEY>}	encrypted active user's entries	Encrypted active users' entries. These setting is best maintained via the admin interface.
[DEFAULT_APICONTROL]	COUNT	Numeric	Max Rest API access count
	UNIT	Min	Unit (Second, Minute, Hour, Day)
[DATABASES] Supported databases.	SQLite	SQLITE	SQLITE database
	MySQL	MY SQL	MY SQL database

Tag	Key	Values	Description
[ACTIVE_DATA-BASE]	Name	mysql	Specifies the active data-base that the Media Server will use for storing and retrieving data. In this configuration, it is set to mysql, indi-cating that MySQL is the active data-base.
[MYSQL]	SERVER_ADDRESS	MY SQL Server Address	Server ad-dress for MY SQL. 127.0.0.1 or “localhost” If MY SQL is in-stalled lo-cally.
	USER_NAME	MySQL Username	Username for MySQL data-base
	PASSWORD	Encrypted Password	Password for MySQL data-base
	PORT	MY SQL Port	Port for MySQL data-base
	DATABASE_NAME	MY SQL Schema name	Name of the Schema

Tag	Key	Values	Description
	DEBUG_TRANSACTION	True/False	This parameter if set true will print the queries to be executed as part of the MySQL transaction. By default, this will be false.
	CONNECTION_ERROR_CODES	Error codes	This parameter denotes the comma separated connection error codes for MySQL
[LOGS]	MAX_LOG_SIZE	In MB, KB or GB. Example: 10MB	Default to 10MB if not set. Units MB, KB and GB can be used. Once a log file has reached the max size, it will be “rotated” and renamed to <Logfile-name>. <start Timestamp>-<end timestamp>.<log extension>. Once the oldest file has past the defined MAX_FILE_ROTATIONS, it will be removed. This means

Tag	Key	Values	Description
			setting MAXFILESIZE to 100MB and MAX_FILE_ROTATIONS to 5, up to 600MB of storage can be used by each log type.
	MAX_FILE_ROTATIONS	Numeric	Max log rotations kept - once a log-file's rotation index has exceeded the indicated number, the file will be deleted.
	FTPLOG	FTP log file path	Fully qualified path to the current FTP Log. If set to an empty string, commented out, or removed, the ftp log is disabled. Default Location= C:\media-server-images\logs\ftplog.log
	FILESYNCLOG	File Synch log file path	Fully qualified path to the current File Sync logs. If

Tag	Key	Values	Description
			set to an empty string, commented out, or removed, the File Sync log is disabled. Default Location= C:\media-server-images\logs\filesynclog.log
	FTPSLOG	FTPS log file path	Fully qualified path to the current FTPS logs. If set to an empty string, commented out, or removed, the FTPS log is disabled. Default Location= C:\media-server-images\logs\ftpslog.log
	SFTPLOG	SFTP log file path	Fully qualified path to the current SFTP logs. If set to an empty string, commented out, or removed, the SFTP log is disabled. Default Location= C:\media-server-images\logs\sftplog.log

Tag	Key	Values	Description
	GENLOG	General log file path	Fully qualified path to the current general log. If set to an empty string, commented out, or removed, the general log is disabled. Default Location= C:\media-server-images\logs\genlog.log
	CLEANUPLOG	Cleanup log file path	Fully qualified path to the current file cleanup log. If set to an empty string, commented out, or removed, the cleanup log is disabled. Default Location= C:\media-server-images\logs\cleanuplog.log
	ETLLOG	ETL log file path	Fully qualified path to the current ETL log. If set to an empty string, commented out, or removed, the ETL log is disabled.

Tag	Key	Values	Description
			Default Location= C:\media-server-images\logs\etllog.log
	ETLPLOG	ETL Process profiling log file path	Fully qualified path to the current ETLP log. If set to an empty string, commented out, or removed, the ETLP log is disabled. Default Location= C:\media-server-images\logs\etlprofile.csv
	ETLLOCK	ETL Lock file path	Lock files which contain the offset of the record during ETL process, 0 is the default value. Default Location= C:\media-server-images\logs\etl.lock
	OIDCLOG	OIDC log file path	Fully qualified path to the OIDC (OpenID Connect) log file. If set to an empty string,

Tag	Key	Values	Description
			commented out, or removed, OIDC logging is disabled. Default Location= C:\media-server-images\logs\oidc.log
	FILESYNCLOG_LEVEL	DEBUG|INFO|WARN|ERROR|FATAL|OFF	Default Log level for the File Sync logs. Possible Options are in order of most details logged to least: DEBUG|INFO|WARN|ERROR|FATAL|OFF
	FTPLOG_LEVEL	DEBUG|INFO|WARN|ERROR|FATAL|OFF	Default Log level for the FTP logs. Possible Options are in order of most details logged to least: DEBUG|INFO|WARN|ERROR|FATAL|OFF
	SFTPLOG_LEVEL	DEBUG|INFO|WARN|ERROR|FATAL|OFF	Default Log level for the SFTP logs. Possible Options are in order of most

Tag	Key	Values	Description
			details logged to least: DE-BUG|INFO|W ARN|ER-ROR|FA-TAL|OFF
	FTPSLOG_LEVEL	DEBUG|INFO|WARN|ER-ROR|FATAL|OFF	Default Log level for the FTPS logs. Possible Op-tions are in order of most details logged to least: DE-BUG|INFO|W ARN|ER-ROR|FA-TAL|OFF
	GENLOG_LEVEL	DEBUG|INFO|WARN|ER-ROR|FATAL|OFF	Default Log level for the GENLOG logs. Possible Options are in order of most details logged to least: DE-BUG|INFO|W ARN|ER-ROR|FA-TAL|OFF
	CLEANUPLOG_LEVEL	DEBUG|INFO|WARN|ER-ROR|FATAL|OFF	Default Log level for the CLEANUP-LOG logs. Possible Op-tions are in order of most details logged to least: DE-BUG|INFO|W

Tag	Key	Values	Description
			ARN|ER-ROR|FA-TAL|OFF
	ETLLOG_LEVEL	DEBUG|INFO|WARN|ER-ROR|FATAL|OFF	Default Log level for the ETLLOG logs. Possible Options are in order of most details logged to least: DE-BUG|INFO|W ARN|ER-ROR|FA-TAL|OFF
ETLPLOG_LEVEL	DEBUG|INFO|WARN|ER-ROR|FATAL|OFF	Default Log level for the ETLPLOG i.e., ETL pro-cess profiling logs. Possible Options are in order of most details logged to least: DE-BUG|INFO|WARN|ER-ROR|FATAL|OFF	
OIDCLOG_LEVEL	DEBUG|INFO|WARN|ER-ROR|FATAL|OFF	Default Log level for the OIDCLOG logs. Possible Options are in order of most details logged to least: DE-BUG|INFO|WARN|ER-ROR|FATAL|OFF.	
[DEVICE_TYPES] List of Device types available on the device dropdown on the FTP De-vices dialog of the	LECTOR	Lector	Lector device type
	ICR	ICR	ICR device type

Tag	Key	Values	Description
admin web interface and their internal representation. The external representation can be changes to reflect localization etc.	IP1TEXTFILE	IPCam - 1 text file mode	IPCAM 1 text file mode device type
	IP2TEXTFILE	IPCam - 2 text file mode	IPCAM 2 text file mode device type
	EVENTCAM	Event Cam	Event Cam device type
	OTHER	Other Source	Device Types other than mentioned above
	ICR890-4	ICR890-4	Configuring SAMBA server devices
	Inspector-P	Inspector-P	Inspector P cameras are supported by Sick MS
	CERT_PATH	PFX Certificate File Path	The file path where the certificate is placed.
	CERT_PASSWORD	PFX Certificate password	PFX Certificate password

Tag	Key	Values	Description
	CERTIFICATE_KEY	Key	PEM format certificate public key path
	PRIVATE_KEY	Key	PEM format certificate private key path
	* VALIDATION_INTERVAL	Minutes	Time interval to validate the certificate expiry. The interval is in minutes. Default is 2.
	CERTIFICATE_FORMAT	PFX / PEM	Defines the format of the certificate file. Default is PFX.
	USE_CUSTOM_CERTIFICATE	true/false	Decides if certificate details are taken from a dedicated properties file. Default is false.
	CERT_CONFIG_PROPERTIES	File Path	Complete path of the dedicated certificate properties file. Default is empty.

Tag	Key	Values	Description
	PROPER-TIES_CERT_PATH_FIEL D	Key	Field name in the properties file for the certificate path. Default is empty.
	PROPERTIES_PASS-WORD_FIELD	Key	Field name in the properties file for the certificate password. Default is empty.
	PROPERTIES_PASS-WORD_ENCODED	true/false	Indicates if the certificate password is encoded in the properties file. Default is false.
[FILESYNC_SERV ER] List of valid ports by protocol. Addi-tional protocol will be added to the list as implemented.	PORT	Port	SFTP Server Port
	TIMEOUT	Numeric	SFTP Server/De-vice Connec-tion timeout
	USER_NAME	username	SFTP server username
	PASSWORD	Encrypted Password	SFTP server password

Tag	Key	Values	Description
	ENABLED	True/false	Enable/Disable the File Sync operation
[FILESYNC_Client] List of valid ports by protocol. Additional protocol will be added to the list as implemented.	SERVER_ADDR	IP	Backup server IP address
	USER_NAME	username	Backup server username
	PASSWORD	Encrypted Password	Backup server password
	PORT	Port	Backup server port number. Communication established using SFTP protocol
	TIMEOUT	Numeric	SFTP Server/ Device Connection timeout
	RETRY_INTERVAL	Numeric	Retry Interval for file sync operation in seconds (E.g., 5 minutes: 5 * 60 = 300)

Tag	Key	Values	Description
	RETRY_COUNT	Numeric	Retry Count for file sync operation
	NO_OF_FS_Clients	Numeric	Number of File sync client threads to serve the incoming data. Default will be 1
	FILESYNC_QUERY_COUNT	Numeric	Number of data to be retrieved from Filesyncindex for processing. Default will be 2000
	FILESYNC_QUERY_COUNT	Numeric	Number of data to be retrieved from File index for syncing. Default will be 2000
	COMPRESS_FEATURE	True/False	If set to true, the compress feature will be available. By default, it will be false.
	COMPRESS	True/False	Data to be synced will be zipped if set to true.

Tag	Key	Values	Description
	COMPRESS_BATCH	Zip file	Batch size for zip file
	USE_DOWNTIME	True/False	If set to true it will update the file sync schedules with Down-time sched-ules. If even one down-time schedule is selected, this will be set to true and if none is selected this will be set to false. If false, Downtime schedules will not be up-dated.
	BANDWIDTH_TYPE	MAX, Custom	The band-width type can be MAX which will uti-lize the full available bandwidth. The other type is CUS-TOM, which allows the user to cus-tomize the bandwidth
	BANDWIDTH_UNIT	MBPS, KBPS, IPM	Customized bandwidth unit. Can be MBPS, KBPS, IPS

Tag	Key	Values	Description
			(images per sec) or IPM (images per min)
	BANDWIDTH_VAL	Numeric	Customized bandwidth value.
	SECOND-ARY_HTTP_AUTH	True/False	If set to true primary server will au-thenticate while con-necting to Secondary server using HTTP/S pro-tocol. Default will be true.
	SECOND-ARY_HTTP_USER	Username	Username to connect to secondary server using HTTP/S pro-tocol.
	SECOND-ARY_HTTP_PWD	Password	Encrypted password to connect to secondary server using HTTP/S pro-tocol
	SECOND-ARY_HTTPS_BINDIP	IP	Secondary server HTTPS bind IP. By de-fault, it will consider the

Tag	Key	Values	Description
			server address
	SECONDARY_HTTPS_PORT	Ports	Secondary server HTTPS port. By default, it will be 443.
	SECONDARY_HTTP_BINDIP	IP	Secondary server HTTP bind IP. By default, it will consider the server address
	SECONDARY_HTTP_PORT	Ports	Secondary server HTTP port. By default, it will be 8084
	UPDATE_USER_INTERVAL	Seconds	Interval in seconds for updating the user details to secondary server. By default, it will be 60 seconds
	DELETE_IDLE_TIME	Minutes, seconds and hours	This parameter decides how long should cleanup be idle before resetting an internal flag to false. By

Tag	Key	Values	Description
			default, this will be 30M. Minimum can be 5 mins and maximum can be 1 hour. Anything less than 5 Mins it will reset to 5Mins, and anything more than an hour will reset it to an hour
	SEND_USERNAMES_INTERVAL	Minutes, seconds and hours	Based on the interval value set in this parameter it will be checked if all user details are sent to secondary. If even one user is found whose details are not sent to the secondary the user details will again be sent and this repeats in the configured interval time. This value is in seconds. By default, it is 300 seconds which is 5 mins.
	SYNC_UPLOAD_TIMEOUT	Minutes, seconds and hours	If the upload of file takes more than

Tag	Key	Values	Description
			this configured value, it will terminate the upload operation. By default, this is set to 2 minutes.
	*CHECK_EXT_SERVER_HTTP_CONNECTION	Minutes, seconds and hours	Time interval to keep checking HTTP connection to secondary server. The time is in seconds. Default is 60
	* FS_INTERVAL	Days, Minutes, seconds and hours	Amount of time between two consecutive File sync cycles per file sync client. It can be set in milli seconds (MS), seconds(S), minutes(M), hours(H), days(D). By default, it is 10S.
	* PARALLEL_SYNC	True/False	Send Sync Data to secondary server parallelly for all File sync clients. By default, it is true.

Tag	Key	Values	Description
	*FW_QUEUE_COUNT_FS	Numeric	The File writer Queue size when File sync needs to be slowed down. The default value is 200
	* FS_SLOWDOWN_TIME	Milli seconds	Slowing down File sync operation by introducing a time gap determined by this parameter when File writer Queue is high. This value is in milli seconds. By default, it is 500
	* MAX_UPDATE_Q	Numeric	The Maximum size of DB Update Queue. When Queue size is greater than equal to this value the file sync status update will be halted until the size reduces to zero. By default, the value is 200
	* MAX_STATUS_UPDATE_WAIT	Days, Minutes, seconds and hours	Wait time for Update Queue being

Tag	Key	Values	Description
			processed. If the Queue size is below threshold and the time to process the Queue is beyond this parameter value, it terminates the halt and continue with Status update. It can be set in milli seconds (MS), seconds(S), minutes(M), hours(H), days(D). By default, it is 10M.
BYPASS_USERS	USERS	API	Encrypted list of API users for which session verification will be bypassed when Authenticate API is enabled
[INVENTORY]	INSERT_BATCH	Numeric	This will decide the batch size for the records being inserted during migration. By default, the value will be 500. This value should

Tag	Key	Values	Description
			be set based on the query length supported by MYSQL. Minimum value should be 1.
	IS_ETL_ACTIVE	True/False	These settings are indicators for Media Server to decide whether it must check for migration or not. MS will set this flag to true, when migration from SQLite to MySQL starts and sets it to false when the migration gets completed. Default value is false. Note: This value will be set to false if Active DB is SQLITE. If these settings are changed manually to false, it will stop the migration to trigger during MS restart. It is recommended not to change

Tag	Key	Values	Description
			these settings manually.
	RETRY_DURATION	Numeric	Time duration to retry connecting to the MySQL database when it's failed to establish the connection between MS and MySQL, default value is 1 second
	IS_DATA_TO_MIGRATE	True/False	To identify if there are records to migrate, this will set by MS when migration from SQLite to MySQL fails, default value is false. This value will be set to false if Active db is SQLITE
	INVENTORY_FILETYPE	jpeg, jpg,xml,bmp,mp4,pcd,mkv,txt,zip,png,ply,tiff,tif	Specifies the file types to be inventoried. By default, jpeg, jpg, xml, bmp, mp4, pcd, mkv, txt, zip, png, ply, tiff, tif will be considered

Tag	Key	Values	Description
[SMB_Device]	CONN_TIMOUT	In seconds /minutes/hours. Example: 60M	SAMBA Server/Device Connection timeout (S/M/H)
	RETRY_COUNT	Numeric	Retry Count for SAMBA device-server connection
	RETRY_DURATION	Numeric	Retry Interval for SAMBA device-server connection in milliseconds
[ERROR_IMAGE]	FORMATS	Extensions. Example: FORMATS=jpg, jpeg,bmp,png	Supported image formats
[LINUX]	SUPPORTED_FILESYSTEM	Filesystem Names. Example: | EXT4|BTRFS|XFS|	These are the supported Filesystems. To add a new filesystem append it to the list followed by "|". To remove any filesystem remove it along with "|" succeeding the filesystem.
SCHEDULE_ACTIVITY	FILESYNC	True/False	By default, it is true

Tag	Key	Values	Description
This represents the services which will function based on schedule. Services set to true will function based on a schedule.	TAGGING	True/False	By default, it is true
	TAGGED_DELETION	True/False	By default, it is true
USE_DOWNTIME This represents the services which would be using Downtime schedule. Services set to true will use downtime schedule.	FILESYNC	True/False	By default, it is true
	TAGGING	True/False	By default, it is true
	TAGGED_DELETION	True/False	By default, it is true
TAGGING_SERVICE	ENABLED	True/False	This parameter decides if the tagging feature is enabled or disabled. If set to true tagging will be enabled. By default, it is set to false
	*FW_QUEUE_COUNT_TAG	Numeric	The File writer Queue size when tagging needs to be slowed down. The default value is 200

Tag	Key	Values	Description
	*TAGGING_SLOW-DOWN_TIME	Numeric	Slowing down Tagging operation by introducing a time gap determined by this parameter when File writer Queue is high. This value is in milli seconds. By default, it is 500
	*ACTION_CRITERIA_INTERVAL	Numeric	Time interval between consecutive cycles to update the action criteria. It can be set in milli seconds (MS), seconds(S), minutes(M), hours(H), days(D). By default, it is 15S.
	*PARALLEL_REQUEST	True/False	Send inference request to Deep Learning App parallelly for all users when this parameter is true. By default, it is set to false

Tag	Key	Values	Description
	TAG_ACTION_UP-DATE_BATCH	Numeric	Number of media Keys to be updated at a time is determined by this parameter. By default, it is 100.
IMAGE_INFER-ENCE APP	HTTPS_SUPPORT	True/False	This indicates if image inference app has https support. By Default, this will be false
	HTTPS_IP	IP	The HTTPS IP Address where the App Engine Image Inference App is running
	HTTPS_PORT	Port	The HTTPS Port where the App Engine Image Inference App is running
	HTTP_IP	IP	The HTTP IP Address where the App Engine Image Inference App is running

Tag	Key	Values	Description
	HTTP_PORT	Port	The HTTP Port where the App Engine Image Inference App is running
	ALGORITHM_API	API	API to get Algorithms from App Engine
	INFERENCE_API	API	API to get the inferences from App Engine
TAGGING_INTERVALS	BATCH_INTERVAL	Numeric and Text	The Image Tagging is done in batches of this specified interval. The minimum value can be 1H and maximum 30D. By default, it will be 1D.
	OLDEST_TS_INTERVAL	Numeric and Text	The Image Tagging calculates the timestamp of the oldest untagged image for each User. It refreshes this timestamp value at THIS interval, so it doesn't miss

Tag	Key	Values	Description
			anything. By default, it will be 1H.
RULE_TYPES It provides the available rule types of an corresponding priority. The priority is a numerical value. 1 being the highest priority	MAX_COUNT	Count	This describes rules for clearing data based on count (no of files)
	MAX_SPACE	Space	This describes rules for clearing data based on the space occupied.
[BARCODE_COUNTER]	ENABLED	FALSE	Toggles the barcode counter feature on/off.
	OBJECT_DETAILS_FILEPATH	C:\media-server-images\DataAcqImgDir	Directory where XML-parsed details or barcode data files are stored.
	UID_FILENAME_IDX	0	Zero-based index of the UID in the incoming filename (split by delimiter).
	DATE_FILENAME_IDX	1	Zero-based index of the

Tag	Key	Values	Description
			date component in the incoming filename.
	TIME_FILENAME_IDX	2	Zero-based index of the time component in the incoming filename.
	DELIMITED_TS	FALSE	Indicates whether date and time are separated by a delimiter in the filename.
	DELIMITED_TS_OUTPUT	TRUE	If true, outputs date and time separated by _ in the output filename.
	TS_FILENAME_IDX	1	Zero-based index of the timestamp field if date/time are combined in a single field.
	DELIMITER	_	Delimiter used in the incoming filename (e.g., _, -).

Tag	Key	Values	Description
	RETRY_ATTEMPT	3	Number of retry attempts to retrieve file path and metadata in case of failure.
	RETRY_INTERVAL	2S	Time interval between retries (e.g., 2S = 2 seconds).
	GET_2_ON_FULL_FAILURE	FALSE	If true, attempts to fetch a _2 version of the file if the primary file is missing.
	CHECK_TRACKING_ID_LENGTH	TRUE	If true, validates the length of the extracted tracking ID. Mismatch results in ???.
	TRACKING_ID_LENGTH	18	Expected length (in characters) of the tracking ID. Used when CHECK_TRACKING_ID_LENGTH is enabled.

Tag	Key	Values	Description
	POPULATE_PARTICULAR_PATTERN	TRUE	If true, the tracking ID must match the regex defined in PARTICULAR_PATTERN.
	PARTICULAR_PATTERN	^[1-9][zZ].*	Regular expression pattern that the tracking ID must match (e.g., starts with digit 1–9 followed by z or Z).
	ROTATE_OUTPUT_FILE	TRUE	If true, output files are rotated and retained based on file size and retention days. Default is TRUE.
	OUTPUT_FILESIZE_THRESHOLD	30MB	Output file size threshold for rotation. Supported units are KB, MB, GB, and TB. Default is 30MB; if set to 0, it resets to 30MB.
	OUTPUT_FILE_RETENTION_PERIOD	7D	Number of days to retain output files before

Tag	Key	Values	Description
			deletion. Default is 7D; if less than 1 day, it resets to 1 day.
[BARCODE_COMBINATION_PRIORITY]	1=C128;^1Z.*	N/A	Defines priority-based mapping for barcode types and regex patterns. The number indicates priority (1 = highest). Format: priority=type;regex.
[EMBED_TEXT_ON_IMAGE]	ENABLED	TRUE/FALSE	Enables or disables embedding disclaimer text on top of images. If true, the configured message strip will be generated and overlaid on images.
	EMBED_MSG	String	The text message to embed over the image (for example, legal or disclaimer text). This text can be customized.

Tag	Key	Values	Description
	EMBED_MSG_LENGTH	Numeric	Maximum number of characters allowed for the embedded message. Messages longer than this will be truncated. Default is 500.
	STRIP_CACHE_SIZE	Numeric	Size of the cache that stores strips of different resolutions so that they can be reused for similar images.
	STRIP_CACHED	TRUE/FALSE	If true, generated strips are cached so they can be reused for images with the same resolution, improving performance.
	MINIMUM_FONTSCALE	Decimal	Lower bound for the font scale used when rendering the message. If the computed font scale is below this value, it is

Tag	Key	Values	Description
			clamped to this minimum. Values lower than 0.3 are reset to 0.3.
	RE-STRICT_STRIP_HEIGHT	TRUE/FALSE	If true, the strip will only be attached if its height does not exceed the configured percentage of the image height.
	STRIP_HT_PERCENT-AGE	Numeric	Maximum allowed strip height as a percentage of the image height. If the strip is taller than this, it will not be attached. Default is 100.
[CORS_RE-SPONSE_HEAD-ERS]	Access-Control-Allow-Origin	*	Allows requests from all origins (*).
	Access-Control-Allow-Credentials	TRUE	Allows browsers to expose response to front-end JavaScript when credentials are included.

Tag	Key	Values	Description
	Access-Control-Allow-Methods	GET, PUT, POST, DELETE	HTTP methods allowed for cross-origin requests.
	X-Content-Type-Options	nosniff	Prevents MIME type sniffing for security.
	X-XSS-Protection	1;mode=block	Enables XSS protection in browsers and blocks detected attacks.
	Strict-Transport-Security	max-age=31536000	Forces HTTPS for 1 year (31536000 seconds).
	Content-Security-Policy	frame-ancestors *	Controls which sites can embed this content in a frame/iframe.
	X-Frame-Options	SAMEORIGIN	Allows the page to be displayed in frames only from the same origin.

Tag	Key	Values	Description
	Cross-Origin-Embedder-Policy	unsafe-none	Disables cross-origin isolation; required for certain embedded resources.
	Cross-Origin-Opener-Policy	same-origin-allow-popups	Allows popups from same origin to share browsing context.
	Cross-Origin-Resource-Policy	cross-origin	Controls loading of cross-origin resources.
	X-Permitted-Cross-Domain-Policies	none	Disables Adobe cross-domain policy file access.
	Referrer-Policy	strict-origin-when-cross-origin	Sends only origin on cross-origin requests unless secure.
	Permissions-Policy	geolocation=(self), microphone=(), camera=()	Controls access to browser features like geolocation, microphone, and camera.

Tag	Key	Values	Description
	Cache-Control	no-store	Prevents caching of responses.
	Clear-Site-Data	"cache"	Clears browser cache data when requested.

23.4Queue Details

Queue	Config parameter	Description	Impact
Cache	FileMetaCache	Contains the meta data of the image file. This is set as 1000 in config file. If this value is not set in the config file, then the default value will be set to 0. The information in this queue is helpful for faster retrieval of image.	High Value: It can be set to a high value, which will not affect the memory usage adversely. In addition, it could make the image retrieval process faster if the image searched for is a recent image. **Low Value**: For Example, if it is set to 0, every time the image retrieval will have to search in the DB and the chance of searching the DB becomes higher. This will put additional load on the DB.
File writer Queue	FW_QUEUE_LIMIT_BY_SIZE	This parameter decides if the file writer queue capacity will be size based, or count based. If true it will be size based. By default, it will be set to true.	

Queue	Config parameter	Description	Impact
	FW_QUEUE_SIZE_LIMIT	The maximum capacity based on number of bytes that can be stored in the file writer queue. If it is set to zero, then by default it will be quarter of the total physical memory. It needs to be set properly to not exceed the total physical memory. If it exceeds the total physical memory, it will be reset to default.	
	FW_TEMP_QUEUE_SIZE_LIMIT	The size of the temp File writer queue to store data when minimum free space has reached. The size will be based on number of bytes. If it is set to zero, then by default it will be quarter of the total physical memory. It needs to be set properly to not exceed the total physical memory. If it exceeds the total physical memory, it will be reset to default.	
File Index Queue	Not configured	This queue contains the Data insertion query (for both file index and file sync index tables). The queue size is unlimited.	There is no value set for this queue. It is **Unlimited.** However, if there is a lot of data queued up in this queue (which could happen due to various reasons like system being busy or processing some other query etc.) the processing might take time.

Table 14: Queue Details

Note: *There are four File writer Queues that are*

- ***Full*** *- For processing Full images*
- ***Thumb*** *- To process thumb images*
- ***Thumb_copy*** *--To process txt files for IPCam type of device*
- ***Support*** *- To process xml (or other support files) files*

Each of these queues will be assigned the configured file writer queue size

23.5 Configuring Barcode Counter Using sick-bip-is.cfg

This section provides step-by-step instructions for configuring the **Barcode Counter** in the sick-bip-is.cfg file. It explains how to enable barcode tracking, define file paths, set filename parsing rules, configure retry mechanisms, validate tracking IDs, and establish barcode processing priorities.

1. Enabling the Barcode Counter

You can enable or disable barcode tracking by modifying the configuration:

```
[BARCODE_COUNTER]
 ENABLED=true
```

Set `ENABLED` to `true` to enable barcode tracking. If set to `false`, barcode data will not be processed.

2. Specifying the Output File Path

Define the directory where the output file containing parsed XML details will be stored:

```
OBJECT_DETAILS_FILEPATH=D:\media-server-images\DataAcqImgDir
```

Modify this path to match your system's storage location.

3. Configuring Filename Parsing Rules

You can specify the positions of UID, Date, and Time in the filename. Indexing starts from 0:

```
UID_FILENAME_IDX=0
DATE_FILENAME_IDX=1
TIME_FILENAME_IDX=2
```

If the filename follows the format YYYYMMDD_UID_HHMMSS.xml, update the indices accordingly:

```
DATE_FILENAME_IDX=0
UID_FILENAME_IDX=1
TIME_FILENAME_IDX=2
```

Ensure the correct delimiter is set:


```
DELIMITER=_
```

4. Handling Timestamps

Control how timestamps are extracted and formatted in filenames and output files:

```
DELIMITED_TS=false
DELIMITED_TS_OUTPUT=true
TS_FILENAME_IDX=1
```

If `DELIMITED_TS=false`, the system expects the date and time to be combined without a separator in the filename. In the output file, they will be separated by _.

5. Configuring Retry Mechanisms

Define how the system handles missing files by setting retry attempts and intervals:

```
RETRY_ATTEMPT=3
RETRY_INTERVAL=2S
GET_2_ON_FULL_FAILURE=false
```

The system retries three times at two-second intervals. If `GET_2_ON_FULL_FAILURE=true`, it will attempt to retrieve an alternate "_2" file when the primary file is unavailable.

6. Configuring Tracking ID Validation

```
CHECK_TRACKING_ID_LENGTH=true
TRACKING_ID_LENGTH=18
POPULATE_PARTICULAR_PATTERN=true
PARTICULAR_PATTERN=^[1-9][zZ].*
```

If a tracking ID does not meet the required length or match the defined pattern, it will be replaced with "???". Modify these parameters based on your validation requirements.

7. Defining Barcode Type and Pattern Mappings

Specify barcode types and their corresponding patterns:

```
{93dd7140-fe5c-11ee-b56f-848bcd401ebe}=C128$$1z.*
{93dfbaae-fe5c-11ee-b56f-848bcd401ebe}=PDF$$3Z.*
{93e46e78-fe5c-11ee-b56f-848bcd401ebe}=EAN128$$2z.*
{dc7429d4-23b0-11ef-b791-848bcd401ebe}=C128$$.*006
{e4df8802-23b0-11ef-b872-848bcd401ebe}=MAXI$$.*
```

Modify these mappings to match the barcode formats used in your system.

8. Setting Barcode Processing Priorities

If a package contains multiple barcodes, you can define the processing priority. The system will first attempt to process the highest-priority barcode. If that barcode is not present, it moves to the next priority, ensuring only the most relevant barcode is used.

```
 [BARCODE_COMBINATION_PRIORITY]
1=C128;^1z.*
2=C128;^1z.*
```

In this example:

- If a package contains multiple barcodes, the system first checks for `C128;^1z.*`.
- If `C128;^1z.*` is not present, it moves to the next priority barcode, `C128;^1Z.*`.
- You can define multiple barcode priorities based on your system's processing needs.

Configurable Filename Date Format

The date format used in the barcode counter filename can be configured using the parameter **OBJECT_DETAILS_FILENAME_DATE_FORMAT**.

This parameter is located under the **barcode_counter** configuration and can be modified using the Configuration API.

Example Configuration

The following example configures the filename format to include **year, month, day, and hour**:

```
barcode_counter {
    OBJECT_DETAILS_FILENAME_DATE_FORMAT = YMD_H
}
```

With this configuration, the generated barcode counter file follows this pattern:

```
DataAcqImgDir_YYYYMMDD_H.log
```

Example:

```
DataAcqImgDir_20260304_14.log
```

Supported Formats

Format	Example Filename
YM	DataAcqImgDir_202603
YMD	DataAcqImgDir_20260304
YMD_H	DataAcqImgDir_20260304_14
YMD_HM	DataAcqImgDir_20260304_1430

If an unsupported format is configured, the system automatically falls back to the default format **YMD_H**.

24 Troubleshooting

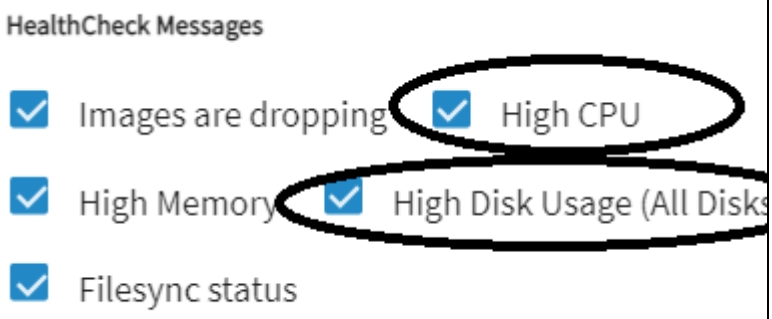
Acronyms	Meaning
MS	Media Server
DB	Database
FV	Facility View

#	Known Conflicts
1	Make sure the port used by the Anti-virus does not conflict with any of the port used by Media Server
2	Make sure the Anti-virus does not block the ports used by Media Server. Please connect with organization IT team to open associated ports

#	Issue	Possible Known Causes & Resolution/Workaround
1	Installer message - "Error while Checking for Instances" or Installer says "Repair".	Delete the hidden folder -"C:\Program Files\Zero G Registry"
2	Application not working/ Services not coming up	**Cause** Port conflict between HTTP and HTTPS with already running processes Resolution Update this port range from the sick-bip-is.cfg config file. **Cause** Port conflict between FTP, SFTP, FTPS File sync, UDS along with any existing process running in machine Resolution

		You can update the Port values by launching the Media Server application and editing the FTP, SFTP FTPS, HTTP and HTTPS File sync Ports OR from the sick-bip-is.cfg config file
3	License is applied but MAC does not match	**Cause** The license generated is with a MAC that is not present in the list. **Resolution** Send an e-mail to analytics.registration@sick.com and request a new license with all MACs added to it.
4	Unable to start/stop/restart services using Services application in windows	**Cause** The services are installed with admin privileges, so a non-admin user may not have permissions to start/stop/restart an admin process. **Resolution** Log in as admin or as a user with admin privileges
5	Images getting discarded/rejected if the Min free disk limit is reached and deletion rate is less than the incoming rate	Cause Disk Usage issue. Minimum free disk limit has reached, and the deleting rate is less than the incoming file rate. **Resolution** Decrease the minimum free disk space value. Refer to Disk Usage Summary.
6	Unable to publish heartbeat data over HTTPS (publish URI and auth URI in heartbeat settings)	Cause You do not have permission for HTTPS protocol or Certificate is expired/invalid. **Resolution** Send an e-mail to analytics.registration@sick.com and request a new license with HTTPS enabled or apply a valid certificate
7	Any of the feature stopped working after few successful attempts.	Cause API control limit exceeded. **Resolution** Wait for the next time interval OR request to increase the API control limit if the feature is used extensively Refer to API Configuration
8	Application is not working over HTTPS	Cause You do not have permission OR Certificate is invalid/expired. **Resolution**

		Send an e-mail to analytics.registration@sick.com and request a new license with HTTPS enabled or apply a valid certificate
9	IPCam images are not getting stored at correct location or are getting stored in tmp folder.	**Cause** Issue with IPCam configuration. **Resolution** Make sure IPCam configuration (Username, Password, protocol) is correct. Navigate to IPCam device under Devices tab and edit/update the configuration. Refer Edit Device **Cause** Control file is not received. **Resolution** Make sure you have permission for control file type. If you do not have permission, send an e-mail to analytics.registration@sick.com and request a new license with control file permissions. **Cause** Sequence ID is resetting before TEMPFILE_MAXAGE is clearing out older tmp file. **Resolution** TEMPFILE_MAXAGE should be tuned in such a way so that the tmp file cleanup happens before IPCam tmp file SEQ ID is reset. IPCam Seq ID resets after sending out 1024 tmp files. Identify the fastest time taken to push 1024 images to IPCam and set TEMPFILE_MAXAGE less than this time.
10	Data not getting stored in MySQL DB	Cause MySQL is down. **Resolution** Start Media server services if down. If Media Server service fails to restart due to no space, then clear out space from disk where MySQL and MySQL data is available. Then restart Media Server Service. **Cause** Permission issue with MySQL user. **Resolution** User used to connect to MySQL DB should have appropriate permissions.

11	Files with specific extensions are getting discarded	**Cause** File Type is not Licensed. **Resolution** Send an e-mail to analytics.registration@sick.com and request a new license with file type permissions.
14	Errors in console on trying to start two services quickly within seconds	**Cause** Known issue on trying to start two services quickly within seconds. **Resolution** Wait for some time say around 3- 5 minutes before starting the second service.
15	High CPU Utilization is observed on pushing Heartbeat data	**Cause** Known issue on pushing Heartbeat messages to FV when High CPU and High Disk Usage option is selected for Health Check. **Resolution** Disable CPU Utilization and Disk Utilization Heartbeat check messages from UI if not required. This issue will be fixed in next release. 
16	Image Loss/ Files available in file index queue not getting saved in DB on MS shutdown	**Cause** Media Server is busy Media Server is stopped or restarted Images are being acquired at high rate High file index queue depth **Resolution** When high file index queue (refer debug mode for genlog) keep MS idle for few minutes and then perform Media Server shutdown.
17	Application stopped working after Antivirus update	**Cause** Ports used by the application are not exempted from file scanning.

		Resolution Exempt the ports used by the application from file scanning.
18	Application stopped working after Anti-virus update even though Ports are exempted from scanning.	**Cause** Anti-virus update is blocking ports **Resolution** Exclude Media Server from Anti-virus scanning Gracefully Shut down Media Server before Anti-virus update is done.
19	Application is not acquiring images and user is unable to shut down the application gracefully	**Cause** The connection hangs when there is an anti-virus update followed by a restart. **Resolution** Allow Media Server for Anti-virus scanning Gracefully Shut down Media Server before Anti-virus update is done.
20	Slow Performance due Spike in Memory	**Cause** Memory goes high when recalculation query is running. **Resolution** It will automatically get too normal after some time once the recalculation query is completed.
21	Application crashes on starting	**Cause** This issue rarely happens and could be due to faulty module secureblackbox20.dll **Resolution** Third party Library provider will have to provide fixes for secureblackbox20.dll
22	The folder location does not get deleted while Manual clean-up	**Cause** This could be due to the Folder opened in Windows explorer **Resolution** Close the folder and manually delete it.
23	Few Images are not deleted during clean-up	**Cause** Folders are not purging in the root directory on clean-up due to high age-out rule of IPCAM.

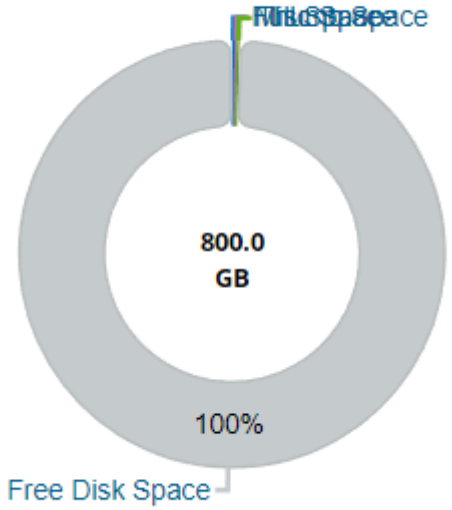
		Resolution Delete data manually from the folder location.
24	Large set of images are accumulated for deletion at the Start of Media Server	**Cause** Cleanup operation only starts after MS has calculated the total space taken by full and thumb images. **Resolution** Wait for recalculation to happen.
25	Images are getting discarded	**Cause** Images are missing/getting discarded due to file-writer-queue at max-depth. Check application logs in debug mode. **Resolution** Increase the file-writer-queue size in media server config file **Cause** Images are being discarded due to low disk space. Check application logs in debug mode. **Resolution** Clear the disk space **Cause** Image type is not licensed Check application logs in debug mode. **Resolution** Request for updated license with supported image type **Cause** Media Server IP Address mentioned as 127.0.0.1 and bind IP is mentioned as localhost in the config file **Resolution** Update the IP Address to Global IP 0.0.0.0 OR Machine IP if the Media Server is installed locally and IP Address is mentioned as 127.0.0.1
27	Image for IPcam device is not coming up as expected	**Cause** Issue could be due to Duplicate control file received. **Resolution** In case of Duplicate control file, First In First Out concept will be used and the associated image will be renamed based on the first control file received.

29	Connection with MySQL Server could not be established	**Cause** Issue with connection settings. Check application log files. **Resolution** Revisit the MS config file and make sure all the connection settings including MySQL Server address and port is correct. Refer to Database **Cause** Traffic from a different source is not supported in my.ini file. Check bind-address value in my.ini file. **Resolution** Update FV MySQL my.ini to support traffic from a different source. Open my.ini file at location C:\Program Files\SICK\Analytics Solutions\MySQL Data and update the bind-address value to 0.0.0.0 **Cause** Server is not listening on the specified port as Antivirus or Firewall is blocking the ports. You can check it by running netstat -an | find "8406" command in command prompt. If the port does not get listed, then server is not listening on the specified port. Username used for MySQL connection does have enough permission **Resolution** Ports used and ports for FTP passive mode may need any random ports. Make sure MS is added to exception from Antivirus and Firewall. Give complete CRUD writes to the user
30	Clean-up activity and purging process is halted	**Cause** ETL is in progress i.e., application is coping data from SQLite to MySQL on patching or Database rebuilding is in progress. **Resolution** While ETL is in progress, Clean-up activity, File size recalculation and purging will be halted. Wait for ETL to get completed or bring back MySQL. You can check the log files in debug or info mode. It displays a log line “Migrating from SQLite to MYSQL is completed” once ETL is completed.
31	User is not able to make configuration changes from UI	**Cause** ETL is in progress. **Resolution** Wait for ETL to get completed.

32	IPCam images with UDS mode are not getting stored at correct location or are getting stored in tmp folder.	**Cause** Control file was not received. Check the log files in debug mode. There will be no entry for the respective control file. **Resolution** Make sure you have permission for control file type. If you do not have permission, send an e-mail to analytics.registration@sick.com and request a new license with control file permissions. **Cause** Out of Sync issue. Check control file timestamp in the log files in debug mode. The Media Server might have received control file before the image. **Resolution** Out of sync support for UDS mode should always have <subdir>thumb</subdir> in its control message. It won't work if subdir is set as <subdir>full</subdir> Sample that will not work: <cpreq><src>PS06Test_20111128_142249000_00001.jpg</src><dst>PS06Test_20111128_142249_00000001.jpg</dst><subdir>full</subdir></cpreq> Sample that works: <cpreq><src>PS06Test_20111128_142249000_00001.jpg</src><dst>PS06Test_20111128_142249_00000001.jpg</dst><subdir>thumb</subdir></cpreq>
33	High Media Retrieval Time is observed	**Cause** MySQL is down **Resolution** Bring MySQL up and running. Start Media server services if down. If Media Server service fails to restart because of low disk space, then clear out space from disk where MySQL and MySQL data is available. Then restart Media Server Service.
35	Miscellaneous information is displayed as 0 percentage even when there is Miscellaneous Data in the Drive	**Cause** The value goes to 0 when the purge cycle starts and purging of records from filesystem are deleted but not from DB. This eventually leads to the disk used space to be lesser than the sum of full and thumb size making the miscellaneous value 0. **Resolution**

		Message shown in the UI "Miscellaneous Data size to be rectified in subsequent cleanup cycle." This is a background process and will be Fixed in the Next Cleanup Cycle.
36	ICR890-4 images are not getting retrieved	**Cause** Time difference between MSC and ICR890-4. **Resolution** Sync time for MSC and ICR890-4 device
37	Observing Image loss in for devices	**Cause** Camera's FTP connection is getting stuck on pushing out images, due to which camera loses consecutive images for the packages. **Resolution** Update SOCKET_POLLING_TIMEOUT to 10S and restart MS services
38	Media server is not retaining full size images more than few hours	**Cause** Size based cleanup in MS happens based on ratio configured under parameter RATIO of STORAGE. Default ratio 1:2 is set to retain maximum thumbnail so that we have more images each capture. This decays full size images over time. **Resolution** Update RATIO_ENABLED to false and restart MS services. This will disable ratio cleanup and cleanup will only happen based on FIFO
39	Unable to set Time Based rule more than 999 Hours	**Cause** There is a limitation to the max number that can be set as hours **Resolution** Add parameter MAX_HOURS under PROFILE_FULL and PROFILE_THUMB with max number to be set for hours. Restart Media server service. Note: You won't be able to update cleanup settings from UI after making this change
40	Unable to set Time Based rule more than 999 Days	**Cause** There is a limitation to the max number that can be set as Days. **Resolution** Add parameter MAX_DAYS under PROFILE_DEFAULT, PROFILE_FULL and PROFILE_THUMB with max number to be set for days. Update THUMB_MAXAGE and FULL_MAXAGE with age out details for thumb and full in days. Restart Media server service.

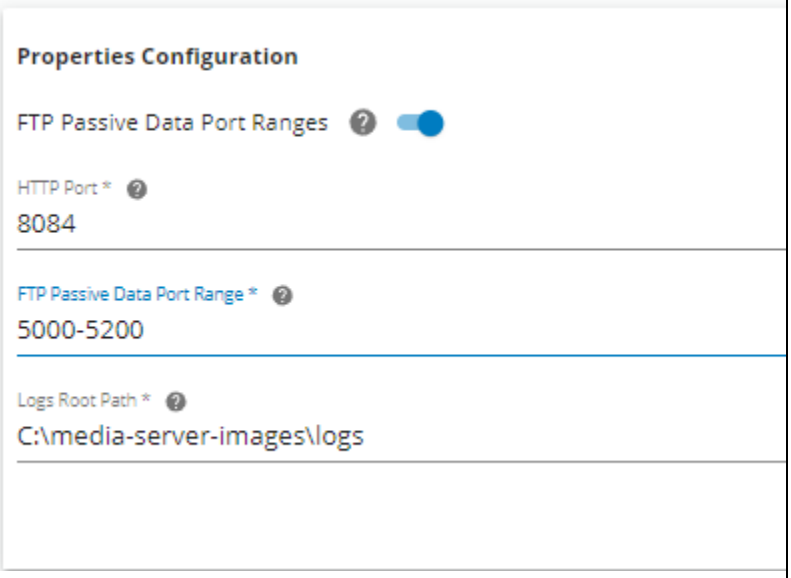
41	User will not be intimated with Warning message, informing the Value allotted to a Rule might exceed the Actual Free Space.	**Cause** There is a limitation to the Minimum Free Space Value. **Resolution** Revisit your configured Rules created for Max Space and reconfigure the rules
42	Action criterion mapping with device/device group is not allowed for different relation of same tag and same criteria.	**Cause** If same tag criterions already exist **Resolution** Ensure that Action criterion for Device/device group has unique tag criterions
43	Special character (\\<>&\"$^?%()[]{}~|;*!`,'/#=:]) validation will be restricted for media retrieval using File location	**Cause** When special characters used in the file name format **Resolution** Ensure that the filename format for images has only allowed list of characters [A-Z][a-z][0-9][`-=~!@$&()_+[]{},.]
44	Rule Based cleanup is only supported for single drive mode.	**Cause** It supports only single drive mode **Resolution** Please connect with product team to prioritize support for rule-based cleanup when Full and thumb images are being stored in different drives
45	Changes made in the client (example device type) of primary server will not be updated in the synced client of secondary server.	**Cause** Primary server client and synced client of secondary client are different **Resolution** Manually change the filetype/Password of the client in the secondary server. Following logs suggest these changes are required

		20230901.114237.838 DEBUG ConfigureSFTP server port: 2020 20230901.114237.838 ERROR Waiting for found in secondary server whose credent server. Thread: 5 20230901.114237.838 DEBUG Started Inter 20230901.114237.838 DEBUG ConfigureSFTP server port: 2020 20230901.114237.838 ERROR Waiting for found in secondary server whose credent server. Thread: 3
46	Tag creation/up-dation/deletion is case insensitive	**Cause** Duplicate names might be used **Resolution** Algorithms used for tagging should use unique tag names
47	User logs out of the application if license with authentication enabled is applied in MS	**Cause** To Login with Authentication enabled license, it logs out of applica-tion **Resolution** Re-login into the application
48	Overlapping is ob-served in the Donut Chart in cleanup page for Full& Thumb and Miscel-laneous	**Resolution** Overlapping will rectify when drive is filled 

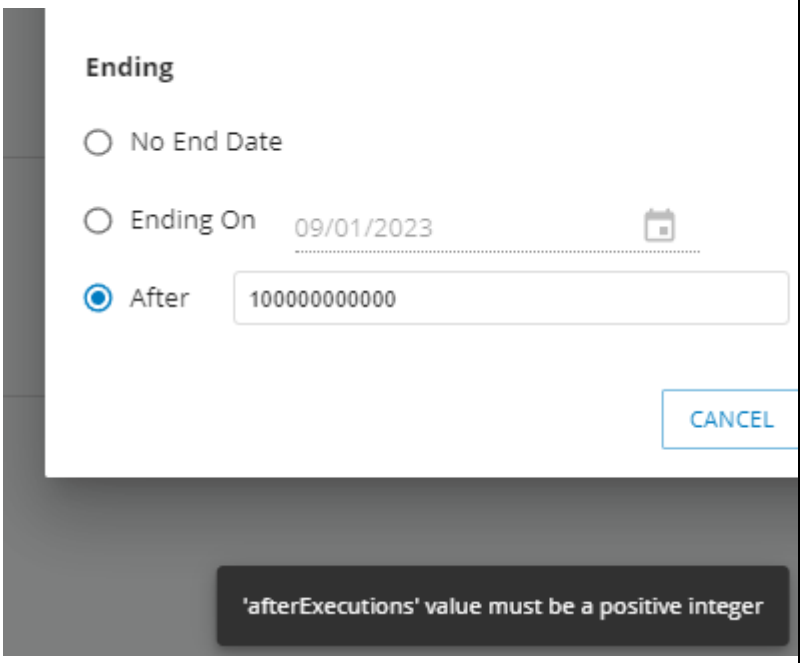
49	Multiple "Authentication request rejected" errors might be observed in File sync logs though the connection is successfully established.	**Cause** Reason: Sftp connection tries two authentication one with password and one without password. The one without password shows rejected message and with password it accepts if all credentials are correct. This happens every connection request made. Please Ignore these logs

50	Adding up a new device to MS device list , we need to make sure that the device should be unique.
	Also, the device type cannot be duplicated under different device family.
		Resolution
		Not Allowed:
		1.
		`Device1=TRACK_TRACE,Device,Device1`
		`Device2=IPCAM_1TEXTFILEMODE,Device,Devi`
		`Device=TRACK_TRACE,Device,Device1`
		`Device=TRACK_TRACE,Device,Device2`
		2.

51	Due to network congestion, user might see delay in media retrieval for the image that is available only in secondary server, given the media request was made from primary server	**Resolution** Retry Image fetch operation
52	Age out based cleanup can deleted images that are part of a rule	**Resolution** Please connect with product team to prioritize this feature.
53	Unable to view entire text of the selected entry in days/hour dropdown of Ageout rule	**Resolution** Zoom out the browser or upgrade your screen resolution settings
54	Filesync and Tagging happen based on FIFO, so if there are a greater number of thumbnails than full images in MS, full size images might not get tagged/synced.	**Resolution** Setup cleanup rules for sizeout with 1:1 ratio in cfg to maintain equal number of full and thumb images `RATIO=1:2`

55	MySQL 5.7 is not supported DB for MS 1.4 and above versions	**Resolution** Upgrade DB to MySQL v 8.0.33
56	Images using FTP passive Data port range on is losing images or acquisition is slow	Cause When "FTP Passive Data Port Range" is enabled, we need to ensure that the FTP data port range configured should have enough ports its range to support the feature. It is suggested to have port range to equivalent to the camera's configured X20 times to acquire images using passive mode to avoid slowness in acquisition **Resolution** If we will be using 10 clients to acquire images via passive FTP mode and we need to restrict the data ports usage; Ensure that the Data range selected has atleast 20X10 = 200 ports 
57	Observing Max aggressive cleanup happening frequently and rules created to cleanup are hot honoured	**Cause** If Cleanup mechanism is not able to cope up with the high incoming image rate, and disk utilization limit is hit (Minimum free limit), Media Server will start cleaning up the data based on FIFO ignoring the configured rules to make space for incoming images to be saved **Resolution** This is the coping mechanism for MS to ensure the latest incoming images are not discarded and latest set of images is maintained. Try reducing the throughput of incoming images to avoid this.
58	Media retrieval is failing if the images are in secondary server	**Cause**

		Media Extraction from secondary media server will fail if extraction from secondary takes more than 5s. This timeout can be increased by adding RETRIEVAL_WAIT_TIME **Resolution** Retry to retrieve images. Logs observed in MS in such case HTTPS Timed out waiting for Retrieval lock This timeout can be increased by adding parameter RE-TRIEVAL_WAIT_TIME under [Filesync_Service] in cfg file
59	File Sync for few clients will stop in-termittently if FileSync client changes are done from the UI	**Cause** If Client connection changes are done from MS UI post connection it is required to restart File Sync services
60	Unable to create multiple smb clients with same username	**Cause** Device names in MS should be unique there cannot be client/servers of same username Example: if Device of type ICR with name engineering is created, you cannot create Device of type SAMBA with the same name.
62	Unable to install only database from MS installer	**Cause** The distributed installation is not supported by the MS installer. **Resolution** If the DB Feature is not selected from the MS Custom installation, the MS could either use the SQLite, or connect to the existing MySQL from the MS UI
63	Database is running error is appearing on MS installation.	**Cause** If MySQL is already installed in machine and user tries to install MS in full mode, MS installation will not be allowed and error "Database is running" will appear. **Resolution** User can use custom installation and deselect Database while instal-lation in this case.
64	Patching over PA 4.4 is not starting proper functioning of MS	**Cause** Upgrading Media Server Patch on previous version of PA will not support MySQL Database (MySQL v5.7.37). **Resolution** MS should use MySQL version 8.0.33. Patch PA 4.5.1 over older PA version.

65	If Algorithms are deleted from MS, then at the start of Tagging schedule, MS will not attempt to fetch algorithms from DLA.	**Resolution** If DLA algorithms fetched by MS are deleted, tagging service must be restarted to fetch the algorithms again from the connected DLA
66	Media Extraction using wild cards is not giving results	**Cause** Media request cannot serve images from secondary server if image request is made with wildcards **Resolution** Image request to secondary server should not have wild cards
67	Validation message for schedule creation can mislead if value entered is huge	 **Resolution** Add number of executions below 999999999
68	Older instances of image that failed earlier are not being tagged	**Resolution** Restart Tagging schedule/ Restart MS service
69	Image retrieval becomes temporarily slow during aggressive cleanup operations.	**Cause** Aggressive cleanup operations delete folders to free up disk space, consuming high disk IOPS. **Resolution**

		The issue resolves automatically after the cleanup process completes. No action is required.
70	Unable to switch MS DB from SQLite to MySQL on performing custom installation using PA installers	**Cause 1:** Database was not installed along with Media Server during custom installation. **Resolution 1:** • Launch the PA Uninstaller. • Use the **Add Feature** option to install the **Database** component. **Cause 2:** The installer requires the actual IP address of the machine to bind the database IP (to support distributed installation). This restricts Media Server access to the database on `127.0.0.1`. **Resolution 2:** **If only Media Server and MySQL are installed on the same machine:** • Navigate to the MySQL data location set during installation. • Open the `my.ini` file. • Comment out the `bind-address` entry. Restart the MySQL service. **• If it is a distributed installation and other PA components are installed on another machine:** o Connect via the SICK Support Portal for proper configuration guidance. This version now:
71	Observing image loss when a lot of devices are	**Cause 1:** Media Server loses images for recently acquired objects due to FTP connection count reaching the maximum limit.

	connected to one MS instance.	**Resolution 1:** Enable MS logs in DEBUG mode to identify the issue. Navigate to the FTP logs and check for the following entry: DEBUG _AddConnection:FTP Connection count:1000 Update the configuration file: Locate the [THREAD POOL SIZE] section in the configuration file. Change the value of FTP_CONNEC- TION_MAX_THREADS to 2000. Save the configuration file. Restart the Media Server. **Cause 2:** IPCam devices may lose images due to synchronization issues with the MSC service. **Resolution 2:** Restart the MSC service if IPCam devices are also losing images.
72	Source 2/_2 files are not appearing in the barcode counter file.	**Cause:** Support for Source 2/_2 files is disabled by default. **Resolution:** Stop the Media Server services. Open the sick-bip-is.cfg file from the installation directory. Update the parameter GET_2_ON_FULL_FAILURE to true as shown below: GET_2_ON_FULL_FAILURE=true Save the file. Restart the Media Server services to apply the change.
73	The system reboots without any warning while uninstalling the Media Server patch and selecting the "uninstall prod-uct" option.	**Cause:** Compatibility issue between the Media Server patch uninstallation process and the current Windows version. **Resolution:** Update the Windows operating system to the latest version to ensure compatibility and prevent unexpected reboots during the uninstalla-tion process.
74	MySQL is crashing frequently with AIO error	**Cause:** MySQL crashes due to Windows compatibility issues that result in AIO errors logged in the MySQL error file. **Resolution:** • Stop the MySQL service.

		• Navigate to the MySQL data folder installation location. • Open `my.ini`. • Add the line `innodb_use_native_aio=0` under the `[mysqld]` section. • Save the file and restart MySQL service.
75	Windows reboots unexpectedly while uninstalling MS patch	**Cause:** Compatibility issue between the Media Server uninstaller and older Windows versions. **Resolution:** Update the operating system to the latest Windows version before uninstalling the Media Server patch to prevent unexpected reboot.
76	MySQL is not starting in Ubuntu with error "PID already in use" / "Unable to setup unix socket lock file"	**Cause** MySQL service did not shut down cleanly, leaving stale PID or socket lock files. Another MySQL process is already running and holding the socket. Server reboot or crash left orphaned .pid / .sock files. Socket file is locked by another process. **Resolution** 1. Stop MySQL service: sudo systemctl stop SICK_An_MySQL 2. Identify MySQL data directory from my.cnf (datadir property). 3. Navigate to the MySQL data directory. 4. Delete stale lock files: • mysql.sock • mysql.sock.lock • *.pid files Example: sudo rm -rf /var/lib/mysql/mysql.sock sudo rm -rf /var/lib/mysql/mysql.sock.lock sudo rm -rf /var/lib/mysql/*.pid 5. Restart MySQL service:

		sudo systemctl start SICK_An_MySQL 6. Verify service status: sudo systemctl status SICK_An_MySQL

If you are still facing issues, drop an e-mail and share the genlog files spm-analytics@sick.com **,** Deepak.Kolippakkam@sick.com **and** Deepak.padmanabhan@sick.com **for troubleshooting.**

25 Known Issues and Limitations

Following are the known Issues and Limitations for this software:

Limitations
SSD is recommended for sites having high load as HDD may result into High Response Time and Images getting discarded
SMART_UDS mode will work only if there is one to one relation between MSC and IP Cam (UDS mode). Multiple such one-to-one combination is supported in SMART_UDS mode.
Image loss is observed when files available in file index queue is not getting saved in DB on MS shutdown. This happens when Media Server is running as a Service.
Image loss may be observed when file index queue is high and image size recalculation is happening. Generally, this may happen on Media Server shut down or restart.
MS does not support file transfers over EPSV mode.
If Control files are received with Duplicate Sequence ID, then FIFO concept will be used, and the associated image will be renamed based on the first control file received.
Purge based on Age-out value takes a lot of time to delete folders from file location. This causes high disk time % resulting in server disk to be busy until the heavy folders are deleted. Cleanup cycle will be stopped until the purging activity is completed.

If the Machine C:\Program Files\Zero G folder is not cleaned, the installer might throw an Instance Management Error.
Clean up will be paused while inventorying is going on. If images are being pushed in during inventorying, then enough disk space needs to be available as a precautionary measure in order to avoid image loses due to low storage space.
Image will be discarded due to high file writer queue when image acquisition is also happening while image inventorying is in progress. Thus, it is recommended for migration to happen in downtime.
If MySQL server is busy around midnight, creation of the partition is queued up and is executed later. There is no log generated to notify when the queued-up partitions are getting generated. During this time when we see partition queued up log and actual partition getting created (which is not printed), the user won't be able to view these acquired images on the Facility View. The images will be available once the partition is created, and the queued image data is executed.
Once in every 24 hours recalculation happens. During this time images are not retrieved for approx. 3-4 min for MySQL. You can change every 24-hour time interval by changing the value in the config file RECAL_FILESIZE_INTERVAL property.
On abrupt stopping of MySQL or MS process (i.e., if the process is killed), we might lose some data while performing ETL
Media Server storage status may deviate by 5 files (if each file is 1 MB, deviation will be 5 MB). However, Media server once in 24 hours corrects any deviations to ensure cleanup and maintenance functions are robust.
Image retrieval will fail for the images having specific characters #%& {}\<>*?/ $!'":@+`|=; in filenames as these characters are not supported due to security reasons.
Filename is updated to 255 characters. However, filename size should be less than 100 characters.
Device is updated to 64 characters. However, MAX_USERNAME_LENGTH should not be more than 64 characters.
Root path is varchar i.e., up to 255 characters. However, root path length should not be more than 120 characters and MAX_FIELD_LENGTH should be less than 130 always.

Media Server storage status may deviate by 5 files which can impact size out clean-up. The size out based cleanups will not be accurate for the duration until the correction in size deviations are made. Media server once in 24 hours corrects any deviations to ensure cleanup and maintenance function is robust.
Miscellaneous size is increasing in the disk and visible in drive dedicated to images only. This is due to disk fragmentation
Media Server is not supported with latest open ssl version
When images are acquired for the first time in a day and retrieved simultaneously, high response times are observed. This happens because the database is busy creating partitions during this period. The issue lasts for a few seconds and resolves once the partition creation is complete.
On Media Server startup, if the database schema is not available, the server takes extra time (approximately 20 seconds) to populate the required tables, indexes, and partitions. This results in a delayed initialization of protocols such as HTTP, HTTPS, SFTP, FTPS, FTP, and UDS.
During installation, if incorrect username/password credentials are provided in the gMSA screen, the installation will proceed, but the application will fail to function post-installation. Users must ensure correct credentials are entered to avoid this issue.
Unrelated MySQL instances must be uninstalled before running the Media Server patch installer to avoid conflicts. The installer interacts exclusively with the Analytics MySQL service and may not validate unrelated MySQL instances.
Changes made in the Advanced Configuration Page (visible to Admin users) will not take effect until the Media Server services are restarted. Users must restart the services after making changes for them to be applied. If the services are not restarted, the changes will not be visible or functional.
During Manual Cleanup, Max Aggressive, Aggressive, and Ageout activities, where entire folders containing image data are deleted to create space, MySQL queries may experience a delay of around 3 seconds due to high disk operations. This occurs because the disk is heavily used for cleaning up image data, which can temporarily impact the performance of MySQL queries.
If there are duplicate images with the same name for the same device in the Media Server, only the first image encountered by the system will be shown during media

retrieval. To avoid this issue, users must ensure that each image associated with a device has a unique name.
Devices or filenames containing non-ASCII characters will not function correctly in the Media Server. If a device name or filename includes non-ASCII characters, the Media Server will not be able to acquire or save images for such devices. Users should ensure all device names and filenames use ASCII characters only to avoid issues.
Installing MS 1.5 on the same server as PA 4.4 or lower is not supported due to MySQL compatibility limitations. MS 1.5 has deprecated SQLite and does not support MySQL v5.7, which is used by PA 4.4 and lower versions. **Not Supported Configuration:** • MS along with Database installed using PA 4.4 / 4.3 • Applying MS 1.5 Patch over PA 4.4 installation • Using MySQL v5.7 with MS 1.5 or MS 1.4 **Supported Configuration:** • If only MS is installed using PA installer • If MS along with MySQL DB is installed using PA installer version 4.5 or above • If PA is upgraded to version 4.5.1 or 4.6 before applying MS 1.5 Patch **Mitigation:** Upgrade PA to version 4.5.1 or above before applying the MS 1.5 Patch.
MS 1.5 supports storing data for a maximum of 340 days. Any data older than 340 days is automatically deleted by the system. For example, if the current date is December 6, 2024, only data from January 1, 2024, onward will be retained. Data created before December 31, 2023, will be purged. Users requiring longer data retention should back up data externally before it exceeds the retention period.
When there is a time difference of more than one day between the Media Server and the filesystem in MS 1.3.2, and if inventorying was performed to rebuild the database, image loss may occur during migration to MS 1.5.
If the File Transfer Protocol (FTP) passive data port is updated during active image acquisition, FTP operations will pause for a few seconds. When the passive data port configuration is modified while image transfers are in progress, Media Server requires a few seconds to release the previously allocated ports and activate the new set of ports. During this transition period, image acquisition using FTP is temporarily halted. This behavior is expected and occurs by design in all FTP-based acquisition setups that use passive mode.

If a media request is made for an inactive client, Media Server does not return an error message indicating that the client is inactive. Instead, the request is forwarded to connected FileSync Media Servers for image retrieval. The response may return code 200 if the image is found or 404 if it is not. This behavior supports fallback retrieval in distributed environments.
When a wildcard-based image request is initiated from the primary Media Server, and the requested images have already been synced to the secondary server, the primary Media Server will not return those images. Even if the images still exist on the primary server, the system is designed to avoid serving them in wildcard requests once they have been synchronized. If those images have been deleted from the secondary server, the wildcard request will fail to retrieve them. This limitation does not affect Facility View, as it does not use wildcard-based retrieval.
When the User Manual is opened from the Help section, selecting topics from the left navigation panel triggers a full page refresh instead of dynamic content loading.

Known Issues	Type
[Linux] Purging is of both full and thumb location is happening as per thumb rule	Functional
images are being discarded when the disk size reaches maximum free limit and cleanup is not happening	Functional
API authentication and HTTPS servers are working for corrupted license	Functional
Application does not automatically redirect user to HTTPS, if HTTP is disabled and HTTPS is enabled from the License file.	Functional
User is not able to enter HTTPS publish URI and auth URI in heartbeat settings if HTTPS is disabled from license for MS	Functional
All MS protocol servers are restarted on applying license	Functional
Inventorying of data from file location is initiated for already existing drive as well when the user switches to a location that is empty	Functional
FTP is stopped until all the files in the queue are written when user switches min free limit to hit immediately when file writer queue is high	Functional
UDS control files are not being cleared on Manual cleanup	Functional

[Linux] Media Server is not starting if UDS port is set to any of the port that is being utilized by FV on the same machine	Functional
UDS server is not coming up after creating 1 txt file mode device	Functional
Heartbeat is stopping and no retry attempts are made if FV throws 500 error	Functional
Manual cleanup of MS images is very slow when network drive is chosen as full /thumb /files.idx location	Functional
Queue depth is increasing if network drive is chosen as full and thumb storage location	Functional
[Linux] MAX_QUEUEITEMS, NO_OF_FS_DEVICES, NO_OF_DB_FS_DEVICES, FILESYNC_QUERY_COUNT parameters are not available in the .cfg file of all Linux Builds	Functional
Folders are not purging in root directory on cleanup if the Time-Based rule of tmp images of IPCam is high	Functional
Age out rules for thumb and full are not changing back as per default profile after switching MS from 2 drives to single drive mode	Functional
IPCam connections are going in CLOSE_WAIT mode thus restricting any new images to acquire	Functional
Devices with different cases example 'TOP' and 'top' share the same folder structure	Functional
UDS server does not gets disabled on disabling it from license	Functional
UDS out of sync SMART_UDS is not working, and the User ID and System ID mapping is not getting updated if a new image with new User D is pushed to an IPCam Device	Functional
Text file is not getting interpreted correctly	Functional
Media server does not delete the folder location that the user has opened in windows explorer	Functional
Incoming image data is lost in deadlock when MySQL comes back up	Functional
Device folders are not deleted when the user performs manual cleanup	Functional

Image data in tmp folder is not being cleared from tmp queue in code on manual cleanup	Functional
Recalculation is not happening after changing drive of full/thumb location when DB is MySQL	Functional
Unable to set mapped network drive as full and thumb location	Functional
Storage based cleanup based on ratio is not accurate	Functional
Cleanup is starting before recalculation is completed after ETL	Functional
Heartbeat is restarted even if the heartbeat info in the edit heartbeat window is incorrect	Functional
User not able to create ICR devices and MAX ICR users shows green tick and existing devices shows false under Device Management tab	Functional
Already used password in edit MySQL config window is not used if changes are done on configured MySQL DB settings	Functional
User can search Devices with special characters and leading and trailing spaces	Functional
If multiple devices with same username and different IP Addresses are created in Media Server and Media Server relates to Facility View, then Facility View application considers the devices with same username as one device and updates the details of the existing one.	Functional
Xml files are not getting deleted when User performs Manual Cleanup	Functional
Purge using FIFO is not happening for quite some time after heavy purge operation has been performed	Functional
[Intermittent] Image is not being deleted from File system	Functional
Thumbnail and Full Size is appearing in Negative when the User performs Manual Cleanup	Functional
Unable to shut down FTP server after performance tests	Functional
Media server is not clearing out images if aggressive or regular cleanup in a corner case	Functional

Maximum Aggressive Cleanup is stopping, and Regular and Aggressive Cleanup is happening even when Minimum Free Space is being used	Functional
[Intermittent] IPCam files are not being renamed for Live camera if IPCam images are being pushed in high rate	Functional
Recalculation query is not getting paused/stopped if minimum free limit is reached	Functional
[Intermittent]FTPS is not starting on all the ports	Functional
Media server is not able to fetch images with jpeg extension from file location/SAMBA server	Functional
Inventorying is not happening for the rest of the folders if any one of the folder inventorying throws exceptions	Functional
Images still exist in the Folder when the metadata has been deleted from the DB	Functional
Media Server is getting restarted and Age out is getting Stuck	Functional
Only a single image is being deleted in regular size out when ratio is disabled	Functional
[Intermittent]ERROR Exceeded access limit of 100\min to REST_1_0_storagedetails is appearing in the logs when the User has applied a License with Authenticate API as true	Functional
Missing \ in the thumb and full path for windows drive is being accepted which is causing MS operations	Functional
License with MAC address in lower case is not accepted by MS	Functional
Trusted License API is throwing 500 error or gets stuck intermittently	Functional
[Linux]All machine MAC addresses are not appearing in the license and registration tab	Functional
Media Server APIs are going in pending state in a setup where authentication is enabled, and we are using HTTPS server	Functional
The date-time calendar used to configure start and end dates in Manual Cleanup and Schedules does not work in Firefox due to a library limitation. Users must use Chrome or Edge for these functionalities.	Functional

ERROR observed in performance test: PocoErrorHandler Exception from Poco library: Software caused connection abort	Performance
Images are getting discarded due to high file writer queue while processing images from temp file writer queue	Performance
Images are discarding after MS recovers from temp file writer queue insertions	Performance
[Linux/AWS specific] Media server is taking 2-3 mins to start if the current DB is MySQL and MySQL server is down	Performance
Media Server is taking time to get started and UI is not coming up when Indexed are being created	Performance
MySQL Database is not recreated by Media server if the DB is dropped by the user	Performance
High Query time is observed for recalculation queries	Performance
Application crashed if user performs manual cleanup for large amount of data	Performance
Queue Depth of file index is increasing on pushing objects to multiple devices at high rate when there are 100M + files data in files.idx	Performance
High Query time for the query used to determine files to be deleted for manual cleanup in HDD	Performance
High Query time for the query used to retrieved lector images in HDD	Performance
High response time for image retrieval during the first image acquisition of the day. This occurs because the database is busy with partition creation for a few seconds.	Performance
[FTP + SFTP] Media Server Memory increases with time	Performance
[Intermittent] Cleanup logs are missing for few hours in performance test	Performance
[BE] Delete Ftp Device with invalid idx value returns 412 "Precondition Failed" with HTML response body	Backend
API /3.0/server settings always send 'status' as true for get requests	Backend
Invalid values in license are appearing as response in retrieval API for corrupt license	Backend

404 error appears in retrieval API if incorrect mode is mentioned as a query parameter	Backend
.logs, html.zip, files.idx (unsupported extensions) are also inventoried in database	Backend
Response 400 is appearing instead of 412 on applying invalid/corrupted/expired trusted license to MS	Backend
FTPS/SFTP server stopped logs are not getting generated in gen logs	Backend
Images are not being retrieved from cache for PUT 1.0/media and 2.0/media if MySQL DB is down	Backend
User is unable to push heartbeat for un-auth API	Backend
400 error is appearing instead of 412 with incorrect message on applying expired local license to MS	Backend
FTP ports are not getting updated until the open connections are closed	Backend
Stop heartbeat message is not sent to FV when Media server is stopped/restarted from service	Backend
Other devices file renaming format is not supported by MS for image extraction from file location	Backend
Application does not display any error message on port conflict between UDS and HTTP/HTTPS	Backend
API with Status code 412 , 404 returns HTML response body	Backend
Genlogs gets populated with a lot of licenses expired logs in DEBUG mode when license gets expired	Backend
Login session does not get timed out from backend if the session was idle for more than LOGIN_TIMEOUT set	Backend
412 preconditions failed is appearing instead 426 when the License is expired, and user tries to extract media	Backend
412 preconditions failed is appearing instead of 426 when License HW check failed	Backend
[Linux] Media server restart logs were observed in genlog when MySQL goes down	Backend
[Intermittently] MS does not send 226 OK response to camera if active DB MySQL is down	Backend
Status Invalid Certificate is appearing in heartbeat if the certificate has expired	Backend

User is not able to Edit Undo ICR890-4 Devices in a specific Scenario	Backend
User can set Conflicting ports for FTP, FTPS and SFTP in a specific Scenario	Backend
400 Bad Request is appearing instead of 412 Pre-Condition Failed when the User send invalid value in Json object	Backend
[Intermittent]"ERROR: Exception in auth: device or resource busy: device or resource busy" is appearing when the User tries to Login in the Application	Backend
[Linux]Trusted License API is throwing 500 error intermittently	Backend
Multiple SSL exceptions are observed in genlogs	Backend
MySQL password Entered is visible in the page after user saves MySQL settings	UI
[Internet Explorer] MS UI Login page is not appearing when the User launches the URL	UI
Thumbnail and Miscellaneous percentage is appearing overlapped on Disk Usage Summary Donut Chart	UI
Percentage is going out of bounds of the Donut chart	UI
[FireFox]MS Login Page is taking time to appear after the User launches the URL	UI
Incorrect message "The Current License is Invalid" is appearing when there is No License applied	UI
MAC address 00-00-00-00-00 is also being displayed in license and registration tab	UI
[Firefox version 87 specific] device tables are not rendering properly	UI
[IOT / IE Specific] Media Server UI is not getting launched	UI
Full storage data in disk indicator display incorrect information if the data for full is available in two drives and the cache size is negative	UI
[Intermittent] IP address and ports are appearing blank in FTP/FTPS and SFTP card when user applies a license	UI
Miscellaneous information shown for the disk indicator is incorrect	UI
The applied MAC address is physically present in the License file but not shown in System Macs	UI
Image data for thumbnail in two drive mode is appearing in blue	UI

[Internet Explorer] Proper placement of icons in left navigation panel is not appearing in the application	UI
[Internet Explorer] Miscellaneous field is overlapping with the disk usage indicator border	UI
IPCam UDS mode is appearing as enabled from license if IPCam Is disabled from License	UI
[Intermittent] Content of disk indicator goes out of bounds while configuring thumb and full locations to different drives	UI
User does not log out from UI when session expires if any windows is open	UI
Edit Media Server> Character length validation along with invalid character validation gets enabled.	UI
[Linux] [Edge/IE Specific] Snack bar message is not appearing on saving changes to any protocol intermittently	UI
User is not logged out of the older logged in tab if the user logs into a new session	UI

26 FAQ's

Question	Answer	Additional Comments
What is the default Media Server Username/Password?	Operator/456	
Why incorrect miscellaneous information is being displayed in the disk indicator on MS UI	Incorrect miscellaneous information being displayed in disk indicator can happen when the files are deleted from the disk, but the records are still present in DB. It is recommended not to delete miscellaneous files manually.	Media server can also use network drives and shared folders on network PCs to store image data. As these locations are not specific to the machine where MS is installed, there is a chance when someone deletes images data from these locations, but the file records still exist in DB. This may result into incorrect miscellaneous information being displayed on media server Second case can be when Media server is deleting image data from file location but isn't able to delete data from DB. Practically, this case should never happen.

What happens when ETL is in progress?	While ETL is in progress, the Database services will be down and clean-up, File size recalculation and purging activity will be halted.	
Why are two clean-up logs getting generated on upgrading M1.1 or newer version	The clean log in MS 1.1 is now renamed as cleanup log in MS 1.3.2 and newer versions. So, upon upgrading MS 1.1 to MS 1.3.2 or newer versions you will see two log files one from the older version i.e., MS 1.1 and the other from the new installed version.	
Is FTPS Feature functional?	Yes, FTPS is functional, but this is beta release for FTPS and not the final version.	
Is SFTP Feature functional?	Yes, SFTP is functional, but this is beta release for SFTP and not the final version.	
Why the updated Filetype size mismatch after recalculation?	The small mismatch could be due to the time difference between the time when the recalculation flag becomes false, and the update happens.	
What is the supported filename format for extracting image using filename?	Supported filename format: USERNAME_yyyymmdd_hhmmss_3.jpg USERNAME_yyyymmdd_hhmmss.jpg USERNAME_yyyymmdd_hhmmssSSS_3.jpg USERNAME_yyyymmdd_hhmmssSSS.jpg yyyymmdd_hhmmss_3.jpg yyyymmdd_hhmmss.jpg yyyymmdd_hhmmssSSS_3.jpg yyyymmdd_hhmmssSSS.jpg USERNAME_yyyymmdd_hhmmss_SEQID_3.jpg USERNAME_yyyymmdd_hhmmss_SEQID.jpg USERNAME_yyyymmdd_hhmmssSSS_SEQID_3.jpg	

	USERNAME_yyyymmdd_hhmmssSSS_SEQID.jpg yyyymmdd_hhmmss_SEQID_3.jpg yyyymmdd_hhmmss_SEQID.jpg yyyymmdd_hhmmssSSS_SEQID_3.jpg yyyymmdd_hhmmssSSS_SEQID.jpg	
How to support multiple UDS Devices?	Make sure we send <userid> is UDS packet to support multiple UDS Devices Make sure the image name is of supported filename pattern to get image data directly from file location if the image data is not available in DB.	
When is the inventorying process expected to happen?	On MS startup if the expected database does not exists and there are files in the rootpath location	
What Ports are used by the application?	HTTP: Default Port 8084 HTTPS: Default Port 443 FTP: Default Port 2021. Port range 20,21,1024-65535 SFTP: Default Port 3121. Port range 22,1024-65535 FTPS: Default Port 4121. Port range 21,990,1024-65535 UDS: Default Port 3030 MySQL: Default Port 8406 File Sync: Default Port: 2020 Tagging: Default Port:80	
How to configure/update a valid Certificate?	Certificate can be applied while installation. In case you want to update the certificate after installation, you need to place/replace the valid PFX certificate file in Certificate folder	
What all features will be impacted if Certificate is	All secured protocols and related features will not work.	

invalid/expired		
Does Media Server allow user to login to multiple browser?	For security purpose, user is only able to login to the application in a single browser. Any attempt to login to a new session will terminate the previous session.	
How to configure the Media Server application to use HTTPS?	HTTPS should be licensed. HTTP and HTTPS should run on different ports. HTTPS settings can be viewed/updated from the config file.	
How to configure the Media Server application to use SFTP?	SFTP should be licensed. A valid Certificate is required. You can enable SFTP and update its settings from UI or from the config file.	
How to configure the Media Server application to use FTPS?	FTPS should be licensed. A valid Certificate is required. You can enable FTPS and update its settings from UI or from the config file.	
How to encrypt passwords?	1. Open Encryption app (Encryption.exe) in command prompt. 2. It will provide you two choice (1/2) to Encrypt Application User Information and to Encrypt Password. 3. Enter 2 to Encrypt Password. It will prompt you to provide password. 4. Enter Password. 5. Click on 'Enter'. It will encrypt the password.	
How to change the passwords?	1. Copy the encrypted string. 2. Open the config file in Text Editor. 3. Navigate to the section for which you want to update the password.	

	4. Paste the encrypted password string. 5. Save and Restart the application server. The updated password will take place on re-starting the application server.	
What if there is a power outage and MySQL DB does not come up before Media Server?	Media Server will switch back to SQLite temporarily.	
Why changing the Storage location is not getting reflected on Media Server?	On changing the storage location, Media Server needs to be restarted in order to get the change reflected or else you need to wait for the recalculation to get completed.	
Recalculation is not happening after changing drive of full/thumb location when DB is MySQL?	On changing the storage location, Media Server needs to be restarted. Please restart the Media Server.	
Why ICR890-4 images are not retrieved even though all the configurations are correct?	The images are stored in folders based on date and time. If there is a time difference between MSC and ICR890-4, images will be stored in different file location. Media Server will investigate the folder structure of SAMBA server as per the filename and will not be able to retrieve the images.	
I have Auto disk management enabled. However Older files in previous drive location is not cleaning up.	Auto disk management or size-based cleanup is used for cleanup of current drive only. It is required to setup age out rule for thumb and full location for cleanup of image data in older drives.	

Started Manual Cleanup By mistake and would like to stop further deletion of data. What should I do?	Restart Media Server services to stop Manual Cleanup process to further delete image data. Image data deleted while Manual cleanup was ongoing, cannot be retained. Contact support team to reindex the database to retain the images data.	
What operations are blocked during Media Server 1.5 migration process?	**During migration to MS 1.5, these operations are disabled:** Properties configuration changes in advanced configuration Heartbeat configuration changes Create/edit/delete operations for devices/groups Filesync and tagging operations Metadata extraction via /1.0/mediaMetaExtractor API Image extraction for non-migrated content Rule-based cleanups (enabling/adding) Manual cleanup operations FTP/FTPS/SFTP port updates	**MySQL Configuration Special Cases:** ALLOWED WHEN: Fresh installation (no migration needed) with MySQL down Patch installation (migration required) with MySQL down BLOCKED WHEN: Migration in progress + MySQL edit attempted Migration in progress + MySQL down + edit attempted Migration in progress + MySQL down + server restart + edit attempted System will display appropriate snackbar messages when changes are prohibited.
What happens if I try to modify MySQL settings during migration?	The system will prevent MySQL configuration changes during active migration and display one of these messages: "Migration is in-progress. MySQL Configuration change not allowed" "Migration is in-progress. Please ensure that the connected DB is up and running" (after restart)	These restrictions ensure data integrity during the sensitive migration period. Wait until migration completes before attempting configuration changes.
How can I restrict or allow specific TLS cipher suites and elliptic curves for	FTPS in Media Server operates using **TLS 1.3**, which complies with the latest security standards. Vulnerable cipher suites and curves are disabled by default. If there is a requirement to restrict or allow specific ciphers or curves, this can be configured	**Default Allowed Ciphers:** • ECDHE_RSA_AES256_GCM_SHA384 • EC-DHE_RSA_CHACHA20_POLY1305_SHA256 • AES128_GCM_SHA256 • AES256_GCM_SHA384 • CHACHA20_POLY1305_SHA256 **Default Curve Behavior:** All curves allowed except: • secp521R1 • X448

the FTPS protocol?	through the Media Server configuration file. **Procedure:** 1. Stop the Media Server service. 2. Navigate to the Media Server installation directory. 3. Open the configuration file: sick-bip-is.cfg. 4. Locate the section [FTPSD]. 5. Add or update the properties: • TLS_CURVES= • CIPHER-SUITES= 6. To block a cipher/curve, prefix it with -. 7. To allow, add the name without prefix. 8. Save the file. 9. Restart Media Server service.	**Example:** TLS_CURVES=SECP192R1,SECP256R1,-SECT163K1,-SECT163R1 CIPHER-SUITES=EC-DHE_RSA_AES128_GCM_SHA256,-DHE_RSA_AES128_GCM_SHA256

27 Glossary

Intelligent Sensor	Intelligent Sensors are devices which collected data and send to a central controller. These sensors include barcode scanners, dimensioners, and cameras, among others. Also referred to as devices
LA	Logistics Analytics
auto ID system	All SICK systems that are part of the process of automatic data collection and identification for object processing, for example, camera tunnels, and scan systems. Auto ID systems may consist of a network of data collection components, such as cameras, laser scanners, dimensioners, and scales, which work together to provide data on objects being processed through the system.
Device	In LA, a system component which collects analytical data which is transmitted to PA. Devices include CLVs, ICRs, MSC/SIMs Also referred to as Intelligent Sensor
device group	A logical grouping of devices, for example all CLVs or all ICRs. In PA, devices may be grouped in order to enable collective reporting and analysis of the group.
LECTOR	SICK Image Code reader, used for finding and detecting barcodes. This device captures multiple images for an object.
IPCam	Low-resolution Image capturing device, used for monitoring object images. The images captured by this device are initially stored in tmp folder. These images are then renamed as per the txt file received from MSC (media server search the txt file for the image as per IPCAM_SEQ_MASK set) and then stored in the file tree.
ICR	SICK's Image Code Reader, used for finding and detecting barcodes.
MAC	The system Media Access Controller (MAC) is a unique computer ID. It is used by PA to secure your software license to a physical computer.
Object	In LA, objects are items that are scanned by auto ID systems for data points, such as barcodes, weight, dimensions, and more.
System	See auto ID system

Tunnel	An auto ID system that is configured as a tunnel system, with one or more reading devices mounted to a framework above, below, and to the side of tires, such as a camera tunnel. See also auto ID system.
Web Device	The device program which is used to launch PA. The web device opens the LA user interface using the Chrome browser by default.
Media Server	Media data captured by the media capturing devices (ICR, Lector, IP cams, etc.) of the auto ID systems are stored in remote PC/server host where Media server is running.
Operator	Operator is the default user in Media Server with rights to configure SICK Media Server.
Device computer	The device computer is any PC connected to the LA network. LA's device applications are Rich Internet Applications (RIA). The device applications connect to the PA Application Server to access rich data content and provide a powerful user experience.
Valid License	A valid license should not be expired, the signature should be valid, and the MAC Addresses (meant for local licenses) should be valid. One of the transfer protocols (FTP/SFTP) should be licensed. The JSON format of the license should be valid.
Trusted License	License applied to Media Server via Facility Server
FTP/SFTP	The available file transfer protocols. All three are licensed. Certificate validation is done for SFTP for secured file transfer.
SMB	Samba protocol. ICR890-4 can store images in its local SSD disk. Media server can extract these images from ICR890-4 storage location using SAMBA server running in the ICR890-4
Regular Buffer	Buffer space reserved for Size Based Cleanup by media server for normal cleanup operation
Additional Buffer	Buffer Space reserved by Media Server for size-based cleanup for aggressive cleanup of drive.
Regular Cleanup	Normal size our based cleanup. This type of cleanup is performed to when the available disk is less than the sum of Regular Buffer, Additional Buffer, and Minimum Free Space

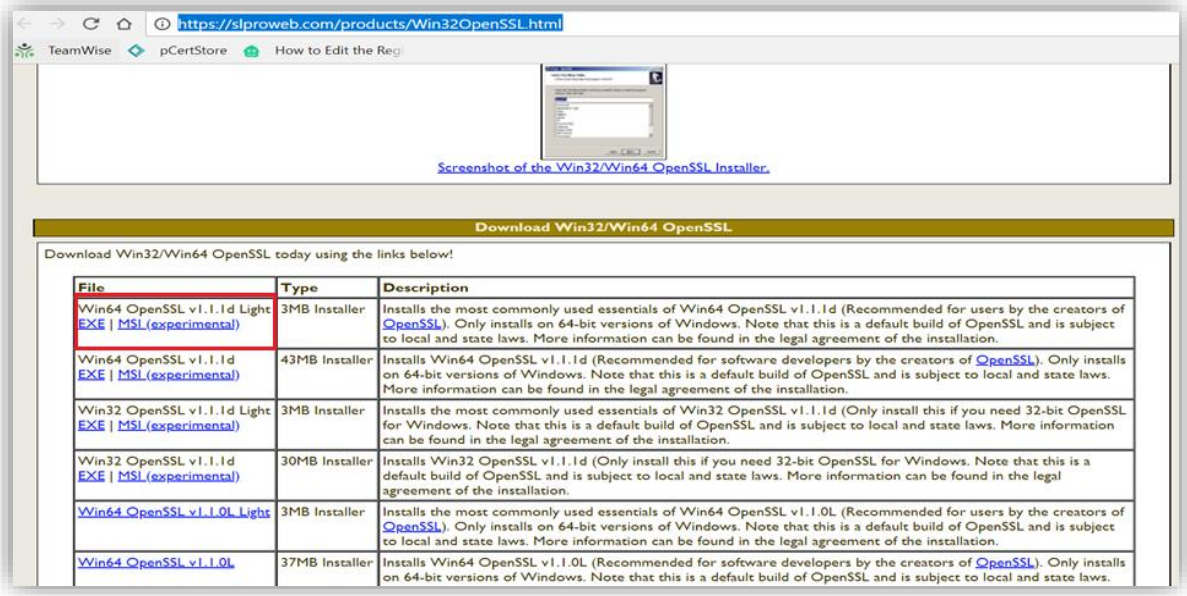
Aggressive Cleanup	Type of cleanup that is performed during size-based cleanup when the available disk is less than the sum of Addition Buffer and Minimum Free Space
Maximum Aggressive Cleanup	Type of cleanup that is performed during size-based cleanup when the available disk is less than the Minimum Free space
Minimum Free Space	Minimum free space is the free space configured under Size Cleanup Settings. This is the minimum space that should be available in the drives where full-size and thumbnail locations are configured. Size based cleanup on these drives happen based on this configured setting.
ETL	Extract, Transform, Load. Operation performed to transfer image metadata from SQLite to MySQL when database is switched
Recalculation	Interval in media server when media server corrects its cache with the information of total size of full size and thumbnail images available in media server
Facility	Facility is a place where the SICK products are being used. Example: Warehouse in Stoughton is Using SICK auto-identification systems and Analytics software to track and trace the objects. This warehouse will be called a facility.
Maximum Usage Limit	Maximum disk space that can be utilized by Media server. This is calculated based on the minimum free limit set for Size Based Cleanup. Example: For a 100Gb disk where minimum free limit is set to 10Gb; Miscellaneous space in the disc is 5Gb; Additional and regular buffer is 20Gb in total. In this case Maximum Usage limit for the disc will be 65Gb (Total disk space[100Gb] - min free limit[10Gb] – Miscellaneous space[5Gb] – Additional and regular buffers[20Gb]). Refer to Appendix B for details related to cleanup.

28 Appendix A

Steps to generate pem Certificate with SAN

Follow the below steps to create the certificate.

Step 1: Download Open SSL from the link https://slproweb.com/products/Win32OpenSSL.html



Step 2: Install Open SSL by double clicking the executable.

Step 3: Run the command prompt as Administrator mode

Step 4: Traverse to the path C:\Program Files\OpenSSL-Win64\bin

Step 5: Create a file and save as "san.cnf ".Below commands need to be written in san.cnf file

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = US
ST = MA
L = Stoughton
O = SICK Product & Competence Center Americas
OU = SICK Product & Competence Center Americas
CN = sick.co.in
[v3_req]
subjectAltName = @alt_names
[alt_names]
```


DNS.1 = sick.co.in
DNS.2 = mysick.com
DNS.3 = sickmedia.co.in

Note: *Change the names of DNS.1,DNS.2,DNS.3 as per your requirement. Any number of SAN names can be provided.*

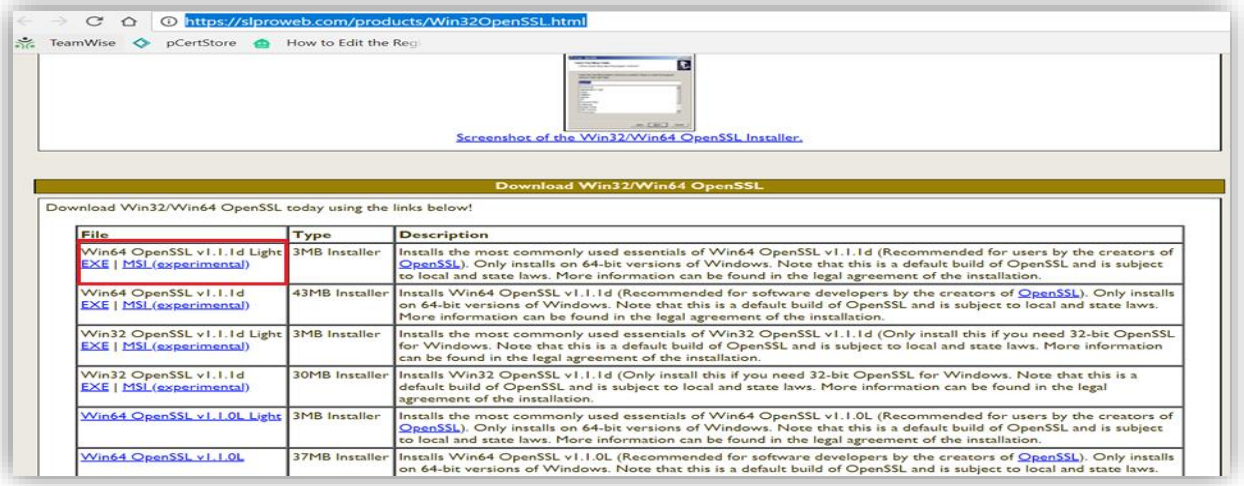
Step 6: Enter the below command to configure SAN details

openssl req -x509 -newkey rsa:2048 -sha256 -keyout privateKey.key -out certificate.crt -days 365 -config san.cnf

Steps to generate pfx Certificate with SAN

Follow the below steps to create the certificate.

Step 1: Download Open SSL from the link https://slproweb.com/products-/Win32OpenSSL.html



Step 2: Install Open SSL by double clicking the executable.
Step 3: Run the command prompt as Administrator mode
Step 4: Traverse to the path C:\Program Files\OpenSSL-Win64\bin
Step 5: Create Public & Private certificates by executing the below command

openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout privateKey.key -out certificate.crt -subj "/CN=sick.co.in"

Note: *Common Name (CN) should be changed as per the customer request*

Enter below pass phrase and re-enter the same again (You can choose anything. This needs to be entered in sick-bip-is.cfg file).

Sick

Step 6: Create a file and save as "san.cnf ".Below commands need to be written in san.cnf file

[req]


```
distinguished_name = req_distinguished_name
x509_extensions = v3_req
prompt = no
[req_distinguished_name]
C = US
ST = MA
L = Stoughton
O = SICK Product & Competence Center Americas
OU = SICK Product & Competence Center Americas
CN = sick.co.in
[v3_req]
subjectAltName = @alt_names
[alt_names]
DNS.1 = sick.co.in
DNS.2 = mysick.com
DNS.3 = sickmedia.co.in
```

> ***Note:*** *Change the names of DNS.1,DNS.2,DNS.3 as per your requirement. Any number of SAN names can be provided.*

Step 7: Enter the below command to configure SAN details

```
openssl req -x509 -newkey rsa:2048 -sha256 -keyout privateKey.key -out certificate.crt -days 365 -config san.cnf
```

Step 8(a): Enter below command to combine the private and public keys into one pfx file.

```
openssl pkcs12 -export -name “sick.co.in” -out sick-media-server-dev.pfx -inkey private-Key.key -in certificate.crt
```

> ***Note:*** *This command can also be used to generate pfx certificate from existing private key and crt certificate.*

Step 8(b): Enter below command to combine the private and public keys into one p12 file.

```
openssl pkcs12 -export -name “sick.co.in” -out sick-media-server-dev.p12 -inkey private-Key.key -in certificate.crt
```

> ***Note:*** *This command can also be used to generate p12 certificate from existing private key and crt certificate.*

Step 9: Enter pass phrase for privateKey.key, Enter Export Password and verify Export Password (The below Pass Phrase is used in the existing sick-bip-is.cfg for all 3 field)

29 Appendix B

Media Server internally configures two buffers, **Regular Buffer** and **Additional Buffer** based on the incoming throughput

- **Regular Buffer:** The size of this buffer is calculated to store 5 mins worth of data based on the incoming bytes throughput. The time duration for which this buffer is calculated is configurable from configuration file parameter SIZEOUT_TIME_BUFFER under STORAGE header. Example: Media server is acquiring 4MB worth of file per second. The size of Regular buffer will be (4MB X 5 min X 60 seconds) ~ 1.2 GB
- **Additional Buffer:** The size of this buffer is calculated to store 15 mins worth of data based on the incoming bytes throughput. The time duration for which this buffer is calculated is configurable from configuration file parameter ADDITIONAL_BUFFER_TIME under STORAGE header. Example: Media server is acquiring 4MB worth of file per second. The size of Additional buffer will be (4MB X 15 min X 60 seconds) ~ 3.6 GB

Size based cleanup will happen when following criterion is met:

- When the Available space in the disk is less than the sum of Minimum Free Space set from UI, Additional Buffer and Regular Buffer, Media server will initiate **Regular Cleanup**. This type of cleanup will follow ratio-based cleanup if enabled from cfg parameter RATIO_ENABLED under STORAGE. Example: Minimum Free limit is set as 10 GB and Media Server is storing its files in a 1 TB drive where Media server is acquiring 4MB worth of file per second. The size of Additional buffer will be (4MB X 15 min X 60 seconds) ~ 3.5 GB and the size of Regular buffer will be (4MB X 5 min X 60 seconds) ~ 1.2 GB. Once the Available free space in the disk becomes less than 14.7 GB (Additional Buffer 3.5GB + Regular Buffer 1.2GB + Minimum Free Space 10GB), Media Server will begin cleanup to maintain minimum free space of 14.7 GB.
- When the Available space in the disk is less than the sum of Minimum Free Space set from UI and Additional Buffer, Media server will start **Aggressive Cleanup** to free up space to achieve available space equal to the sum of Minimum Free Space and Additional Buffer. This cleanup does not follow ratio-based cleanup and clears out images based on First in First Out (FIFO). Example: Minimum Free limit is set as 10 GB and Media Server is storing its files in a 1 TB drive where Media server is acquiring 4MB worth of file per second. The size of Additional buffer will be (4MB X 15 min X 60 seconds) ~ 3.5 GB. Once the Available free space in the disk becomes less than 13.5 GB (Additional Buffer 3.5GB +

Minimum Free Space 10GB), Media Server will begin aggressive cleanup to free space up till available space becomes equal to 13.5 GB

- When the Available space in the disk is less than the Minimum Free Space set from UI, Media server will start **Maximum Aggressive Cleanup** to free up space equal to the sum of Minimum Free and Additional Buffer. This cleanup does not follow ratio-based cleanup and clears out images based on First in First Out (FIFO). Example: Minimum Free limit is set as 10 GB and Media Server is storing its files in a 1 TB drive where Media server is acquiring 4MB worth of file per second. The size of Additional buffer will be (4MB X 15 min X 60 seconds) ~ 3.5 GB. Once the Available free space in the disk becomes less than 10 GB (Minimum Free Space), Media Server will begin maximum aggressive cleanup to free space up till available space becomes equal to 13.5 GB

30 Appendix C

IP Cam and modes of operation

Note: When two objects are passing through a tunnel side by side then only first objects image is captured as they are in proximity and second object is not captured. While processing, it sends message to media server to rename previous image to the name required for the second image.

IP cam sends images to images server in various formats like JPEG, JPG, PNG, BMP etc. IP camera images are classified as thumbnail images in the media server. The controller can only be configured for either hardware trigger or software trigger.

Note: Starting with Media Server 1.6, the rename mechanism for IP cameras supports FTP, SFTP, and FTPS protocols. This enhancement provides greater flexibility and security for file transfer and renaming operations. Earlier versions supported only FTP.

i. Hardware Trigger Mode (Two text file mode)

1. Trigger sensor (TRG) identifies an object and sends a signal to Controller (CTR) to capture Image
2. Controller send a text file containing sequence number to Media Server over FTP
3. Controller sends a signal to IP camera to take image, IP camera sends the image with random filename to the configured Media Server over FTP
4. Controller has a pre-defined timeout after which it sends file another text file to Image Server now having content in the format "sequence Number"; filename; TRUE (example: 00001;samplefilename.jpg;TRUE)

Note: *If above sequence is violated, files and images are disregarded.*

ii. Software Trigger Mode

Software trigger mode is same as hardware trigger mode except determining what must be done upon receipt of a file or FTP commands.

1. One Text File Mode

Note: *Sequence of file operations is not guaranteed.*

1. Trigger sensor identifies an object and sends a signal to controller to capture image
2. Controller sends a command to IP camera to capture a image, postfix a random filename with a sequence number (example: xyz00001.png/ xyz_00001.jpg)
3. IP camera captures image and sends an image to media server with a postfix requested by controller.
4. Controller has a pre-defined timeout after which it sends file another text file to image server now having content in the format "sequenceNumabe;filename;TRUE (example: 00001;samplefilename.jpg;TRUE)

Note: Even if the sequence is violated, Media server can identify the image it needs to rename.

2. Rename Mode

Note: *Sequence of file operations is not guaranteed.*

1. Trigger sensor identifies an object and sends a signal to Controller to capture image
2. Controller Sends a command to IP camera to capture a image, postfix a random filename with a sequence number (example: xyz00001.png/ xyz_00001.jpg)
3. IP camera captures image and sends an image to media server with a postfix requested by Controller.
4. Controller has a pre-defined timeout after which controller sends 2 FTP commands
    a. RNFR sequence#
    b. RNTO newFilename

17. **Note:** If above sequence is violated, files and images are disregarded.

3. UDS Mode

Note: *Sequence of file operations is not guaranteed.*

1. Trigger sensor identifies an object and sends a signal to controller to capture image
2. Controller sends a command to IP camera to capture a image, postfix a random filename with a sequence number (example: xyz00001.png/ xyz_00001.jpg)
3. IP Camera captures image and sends an image to media server with a postfix requested by controller.
4. Controller has a pre-defined timeout after which Controller sends a message to Media Server running TCP/IP socket server at a configured port number.
    a. STX<message>ETX
    b. If UDS IP camera is configured to send a XML metadata file, the file will be named like the final intended image file name but will have an extension XML. This file will be transmitted over from controller to Media Server over FTP using the IP Camera's username.

UDS Message

```
STX<cpreq><src>PS06Test_20111128_142249000_00001.jpg</src><dst>PS06Test_20111128_142249_00000001.jpg<
/dst><subdir>full</subdir></cpreq>ETX
```

Figure 0:1: UDS Message

