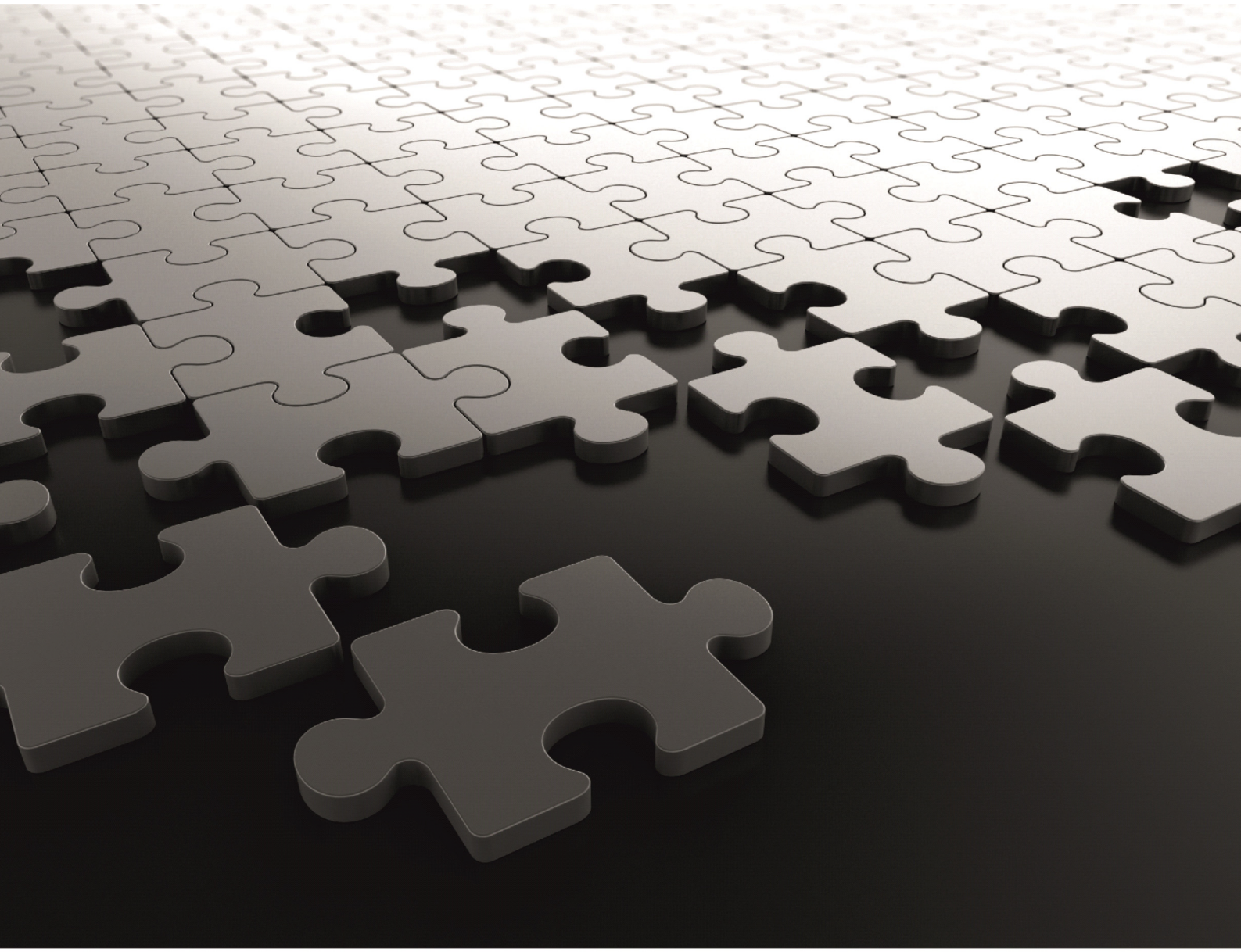
SATATYA SAMAS
Admin Client



MATRIX®
TELECOM | SECURITY

MATRIX®
TELECOM | SECURITY

Matrix SATATYA SAMAS Admin Client

System Manual



Documentation Disclaimer

Matrix Comsec reserves the right to make changes in the design or components of the product as engineering and manufacturing may warrant. Specifications are subject to change without notice.

This is a general documentation for all the variants of the product. The product may not support all the features and facilities described in this document.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise the information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this system manual, Matrix Comsec assumes no responsibility for errors or omissions. No liability is assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the buyer of this product or third parties for damages, losses, costs or expenses incurred by the buyer or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec operating and maintenance instructions.

Copyright

All rights reserved. No part of this system manual may be copied or reproduced in any form or by any means without the prior written consent of Matrix Comsec.

Warranty

For product registration and warranty related details, visit us at;

https://www.matrixcomsec.com/warranty/#IP-video-surveillance

Version 6
Release date: July 24, 2026

Contents

Introduction **1**

Overview **5**

Getting Started **11**

General Settings **23**

System Account *24*
User Groups *25*
Users *39*
ONVIF Users *46*
Vision GUID Authorization *49*
System Settings *52*
Log Management *53*
IP Filter *56*
Active Directory Configuration *58*
Password Settings *59*
Logo Personalization *63*
Report Personalization *66*
Language Settings *69*
Templates *76*
Schedules *77*
Alarms *81*
Message Templates *86*
WhatsApp Integration *96*
File Import *110*
File Export *114*
Audio *119*
Scheduler *122*
Report Scheduler *122*
Manual Triggers *133*
Custom Events *137*
User Profiles *141*
Custom Fields *151*
Activity Log *153*
License Management Settings *156*
Utilities *166*
Vehicle Attributes *167*
User Attributes *173*

Servers & Devices **181**
Management Server *185*
Recording Server *219*
Failover Server *222*
IVA Server *224*
Transcoding Server *226*
ONVIF Server *228*
Recording Server Configuration *230*
Failover Server Configuration *292*
IVA Server Configuration *314*
Transcoding Server Configuration *320*
ONVIF Server Configuration *323*
Device Configuration *331*
Camera Configuration *337*
Servers and Devices-Scenarios *413*
Component Group *415*
Object Counting Group *423*
Servers and Devices - Reports *427*
Vehicle Counting Report *427*
People Counting Report *431*

Emaps **433**

Access Control **447**
Access Control Server *448*
Standalone Panel *457*
Scenarios - Access Control *468*

Cognitive Response Engine with Automated Monitoring **469**
Basic Scenario *471*
Advanced Scenario *485*
Push Notification *502*
Push Video/Snapshot *504*
CREAM - Report *506*

Perimeter Management **513**
Intrusion Zone *514*
Security Line *530*
Perimeter Zone *549*
Perimeter Management-Scenarios *587*
Perimeter Management - Report *588*

Parking Management **595**
Multilevel Parking *596*
Slot *597*
Slot Group *657*
Lane *662*
Area *666*
Level *671*
Facility *675*
Driveway *680*
Security Sections *698*
Parking Premises Group *717*
Parking Management- Scenarios *721*
Parking Management - Reports *722*
Prohibited Parking Report *723*

Wrong Way Detection Report *724*
Unauthorized Parking Report *725*
Improper Parking Report *726*
Vehicle Overstay Report *727*
Parking After Closing Hours Report *728*
Report Configurations *729*
Vehicle Counting Report *736*
Slot Occupancy Reports *740*
Most Occupied Parking Entity Report *747*
Most Visited Parking Entity Report *751*
Least Occupied Parking Entity Report *752*
Least Visited Parking Entity Report *753*
Utilities *754*
Attributes *754*
Rename Entities *758*

Crowd Management **759**
Crowd Premises *760*
Crowd Premises Group *778*
Crowd Management-Scenarios *782*
People Counting Reports *783*

Person Identification **789**
Person Identification-Zone *790*
Person Identification-Scenarios *804*
Face Detection Report *805*

System Monitor **811**
Server Dashboard *812*
Reports *828*
Summary Reports *829*
Analytics Reports *834*
Downtime Analysis Report *839*
Maintenance Report *844*
System Report *845*
Event Log *850*
Online Users *853*
Online ONVIF Users *855*
Blocked IP Address *857*

Vehicle Management **859**
Vehicle Management-Zone *860*
Vehicle Management Scenario *877*
Vehicle Management - Reports *878*
Vehicle Detection Report *879*
Vehicle Identified Report *885*
Vehicle Unidentified Report *892*
Blacklisted Vehicle Identified Report *893*
Whitelisted Vehicle Identified Report *894*
Suspected Vehicle Identified Report *895*
Utilities *896*
Rename Entities *896*

Weighbridge Application **897**
Terminals *899*
Station *910*

Evidence Receipt *920*
Scenarios *933*
Reports *934*

Scenario Events With Actions **941**

Appendix **1015**
Objects and Services supported by BACnet Server *1015*
Known Points related to addition of 400 Camera *1016*
Supported Licenses *1017*
Frequently Asked Questions (FAQs) *1020*
Keyboard Shortcuts *1030*
Disposal of Products/Components after End-Of-Life *1032*

CHAPTER 1

Introduction

Welcome

Thank you for choosing the Matrix SATATYA SAMAS Video Management System!

Organizations are places with constant activity. Such places require uninterrupted, real-time surveillance to track all the activities in their premises. While most organizations today have stepped up with technology, they essentially lack smart analytics and features, when it comes to video surveillance. The SATATYA SAMAS is a new-age Video Management Solution designed for large enterprises with multi-site surveillance requirements. It is specifically designed to meet the all-round security and surveillance needs of organizations. Big enterprises have got diverse and complex needs, all of which are seamlessly addressed by SATATYA SAMAS.

SATATYA SAMAS is a smart video surveillance tool, packed with intelligent features and video analytics. The suite of applications provides comprehensive management and support with centralized monitoring and control. It also supports a large number of cameras and other video surveillance devices. The application is optimized to support different languages. It also supports UTF-8 characters, allowing the users to provide inputs in their local language using international keyboards. This makes it an ideal solution for worldwide usage.

This helps business owners and managers to avoid unwanted accidents with proactive monitoring and management. In addition to this, SATATYA SAMAS can be linked with multiple solutions like POS, Weighbridge, Parking Management, Access Control, Fire Alarm, and so on to strengthen the security on premises.

Please read this document carefully before proceeding with the initial configuration of the Matrix SATATYA SAMAS.The terms Matrix SATATYA SAMAS Admin Client, SATATYA SAMAS Admin Client, and Admin Client are used interchangeably and refer to Matrix SATATYA SAMAS Admin Client.

About this Document

This document is intended to serve as a system administrator's manual for using the SATATYA SAMAS Admin Client. This document shall provide detailed information and instructions to the system administrator for initial setup and configuration of the SATATYA SAMAS, using the Admin Client application.

It is recommended that this manual is read in combination with the following documents:

- SATATYA SAMAS Installation Guide
- SATATYA SAMAS Smart Client Manual
- SATATYA SAMAS Media Player Manual
- SATATYA SAMAS ONVIF Server Manual

Certain information may appear blur in the documents due to security reasons.

Organization of this Document

The SATATYA SAMAS system administrator's manual is organized into the following chapters:

Chapter 1: Introduction provides detailed information on the nature and content of this document.

Chapter 2: Overview provides detailed information on the product and its components.

Chapter 3: Getting Started provides detailed description of the installation, start-up and common user interface elements of the SATATYA SAMAS Admin Client application.

Chapters 4 & 5: General Settings/Servers and Devices provide detailed information about the general settings and configuration of servers and devices.

Chapters 6-14: provide detailed description of the rest of the modules of the Admin Client application, their features, functionality and configuration.

Frequently Asked Questions provides a list of FAQs on the product. Refer to "Frequently Asked Questions (FAQs)" for more information.

The word IP Cameras is used through-out the document and it represents IP Cameras as well as Mobile Cameras, unless specified. Mobile Cameras may not support certain features, the same is mentioned explicitly.

Abbreviations

Some abbreviations/acronyms are used recurrently in the document. These are:

VMS	Video Management System
MS	Management Server
RS	Recording Server
IVA	Intelligent Video Analysis
FoS	Fail-over Server
TS	Transcoding Server
HVR	Hybrid Video Recorder
DVR	Digital Video Recorder
NVR	Network Video Recorder
ONVIF	Open Network Video Interface Forum
FTP	File Transfer Protocol
MPEG	Moving Picture Experts Group
JPEG	Joint Photographic Experts Group
CIF	Common Intermediate Format
QCIF	Quarter Common Intermediate Format
FPS	Frames Per Second
PTZ	Pan, Tilt, Zoom

Symbols

The following symbols are used in the document to draw your attention to important items.



Important: to indicate something that requires your special attention or to remind you of something you might need to do when you are using the system.



Caution: to indicate an action or condition that is likely to result in malfunction or damage to the system or your property.



Warning: *to indicate a hazard or an action that will cause damage to the system and, or cause bodily harm to the user.*



Tip: *to indicate a helpful hint giving you an alternative way to operate the system, carry out a procedure, or use a feature more efficiently.*

Technical Support

For additional information or technical assistance with SATATYA SAMAS Admin Client and other Matrix products, contact our Technical Support Help Desk. We are available from Monday to Saturday- 9.00 AM to 6.00 PM (GMT +5.30), except company holidays.

Phone	(+91) 1800 258 7747
Internet	www.MatrixComSec.com
E-mail	Tech.Support@MatrixComSec.com

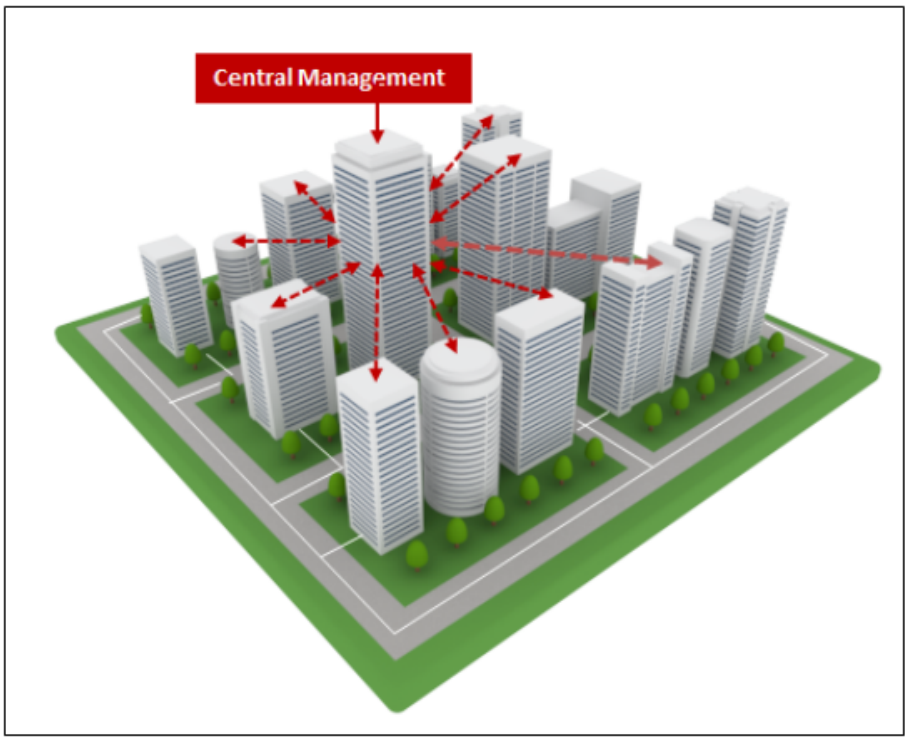
CHAPTER 2

Overview

What is SATATYA SAMAS

The SATATYA SAMAS is a tool for centralized video surveillance management and monitoring. It is a platform that can simultaneously control and communicate with multiple video capturing, encoding and recording devices. It provides an enterprise-level surveillance support for multi-site deployments, that are spread across different physical systems and worldwide geographical locations.

SATATYA SAMAS has intelligent video analytics and features that make it a real-time surveillance solution. It enables security personnel to track and manage various activities by integrating it with various solutions such as crowd management, parking management, and more.



Supported Devices

SATATYA SAMAS supports the following devices:

i. Matrix DVR

ii. Matrix NVR

iii. Matrix HVR

iv. ONVIF Supported and Generic Cameras

v. IP cameras from the following manufacturers:

- Matrix
- Acti
- Axis
- DLink
- HIKVISION
- Infinova
- Samsung
- Panasonic
- Vivotek
- Brickcom
- Dahua
- Grandstream
- Bosch

vi. Mobile Camera; when **Allow Push Video** is enabled for the user. For details, refer to “Users”.

System Components

A typical SATATYA SAMAS setup comprises of the following system components:

Components	Description
Management Server	This is the Main Server responsible for centralized authentication and management. The SATATYA SAMAS architecture allows only one Management Server per system.
Enterprise Database	This is the database for storing configuration settings and logs of the system.
Recording Server	This Server is responsible for communicating with video surveillance devices, recording video streams into its storage drive and streaming live and recorded videos to the clients. A Management Server allows one or more (max. 255) Recording Servers to communicate with it.
Failover Server	This Server is responsible for functioning as a Recording Server when any one of the configured Recording Server is down.
IVA Server	This Server is responsible for real-time event detection and post-event analysis using Intelligent Video Analytics.
Transcoding Server	This Server is responsible for optimizing the bandwidth of stream usage for uninterrupted Live View / Playback.

ONVIF Server	This Server acts as a bridge between SAMAS and 3rd Party ONVIF Clients.This enables easy exchange of video data as well as availability of Live / Playback streams.
Notification Server	This Server is responsible for sending notification through SMS, Email and WhatsApp.
License Server	This Server is responsible for the functioning of SATATYA SAMAS.
Recording Database	This is the database of the Recording Server that stores its local configuration.
Storage Drive	This is the Drive that stores video recordings. This can be a Hard Drive, a Network Drive, an FTP Drive or an USB Device.
SATATYA Devices	These include Matrix SATATYA DVRs, NVRs and HVRs.
IP Cameras	These include supported brands of IP cameras and their models as well as Mobile Camera. Refer to “Supported Devices”.
Admin Client	This is the Desktop Application for centralized configuration and management of SATATYA SAMAS from local / remote locations.
Smart Client	This is the Desktop Application for local / remote viewing of security system media (live and recorded videos).
Media Player	This is the Desktop Application to view the records stored in the Backup Storage.

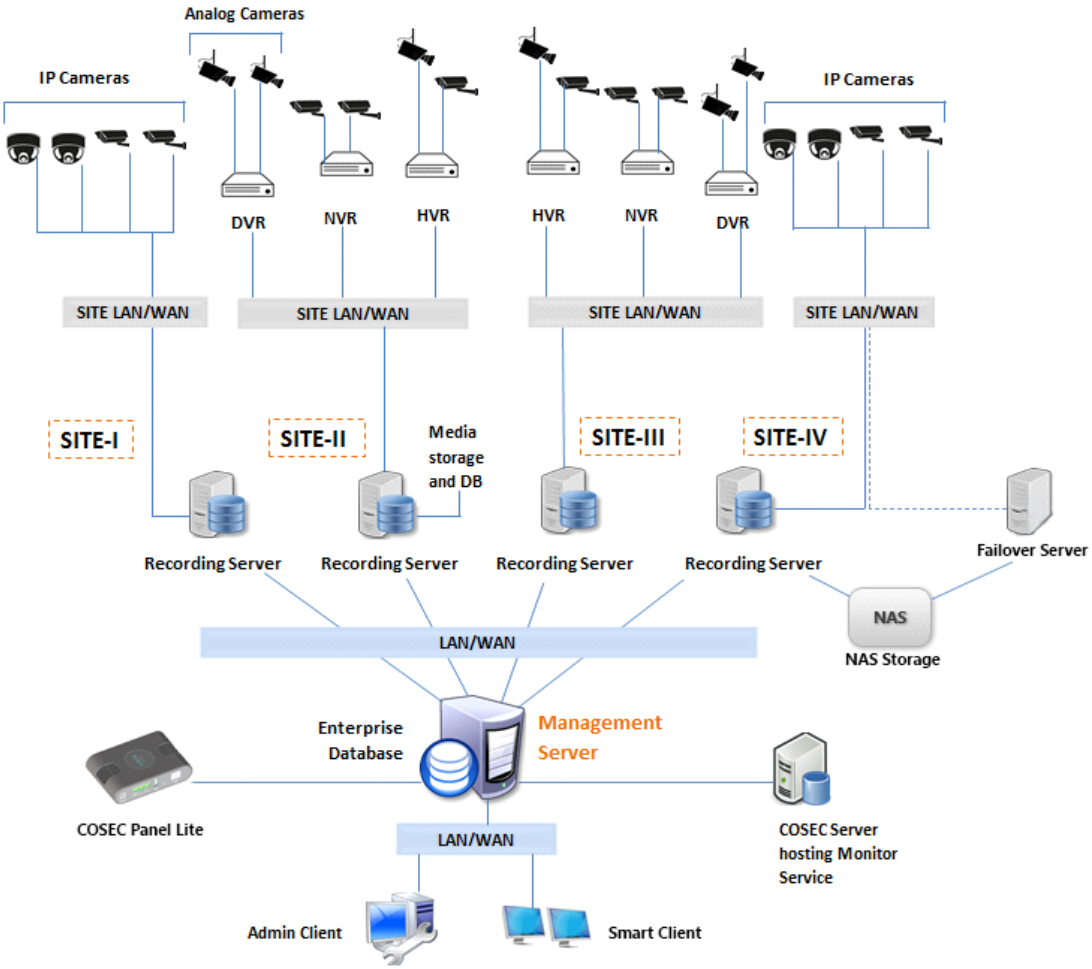
System Architecture

Typically, the SATATYA SAMAS architecture allows only a single Management Server per system. This server acts as the central command unit of the system. It allows to install multiple Recording Servers at local or remote sites which act as streaming servers for assigned devices (DVR, HVR, NVR or IP Cameras). Each Recording Server can support a maximum of 400[1] cameras. These communicate with the central Management Server for authentication as well as configuration.

The Admin Client application is the main configuration tool for SATATYA SAMAS. It is possible to install it on the same system or a different system as the Management Server. It allows the system administrator to configure the general settings and connected servers and devices.

SATATYA SAMAS has another application apart from Admin Client, that is, the Smart Client. The Smart Client application allows to view and monitor live and recorded videos from different locations in the IP network.

The system architecture of the SATATYA SAMAS based on a typical multi-site setup is illustrated below:



1. *For Known Points related to 400 cameras, refer to "Known Points related to addition of 400 Camera".*



Admin Client

The Admin Client is the system administrator's primary tool for setting up the SATATYA SAMAS. It offers the basic as well as advanced configuration features to the system administrator to add, create, control as well as monitor different entities in a surveillance setup from a centralized location. The Admin Client provides the following features and functionality:

FEATURES/ FUNCTIONALITIES	DESCRIPTION
SERVERS & DEVICES	Configure servers, devices and cameras along with stream, recording and storage settings.
ACCESS CONTROL	Allows integration of COSEC Access Control Management System with SATATYA SAMAS.
CREAM (Cognitive Response Engine with Automated Monitoring)	Configure scenarios and actions against pre-defined and user-defined Events.
EMAPS	Configure electronic maps for surveillance sites.
PERIMETER MANAGEMENT	Configure directional zones, security lines and zones.
PARKING MANAGEMENT	Configure parking slots, driveways and counting lines.
CROWD MANAGEMENT	Create and configure events like people counting and premise availability.
PERSON IDENTIFICATION	Create and configure detection region and events - Face Detection.
GENERAL SETTINGS	Configure general settings of the application.
SYSTEM MONITOR	Monitor health of the system.
VEHICLE MANAGEMENT	Create and configure zones and events - Vehicle Detection.
WEIGHBRIDGE APPLICATION	Create and configure Stations, Terminals and Evidence Receipts.



To enhance security from SAMAS V6R1 and onwards, we have introduced data security for data at rest as well as in transit (applicable only when Matrix proprietary protocol is used). Hence, if you are upgrading SAMAS to V6R1, then make sure all the components are also upgraded to the same version to ensure smooth functioning.

CHAPTER 3

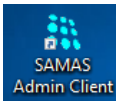
Getting Started

The SATATYA SAMAS offers a simple and easy-to-use installer utility for all components including the Admin Client. Run the SATATYA SAMAS installation setup on the selected system to install the Admin Client component. Refer to the **SATATYA SAMAS Installation Guide** which consists of the complete installation procedure along with the system requirements.

The current chapter will help you get started with the basic elements of the Admin Client, once the installation is completed successfully.

Login into the Admin Client

For step-by-step installation instructions, refer to **SATATYA SAMAS Installation Guide**.

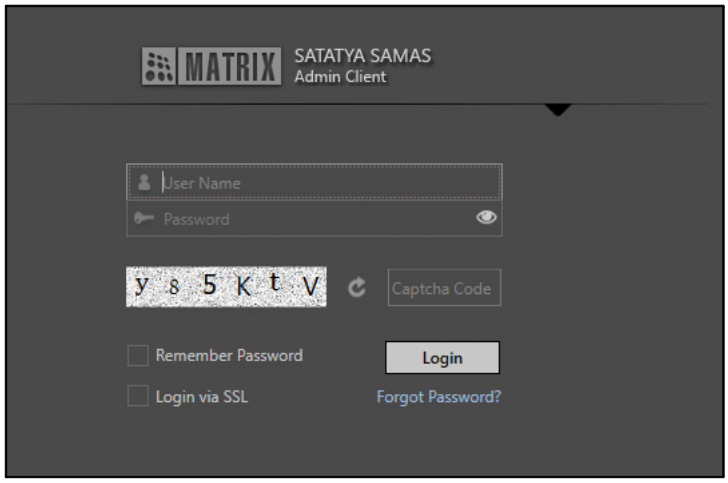
On completion of installation, the Admin Client 

icon appears on your Windows Desktop.

Make sure you have provided full access rights (manually) to the SATATYA SAMAS Admin Client Folder you installed.This is applicable for Software Release V5R4 and later only.

For other Software Releases, windows authentication pop-up will appear to provide administrative rights.

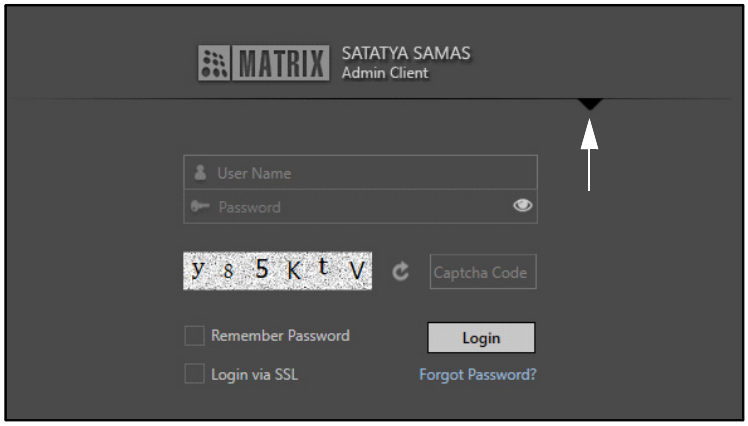
- Double-click on the icon to launch the Admin Client Application. The login page appears.

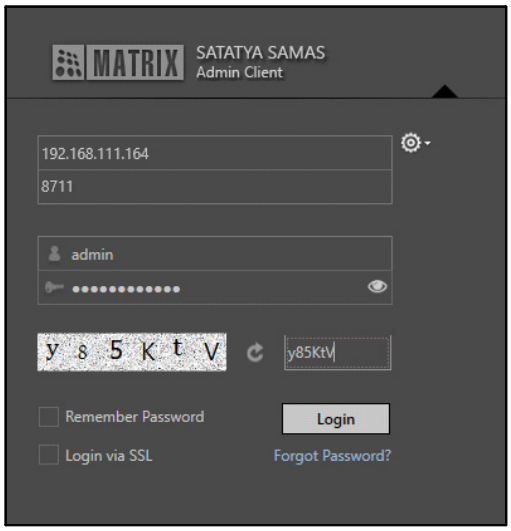


To access the Admin Client, you need to configure the network parameters to establish the connection between the Admin Client and Management Server (MS).

Follow the steps to configure the network parameters.

- Click  to expand the panel. Enter the **IP Address** and **Port**.





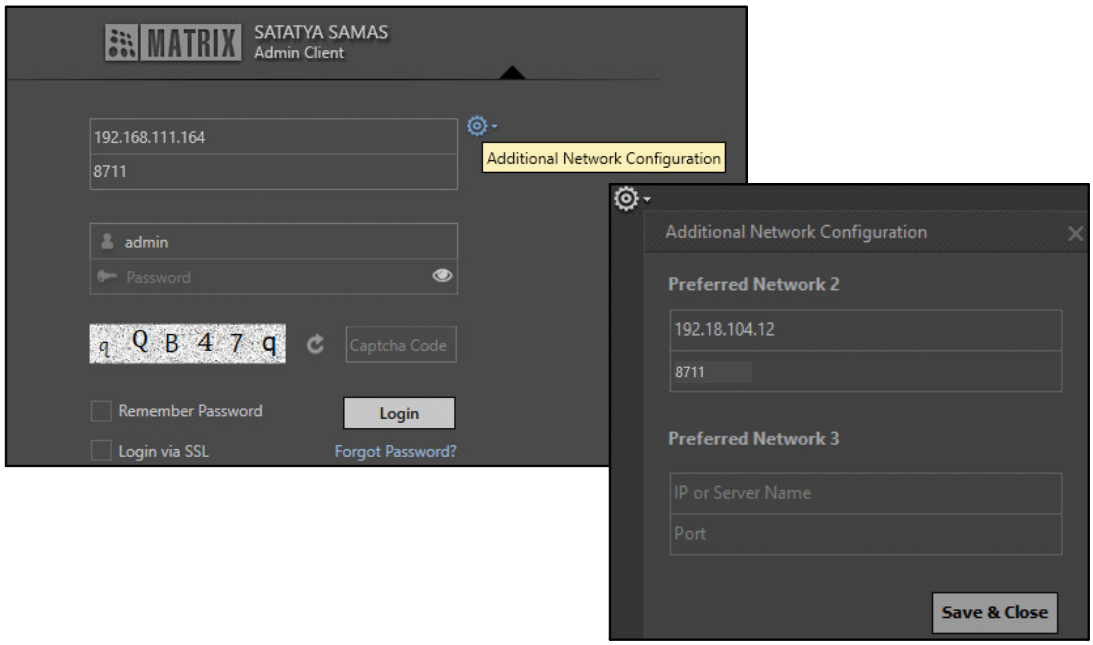
- **IP Address** or **Server Name:** Configure Private or Public IPv4/IPv6 Address of the Management Server. You can also enter Host Name, Domain Name or Server Name of the Internet Service Provider (ISP). By default this is Preferred Network 1. In IP or Server Name, you can enter upto 255 characters. Default: localhost.

If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Port:** Configure the Private or Public Port. Valid Range: 1-65535. Default: 8711.

You can add two more Preferred Networks, that is, Preferred Network 2 and Preferred Network 3. In case Preferred Network 1 fails, the connection is established via Preferred Network 2 or Preferred Network 3. In these three preferred networks, you can either configure Private Network or Public Network (ISPs) for the Management Server.

- To add Preferred Network 2/Preferred Network 3, click **Additional Network Configuration**  .



- Configure the IPv4/IPv6 Addresses and Ports of the respective Preferred Networks.
- Click **Save & Close** to save the configurations.You return to the login page.

Configure the network with the highest priority in Preferred Network 1.

- Enter the User Name and Password. The first login can be performed using the default administrator User Name; **admin**. In User Name, you can enter upto 50 characters and in Password, you can enter upto 128 characters. For Password, Valid Range: 12-128. Default: Blank.
- Enter the Captcha code. The Captcha code helps in increasing security of application by differentiating between real and automated users. Click **Refresh** to refresh the Captcha code.
- Click **Login**.
- At the time of first login, you will be prompted to set a new password. The SAMAS stores a list of frequently used passwords in a database and compares the new password with the same. SAMAS will not allow you to configure such frequently used passwords to enhance security.

  To create a strong password make sure you enter one special character, one number, one lowercase and one uppercase character. The Password Meter displays the strength of the password you enter. Make sure you enter 12 characters (default value) as the password length. For details, refer to "Password Strength". Make sure you note down the created password at a secure place for future reference.

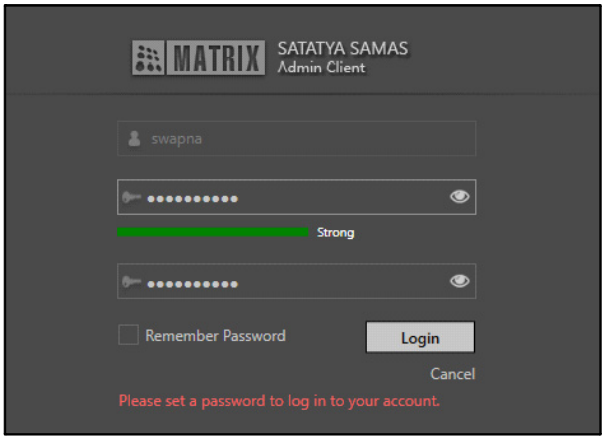
- Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

At the time of installation, under Management Server Settings > License Verification > Select Mode, if you have selected Service/Device Based option, then the Management Server checks for a valid License Key. If only a Generic License Key is detected then a pop-up appears.



*The Generic Key is displayed in **Existing License Key.** In **Enter New License Key** you need to enter the new key you wish to activate and click **Activate**. In Enter New License Key, you can enter upto 104 characters. Default: Blank.*

If you have opted for Virtual License during installation or if you are migrating from Service Based/ Device Based to Virtual License, then as soon as you login, the License Management Settings pop-up appears and you need to register the license. For details, refer to "License Management Settings". Make sure the login user has atleast View and Edit rights of General Settings Module. For details refer to "Configuration Rights" in "User Groups".



- While logging into the Admin Client, you can select the **Remember Password** check box, if you wish the application to remember your password for the successive logins.
- You can also select the **Login via SSL** check box to login into the application securely via SSL. If the Management Server is running on SSL mode, then it is mandatory to enable this check box to login into the Admin Client.

If **Login via SSL** check box is selected and the SSL certificate is not available and/or expired, accordingly a pop-up appears.

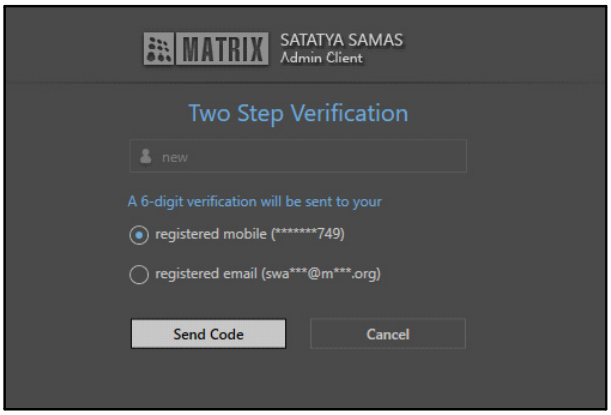


- Click **Yes** to continue to login with untrusted/expired certificate.

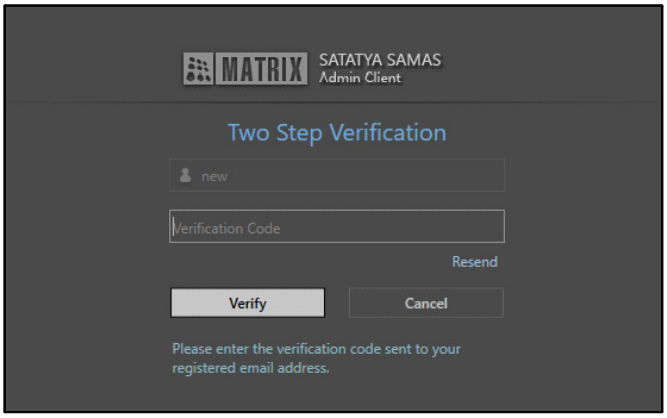
  The events for unavailable/expired SSL certificate will be generated. To view the event details, refer to "Event Log".

Enable Multi-factor Authentication, is not applicable to the default Admin User (admin). Hence for such user the Admin Client Home page will appear.

For other Users, if **Enable Multi-factor Authentication** is enabled, then on clicking **Login**, the **Two Step Verification** page appears.



- Select the desired option — registered Mobile Number or Email Address — on which you wish to receive the 6-digit verification code, that is, OTP. Click **Send Code**.



- Enter the verification code received on the registered Mobile Number or Email Address. The code is valid for 10 minutes only. Click **Verify**. You directly get logged into the Admin Client.

The Maximum Failed OTP Allowed, Maximum OTP Regeneration Allowed and Lock Account will be as per the OTP Policy for Multi-factor Authentication. For details, refer to "OTP Policy".

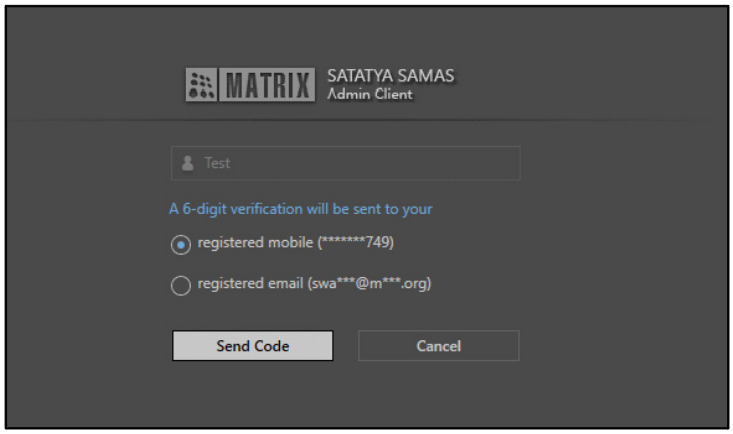
- Click **Login**. The Admin Client Home page appears.

Forgot Password

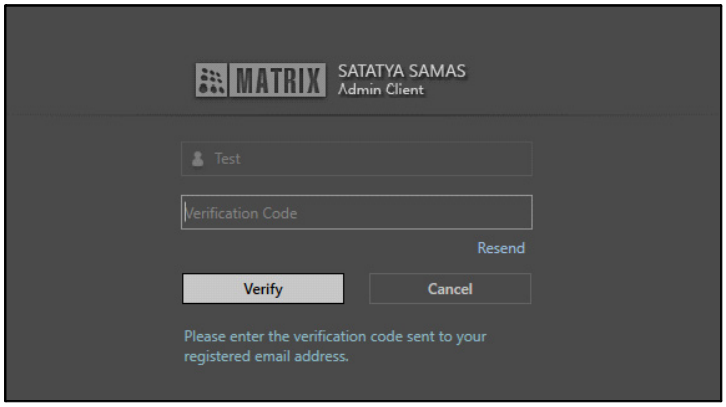
If you have forgotten your current password, **Forgot Password** enables you to receive an OTP and set a new password. The OTP (One Time Password) will be sent either to the registered Mobile Number or Email Address.

To access the Forgot Password feature,

- Click the **Forgot Password** link on the Login page.

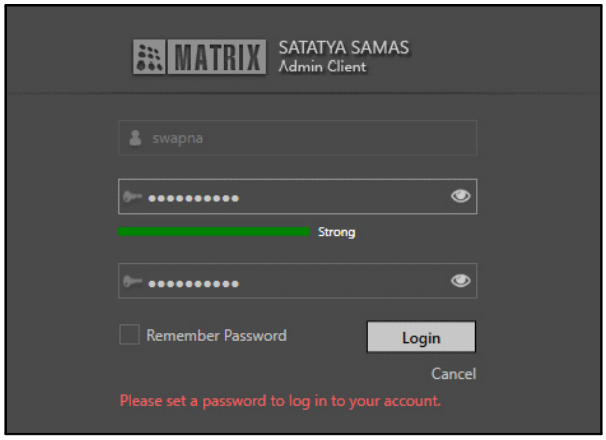


- Select the desired option — registered Mobile Number or Email Address — on which you wish to receive the 6-digit verification code, that is, OTP. Click **Send Code**.



- Enter the verification code received on the registered Mobile Number or Email Address. The code is valid for 10 minutes only. Click **Verify**.

The Maximum Failed OTP Allowed and Maximum OTP Regeneration Allowed on Resend depends on the configured OTP Policy. For details, refer to "OTP Policy".



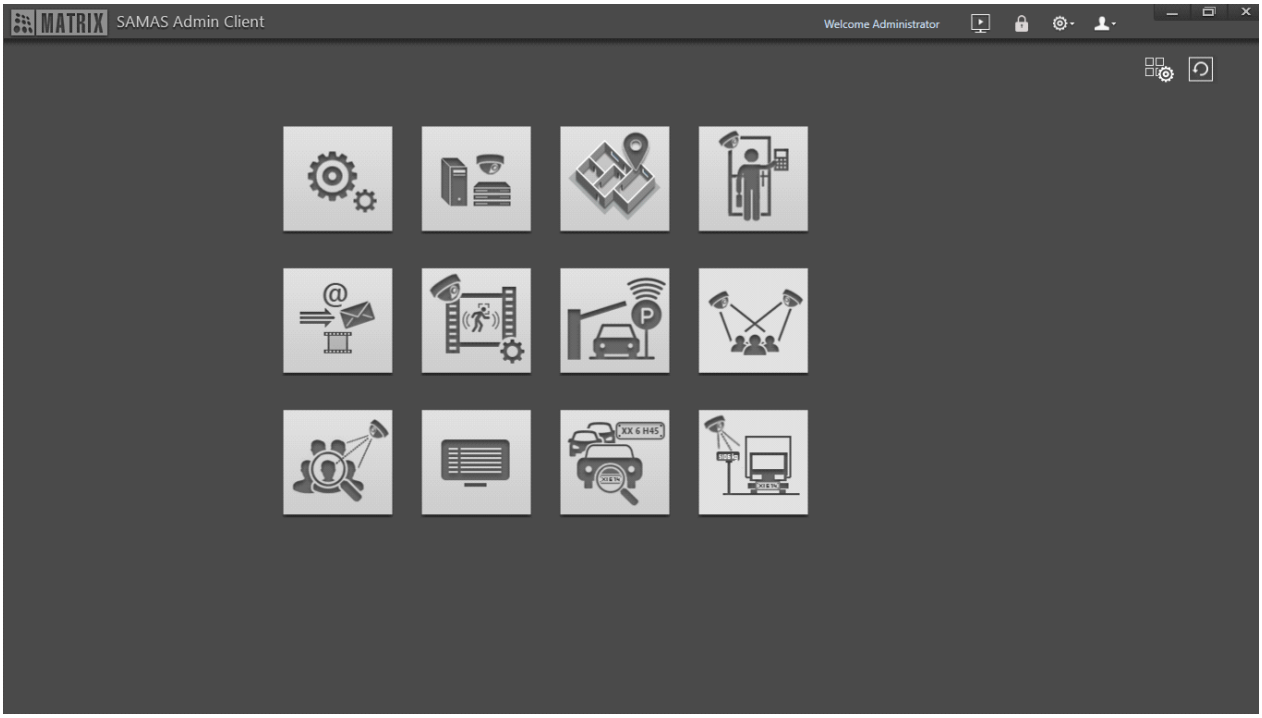
- The Login page appears. Enter the **New Password** and re-enter it in **Confirm Password**. In New Password and Confirm Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank.

- Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **Login.** You directly get logged into the Admin Client.

Admin Client Homepage

Once you login, the SATATYA SAMAS Admin Client Homepage appears.



Admin Client Homepage Icons

The Admin Client Homepage consists of the following:

- Title Bar, for details refer to "Title Bar".
- Module Icons, for details refer to "Module Icons".
- Show or Hide Module, for details refer to "Show or Hide Module".
- Reset Module, for details refer to "Switch Module Icon Position".

Module Icons

The Admin Homepage displays the following Module icons:

Icons	Description
	General Settings

Icons	Description
	Servers & Devices
	Emaps
	Access Control
	Cognitive Response Engine with Automated Monitoring (CREAM)
	Perimeter Management
	Parking Management
	Crowd Management
	Person Identification
	System Monitor
	Vehicle Management
	Weighbridge Application

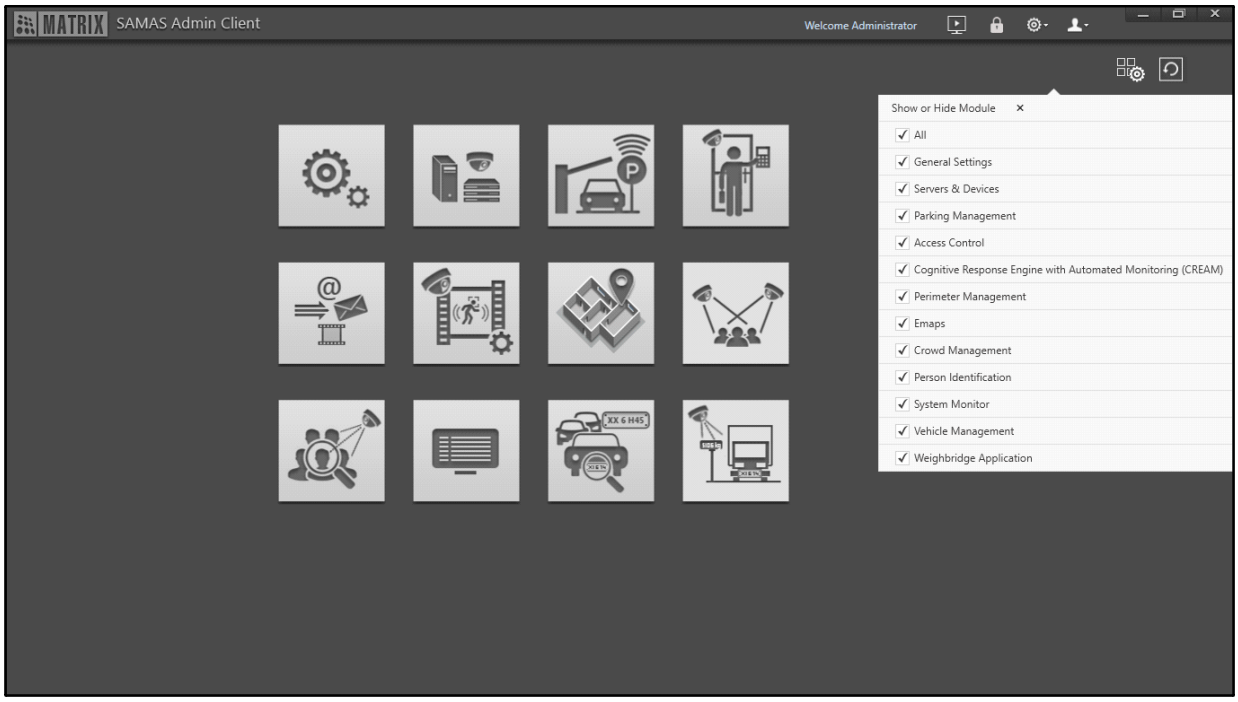
The Module icons appear on the homepage as per the license purchased. Refer to each module for details.

The Face Recognition Cameras License is not available in the current Software Release. Hence, Face Detection in all the IVA Events will also not be available. These will be included in the upcoming release.

You can show or hide particular modules and also change their position on the homepage as per your requirement. Refer to "Show or Hide Module" and "Switch Module Icon Position".

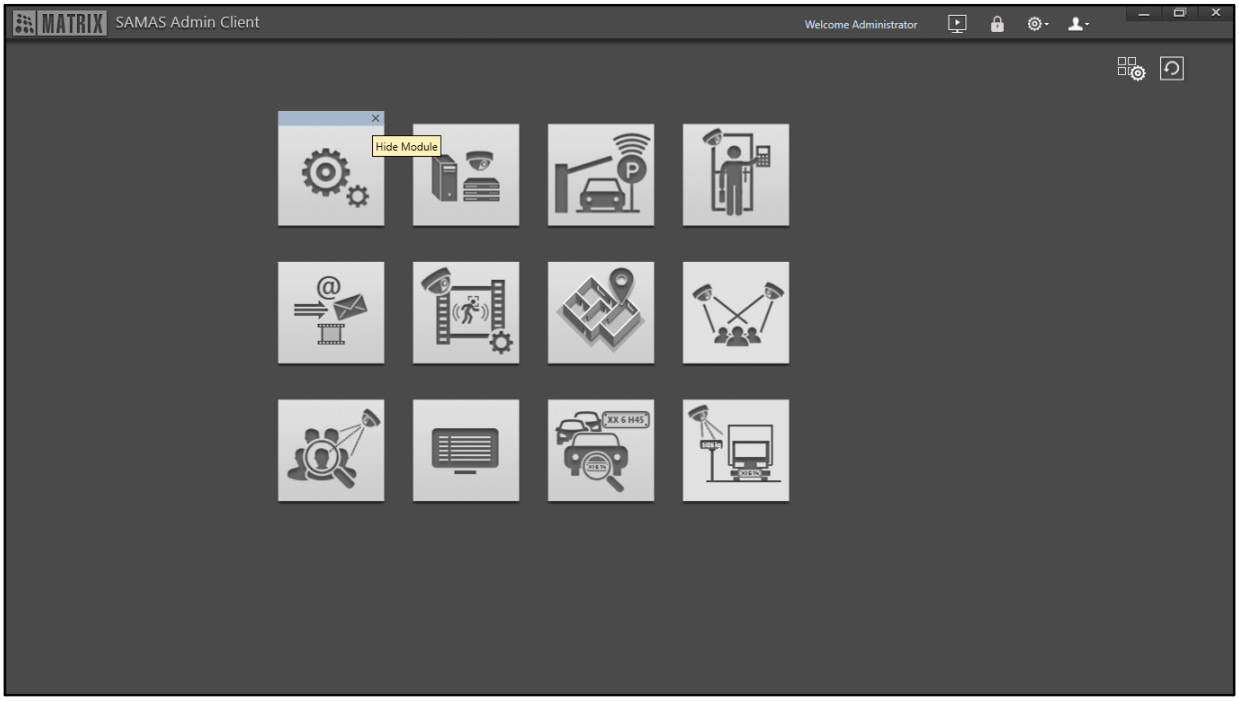
Show or Hide Module

- Click **Show or Hide Module** . A list of all the modules appears.



- By default, the check boxes for all the modules are selected. Clear the check boxes for the modules you wish to hide.

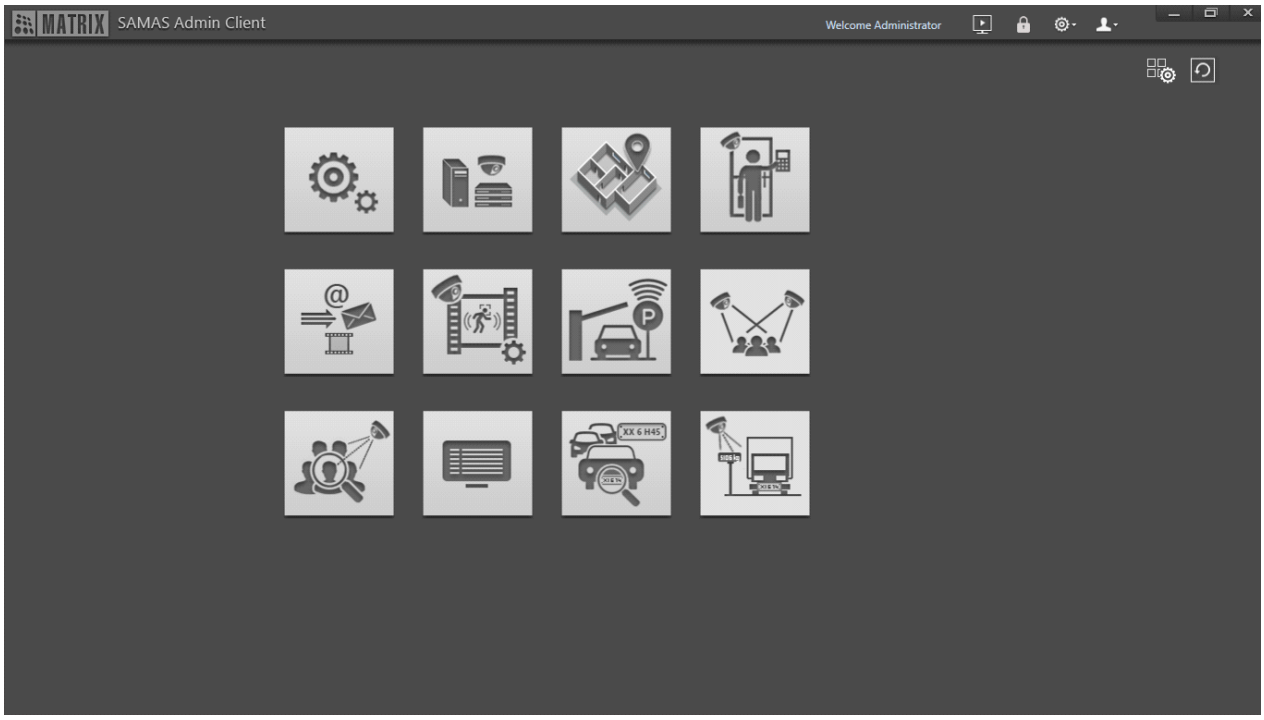
  Alternatively, hover on the desired module. A cross icon appears.



Click the cross icon to hide the module. Similarly, when you click **Show or Hide Module**  again in the list view the check box of this module appears disabled. You can select the check box of the hidden module to view it on the homepage as explained above.

Switch Module Icon Position

By default, the module icons appear on the homepage in this order:



You can switch the position of the module icons on the homepage. To do so,

- Hover-over the top-center of the desired module icon, for example Emaps. A four-sided arrow appears. Drag the icon at the desired position to swap it with the existing icon, here it is placed at the position of the Parking Management module.



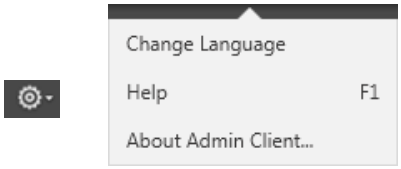
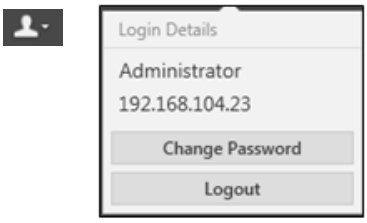
- Similarly, you can switch the positions for multiple module icons. To reset the default position of the module icons, click **Reset Module**  . All the module icons will be reset to their default positions.

Title Bar

The following options appear in the Title Bar.



Icons	Description
	Returns to the Admin Client Homepage.
	Opens the SATATYA SAMAS Smart Client Application. Make sure the Windows User Account Control Settings are set as “Never notify” for smooth operation of this feature.
	Locks the Admin Client. The SAMAS shortcut keys will not function when the client is in locked state. You need to enter the password to unlock the Admin Client. For more details, refer to "Unlock".

Icons	Description
	**Settings** — The following options are displayed: **Change Language:** This option allows you to change the language of the Admin Client. Click on this option to view the saved languages. Select the preferred language. A confirmation message appears. Click **Yes,** to change the language of both Admin and Smart Client permanently**.** **OR** Click **No,** to change the language of the Admin Client temporarily, that is, for the current session only. **Help**: Displays the Admin Client User Guide. **About Admin Client**: Displays information about the SATATYA SAMAS Admin Client — Application Version Revision along with the link to the End User License Agreement.
	**User Details** — Displays the Login details and IPv4/IPv6 Address of the system from which the Admin Client is being accessed. The following options are also displayed: **Change Password:** Opens the **Change Password** window using which you can change the login password. You need to provide the **Old Password**, enter the **New Password** and re-type it in the **Confirm Password** to change the password. Click on **Change Password** to set the new password. **Logout:** Logs you out from the Admin Client Application.

CHAPTER 4

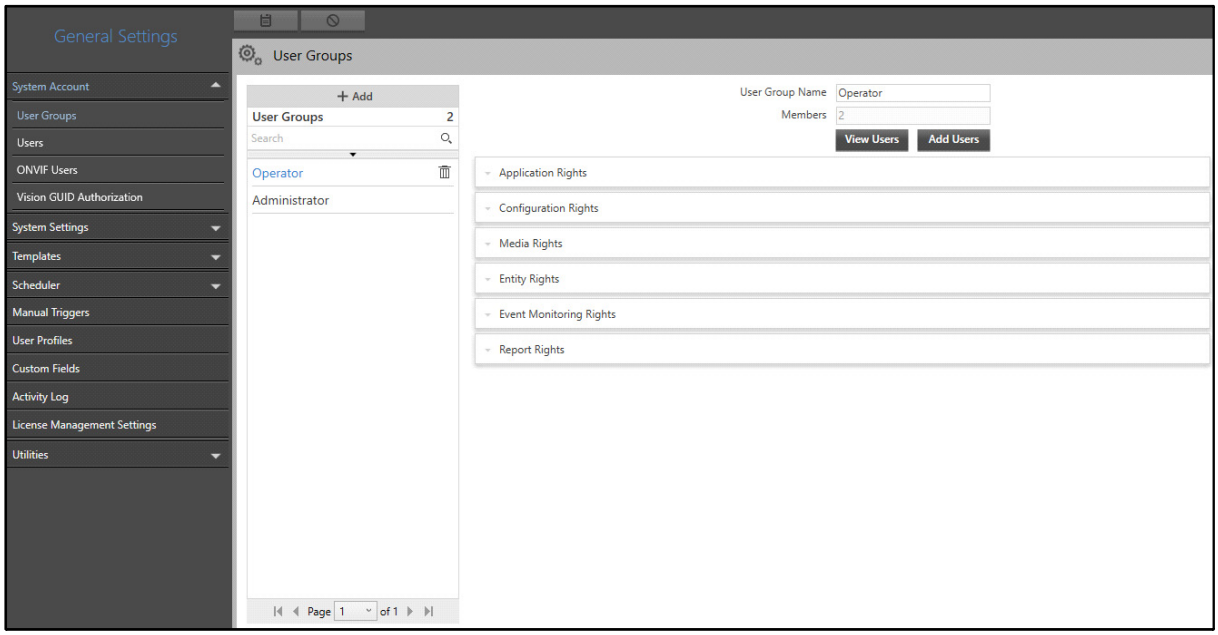
General Settings

The General Settings module enables you to configure various general system parameters — create system Users as well as User Groups, define System Settings, create various Templates, create Schedules, add custom Events and fields, etc. These configurations serve as the basis for the configurations of other modules.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure General Settings,

- Click **General Settings**.



The General Settings module contains these sections and pages — "System Account", "System Settings", "Templates", "Schedules", "Manual Triggers", "Custom Events", "User Profiles", "Custom Fields", "Activity Log", "License Management Settings" and "Utilities".

System Account

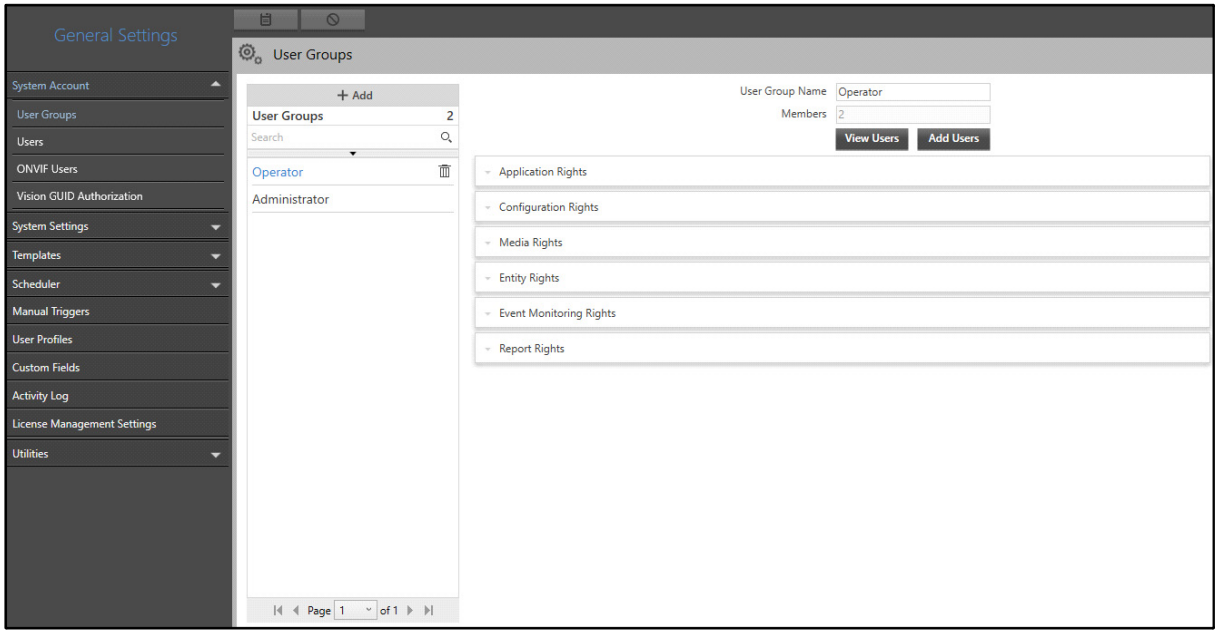
By default there is only one user — Administrator. This user can access the Admin Client. The system administrator can perform the first login being the single default user of the application. The administrator rights cannot be edited. The default username for administrator login is **admin.** The system administrator also needs to set the password during the first login. For details, refer to “Getting Started”. The system administrator can change the password later if required. For changing the Password, refer to “Title Bar”.

The system administrator can login into the Admin Client and create other users too. Each User has a unique User Name and Password. For other Users to login into the Admin Client, they must set their password during the first login. After they set their password, they will be allowed to login. The Users must be assigned User Groups. Each User can be assigned the rights as per the requirements. The access rights are defined as per the User Groups.

The General Settings module enables you to configure System Account, wherein you can create User Groups, Users and ONVIF Users. You can also approve or reject Vision GUID requests from the System Account section.

To configure System Account,

- Click **General Settings**. The **System Account** page appears by default.



The System Account section contains these pages — “User Groups”, “Users”, “ONVIF Users” and “Vision GUID Authorization”.

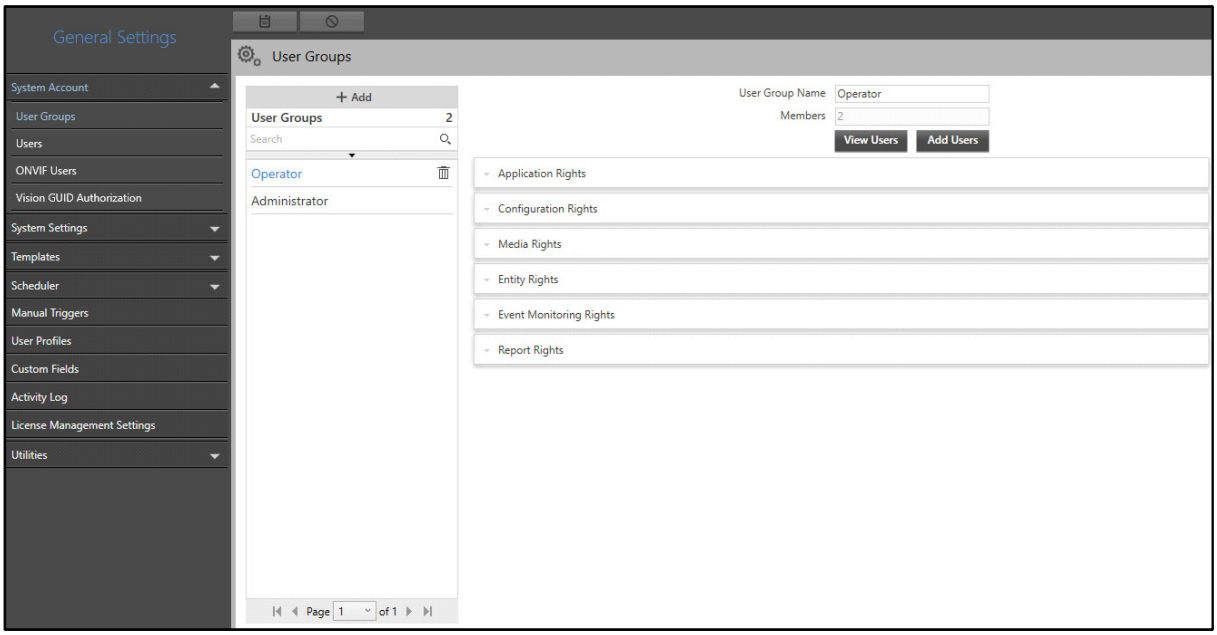
User Groups

The User Groups page displays all the User Groups. You can view and configure User Groups from this page. These groups contain users who can be assigned different rights. For example, you can create a group of users having viewing rights only. Thus, User Groups enables you to assign similar rights to multiple users easily and quickly.

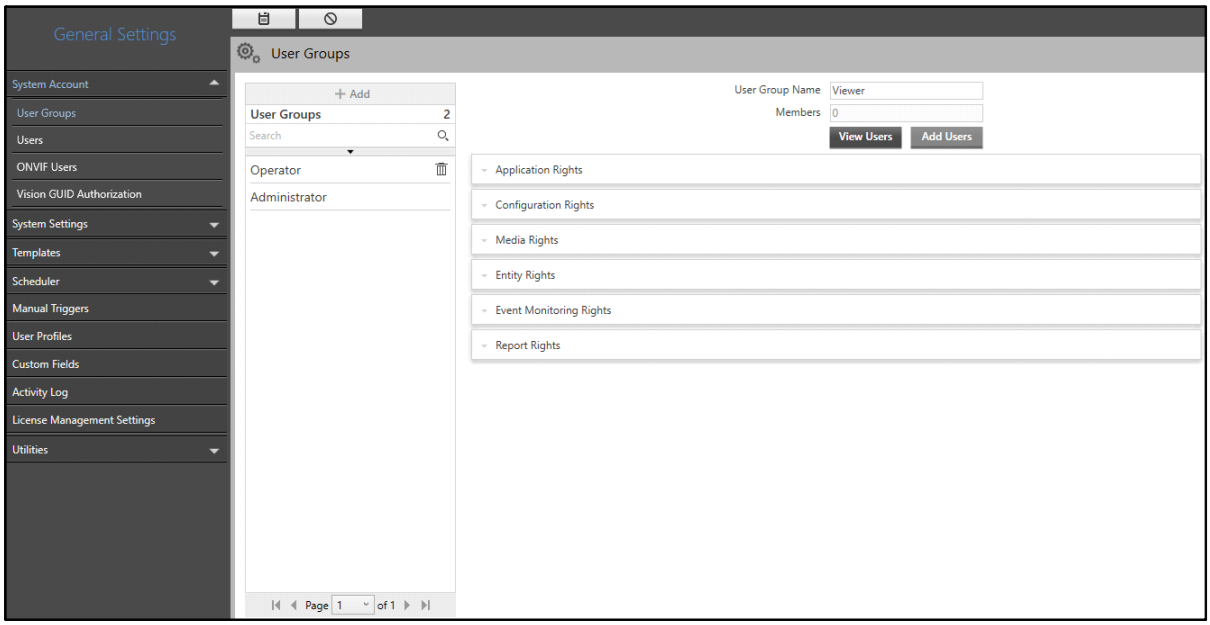
For Smart Client users you can provide Configuration Rights and/or Event Monitoring Rights (only viewing) selectively depending on the access you wish to provide. For example User1 has both Configuration Rights (Media Right > PTZ Controls) as well as Event Monitoring Rights (Scheduled PTZ Tour Started), then from the Smart Client User1 will be able to monitor the Tour at the scheduled time as well as User1 will be able to select the desired PTZ Tour from the Live View > PTZ Controls any point of time. Now, if User1 has only Event Monitoring Rights (Scheduled PTZ Tour Started), then from the Smart Client User1 will only be able to monitor the Tour at the scheduled time.

To configure User Groups,

- Click **General Settings > System Account**. The **User Groups** page appears by default.



- Click **Add**.



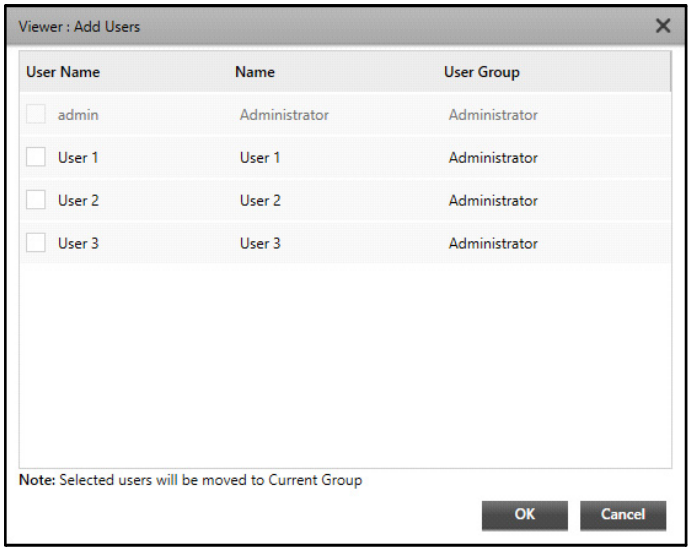
Configure the following parameters:

- **User Group Name:** Specify a suitable name for the User Group. For example, Viewer. In User Group Name, you can enter upto 50 characters. Default: Blank.

- Click **Save** to save the configurations of the new User Group.

Once a User Group is created successfully, you can add users to the group.

- Click **Add User** to add users to the User Group. The **Add Users** pop-up appears.



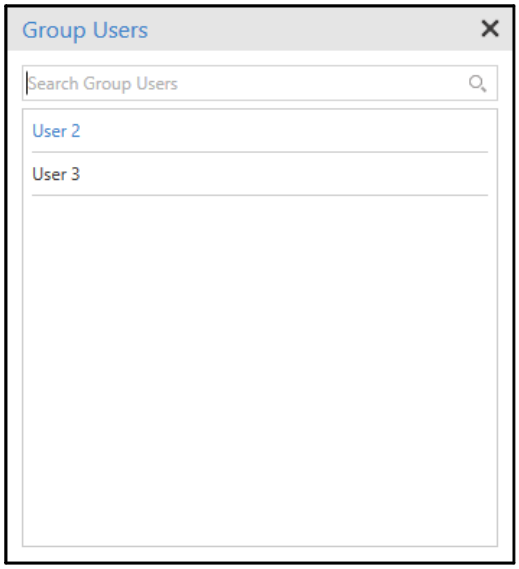
- Select the check boxes for the users you wish to add to the User Group.

- Click **OK** to confirm or click **Cancel** to discard.

- Click **Save** to save the settings or **Cancel** to discard.

Once the Users are added successfully, you can view all users assigned to the selected User Group.

- Click **View Users.** The **Group Users** pop-up appears.



- All the users added to the User Group appear in a list.

After you have assigned the User Groups to the Users, you need to configure the rights for the group. The User Group page contains six collapsible panels for assigning rights — "Application Rights", "Configuration Rights", "Media Rights", "Entity Rights", "Event Monitoring Rights" and "Report Rights".

Make sure each User Group is assigned rights as per requirement. The users' accessibility of various modules, parameters in Smart Client, Servers and Devices, Events and Reports will depend on the rights assigned to their User Group.

*The "BACnet Server" tab is applicable for **Administrator** User Group only.*

Consider the following examples;

Example 1

A **Viewer** User Group has been assigned the following rights:

- **View** rights for **CREAM** module only.

On the Admin Client homepage, only the CREAM module will be displayed. The users can only view the features of the CREAM module. They cannot configure any parameters.

Example 2

An **Operator** User Group has been assigned the following rights:

- **View, Add, Delete, Edit** rights for **Perimeter Management** module.
- **Perimeter Management** Event rights.
- **Entity Rights** for **Camera 1**.

Then the users can configure Intrusion Zone, Security Line, Perimeter Zone, Scenarios and reports using Camera 1 only.

Example 3

A **Maintenance** User Group has been assigned the following rights:

- **View** and **Edit** rights for **System Monitor** module.
- **View, Add, Delete, Edit** rights for **Person Identification** module.
- **Face Detection** Event rights.
- **Entity Rights** for **Camera 2**.

Another User Group, say **Testers** has been assigned the following rights:

- **View, Add, Delete, Edit** rights for **Parking Management** module.
- **Parking Management** Event rights.
- **Entity Rights** for **Camera 1**.

The users of **Testers** group have created a Slot profile and configured Unauthorized Parking event for the same using Camera 1. Similarly, the users of **Maintenance** group have configured Face Detection event for Camera 2. When the users of **Maintenance** group configure Analytics Report, they can only view the Face Detection Event while configuring the Event Group.

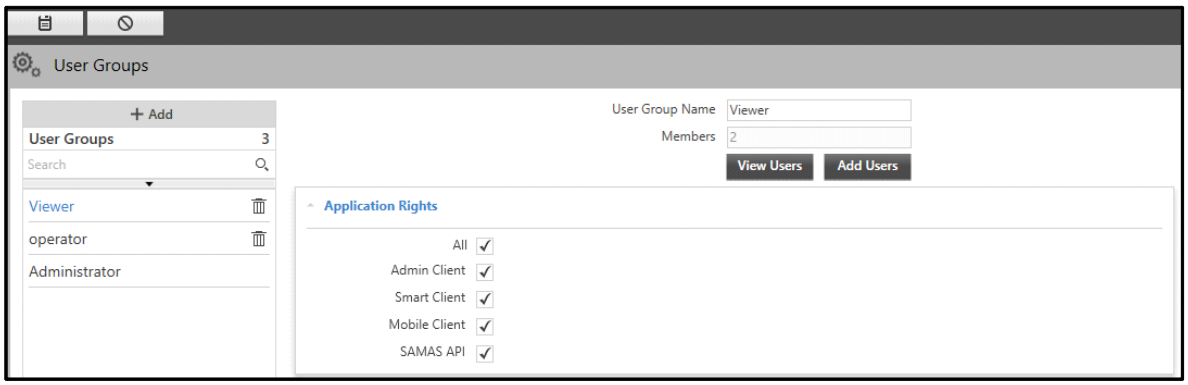
Application Rights

This panel displays the Application Rights for the various SATATYA SAMAS components. This panel allows you to configure the rights to access these Applications.

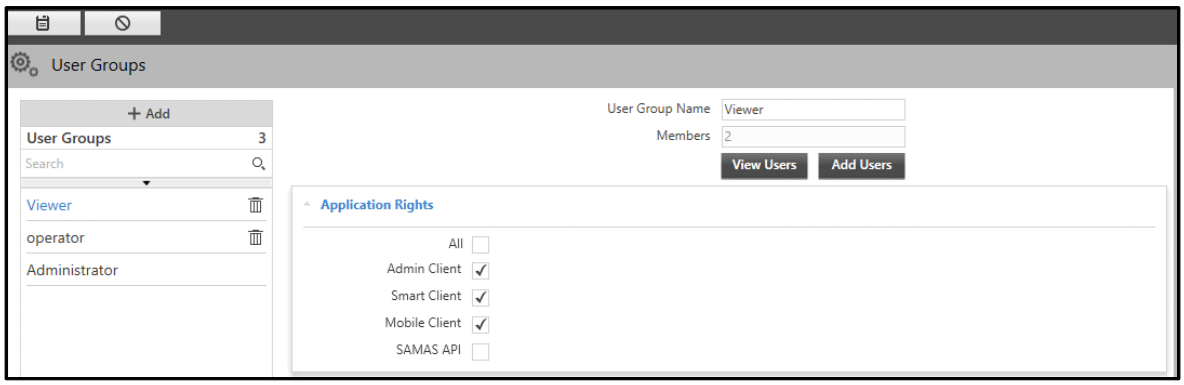
SAMAS API is supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.

To view and edit the Application Rights,

- Click the **Application Rights** collapsible panel.



- By default all the check boxes are selected, that is, all options are enabled. Clear the check boxes for the Applications you wish to disable — Admin Client, Smart Client or Mobile Client. To disable all the applications, clear the **All** check box to disable all the options.



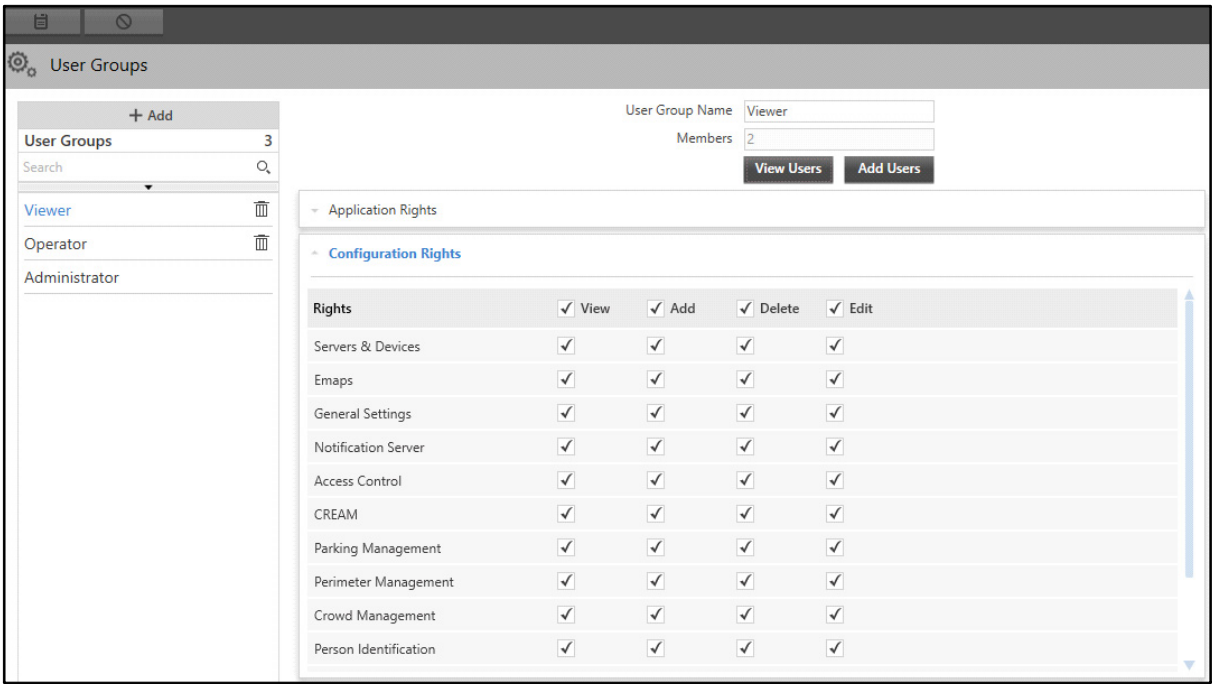
- Click **Save** to save the settings or **Cancel** to discard.

Configuration Rights

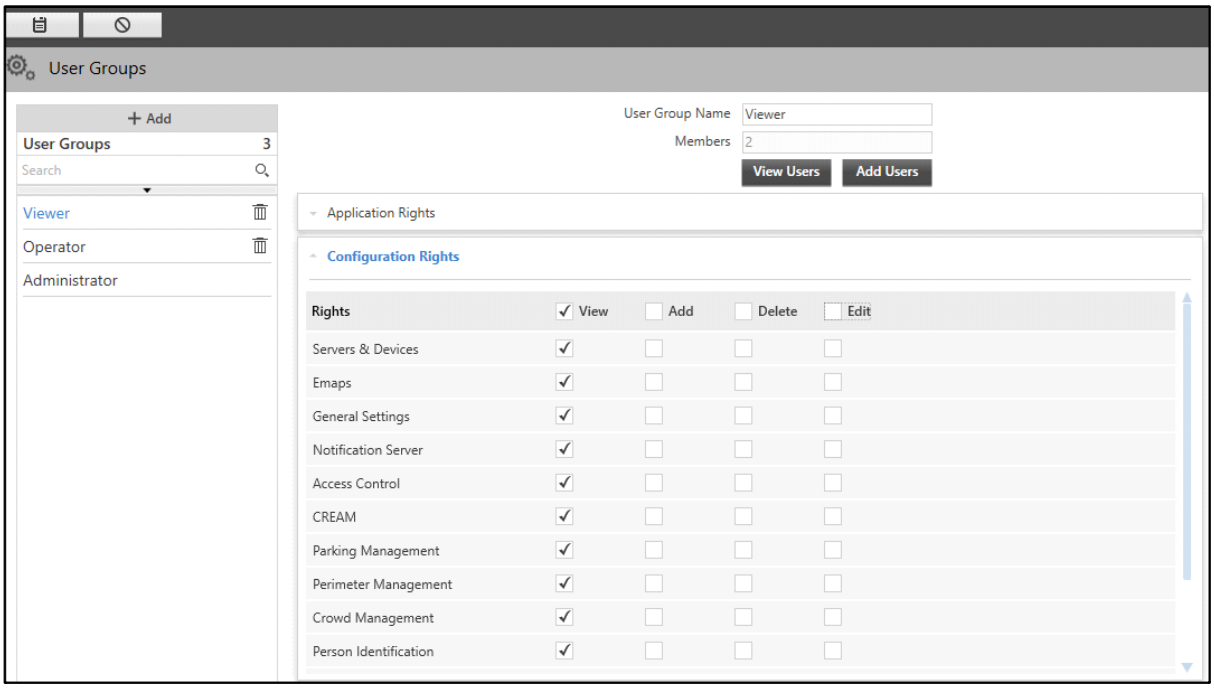
This panel displays the Configuration Rights for the various modules in Admin Client. This panel allows you to configure the rights to view, add, edit or delete for each module.

To view and edit the Configuration Rights,

- Click the **Configuration Rights** collapsible panel.



- The Configuration Rights can be assigned for each module.The Configuration Rights are divided into four types — **View, Add, Edit** and **Delete**. By default, all the check boxes are selected. Clear the desired check boxes for the type of rights against each module you wish to disable.



- Click **Save** to save the settings or **Cancel** to discard.

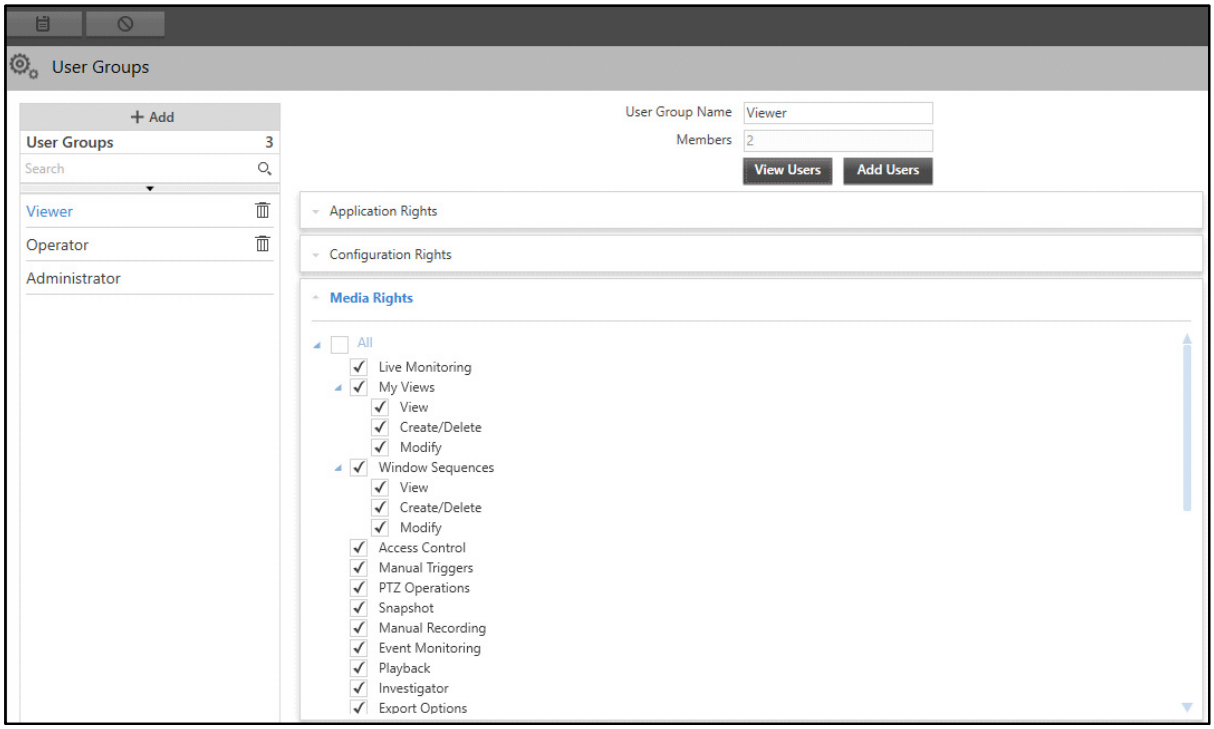
*Admin Client Users who are not assigned **Administrator** as the User Group can download all the reports if they have **View** rights of the respective modules.*

Media Rights

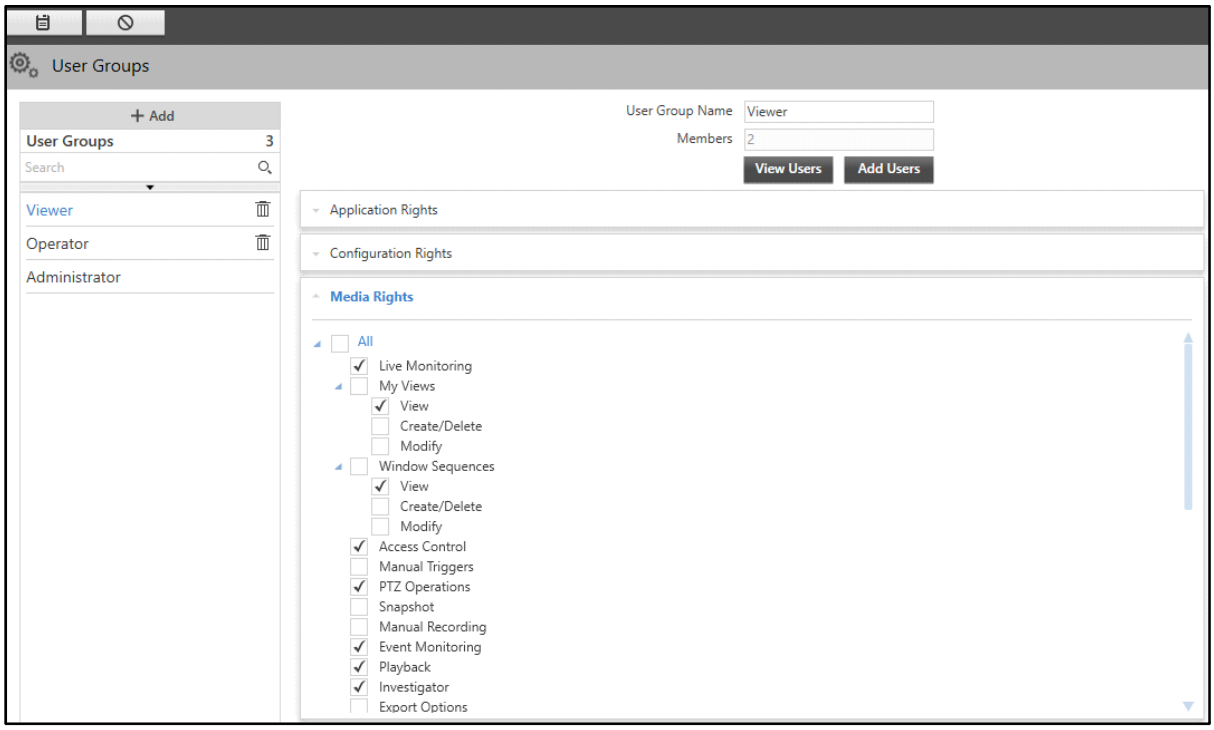
This panel displays the Media Rights for the various parameters in the Smart Client. This panel allows you to configure the rights to view, create, modify and delete various parameters also.

To view and edit the Media Rights,

- Click the **Media Rights** collapsible panel.



- By default, the all the check boxes are selected (except Reset Event Counter and Enroll Vehicle). Clear the check boxes for the parameters you do not wish to assign Media Rights for the User Group. For Reset Event Counter and Enroll Vehicle, select the check box if required.



- Click **Save** to save the settings or **Cancel** to discard.

*The Bookmark Lock parameter can also be enabled from **Servers & Devices > Recording Server > Default Settings**. If the parameter is enabled from Media Rights, it can be disabled from Default Settings, and vice versa.*

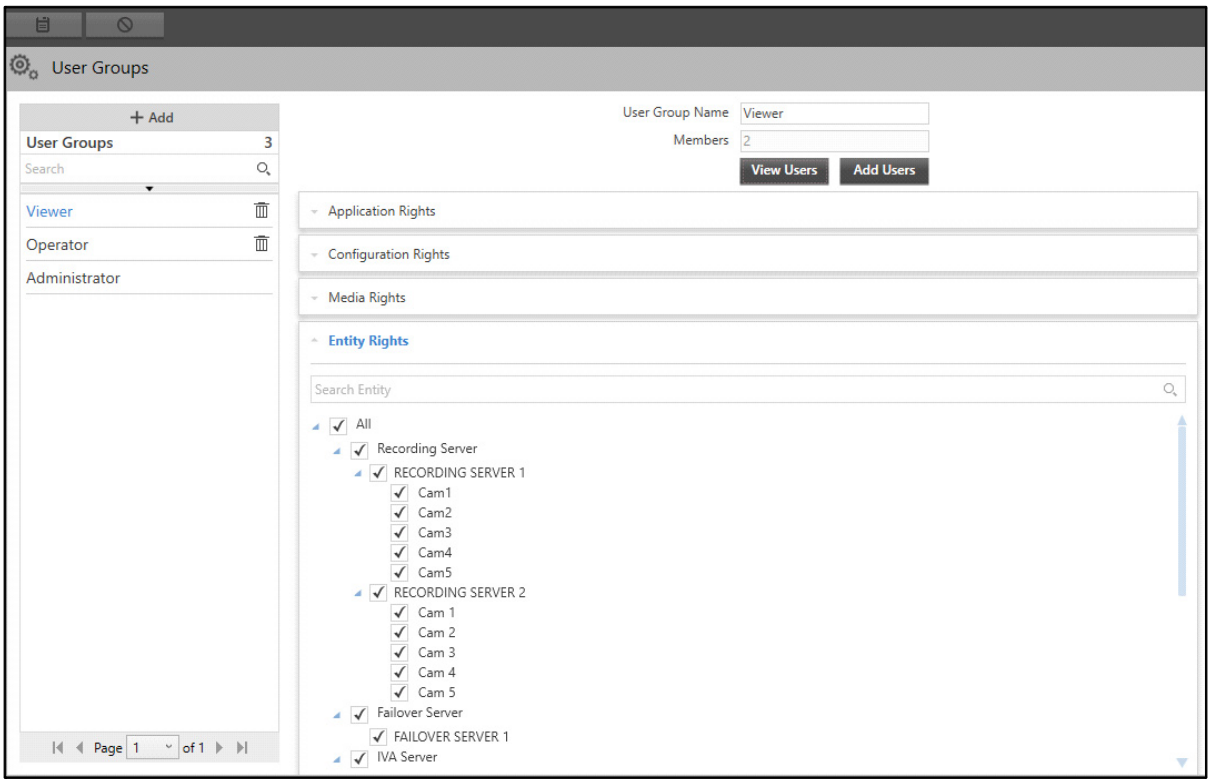
You can enable Push Notification only if Mobile Client rights are enabled from "Application Rights". Make sure you enable Push Notification if you wish to configure and send Push Notifications to the users of the desired User Group.

Entity Rights

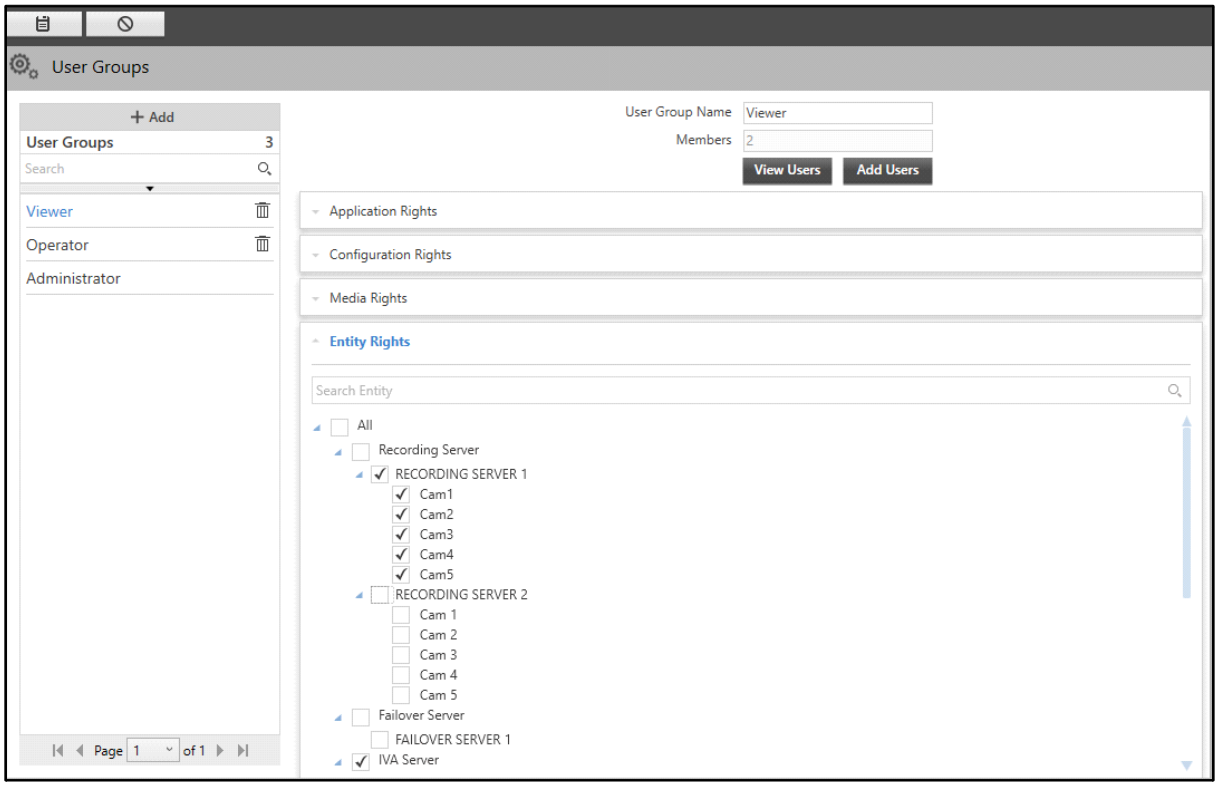
This panel displays the Entity Rights for the various entities in the Smart Client. This panel allows you to configure the rights to access these entities in the Smart Client.

To view and edit the Entity Rights,

- Click the **Entity Rights** collapsible panel.



- By default, the check boxes of all the entities are selected. Clear the check boxes for the entities for which you do not wish to allow access in the Smart Client.



- Click **Save** to save the settings or **Cancel** to discard.

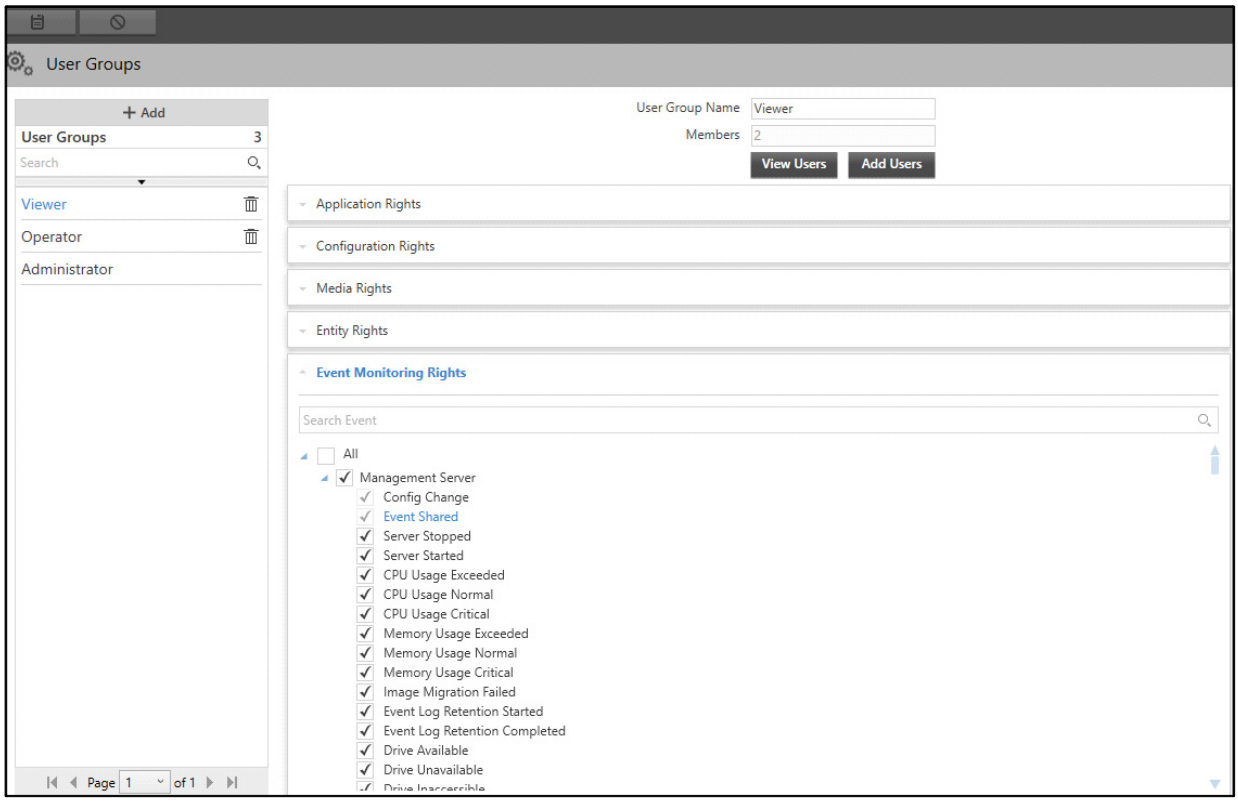
If any changes are made in System Account settings or Access Control settings for currently logged-in user, these changes will be applicable only on the next login.

Event Monitoring Rights

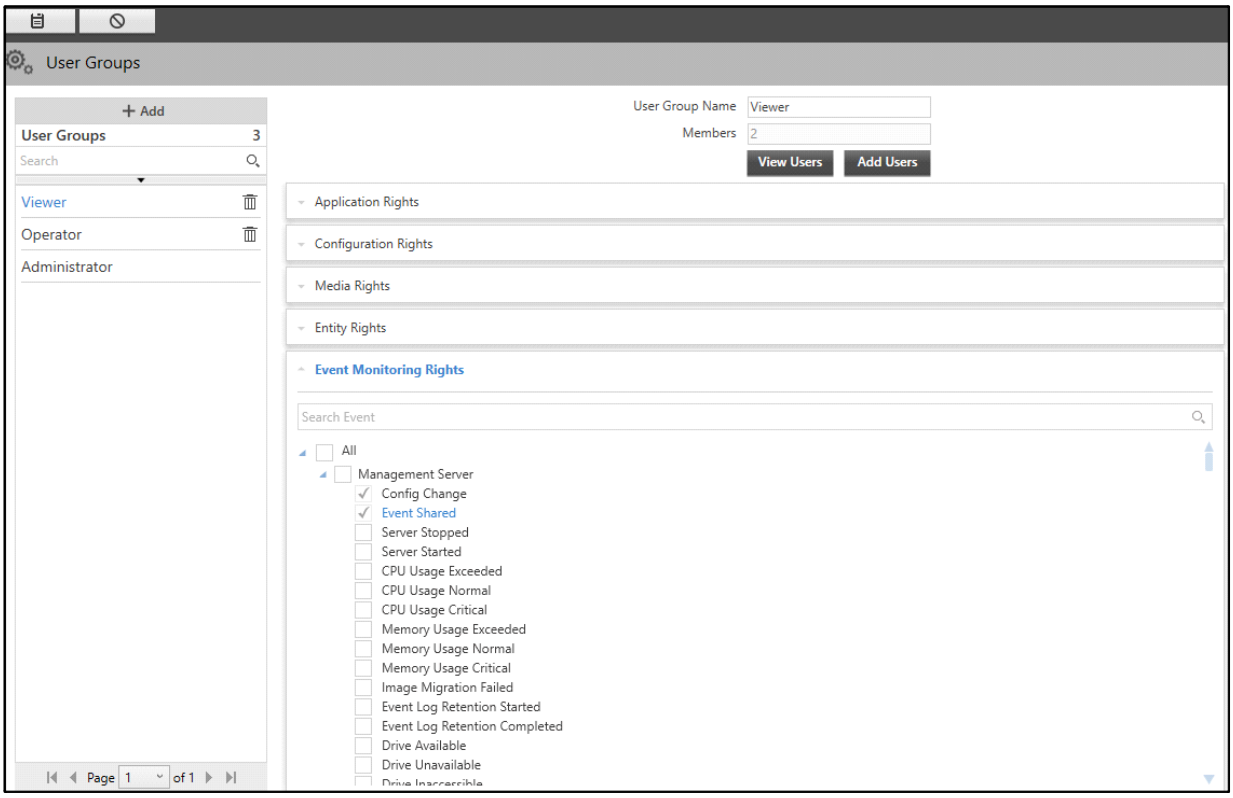
This panel displays the Event Monitoring Rights for the various Event Source Types in the Smart Client. This panel allows you to configure the rights to view these Events in the Smart Client. All the Events for which rights are granted here appear in the list of Events under Event Alerts tab in General Settings of Smart Client. Also, the Event Logs will appear only those events for which rights have been assigned.

To view and edit the Event Monitoring Rights,

- Click the **Event Monitoring Rights** collapsible panel.



- By default, the check boxes of all the Events are selected. Clear the check boxes for the Events for which you do not wish to allow view rights in the Smart Client.



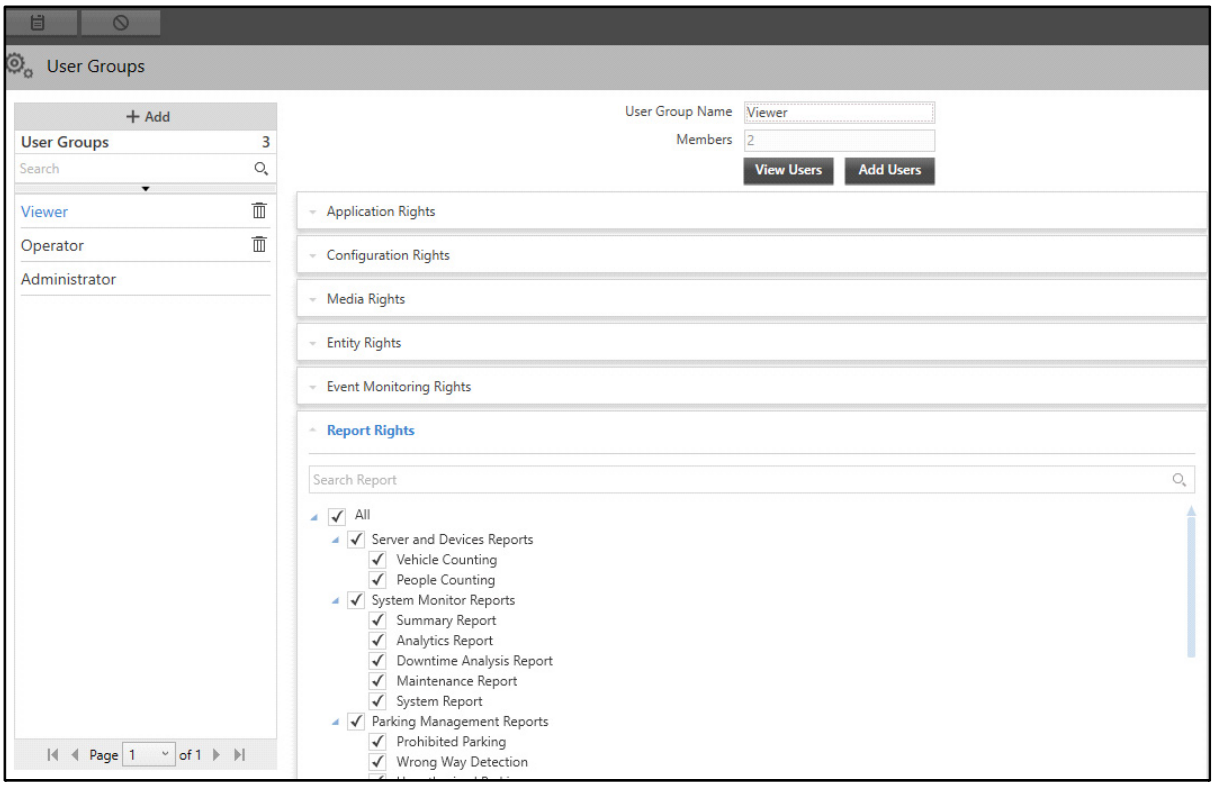
- Click **Save** to save the settings or **Cancel** to discard.

Report Rights

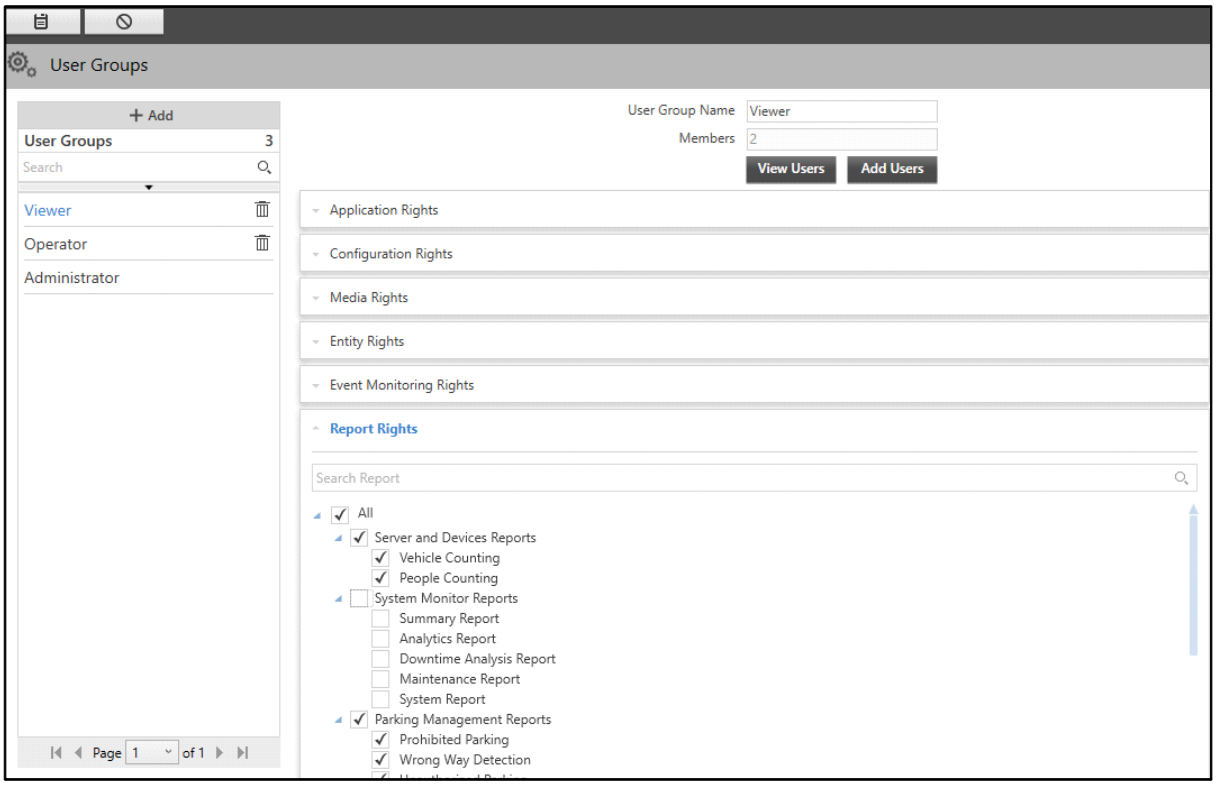
This panel displays the Report Rights for the various reports of all the modules. This panel allows you to configure the rights to access these reports.

To view and edit the Report Rights,

- Click the **Report Rights** collapsible panel.

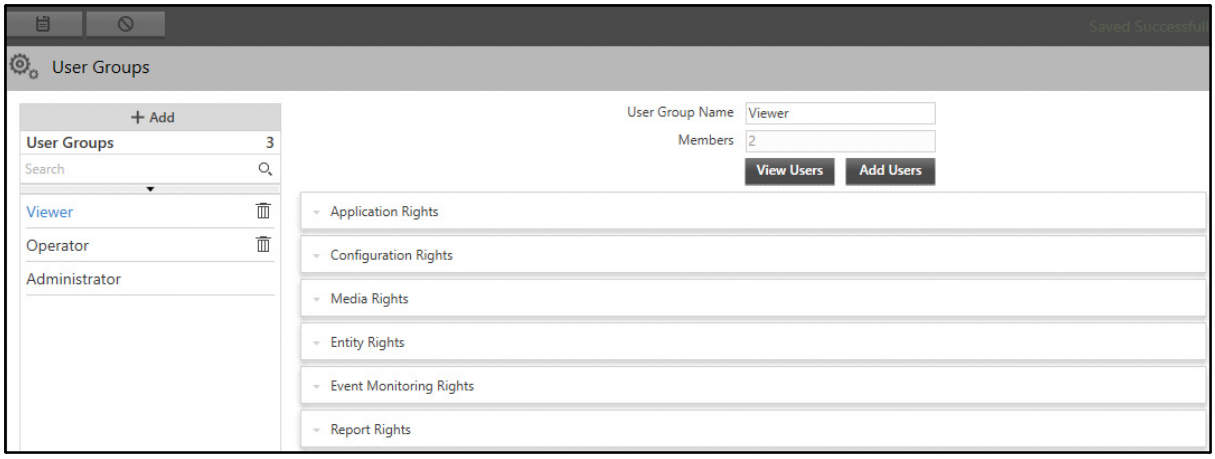


- By default all the check boxes are selected, that is, all options are enabled. Clear the check boxes for the reports you wish to disable. To disable the access of all the reports, clear the **All** check box.

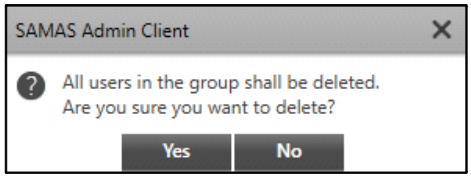


- Click **Save** to save the settings or **Cancel** to discard.

The new User Group will appear in the list on the left hand side. You can view or edit the User Group rights or delete the Groups, if required.

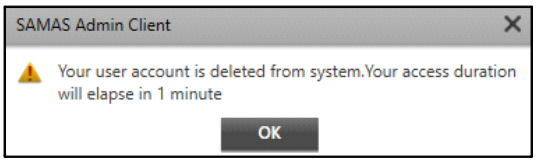


- Select the desired User Group from the list and edit the configurations on the right hand side.
- Click **Delete** corresponding to any User Group to delete it. The following pop-up appears.



- Click **Yes** to delete the User Group or click **No** to discard.

The selected User Group will be removed from the list along with the users in that group. All active user sessions will be terminated once the user is notified. The following pop-up appears on the screen of the users (members) of the deleted User Group.



- Click **OK**.

The user account will be deleted along with the User Group after 1 minute has elapsed. Once deleted, a user will also be removed from the configured actions such as **Send SMS**, **Send Email**, **Trigger Alarm**, etc.

*The users can be created from **System Account > Users**. While creating the Users a single User Group has to be assigned to all users. For details refer to* "Users".

If you wish to assign multiple groups to a single user, click User Groups > Add User option in each group. Then select the check boxes of the desired users.

Application Scenario for User Accessibility

Let us understand the importance and utility of assigning the User Groups and Rights to individual users.

The rights control how and to what extent users of the same group can access, use and modify the features and functionality of SATATYA SAMAS.

Let us understand this with the help of an example as depicted in the figure.

This is a typical multi-site SATATYA SAMAS setup in terms of multiple user roles and user rights distribution.





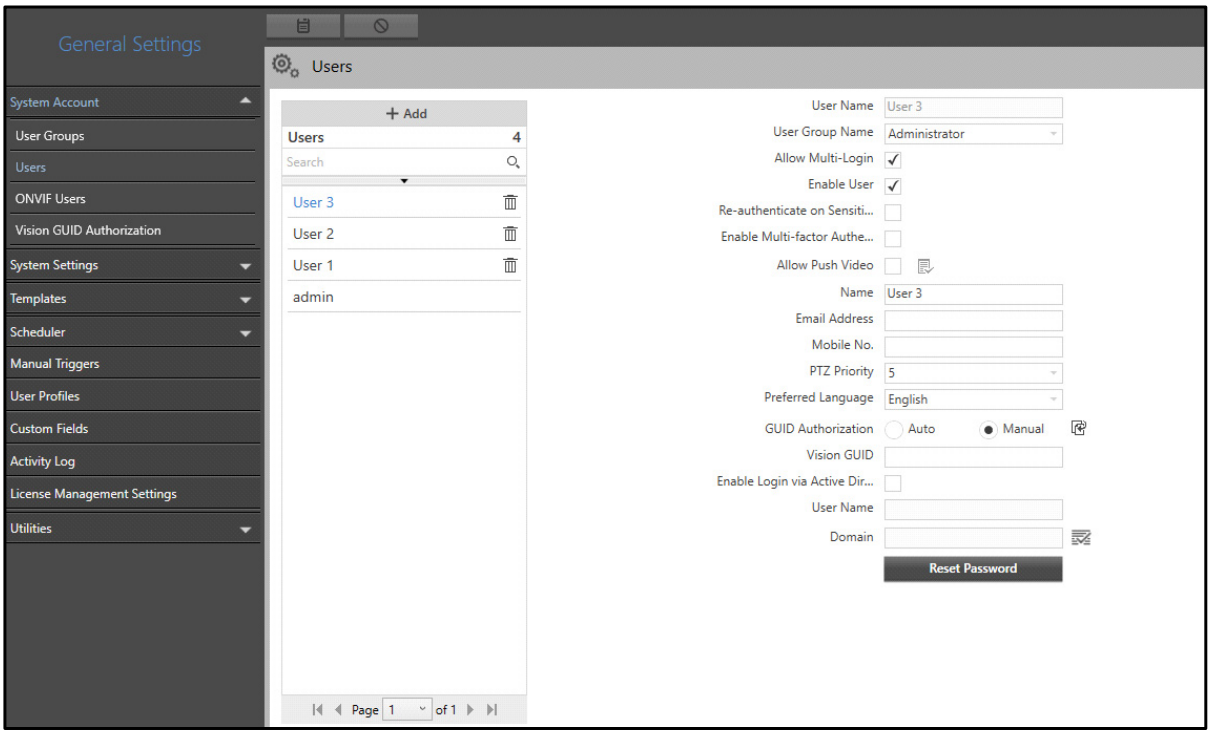
User Rights available for configuration will depend on the product license purchased.

Users

The Users page displays all the Users. You can view, add, edit or delete Users from this page. These Users can be assigned to different User Groups with similar/different user rights. For details, refer to “User Groups”.

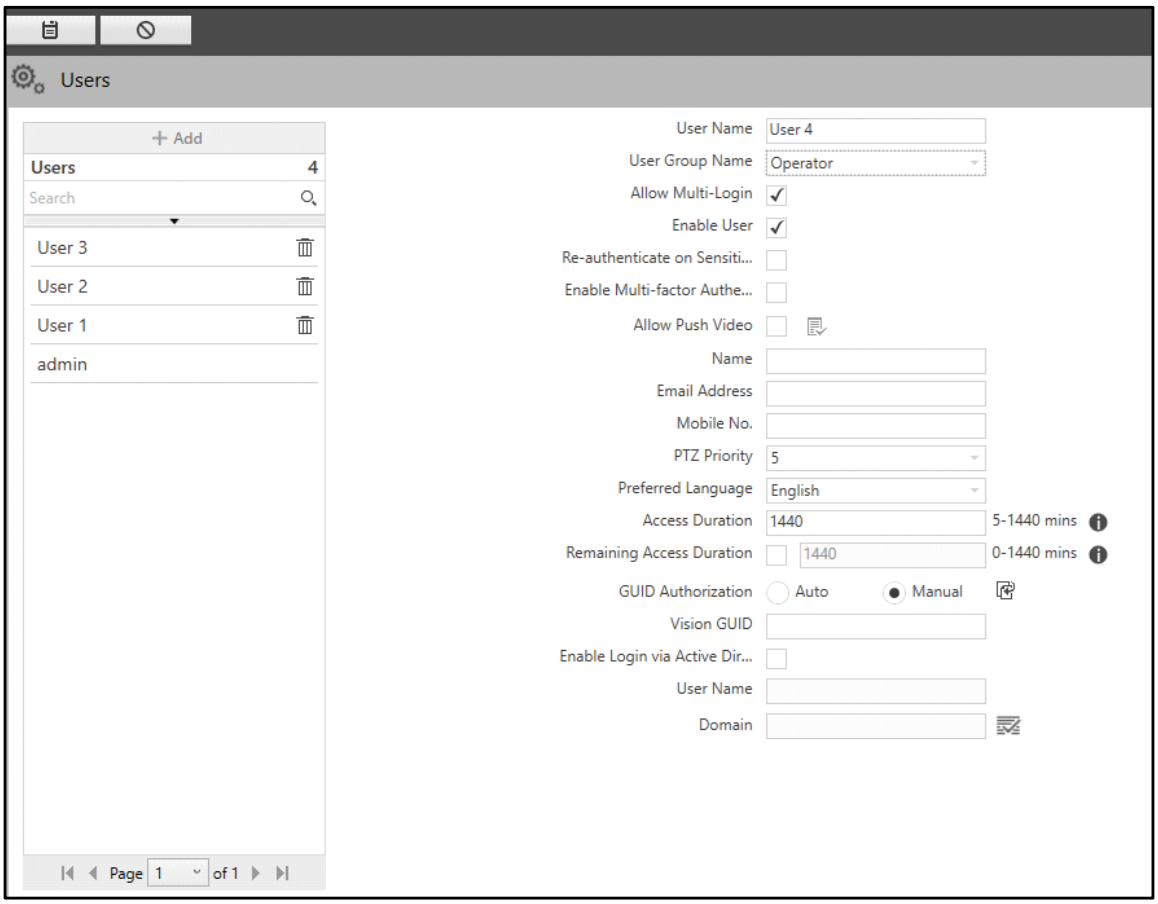
To configure Users,

- Click **General Settings > System Account > Users**.



The default user, **admin** is displayed. You can only edit this user but cannot delete it. To add a new User,

- Click **Add**.



Configure the following parameters:

Users must set their login Password at the time of first login. For details, refer to "Getting Started".

The system administrator must inform the Users about the Password policy details in-advance.To know more about the Password policy, refer to "Password Settings".

- **User Name**: Specify a suitable name for the new user. Once configured this cannot be modified. In User Name, you can enter upto 50 characters. Default: Blank.

- **User Group Name**: Select a User Group Name from the drop-down list to be assigned to the user. When the user is assigned to a User Group, the rights assigned to the User Group get automatically assigned to the user as well.

  For example, if the user is to be given system administrator's rights, select **Administrator** from the User Group Name drop-down list.

- **Allow Multi-Login:** Select the check box to enable simultaneous multiple login for users into the Admin Client as well as Smart Client. If this check box is cleared, the user can login into either Admin Client or Smart Client at a time.

- **Enable User:** Select the check box to enable the user. The check box is selected by default. Clear the check box to disable.

- **Re-authenticate on Sensitive Transaction**: Select the check box to enable re-authentication on certain sensitive actions by the user. The user will have to enter the login password to confirm the

transactions in the Smart Client wherever authentication is required. For more details, refer to **SATATYA SAMAS Smart Client Manual**.

- **Enable Multi-factor Authentication**: Select the check box to enable Two Step Verification for the user. The user will be asked to enter the OTP received on the configured Email Address/Mobile Number to login in the Admin Client, Smart Client and Mobile Client.

  Prior to Two Step Verification, the system will verify Username, Password and Captcha code. Click Login. Enter the Two Step Verification code received on Mobile/Email Address.

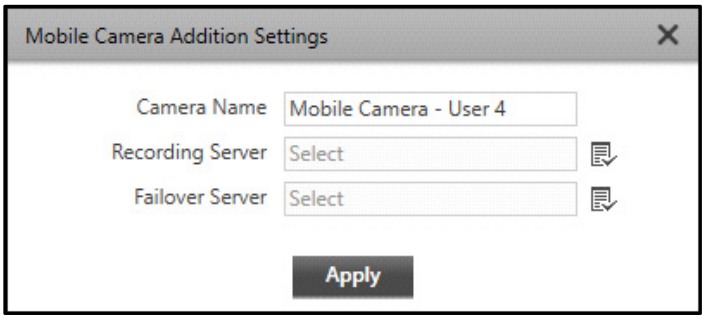
Enable Multi-factor Authentication is not applicable for the default Admin User (admin).

Make sure the Email Address/Mobile No. are configured for Two Step Verification.

Make sure the Notification Server is running and the configurations for Email/SMS are done as per your requirement.

The Maximum Failed OTP Allowed, Maximum OTP Regeneration Allowed and Lock Account will be as per the OTP Policy for Multi-factor Authentication. For details, refer to "OTP Policy".

- **Allow Push Video**: Select the check box to enable the Push Video rights for the user. To know more about this feature, refer to "Push Video/Snapshot".
  - Click **Mobile Camera Setting** picklist. The **Mobile Camera Addition Settings** pop-up appears.



  - **Camera Name**: Specify a name for the camera. In Camera Name, you can enter upto 50 characters. Default: Mobile Camera - User Name.
  - **Recording Server**: Select the desired Recording Server to which you wish to push the data using the **Recording Server** picklist. Only those Recording Servers will appear in the list whose rights are assigned to the user. The data will be stored in the selected Recording Server's Storage Drive.
  - **Failover Server**: Select the desired Failover Server to which you wish to push the data using the **Recording Server** picklist. Only those Failover Servers will appear in the list whose rights are assigned to the user. The selected Failover Server will act as a backup for the Mobile Camera.
- Click **Apply**. The Mobile Camera will appear on the "Devices" page of the selected Recording Server.
- **Name**: Specify the name of the user. In Name, you can enter upto 50 characters. Default: Blank.

- **Email Address**: Specify the email address of the user. In Email Address, you can enter upto 100 characters. Default: Blank.

- **Mobile No.**: Specify the mobile number of the user. In Mobile No., you can enter upto 15 characters. Default: Blank.

The Email Address and Mobile No. entered here will be used to retrieve the user's account in case the user forgets the password.

Make sure WhatsApp is activated on the Mobile Number configured here to receive WhatsApp Messages.

Make sure the Email Address and Mobile Number configured here are configured correctly in — Send Email/Send SMS/Send WhatsApp Message actions to receive the — Email, SMS and WhatsApp alerts.

- **PTZ Priority**: Select the desired PTZ Priority number that you wish to assign to the user from the drop-down list.

  As per the set priority, a higher priority user will be able to overrule the PTZ operations of lower priority users. The lower priority user's operations will be locked for the duration as configured in PTZ Priority Delay Time.

  For example, PTZ operations by a user with PTZ Priority 5 will overrule the PTZ operations of a user with priority 4 and the operations of this user will be locked for the duration as configured in the PTZ Priority Delay Timer. For details, refer to "PTZ Priority Delay Time".

PTZ Priority is not applicable for Mobile Client Users.

We can configure Scenarios from each module, wherein we can select Set PTZ Position as Action. At such places the PTZ Priority assigned to the user will not be applicable. For details refer to "Basic Scenario" and "Advanced Scenario".

We can set Preset Position for the desired cameras from various Profiles (except Terminal in Weighbridge) in each module, in such cases PTZ Priority assigned to the user will be applicable.

To ensure smooth functioning of this feature, make sure the time zones of the Admin Client and RS/FoS are same.

On system upgrade, by default all the users will be assigned with PTZ Priority 5 and the default admin user will be assigned with PTZ Priority 1.

- **Preferred Language:** Select the language in which you wish to access the Admin Client/Smart Client/ Mobile Client from the drop-down list. The selected language will reflect in Smart and Mobile Client as well. All the imported languages that are saved in the system's database appear in the list. To know more about exporting and importing language files, refer to "Language Settings".

- **Access Duration**: Specify the duration till when the user is allowed to access the Smart Client. When a user's group assigned is other than **Administrator**, the user's access to the Smart Client can be restricted to a fixed time duration in a day. This parameter is applicable to Smart Client and Mobile users only. Valid Range: 5-1440 minutes. Default: 1440.

  If the same user has logged in with multiple clients (Smart Client as well as Mobile Client), the provided time duration will be divided amongst the number of logins.

  If the access time duration of a user expires for the day, it will be reset on the next day (at 12.00AM IST).

If Access Duration is changed, the updated access duration will come into effect only on the next day.

For example, for user A, you have assigned 60 minutes as the access duration. If that user is logged into two different Smart Clients (using the same login credentials) at the same time, then 30 minutes of access time will be assigned to each client login.

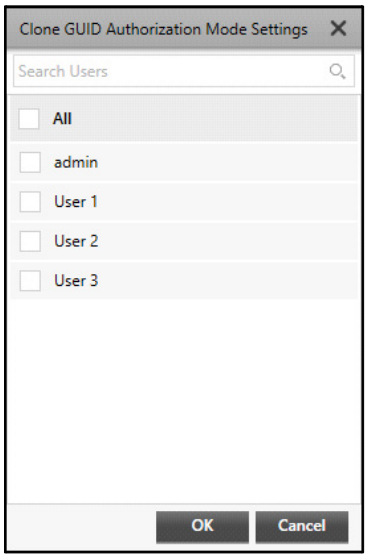
- **Remaining Access Duration:** Select the check box if you wish to change the Remaining Access Duration for this user. This is applicable for the current day only. Hence, you can increase/decrease the login time for a particular user by configuring this parameter.Valid Range: 5-1440 minutes. Default: 1440.

- **GUID Authorization:** The Live View and Playback can be accessed from the Mobile Client (SATATYA VISION). To ensure that the user can install and use SATATYA VISION only from a single authenticated device, the user needs to apply for a GUID Number Authorization request. You can either approve or reject the same. You can select the **GUID Authorization** mode as **Auto** or **Manual**.

  If you select **Auto**, the user request will be approved automatically.

  If you select **Manual**, you need to approve/reject the same. For details, refer to "Vision GUID Authorization".

- If you wish to apply the same configured value of GUID Authorization to other users, click **Clone** . The **Clone GUID Authorization Mode Settings** pop-up appears.



  - Select the check boxes for the desired users for whom you wish to clone the settings.

  - Click **OK** to confirm or click **Cancel** to discard**.**

- **Vision GUID:** This displays the GUID of the authorized device.

  If you have selected **Auto** as the GUID Authorization mode, the GUID of the authorized device will be displayed.

If you have selected **Manual** as the GUID Authorization mode, you need to specify the GUID number. The request will be approved automatically when received. In Vision GUID, you can enter upto 36 characters. Default: Blank.

- **Enable Login via Active Directory**: Select the check box to allow the user to login via Active Directory.



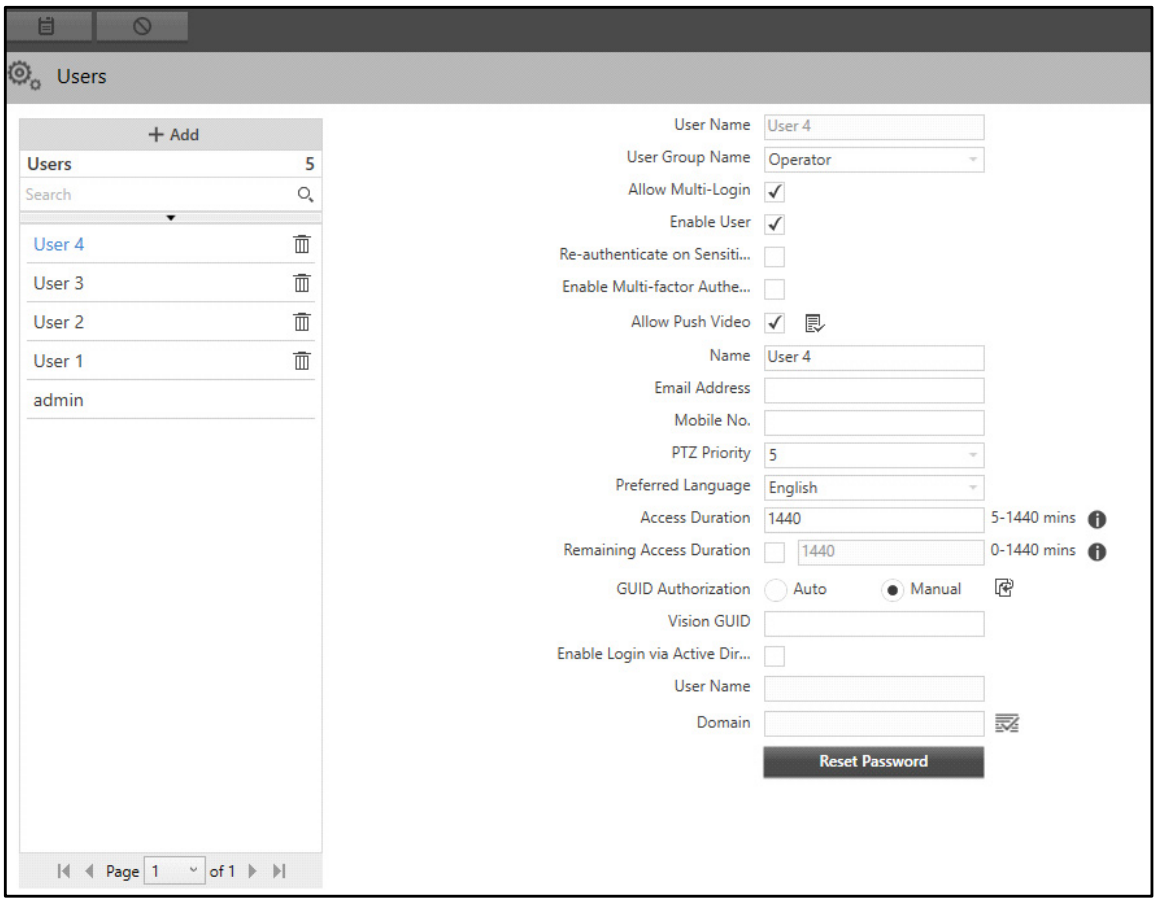
  - **User Name**: Specify the user name for the active directory. In User Name, you can enter upto 100 characters. Default: Blank.
  - **Domain**: Specify the domain name for which the active directory is to be used. Click **Use Default Domain** to use the default domain configured in **General Settings > System.** In Domain, you can enter upto 100 characters. Default: Blank.

    For Active Directory details, refer to "Active Directory Configuration".

- Click **Save** to save the settings or **Cancel** to discard.

The language set here will be changed permanently in the Admin Client as well as in the Smart Client application for that particular user. The language can be changed from the Settings on the Title Bar. For more details, refer to "Title Bar". In Smart Client, the language will be changed by clicking ***Sync Configuration*** *on the Title Bar.*

The new user will appear in the list on the left hand side.

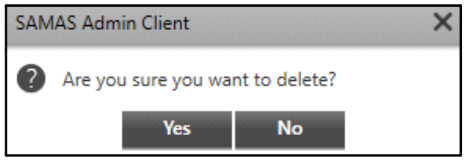


- Select the desired User from the list and edit the configurations on the right hand side.

Whenever any details on the Users page are edited, a notification via SMS and/or Email will be sent to the users Email ID and/or Mobile with the details of the changes. Make sure Email Address and/or Mobile Number are configured for the users.

In case the Email ID and /or Mobile are updated, the User will be notified on the old as well as new Email Address and Mobile Number.

- Click **Reset Password** to reset the password for the user. This may be required when the user forgets his/her password or when the account is locked. Following Password Reset, the user will be prompted to set a new password at the time of next login.
- Click **Delete** corresponding to the desired User you wish to delete. The following pop-up appears.



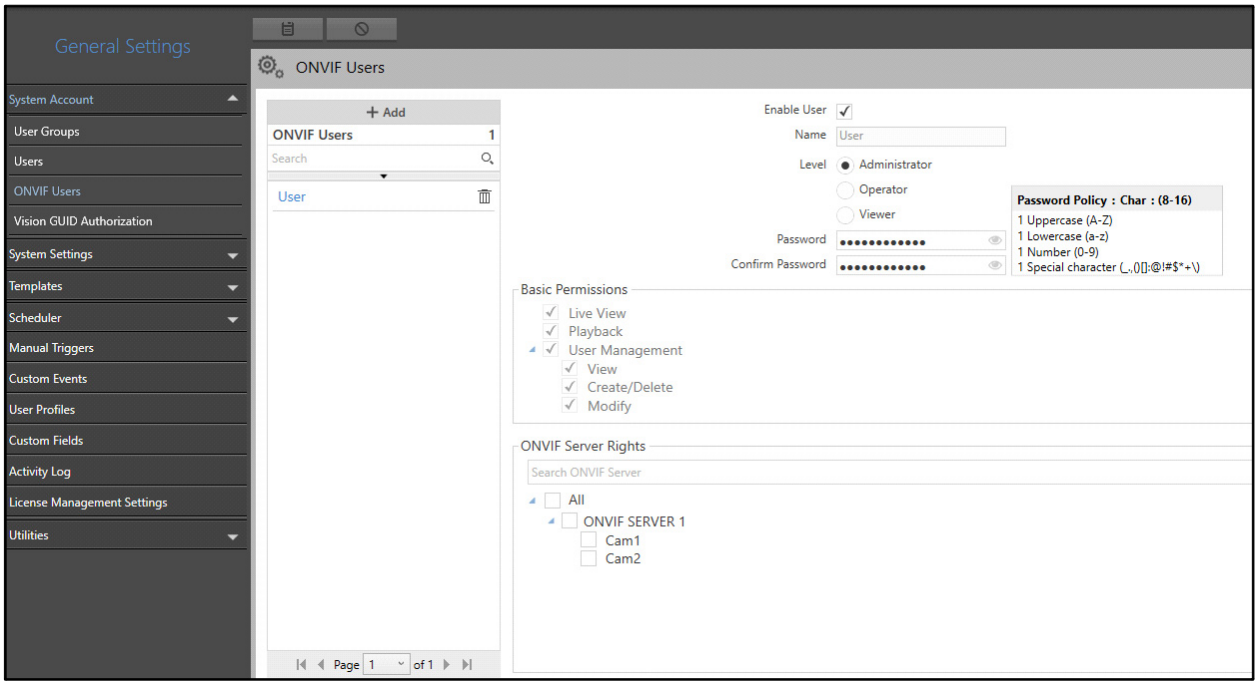
- Click **Yes** to delete the User or click **No** to cancel.

ONVIF Users

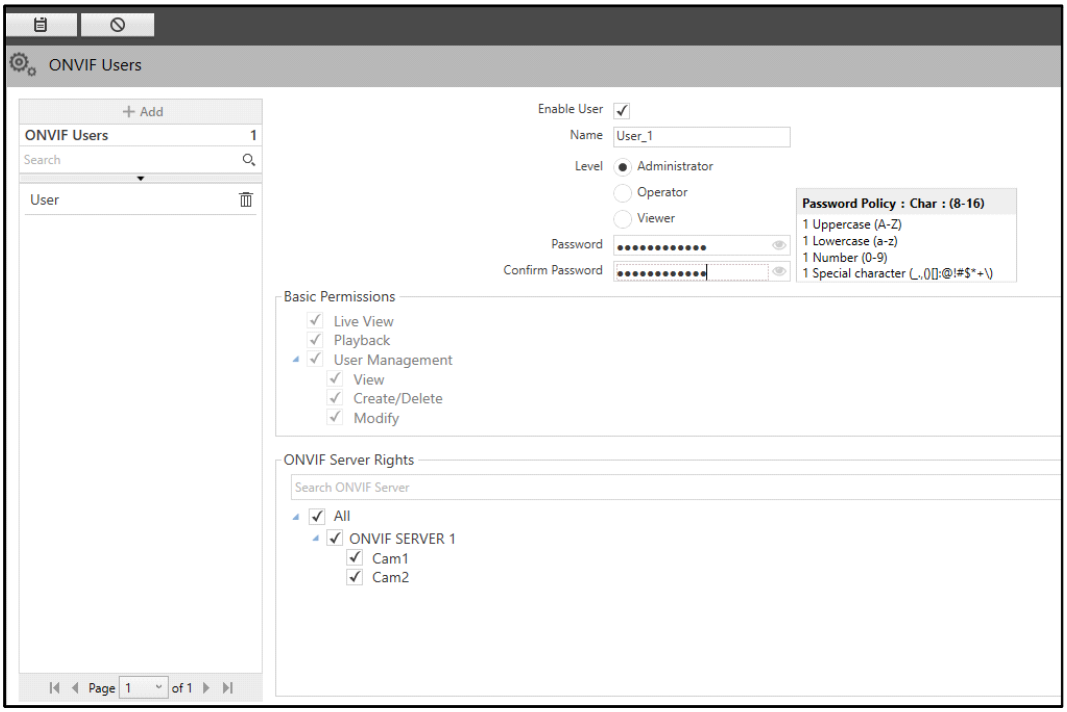
The ONVIF Users page displays all the ONVIF Users. You can view, add, edit or delete ONVIF Users from this page. ONVIF Users can be created either from Admin Client or third party clients. You can add a maximum of 99 ONVIF Users.

To configure ONVIF Users,

- Click **General Settings > System Account > ONVIF Users**



- Click **Add**.



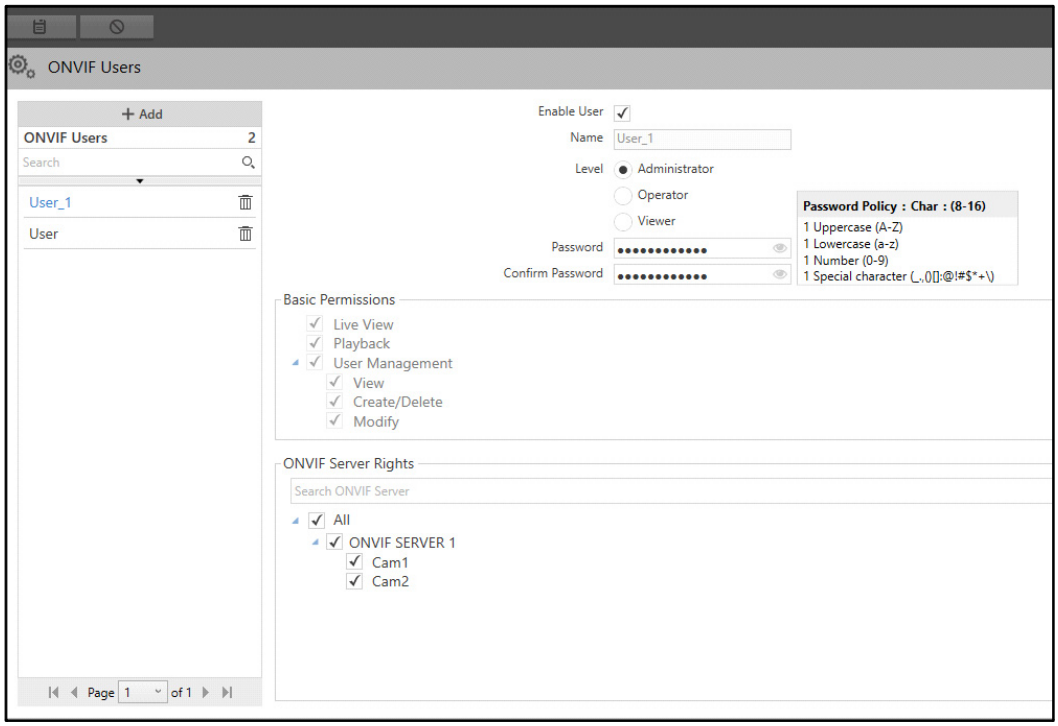
Configure the following parameters:

- **Enable User**: The check box is selected by default. Clear the check box to disable.
- **Name:** Specify the name for the user. In Name, you can enter upto 100 characters. Default: Blank.
- **Level:** Select the level you wish to assign to the user from the options — System Administrator, Operator or Viewer. The **Basic Permissions** assigned to the user differ according to the selected level.
- **Password:** Specify the password as per the displayed Password Policy. Click **Show** to view the password. The icon toggles to **Hide**. Click **Hide** to hide the password. In Password, you can enter upto 16 characters. Valid Range: 8-16. Default: Blank.
- **Confirm Password:** Re-enter the password to confirm. In Confirm Password, you can enter upto 16 characters. Valid Range: 8-16. Default: Blank.

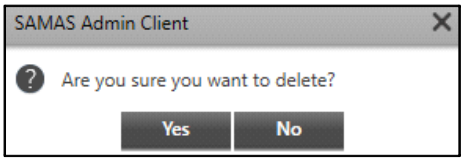
  The Name and Password are required when the users wish to access the ONVIF Server from any ONVIF Client.
- **Basic Permissions:** These permissions differ according to the selected **Level** automatically.
- **ONVIF Server Rights:** Select the check boxes for the ONVIF Servers and their devices for which you wish to give access to the user.

- Click **Save** to save the settings or **Cancel** to discard.

The new ONVIF User will appear in the list on the left hand side.



- Select the desired ONVIF User from the list and edit the configurations on the right hand side.
- Click **Delete** corresponding to the desired ONVIF User to delete. The following pop-up appears.



- Click **Yes** to delete the User or click **No** to cancel.
- You can also view all the ONVIF Users at a glance. For details, refer to “Online ONVIF Users”.

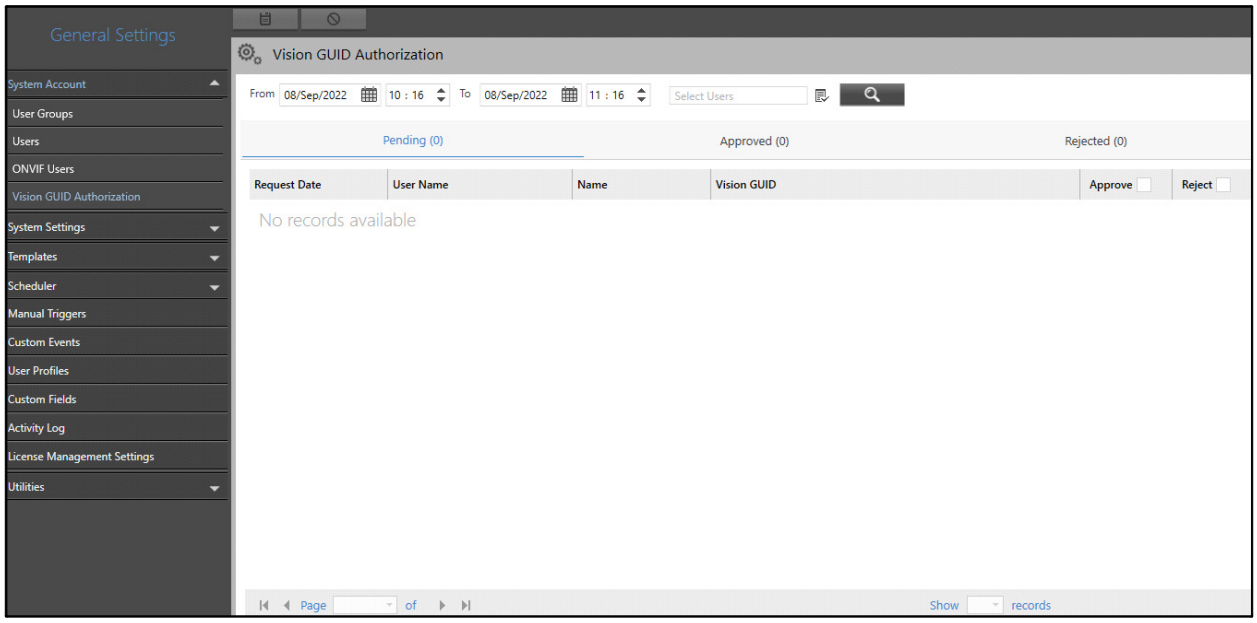
Vision GUID Authorization

The Vision GUID Authorization page displays all the GUID authorization requests received from the Mobile Clients (SATATYA VISION). You can view, approve or reject the authorization requests from this page. For details on GUID authorization, refer to "Users".

If you wish to enable Mobile Client functionality, make sure you approve the Vision GUID requests of the desired Mobile Client users. This will ensure functionality of features such as "Push Notification", "Push Video/Snapshot", etc.

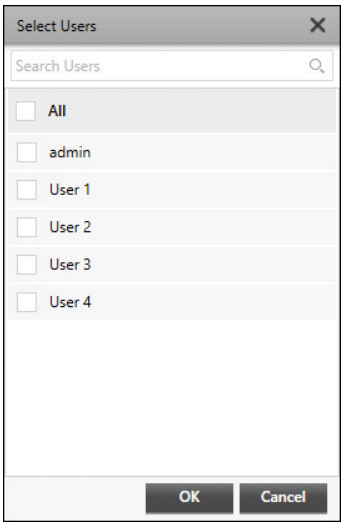
To configure Vision GUID Authorization,

- Click **General Settings > System Account > Vision GUID Authorization**



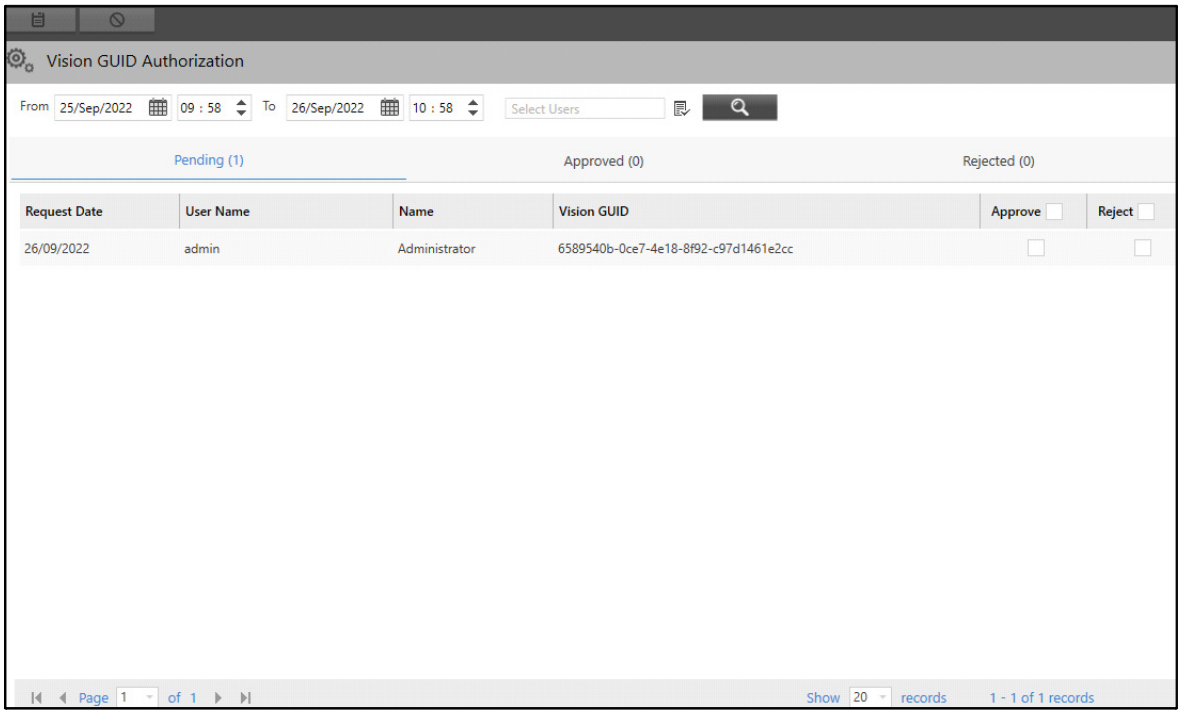
Configure the following parameters:

- **From**: Select the date from which you wish to view the GUID Authorization requests from the calendar and specify the time.
- **To**: Select the date till which you wish to view the GUID Authorization requests from the calendar and specify the time.
- **Users**: Select the users whose GUID Authorization requests you wish to view. To do so,
  - Click the **Select Users** picklist. The **Select Users** pop-up appears.



- Select the check boxes for the desired users. Click **OK**.

- Click **Search** . All the GUID Authorization requests for the selected duration and users appears.



The Vision GUID Authorization page contains three tabs — Pending, Approved and Rejected.

- If you have selected the GUID Authorization mode as **Auto** while creating the users, the requests are approved automatically and will appear in the **Approved** tab. The details displayed are — Request Date, User Name, Name, Vision GUID and Approval Date.

- If you have selected the GUID Authorization mode as **Manual** while creating the users, the requests will appear in the **Pending** tab. You can either approve or reject the request. Select the respective check box to approve or reject the request. The details displayed are — Request Date, User Name, Name, Vision GUID and Approve/Reject check box.

- If you reject the requests, these records are displayed in the **Rejected** tab. The details displayed are — Request Date, User Name, Name, Vision GUID and Rejection Date.

You can also sort the records according to — Request Date, User Name, Name, Vision GUID and Approval Date/ Rejection Date.

- Click on the desired parameter name. The records can be sorted in ascending as well as descending order.

You can also determine the number of records to be displayed on each page.

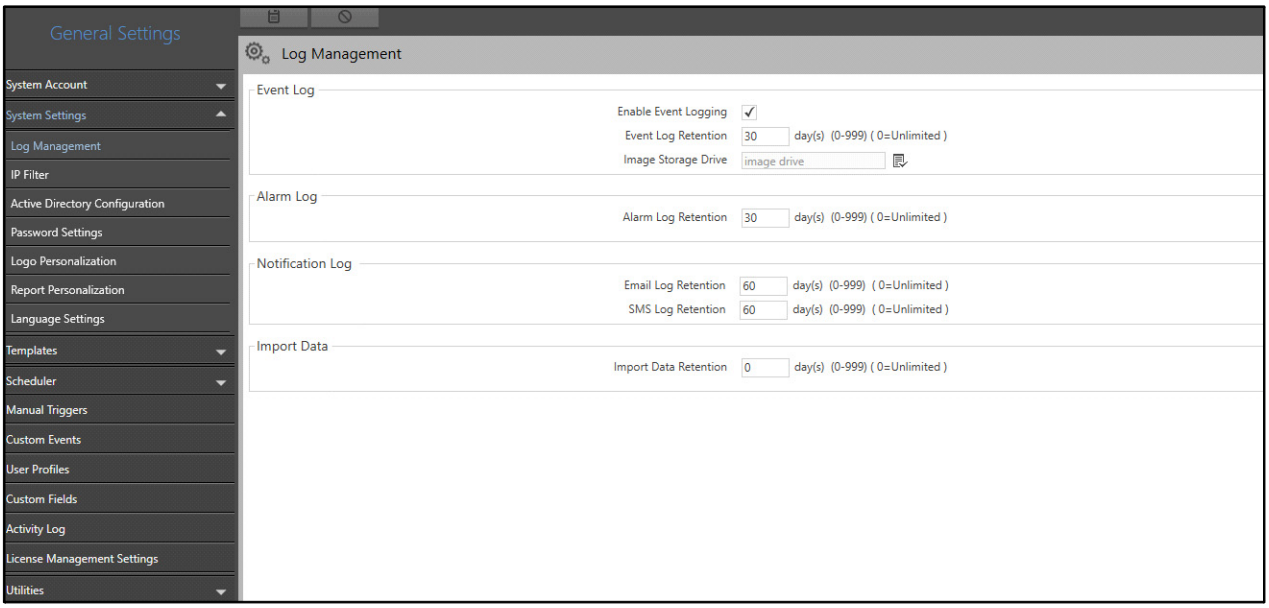
- Specify the number of records in **Show records** to be displayed on the page.

System Settings

The General Settings module enables you to configure System Settings, wherein you can configure logs, retain system events, alarms and notifications, filter IP addresses, manage password settings, personalize reports and configure language settings.

To configure System Settings,

- Click **General Settings > System Settings**.



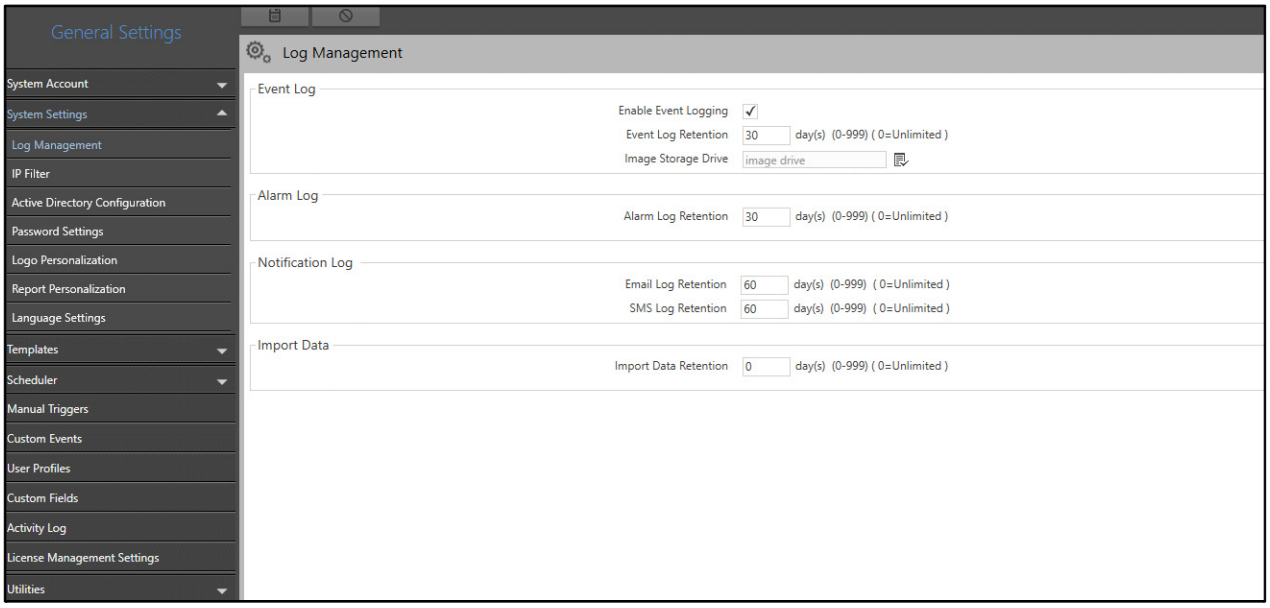
The System Settings section contains these pages — “Log Management”, “IP Filter”, “Active Directory Configuration” , “Password Settings”, “Logo Personalization”, “Report Personalization” and “Language Settings”.

Log Management

The Log Management page displays the settings for various Event logs. You can view and configure Event logs, Alarm logs, Notification logs and also Import data from this page.

To configure Log Management,

- Click **General Settings > System Settings > Log Management**.



The Log Management page contains four sections — "Event Log", "Alarm Log", "Notification Log" and "Import Data".

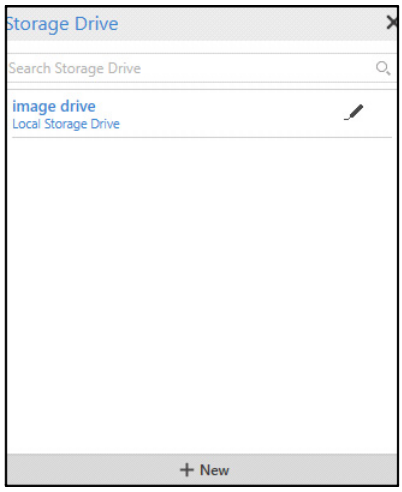
Event Log

- **Enable Event Logging:** Select the check box to enable the system to maintain a log of all the event as per their occurrence.

- **Event Log Retention:** Specify the duration (in days) for which event logs should be retained by the system. If you enter zero, the event log retention duration will be set as infinite. Valid Range: 0-999 days. Default: 30.

- **Image Storage Drive:** It displays the configured Management Server (MS) Storage Drive for images. You can change the Storage Drive, if required.

  - Click the **Select Image Storage Drive** picklist. The **Storage Drive** pop-up appears.

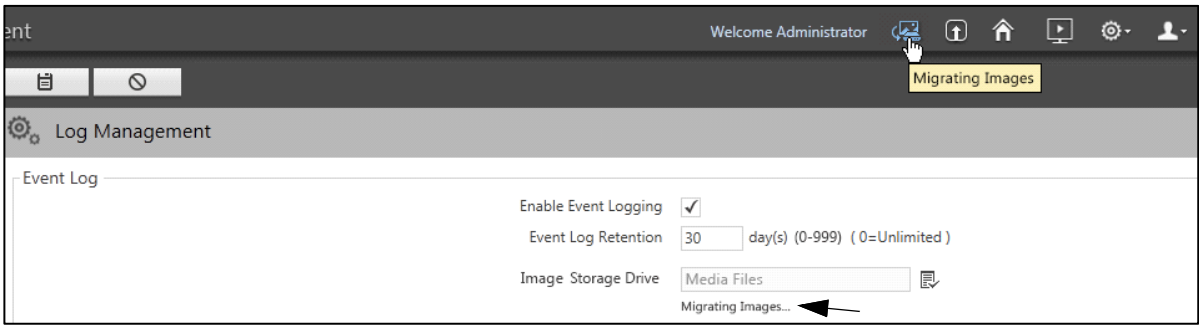


- Double-click to select the desired storage drive from the list. You can edit an existing drive by clicking **Edit** . You can also configure a new storage drive by clicking **New**. You can either add a new Local Drive or a Network Drive. For details, refer to “Local Drive” and “Network Drive”.

The configured FTP drive in MS cannot be used as an Image Storage Drive.

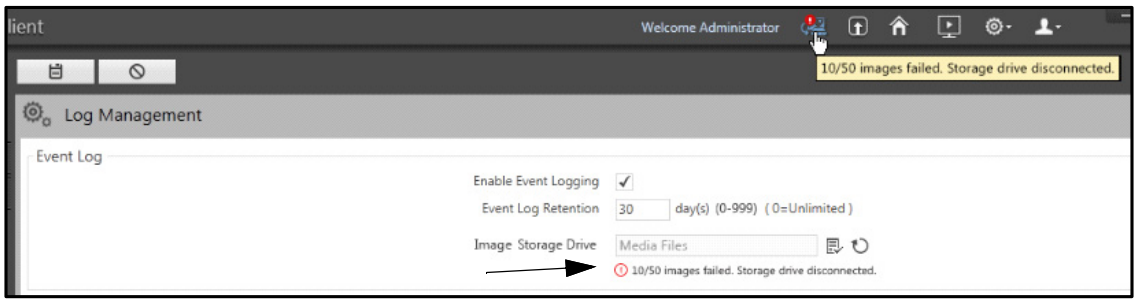
After you upgrade the Management Server from any lower version to V04R03 or later, Image Migration process takes place when the MS starts. During this process, the current images located in the database are transferred into the configured Image Storage Drive.

Once the migration process starts, the **Migrating Images** icon appears on the title bar. If you click on the same, you will be redirected to the Log Management page even if you are accessing any other module.



If the Image Migration fails due to any interruptions during the process, the reason for the same appears with the number of failed images out of total images considered for the transfer.

- Click **Retry** to re-initiate the Image Migration process.



The Image Migration is a one time process after upgrading the MS from any version to V04R03 or later.

Alarm Log

- **Alarm Log Retention:** Specify the duration (in days) for which alarms triggered in the system should be retained. If you enter zero, the alarm log retention duration will be set as infinite. Valid Range: 0-999 days. Default: 30.

Notification Log

- **Email Log Retention:** Specify the duration (in days) for which email notification logs generated by the system should be retained. If you enter zero, the Email log retention duration will be set as infinite. Valid Range: 0-999 days. Default: 60.

- **SMS Log Retention:** Specify the duration (in days) for which SMS notification logs generated by the system should be retained. If you enter zero, the SMS log retention duration will be set as infinite. Valid Range: 0-999 days. Default: 60.

Import Data

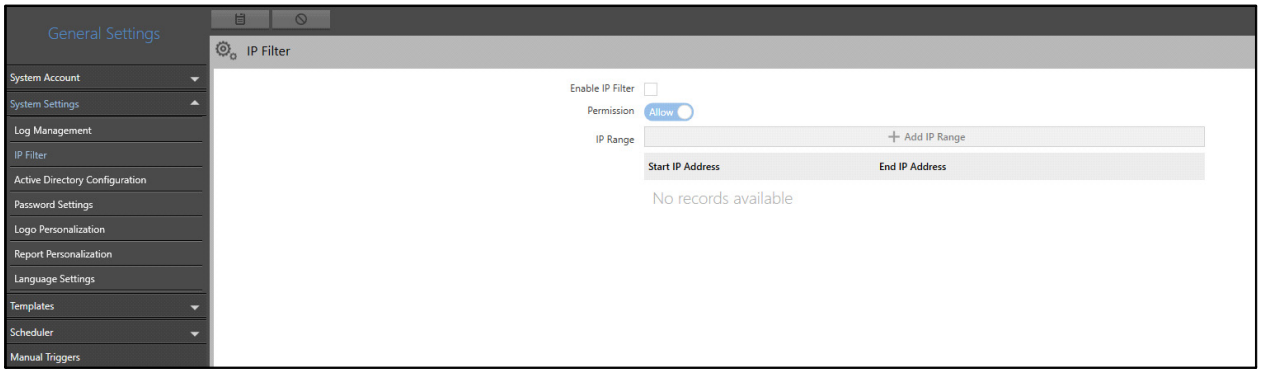
- **Import Data Retention**: Specify the duration (in days) for which Imported Data should be retained by the system. If you enter zero, the Import data retention duration will be set as infinite. Valid Range: 0-999 days. Default: 0.
- Click **Save** to save the settings or **Cancel** to discard.

IP Filter

The IP Filter page displays the settings to block or allow different IP range from accessing the Admin Client. By restricting IP Addresses you can secure the Admin Client from receiving unwanted requests from unknown users.

To configure IP Filter,

- Click **General Settings > System Settings > IP Filter**.



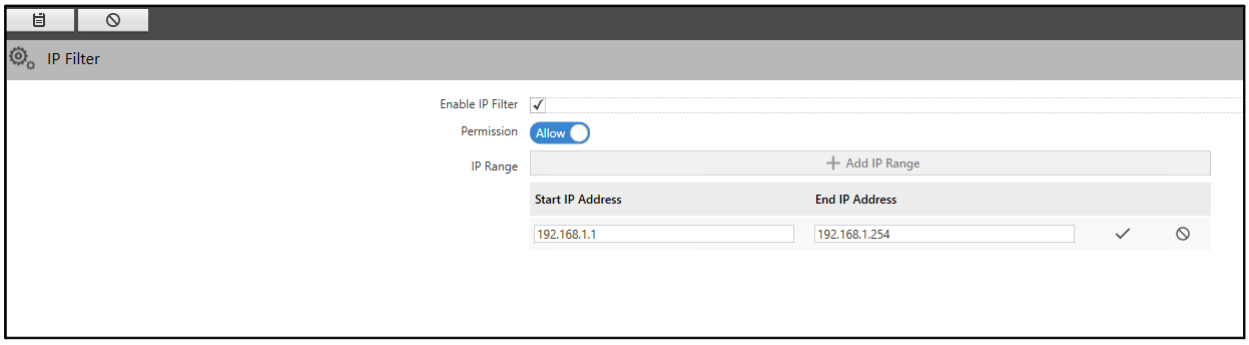
Configure the following parameters:

- **Enable IP Filter**: Select the check box to enable the IP Filter configurations.
- **Permission**: By default, the Permission is set as **Allow**. Click the Permission switch to **Deny**.
  - **Allow**: Set the Permission as **Allow,** to allow the configured IPv4/IPv6 addresses to login and access the Admin Client. The access to other IPv4/IPv6 address(es) outside the configured IP Range will be denied.
  - **Deny**: Set the Permission as **Deny**, to deny the configured IPv4/IPv6 addresses to login and access the Admin Client. The access to other IPv4/IPv6 address(es) outside the configured IP Range will be allowed.
- **IP Range**: Configure the IPv4/IPv6 Address range in the **Start IP Address** and **End IP Address**. In Start IP/End IP Address, you can enter upto 39 characters. Default Range:192.168.1.1 to 192.168.1.254.

- Click **Save** ✓ to save the settings or click **Cancel** ⊘ to discard.

You can add a maximum of 99 IP Address Ranges. To add another IP Range,

- Click **Add IP Range**.

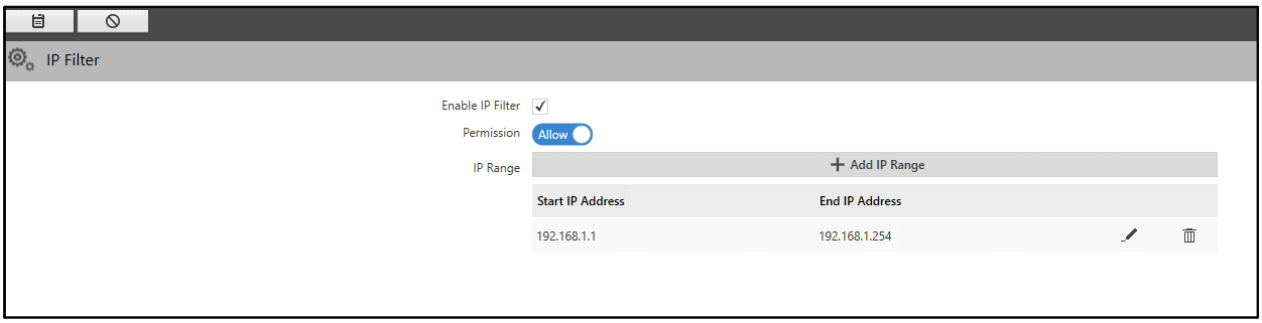


Configure the following parameters:

- **Start IP Address**: Specify the Start IPv4/IPv6 Address for IP Range you want to add. In Start IP Address, you can enter upto 39 characters. Default: 192.168.1.1
- **End IP Address**: Specify the End IPv4/IPv6 Address for the IP Range you want to add. In End IP Address, you can enter upto 39 characters. Default: 192.168.1.254

- Click **Save** to save the settings or click **Cancel** to discard.

The IP Range will appear in a list. If you wish, you can edit or delete the IP Range.



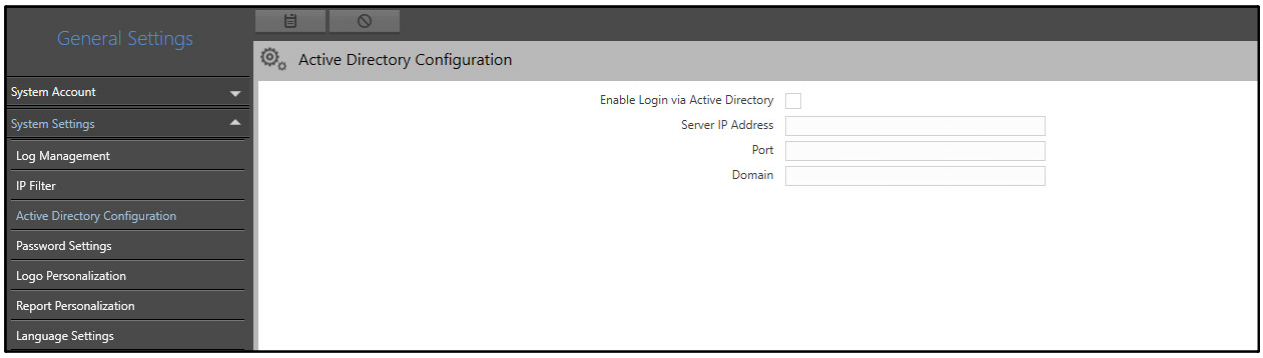
- Click **Edit** to edit the IP Range.
- Click **Delete** to delete the IP Range.
- Click **Save** to save the settings or **Cancel** to discard.

Active Directory Configuration

The Active Directory Configuration page displays the settings to authenticate and authorize a user while logging into the system on a particular domain. You can view and configure Active Directory Configuration from this page.

To configure Active Directory Configuration,

- Click **General Settings > System Settings > Active Directory Configuration**.



Configure the following parameters:

- **Enable Login via Active Directory**: Select the check box to enable the active directory users to login into the Admin Client.
- **Server IP Address**: Specify the IPv4/IPv6 Address of the server where the Active Directory is stored. In Server IP Address, you can enter upto 39 characters. Default: Blank.
- **Port**: Specify the port number of the server. Valid Range: 1-65535. Default: Blank.
- **Domain**: Specify the domain for which active directory service is to be used. In Domain, you can enter upto 100 characters. Default: Blank.

- Click **Save** to save the settings or **Cancel** to discard.

Once the active directory configuration is done, you can select active directory domain and enable the login for the desired users. For details, refer to “Users”.

Password Settings

You can define a password security policy that governs how users can set, reset or reuse passwords for different user account types across all SATATYA SAMAS applications. The SAMAS stores a list of frequently used passwords in a database and compares the new password with the same. SAMAS will not allow you to configure such frequently used passwords to enhance security. It is advisable to set a stringent policy to ensure that all passwords set by Admin Client users are safe and meet the security requirements of your organization. Make sure the details of the Password Policy are communicated to the other users of the Admin Client.

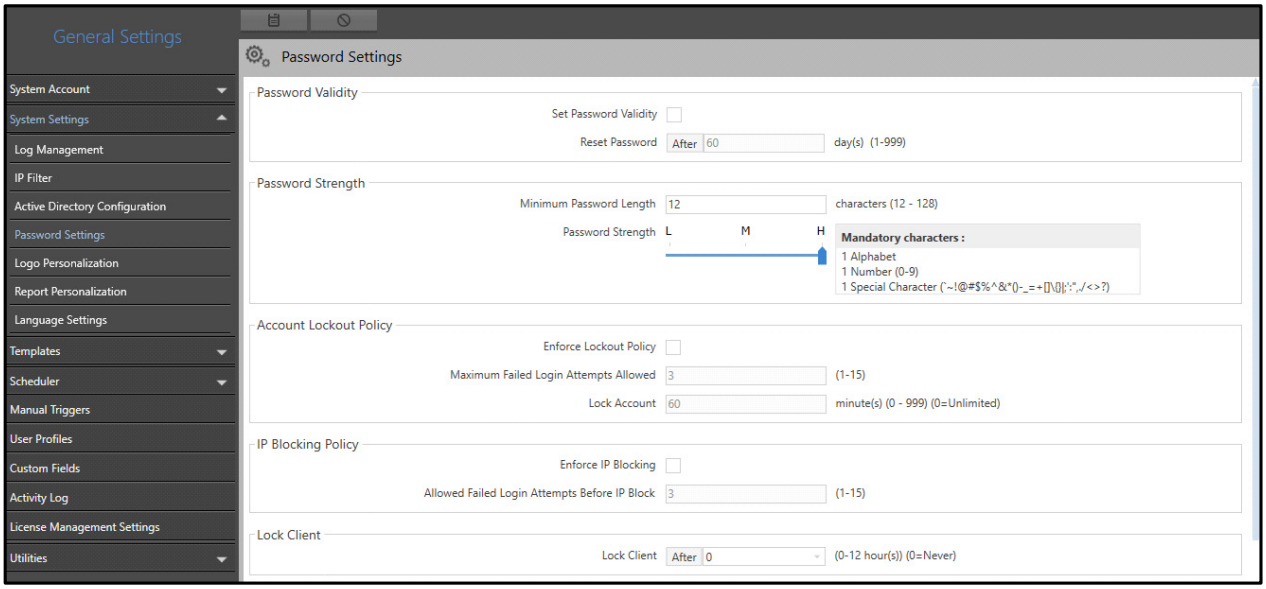
Passwords can be set at the time of first login.

Only you (or users assigned Administrator User Group), can modify the System Account Password from **User Details > *Change Password*** *on the Admin Client Title Bar. For details, refer to "Title Bar".*
For more details regarding user rights, refer to "User Groups".

The Password Settings page displays the settings to create, reset and reuse password for the Admin Client. You can view and configure Password Settings from this page.

To configure Password Settings,

- Click **General Settings > System Settings > Password Settings**.



The Password Settings page contains these sections — "Password Validity", "Password Strength", "Account Lockout Policy", "IP Blocking Policy", "Lock Client", "Password Reuse" and "OTP Policy".

Password Validity

- **Set Password Validity:** Select the check box to fix the validity of the password for a fixed duration. The set password will expire after the set duration expires. On expiry of the validity, the user will be prompted to reset the login password.

- **Reset Password After:** Specify the duration (days) after which the set password should expire. Valid Range: 1-999 days. Default: 60.

Password Strength

- **Minimum Password Length**: Specify the minimum number of characters required while creating the password. Valid Range: 12-128. Default: 12.

- **Password Strength:** Drag the slider to set the desired password strength — Low, Medium or High. Based on the set level **M** or **H**, certain mandatory characters must be used while setting a new password.These are displayed on the right. Level **L** imposes no restriction.

Account Lockout Policy

- **Enforce Lockout Policy:** This check box is enabled by default to lock an account automatically after certain failed login attempts. Clear this check box if you do not wish to lock an account automatically.

- **Maximum Failed Login Attempts Allowed**: Specify the number of maximum failed login attempts to be allowed to the user after which the account will be locked. Valid Range: 1-15. Default: 3.

- **Lock Account**: Specify the time period (in minutes) for which a user account remains locked after invalid login attempts. On expiry of this time, the user's account login will be restored. Valid Range: 0-999 minutes. Default: 60.

  If the Lock Account time period is configured as 0, then after the Maximum Failed Login Attempts Allowed are exhausted, the account will be locked permanently. You will need to reset the password for the locked account to enable the user to login.

IP Blocking Policy

- **Enforce IP Blocking**: Select the check box to enable the blocking of unauthorized IP addresses. To view the blocked IP addresses, refer to "Blocked IP Address".

- **Allowed Failed Login Attempts Before IP Block**: Specify the maximum number of login attempts to be allowed before the IP address is blocked. Valid Range: 1-15. Default: 3.



If the account is locked under Account Lockout Policy and the IP address is blocked under IP Blocking Policy, then on login attempt, the validation message displayed will be for IP Blocking.

Forgot Password functionality will not work for a blocked IP address.

IP Blocking will be done and checked only at the time of login. An active session for a blocked IP will not be affected.

Lock Client

- **Lock Client**: Select the time period (in hours) after which the Admin Client and Smart Client get locked automatically from the drop-down list. Select **0** if the Admin and Smart Client should never be locked.

  Users who are monitoring the screen can lock the client, and return to the same page from where they left. Here the system will not logout and the same session will remain active for the user.



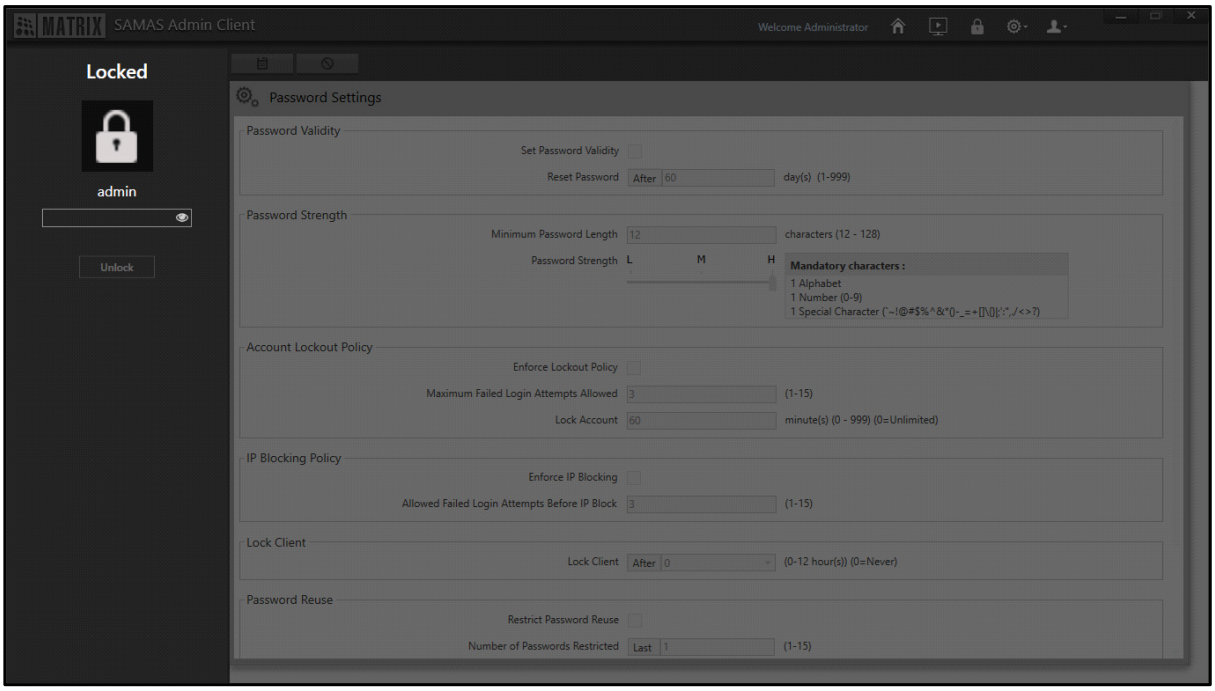
The Lock Client timer starts from the beginning of a login session. The timer is reset on new login or unlock. The timer is also reset if Lock Client time is changed.

All the parameters are disabled once the client is locked.

Unlock

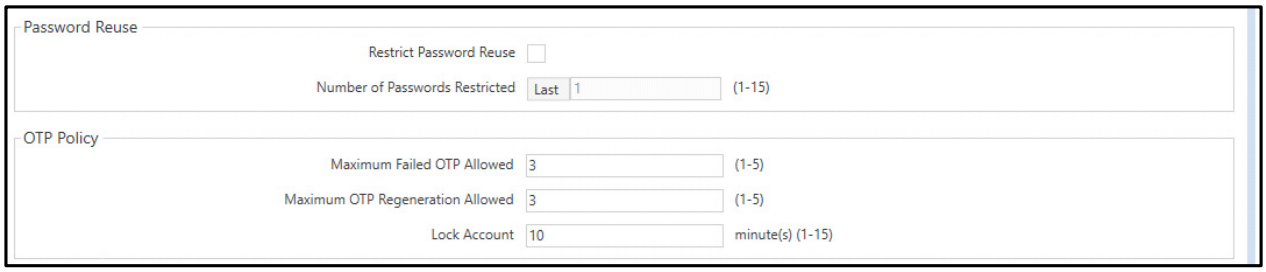
Once the Admin Client is locked Manually or after the expiry of Lock Client time, you need to unlock it by entering the login password.

The following screen appears once the client is locked.



- Enter the login password. Click on **Show**  to view the password, if required.
- Click **Unlock** to unlock the Admin Client.

Password Reuse



- **Restrict Password Reuse:** Select the check box to deny an old password to be set again as a new password.
- **Number of Passwords Restricted:** Specify the number of previously set passwords which are denied to be reused. Valid Range: 1-15. Default: 1.

  For example, if the **Number of Password Restricted** is 2 and **Restrict Password Reuse** is enabled, then consider the following scenario in which a user wants to change the current password.

Consider that the current password is **admin3.** The password previous to admin3 was **admin2,** and the password before admin2 was **admin1.**

In this case, **admin3** and **admin2** will be restricted. But, the user can reset and reuse the old password **admin1,** as the new one.

OTP Policy

- **Maximum Failed OTP Allowed**: Specify the number of times a user can submit a wrong OTP. Valid Range: 1-5. Default: 3.
- **Maximum OTP Regeneration Allowed**: Specify the number of times OTP can be regenerated by the system. Valid Range: 1-5. Default: 3.

  The account will be locked for 2 minutes (system timer non-configurable) when maximum OTP regeneration attempts are exhausted.
- **Lock Account**: Specify the time for which the account should be locked after maximum allowed failed OTP attempts limit is reached. The user can try to login again after expiry of Lock Account time. Valid Range: 1-15 minutes. Default: 10.
- Click **Save**  to save the settings or **Cancel**  to discard.

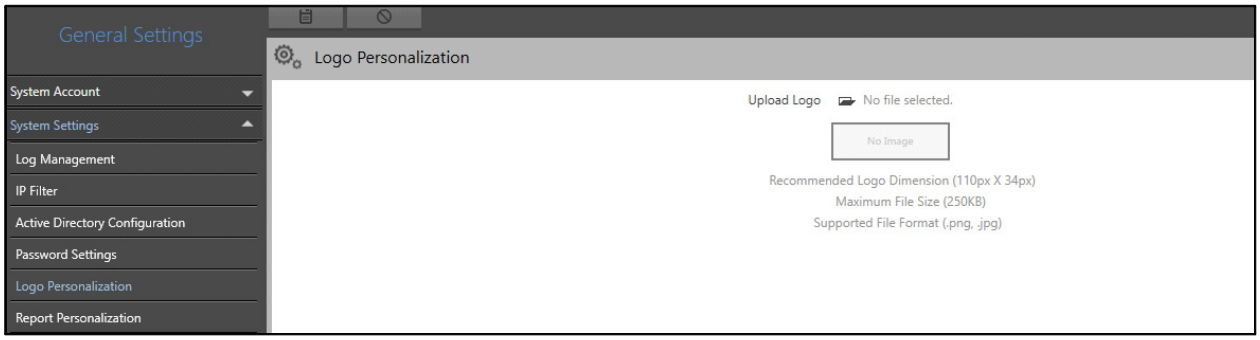
Logo Personalization

The Logo Personalization page displays the settings to upload different logos. You can upload a logo of your choice which will be displayed on the Home page, Login page and the Title bar of the Admin Client. It will also be displayed on the Smart Client's Login page and its Title bar. This logo will also be visible to SATATYA VISION (Mobile Application) users. You can view and configure Logo Personalization from this page.

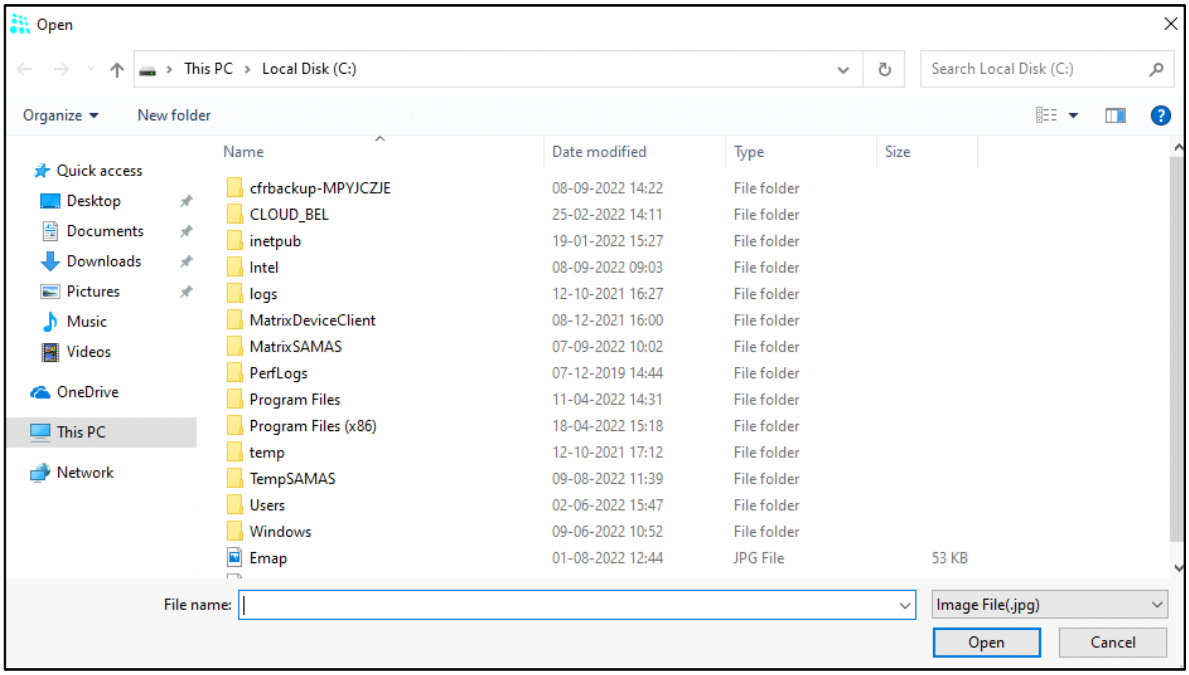
Make sure the Smart Client is connected with the same Management Server to view the Logo changes.

To configure Logo Personalization,

- Click **General Settings > System Settings > Logo Personalization**.



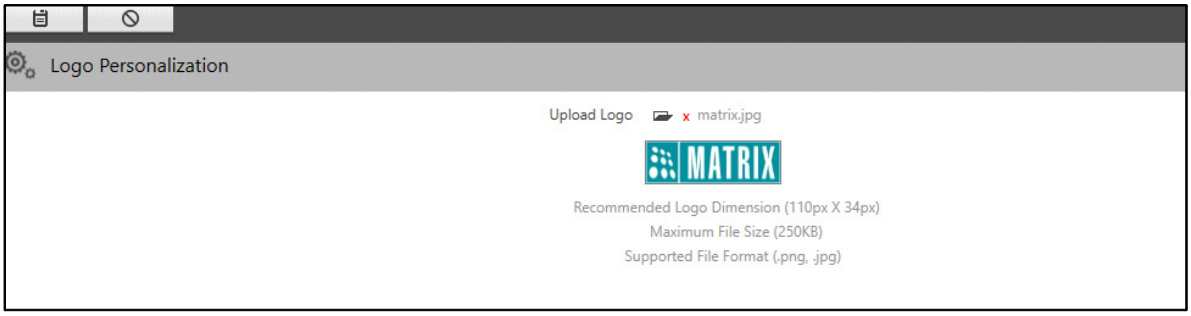
- Click **Upload Logo** . The **Open** pop-up appears.



- Select the desired image from your local PC to upload as the logo.
- Click **Open** to upload the image or click **Cancel** to discard.

Once the logo is uploaded successfully, it is visible in the box.

The ideal dimensions for the logo are 110 x 34 pixels with its maximum size being 250KB. The supported file types are .png and .jpg. The logo will shrink or stretch if the size is not as per the defined dimensions.



- Click **Save** to save the settings or **Cancel** to discard.

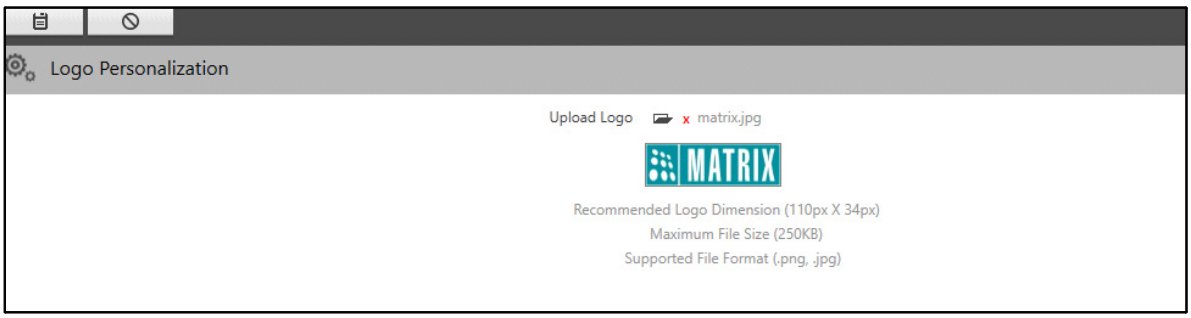
Once the logo is uploaded and saved, it is displayed on the related pages.





If you wish to remove the uploaded logo,

- Click **Remove Logo** .



- Click **Save** to save the settings or **Cancel** to discard.

The default (MATRIX) logo will be displayed automatically on the relevant pages once the custom logo is removed.

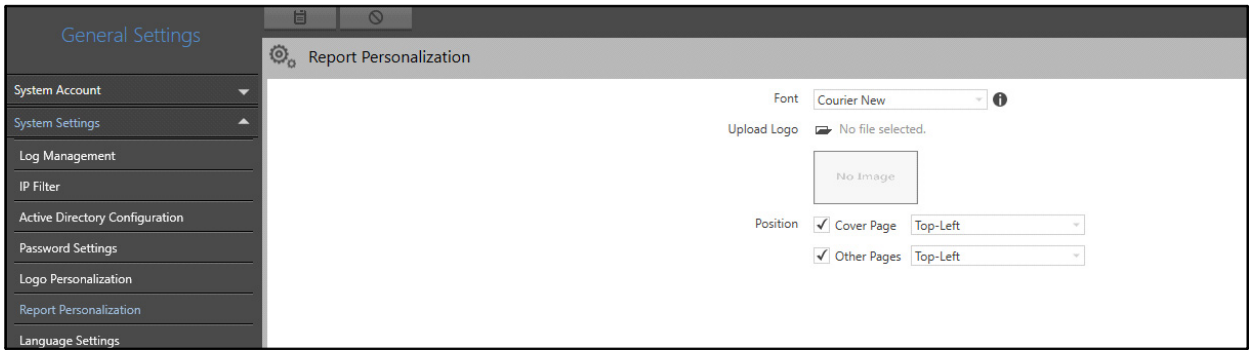
If multiple users are logged in into the same Admin Client and logo is uploaded/removed by any user, the changes will be visible to other users on their next login.

Report Personalization

The Report Personalization page displays the settings to upload logo and change font style for the reports. You can view and configure Report Personalization from this page.

To configure Report Personalization,

- Click **General Settings > System Settings > Report Personalization**.



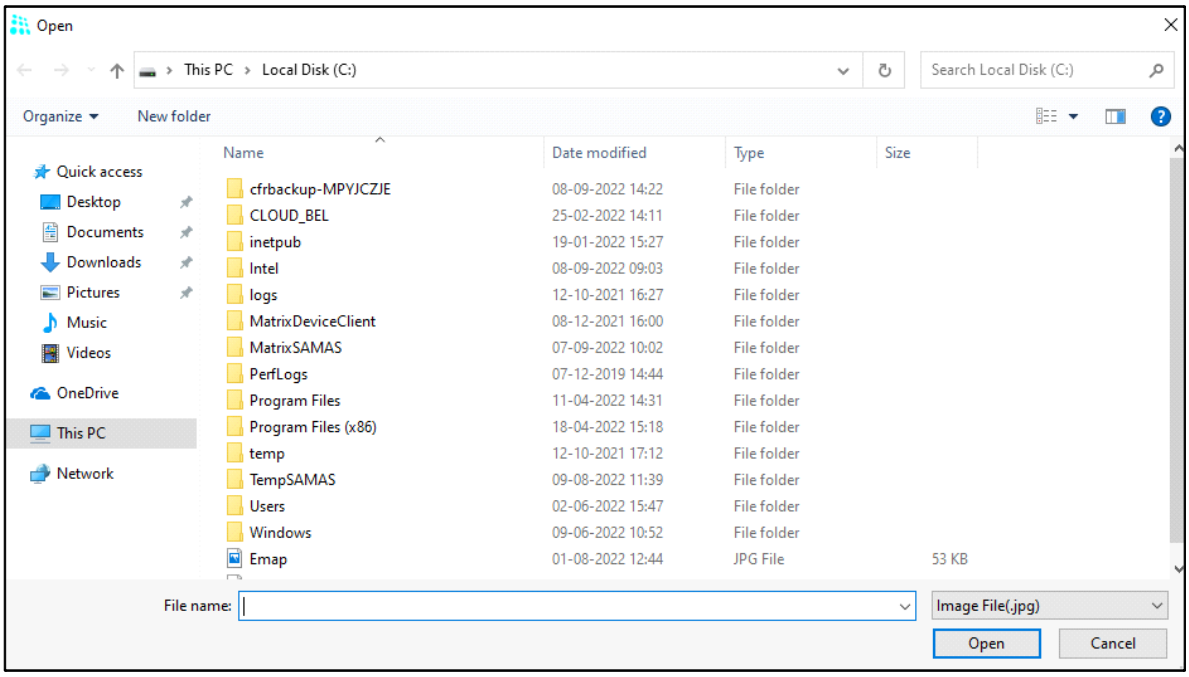
Configure the following parameters:

- **Font:** Select the Font which you wish to assign to the reports from the drop-down list. Changing the font style can be useful when you are using the Multi-language feature. It is because some font styles are not supported by particular languages. This option allows you to generate the report in the font style that is compatible with the desired language.

Fonts that are available for selection in the drop-down list are detected from the system where Management Server is running.

To get the updated list of fonts, you need to restart the Management Server.

- **Upload Logo**: Upload the desired logo which you wish to display in the report.
  - Click **Upload Logo** . The **Open** pop-up appears.

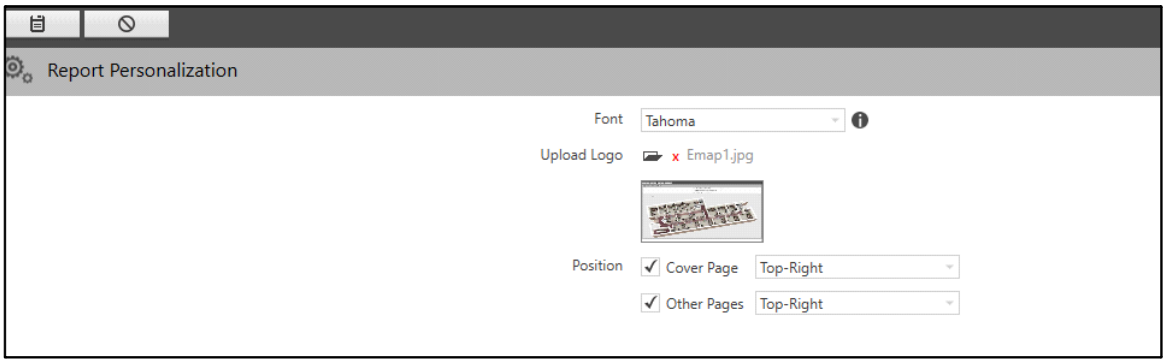


- Select the desired image from your local PC to upload as the logo. The image can be of upto 250 KB. Valid Format: .jpg, .bmp.

- Click **Open** to upload the image or click **Cancel** to discard.

Once the logo is uploaded successfully, it is visible in the box.

The ideal dimensions for the logo are 110 x 34 pixels with its maximum size being 250KB. The supported file types are.png and.jpg. The logo will shrink or stretch if the size is not as per the defined dimensions.



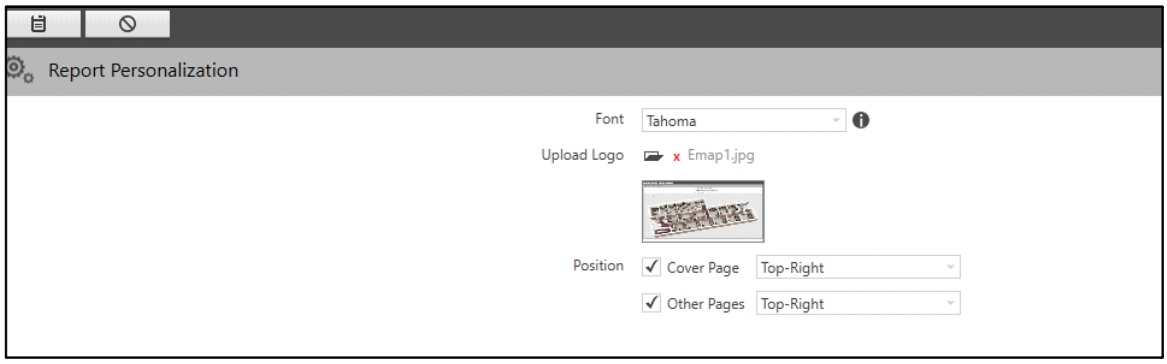
- **Position**: Select the position at which the logo should be displayed — Cover Page or Other Pages.

  - **Cover Page:** Select this check box to place the logo on the Cover Page and select the desired position at which you wish to place the logo from the drop-down list.

  - **Other Pages:** Select this check box to place the logo on the Other Page and select the desired position at which you wish to place the logo from the drop-down list.

- Click **Save** to save the settings or **Cancel** to discard.

Once the report configurations are saved, you can edit them or delete the logo.



- Edit the report configurations as desired.
- Click **Remove Logo** to remove the logo from the report.
- Click **Save** to save the settings or **Cancel** to discard.

No logo will be displayed on the report once the custom logo is removed.

Language Settings

While using SATATYA SAMAS, efficiency is the prime goal. As a result, language should not be a barrier. To ensure this, SATATYA SAMAS is optimized with different languages. It supports UTF-8 characters that helps you to provide inputs in local language using international keyboards. This feature lets you work more efficiently with multiple languages. A maximum of 99 languages can be added.

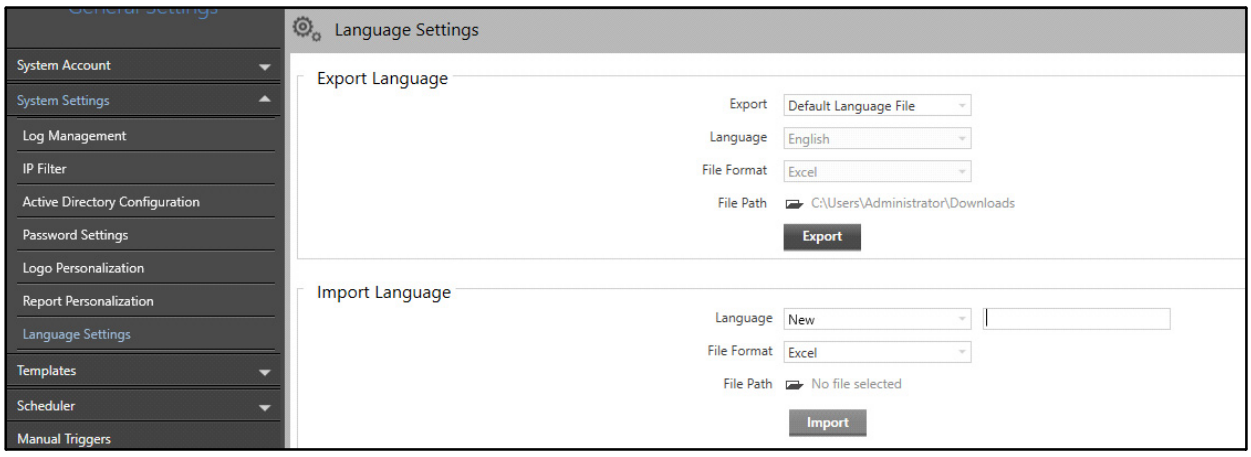
You can export a specific language file, translate the Admin Client labels in the preferred language and import the modified file into the application. These configurations will allow you to translate the static labels everywhere in SATATYA SAMAS.

The Language Settings page displays the settings to export and import language files. You can view and configure Language Settings from this page.

If you are upgrading SAMAS to V6R1 and later, you need to manually re-import the language file.

To configure Language Settings,

- Click **General Settings > System Settings > Language Settings**.



The Language Settings page is divided into two sections — Export Language and Import Language. The Export section allows the you to export Excel or SQLite language files at the defined path. The Admin Client provides three options by which you can export the language files. The Import section allows you to import the translated file to the Admin Client. Each option has been explained in the further section.

You need to install Microsoft Office on your system to read/access the language file that has been exported in the excel format.

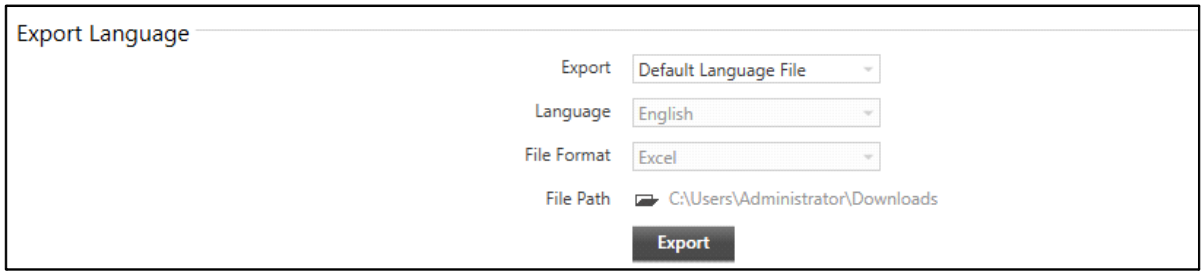
The language file consists labels for General Settings, Servers & Devices, E-maps, Access Control, CREAM, Homepage, Common Messages, Media Client, Reports and all the IVA Modules.
You need to translate the labels accordingly as per your requirement.

Importing language file in SQLite format takes lesser time as compared to the Excel format.

Exporting Default Language File and Importing Translated File

The Admin Client provides you the default language file in English. You can modify this file accordingly, when intended to translate the labels into the preferred language for the first time.

To export the default language file,

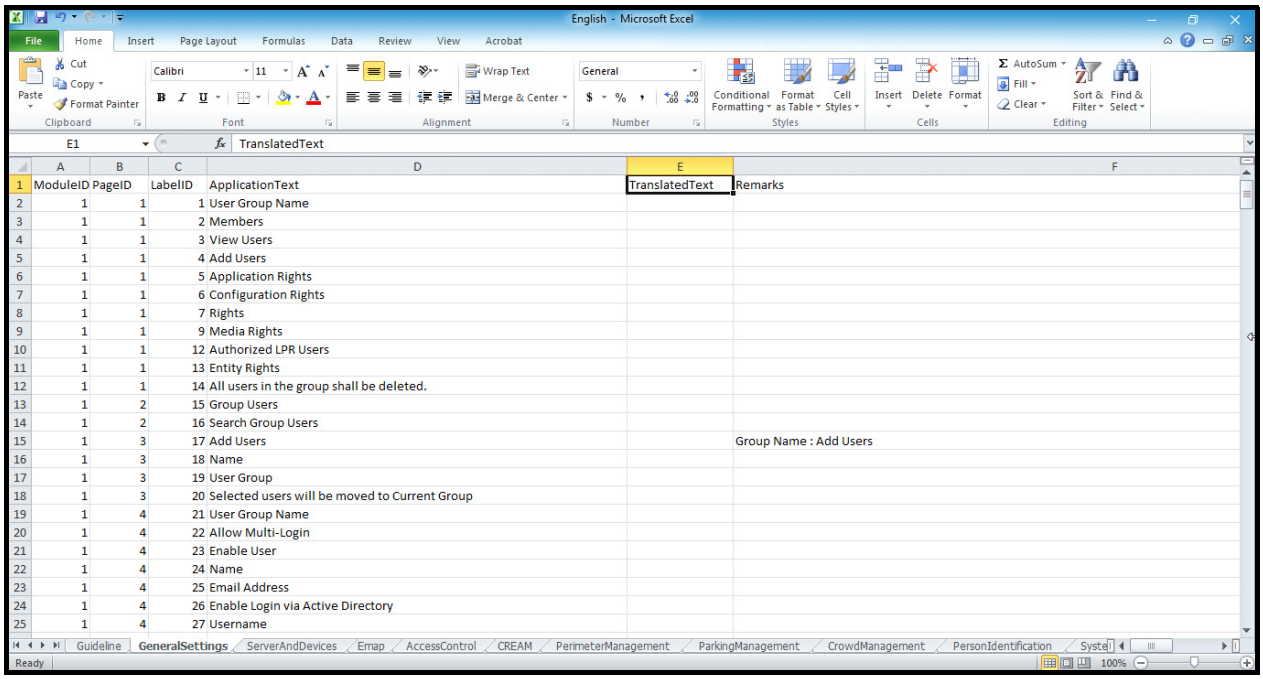


Configure the following parameters:

- **Export**: Select **Default Language File** from the drop-down list.
- **Language**: The language is displayed as English by default when Default Language File option is selected.
- **File Format**: The file format is displayed as Excel by default when Default Language File option is selected.
- **File Path**: You can select the path at which you wish to storage the file on the local PC. Click

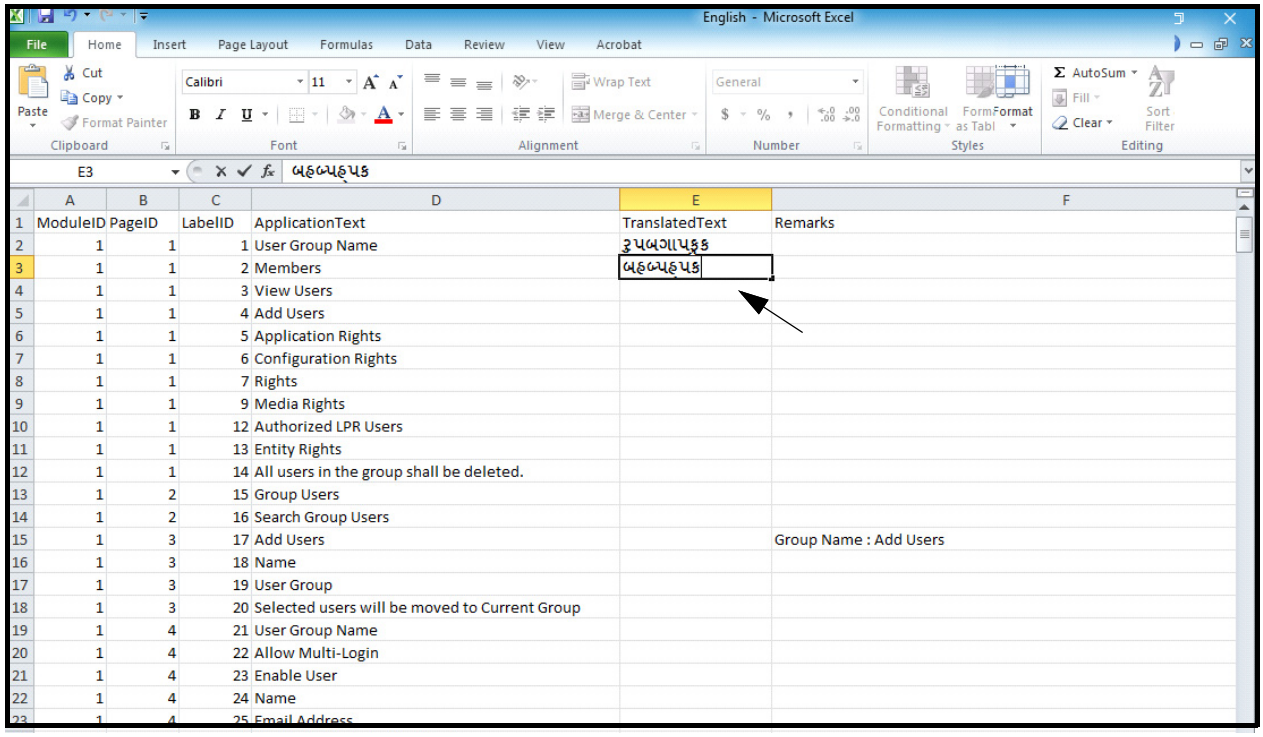
  Browse . It will display all folders which are in the drive. Select the desired folder.

- Click **Export**. The file will be saved at the desired location and a message for the same is displayed on the top-right corner of the page.
- Once the Default Language File is exported at the provided location, open the file.



This default file (in English) can be modified by the user for translating the Application Text into the preferred language for the first time.

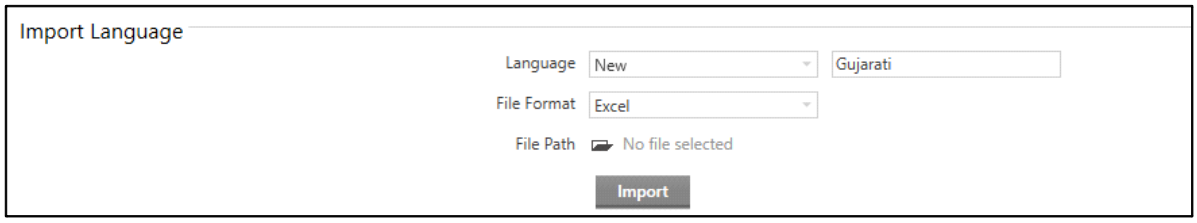
- Enter the text in the language you prefer in the **Translated Text** column against each Application Text.



- After entering all the required Application Text in your language, save the file.

This exported language file that has been modified, can be imported in Admin Client.

To import the language file,



Configure the following parameters:

- **Import**: Select the language file you wish to import from the drop-down list. Specify a name for the language. In name, you can enter upto 100 characters. Default: Blank.
- **File Format**: Select the desired file format in which you wish to import the file from the drop-down list.
- **File Path**: Browse the path from where you wish to import the language file. Click **Browse** . It displays all folders which are in the drive. Select the desired file from the folder. The maximum file size supported is 25MB.

- Click **Import**.

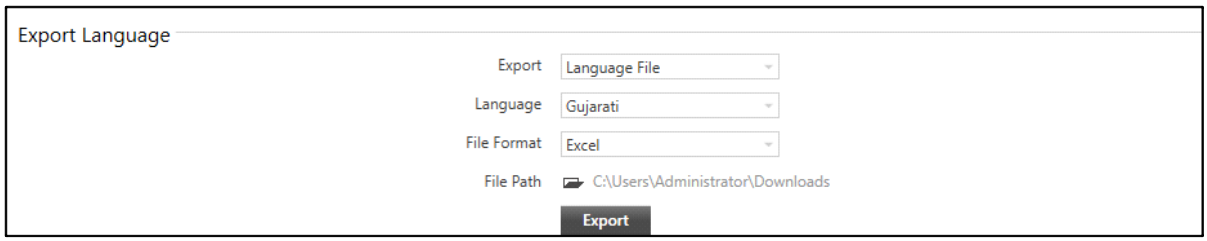
After the Language file is imported successfully, it will be stored in the Admin Client and will be available for selection at the relevant locations in the application.

Exporting and Importing Language File

The Admin Client also allows you to export the entire language file that already exists in the application. This option is useful in case you wish to modify the existing saved language file. This is required to rectify the previous translations if you may have entered wrong text in the translated text column or if you may have configured the language file partially and wish to complete the configuration.

In these scenarios, you need to export the last saved language file.

To export the language file,



Configure the following parameters:

- **Export**: Select **Language File** from the drop-down list.
- **Language**: Select the language file you wish to export from the drop-down list. All the language files imported in the Admin Client appear in this list.
- **File Format**: Select the desired file format in which you wish to export the file from the drop-down list.

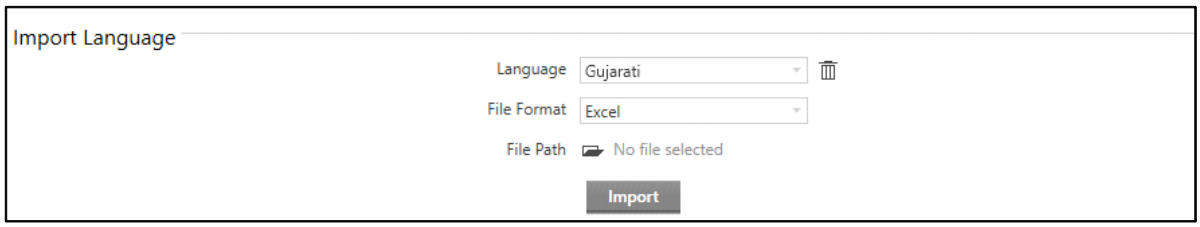
- **File Path**: You can select the path at which you wish to storage the file on the local PC. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

- Click **Export**. The file will be saved at the configured location and a message for the same is displayed on the top-right corner of the page.

The exported language file consists of the last saved data. You can now modify the same as per your requirement For details, refer to "Exporting Default Language File and Importing Translated File".

The modified file can then be imported in the Admin Client.

To import the language file,



Configure the following parameters:

- **Import**: Select the language file you wish to import from the drop-down list.
- **File Format**: Select the desired file format in which you wish to export the file from the drop-down list.
- **File Path**: Browse the path from where you wish to import the language file. Click **Browse** . It displays all folders which are in the drive. Select the desired folder. The maximum file size supported is 25MB.

- Click **Import**.

The Import process may take some time.

After the Language file has been imported successfully, the language file will be updated and stored in the application. This language will be available for selection at the relevant locations in the application. You can also delete the language file, if required.

- Click **Delete** next to the selected language file which you wish to delete.

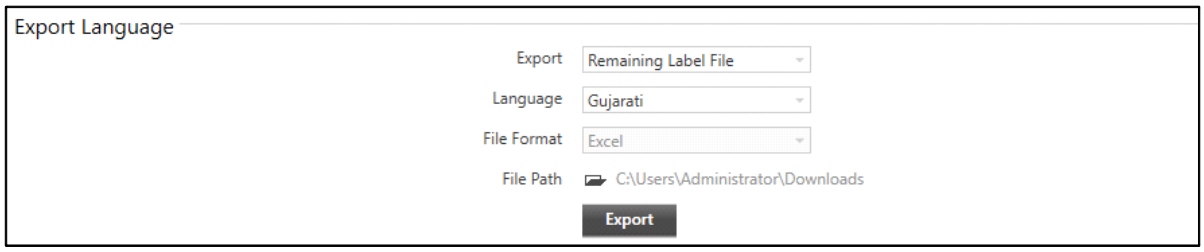
In case any language file is deleted, the default language (English) will be set in the Admin Client.
A maximum of 99 languages can be added.

Exporting and Importing Remaining Label File

Exporting Remaining Label file allows you to translate those labels, which were not translated previously. This option also allows to translate the new labels which may get introduced when SATATYA SAMAS version is upgraded.

The Admin Client allows you to export the already saved language file of the selected language with only new labels or those labels, which were not translated previously. You can select this option to export and translate only the remaining labels of the application instead of exporting the whole language file.

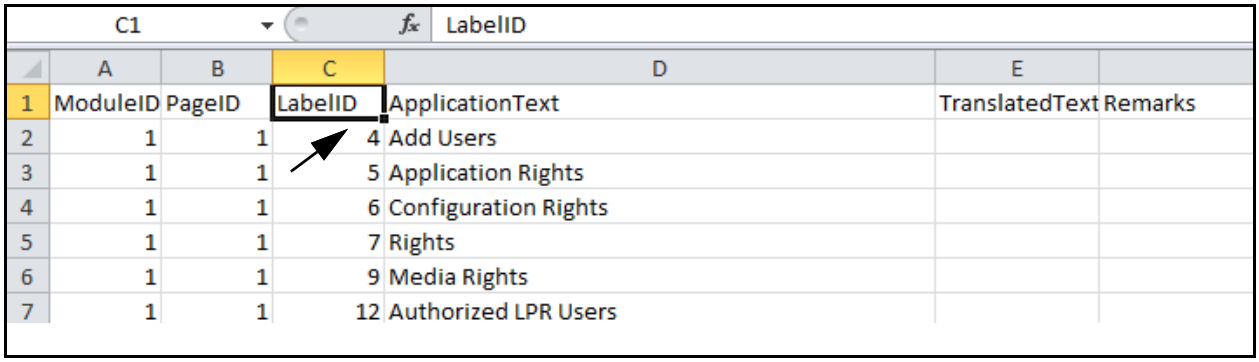
To export the remaining label file,



Configure the following parameters:

- **Export**: Select **Remaining Label File** from the drop-down list.
- **Language**: Select the language file that you wish to export from the drop-down list. All the language files imported in the Admin Client appear in this list.
- **File Format**: The file format is displayed as Excel by default when Remaining Label File option is selected.
- **File Path**: Browse the path where you wish to store the exported file. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

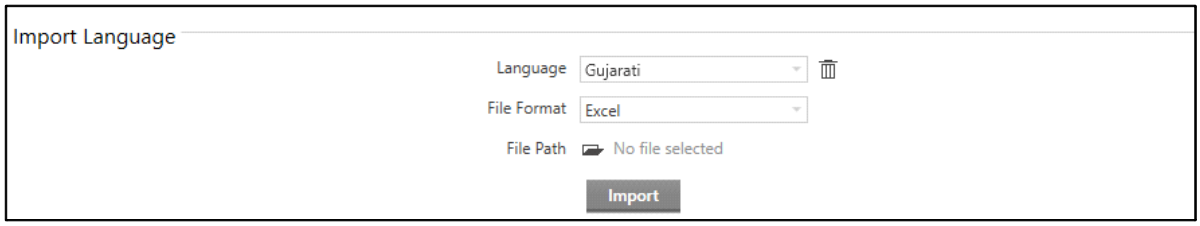
- Click **Export**. The file will be saved at the configured location and a message for the same is displayed on the top-right corner of the page.
- The exported file will consist only those labels of the application which have not been translated previously. This is shown below, where the excel sheet contains some missing Label IDs: 1, 2, 3 and 8 (which have been translated previously) and contains the Label IDs: 4, 5, 6, 7, 9, 12 which still need to be translated.



- You can translate the remaining labels of the application in the exported sheet.

The remaining Label File that has been exported and modified, can now be imported in the Application.

To import the language file,



Configure the following parameters:

- **Import**: Select the modified exported language file you wish to import from the drop-down list.
- **File Format**: Select the desired file format in which you wish to export the file from the drop-down list.
- **File Path**: Browse to select the file from where you wish to import the language file. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.The maximum file size supported is 25MB.

- Click **Import**.

The Import process may take some time.

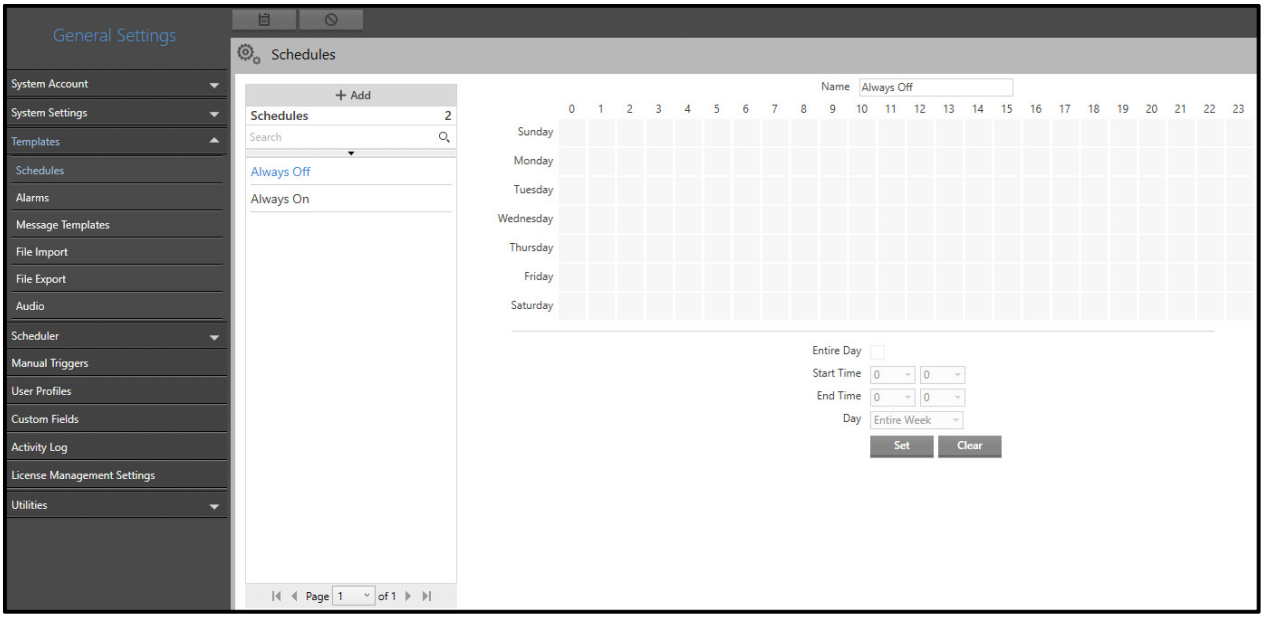
After the Remaining Label File has been imported successfully, the file will be updated and stored in the application. This language will be available for selection at the relevant locations in the application.

Templates

The General Settings module enables you to configure Templates, wherein you can create templates for Schedules, Alarms, Message Templates, File Import, File Export and Audio.

To configure Templates,

- Click **General Settings > Templates**.



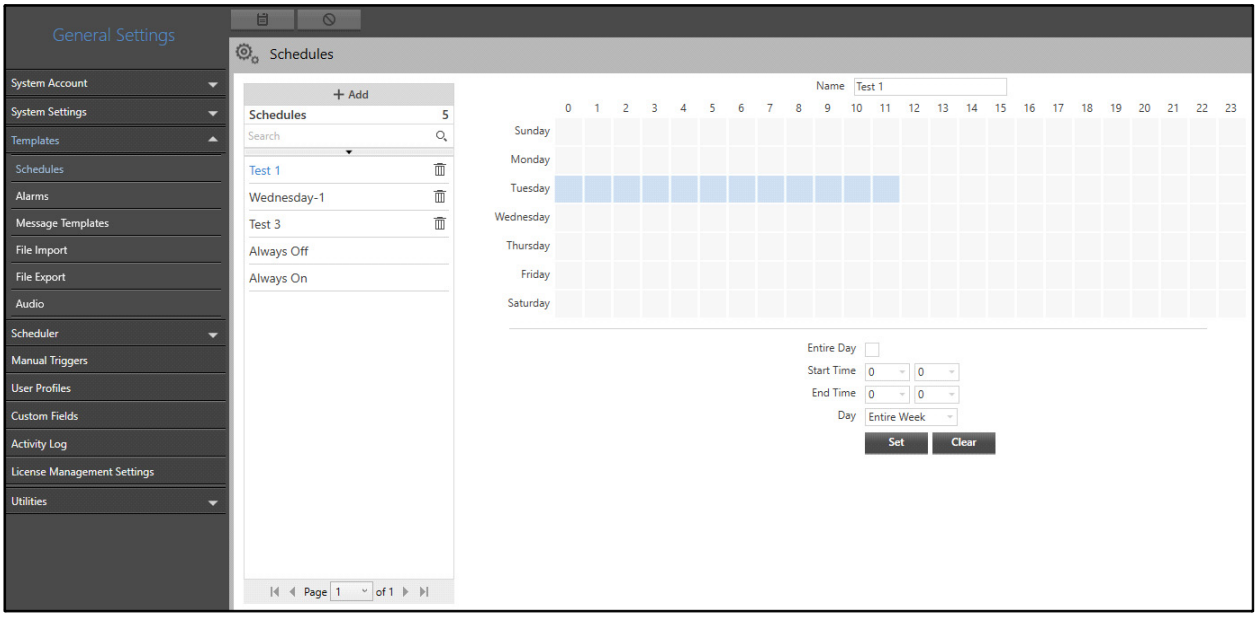
The Templates section contains these pages — “Schedules”, “Alarms”, “Message Templates”, “File Import”, “File Export” and “Audio”.

Schedules

The Schedules page displays the settings to configure schedule for either a day or the entire week. These schedules are useful in configuring Events, Reports, Scenarios, etc. You can view and configure Schedules from this page.

To configure Schedules,

- Click **General Settings > Templates > Schedules**.



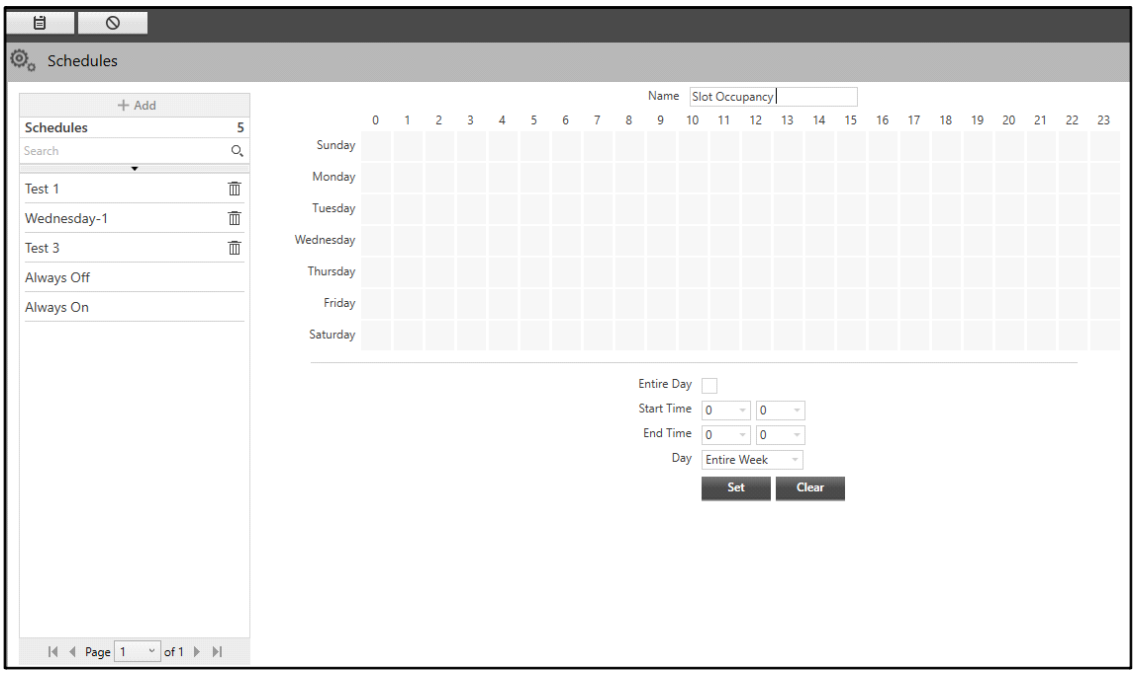
There are two pre-defined schedules which cannot be edited or deleted:

- **Always On**: This schedule is active for all days of the week and all time blocks by default.
- **Always Off**: This schedule is inactive for all days of the week and all time blocks by default.

If new customized scheduled is created and assigned for an action and then the same is deleted, then the **Always On** schedule will be assigned for the action automatically.

To create a Schedule,

- Click **Add**.

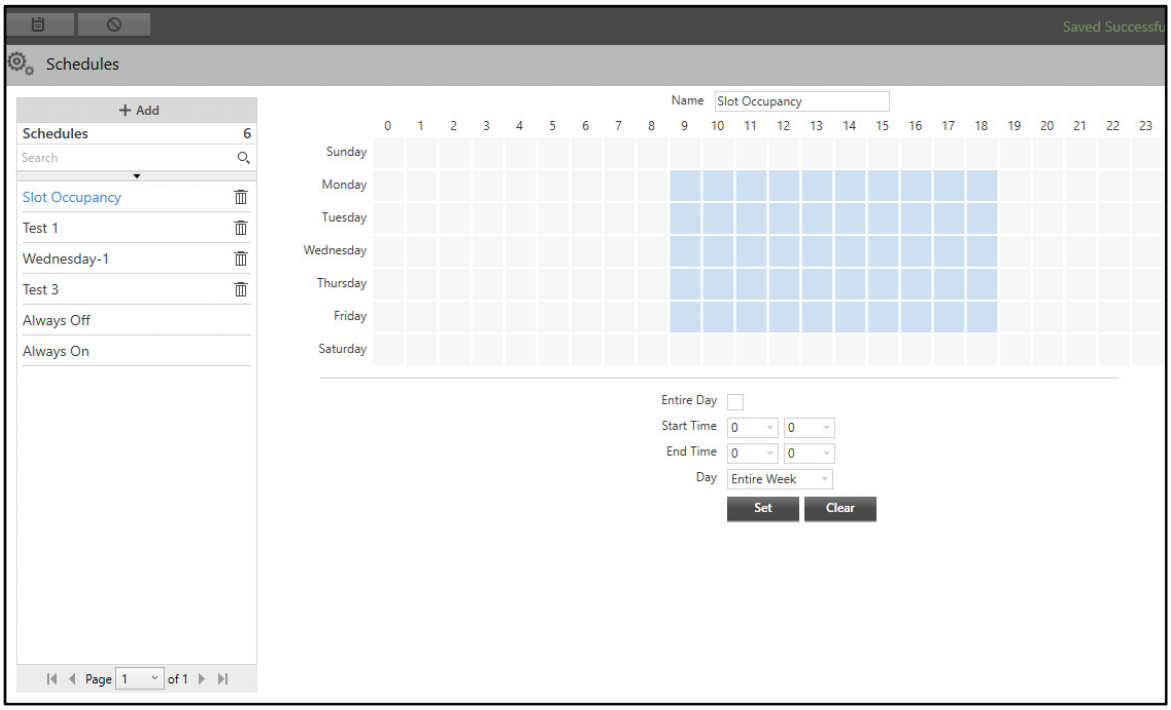


Configure the following parameters:

- **Name**: Specify a suitable name for the schedule. In Name, you can enter upto 50 characters. Default: Blank.
- **Entire Day**: Select the check box if you wish to configure the schedule for an entire day. Clear the check box to set the schedule for certain hours of a day.
- **Start Time**: Specify the start time in hours and minutes from the drop-down lists.
- **End Time**: Specify the end time in hours and minutes from the drop-down lists.
- **Day**: Select the day of the week or the entire week for which you wish to set the schedule from the drop-down list.

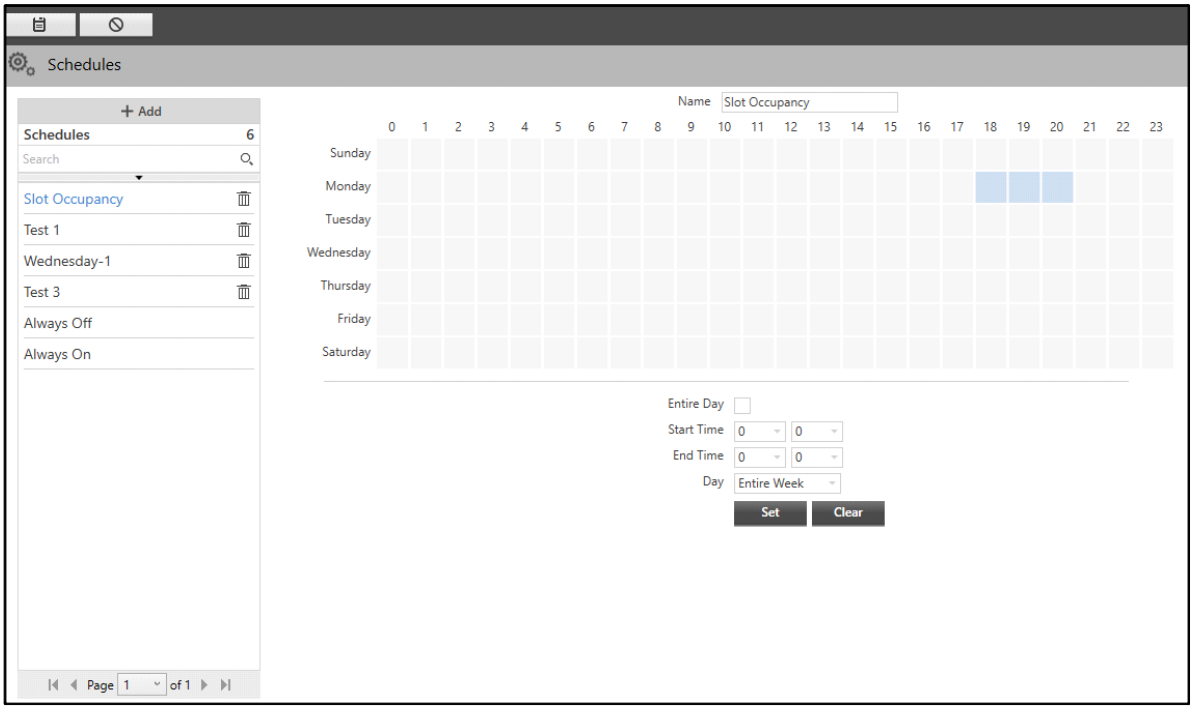
- Click **Set** to set the schedule as per the above configured parameters or click **Clear** to discard.

The set schedule will appear in the grid. Alternatively, you can manually select the time against the days from the grid.



Each day of the week is divided into 24 blocks (1 block is equivalent to 60 minutes), each of which is again sub-divided into 4 blocks of 15 minutes each.

- Set the time slots manually by clicking your mouse or by dragging the selection across multiple time blocks of the day. The starting time of slot 0 is 00.00 and the ending time of slot 23 is 23:59. For example, to create a schedule for Monday from 6 to 9 pm, you can select entire 4 blocks from column 18 to 20.

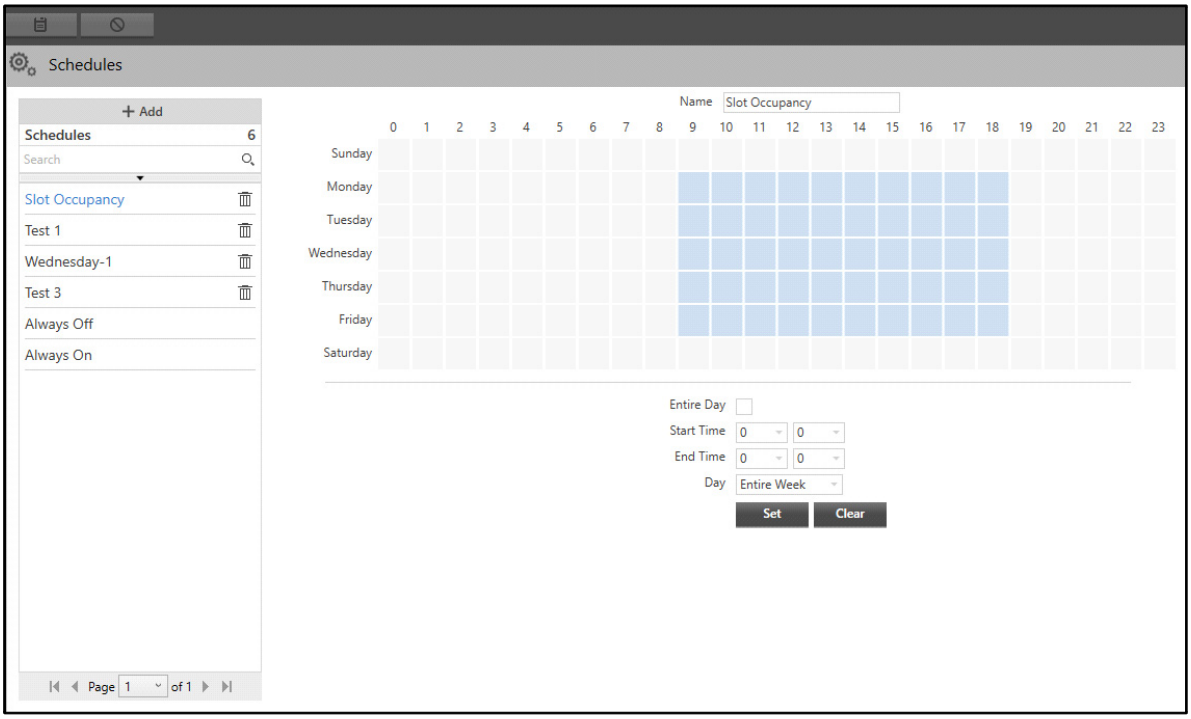


- Click **Set** to view the set schedule or click **Clear** to discard.

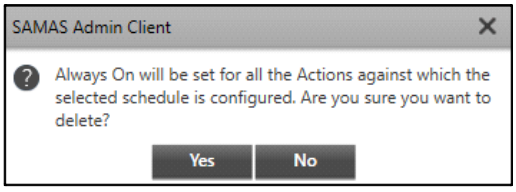
- Click **Save** to save the settings or **Cancel** to discard.

The new schedule appears in the list on the left hand side.

You can also change the configurations of the desired schedule or delete it.



- Select the desired schedule from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired schedule. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

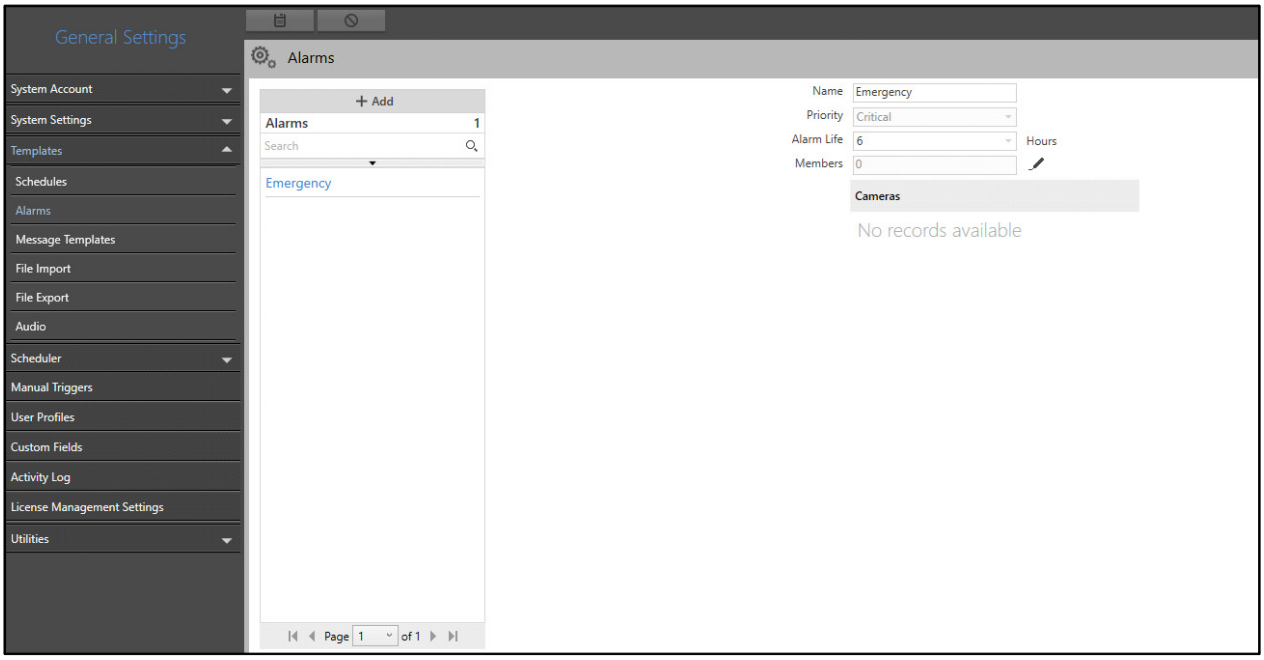
Alarms

Alarm is one of the best methods that can be used to provide an alert regarding the occurrence of an Event that requires immediate attention.

The Alarms page displays the configured alarms. These alarms can be assigned as an action (Trigger Alarm) for Events (For example, Camera Tampered) when configuring various Scenarios. You can view and configure Alarms from this page.

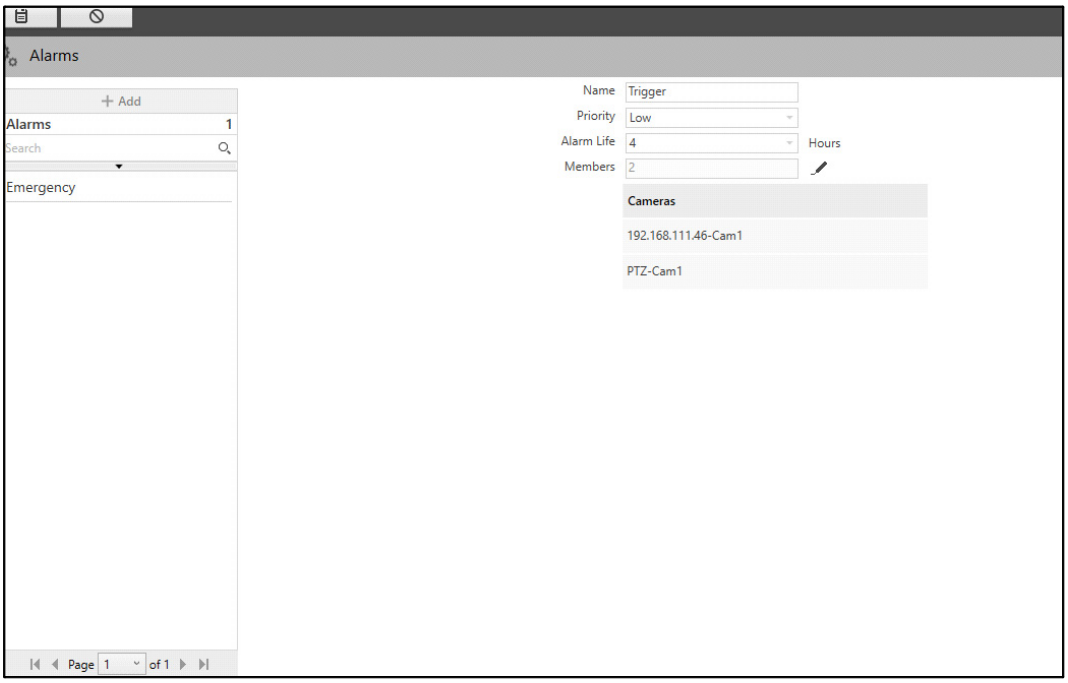
To configure Alarms,

- Click **General Settings > Templates > Alarms**.



The **Emergency** alarm is pre-configured. The configurations for this alarm can be changed but it cannot be deleted. However you can add Alarms as per your requirement.

- Click **Add**.



Configure the following parameters:

- **Name**: Specify a suitable name for the alarm. In Name, you can enter upto 50 characters. Default: Blank.

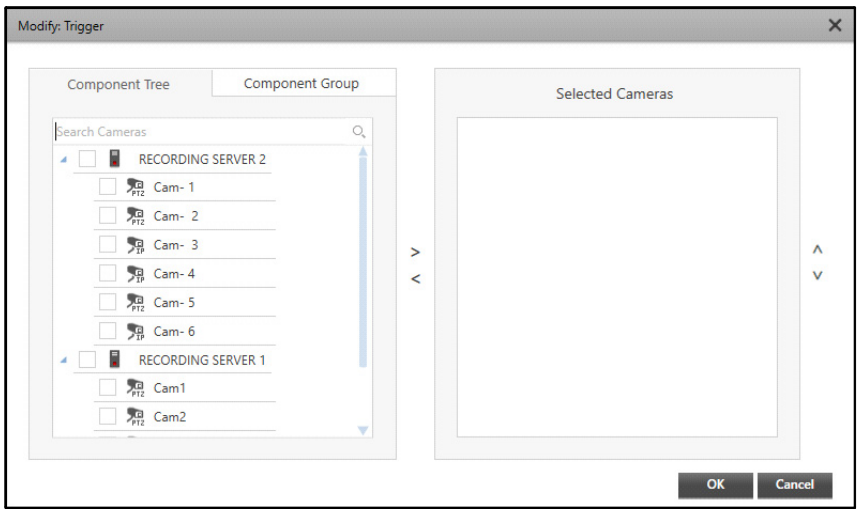
- **Priority**: Select the priority to be assigned to the alarm from the drop-down list — Low, Normal, High, Severe or Critical. The priority of alarm is important when multiple alarms are triggered simultaneously. The priority of the alarm is as follows:

  Critical: First Priority.
  Severe: Second Priority
  High: Third Priority.
  Normal: Fourth Priority.
  Low: Fifth Priority.

- **Alarm Life**: Select the duration of the alarm in hours from the drop-down list. The alarm will stop when this duration expires.

- **Members**: Select the cameras you wish to assign to the alarm. A maximum of 4 cameras can be assigned.

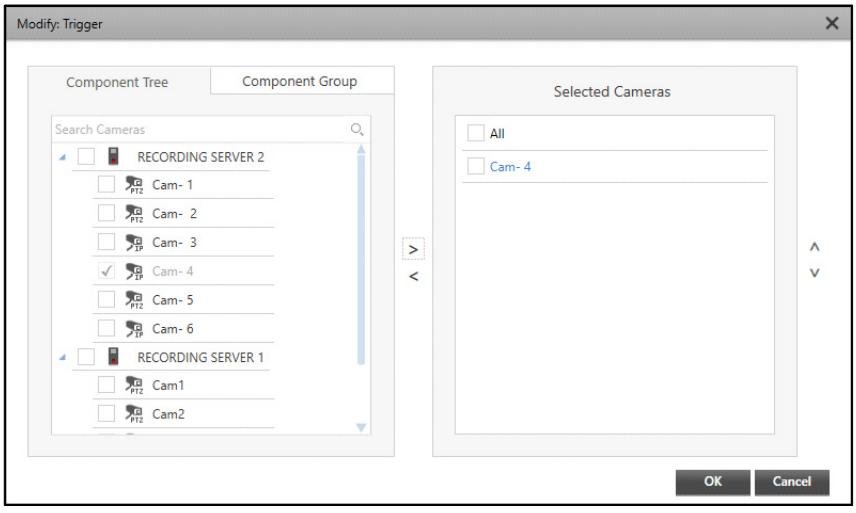
  - Click **Modify Alarm** . The **Modify: Alarm Name** pop-up appears.



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”.

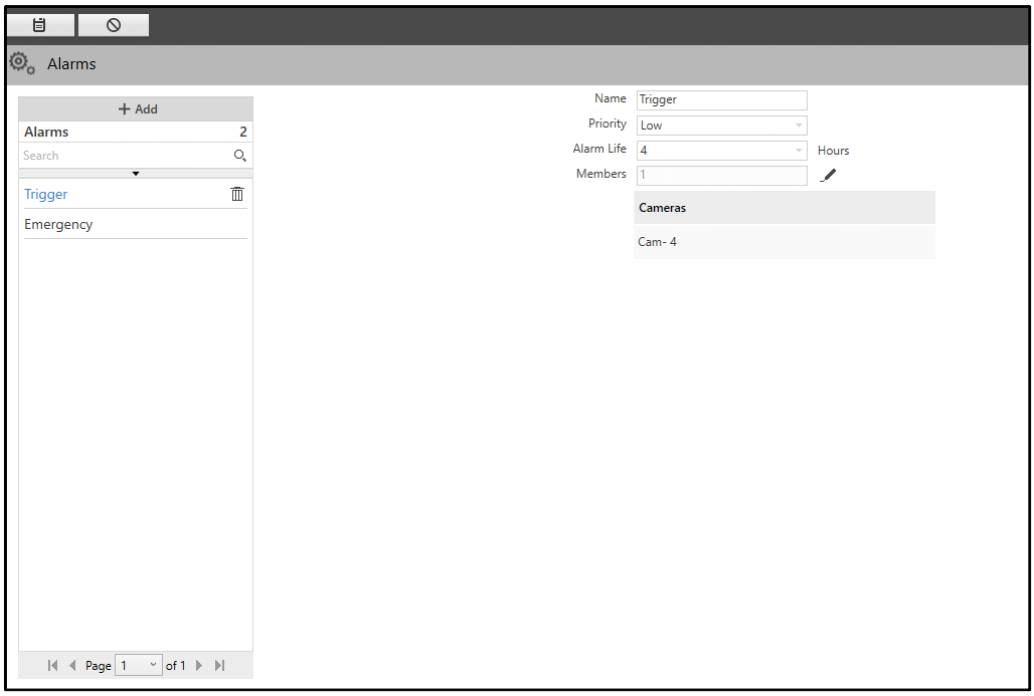
- Select the check boxes of the desired cameras you wish to assign to the alarm from the Component Tree or Component Group tabs. Click the right arrow button to add those cameras in the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

- To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the S**elected Cameras** list. You can change the sequence of the cameras in the Selected Cameras list using the up/down arrow buttons.



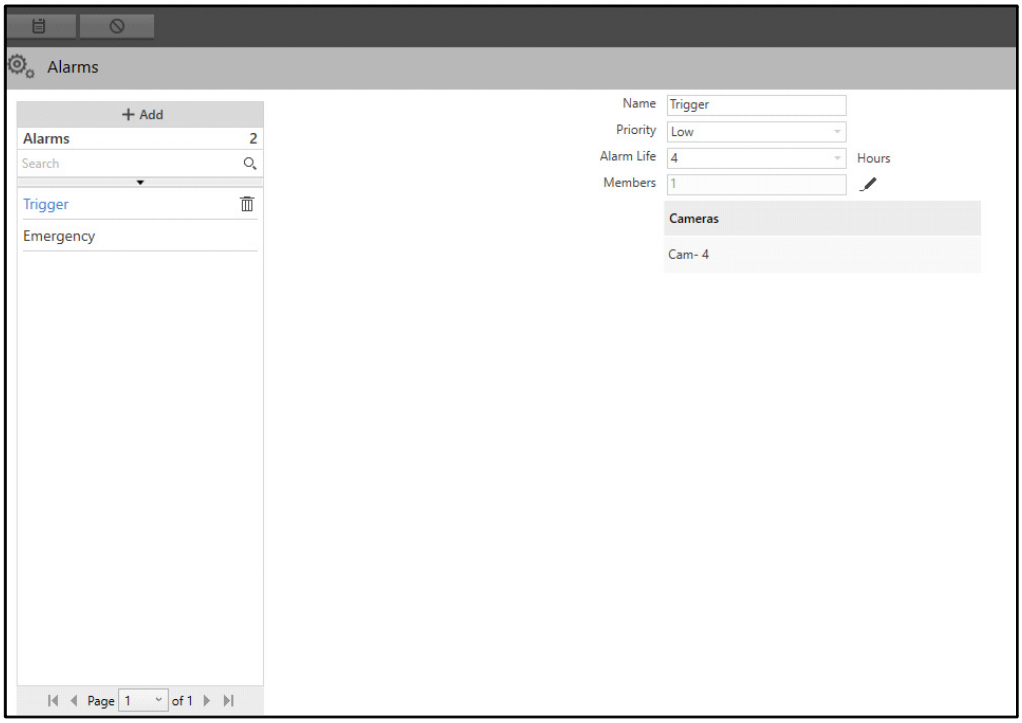
- Click **OK** to confirm or click **Cancel** to discard.

  The list of cameras assigned to the alarm appear in a list.



- Click **Save** to save the settings or **Cancel** to discard.

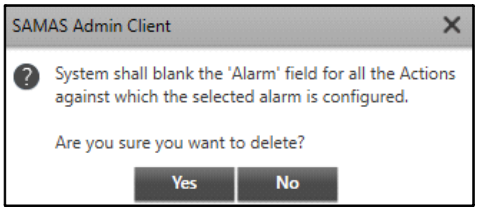
The new alarm appears in the list on the left hand side. You can also change the configurations of the alarm or delete it.



- Select the desired alarm from the list and edit the configurations on the right hand side.

- Click **Save** to save the settings or **Cancel** to discard.

- Click **Delete** to delete the desired alarm. The following pop-up appears.



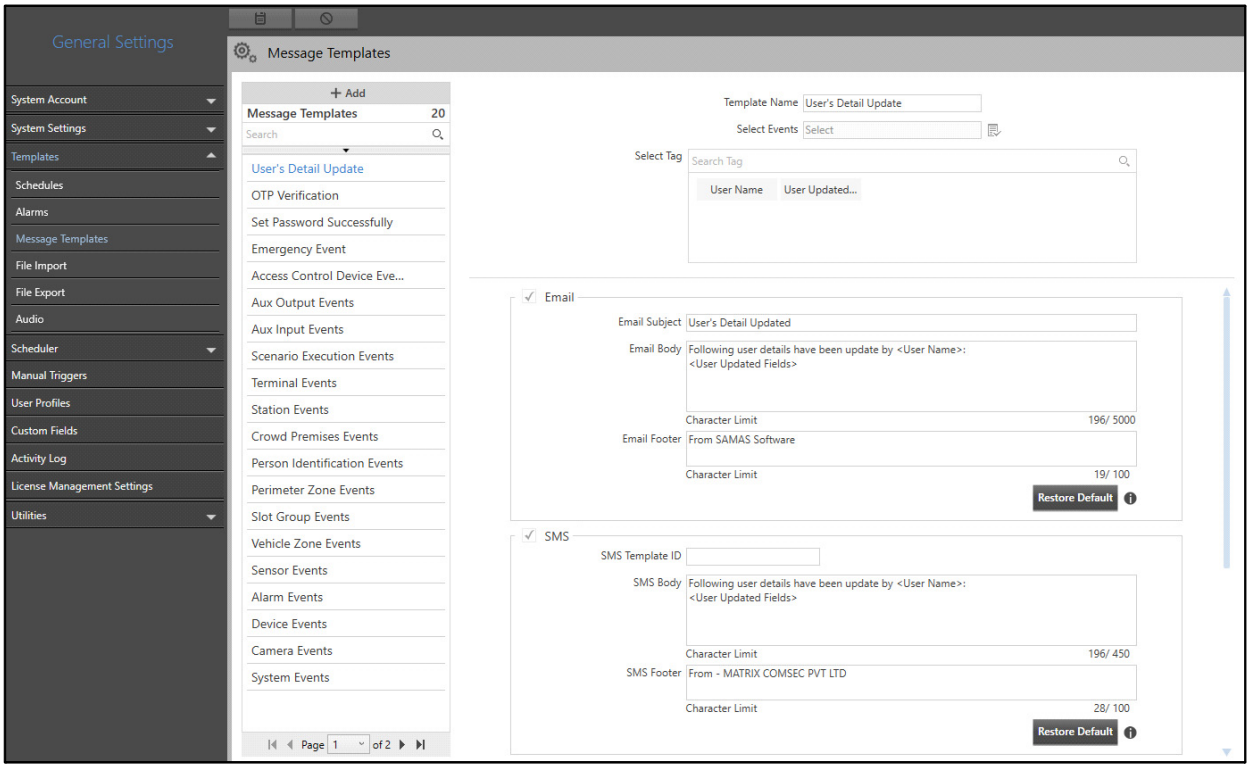
- Click **Yes** to confirm or click **No** to discard.

Message Templates

The Message Templates page displays the default as well as configured Message Templates — Email, SMS, WhatsApp. These templates can be assigned as an action (Send Email, Send SMS or Send WhatsApp Message) for Events (For example, Camera Tampered) when configuring various Scenarios. You can view and configure Message Templates for specific Events from this page.

To configure Message Templates,

- Click **General Settings > Templates > Message Templates**.



The following pre-defined Default Templates with selected associated Events and default configurations are:

- System Events
- Camera Events
- Device Events
- Alarm Events
- Sensor Events
- Vehicle Zone Events
- Slot Group Events
- Perimeter Zone Events
- Person Identification Events
- Crowd Premises Events
- Station Events
- Terminal Events
- Scenario Execution Events
- Aux Input Events
- Aux Output Events
- Access Control Device Events

- Manual Trigger Events
- Emergency Events
- Custom Events
- Set Password Successfully
- OTP Verification
- User's Detail Update



If any of the Default templates supported till Software Version V6R1 are configured against any actions and you upgrade SAMAS to V6R2 or later, then these templates will be visible as Custom templates.

If any template configured in versions earlier than V6R2 are configured against any actions and you upgrade SAMAS to V6R2 or later, then all the Events will be selected in these templates.

If you are upgrading to Software Version V6R2 or later:
- *in all the Default Templates, the WhatsApp section will be visible with default values.*
- *in all the configured Custom Templates, the WhatsApp section will be visible with blank values and the WhatsApp check box will be disabled.*

If you have assigned any template in a scenario and later on this template is deleted/name of the template is changed/Event type is changed, then this template automatically will be replaced with the Default template in all the configured scenarios.

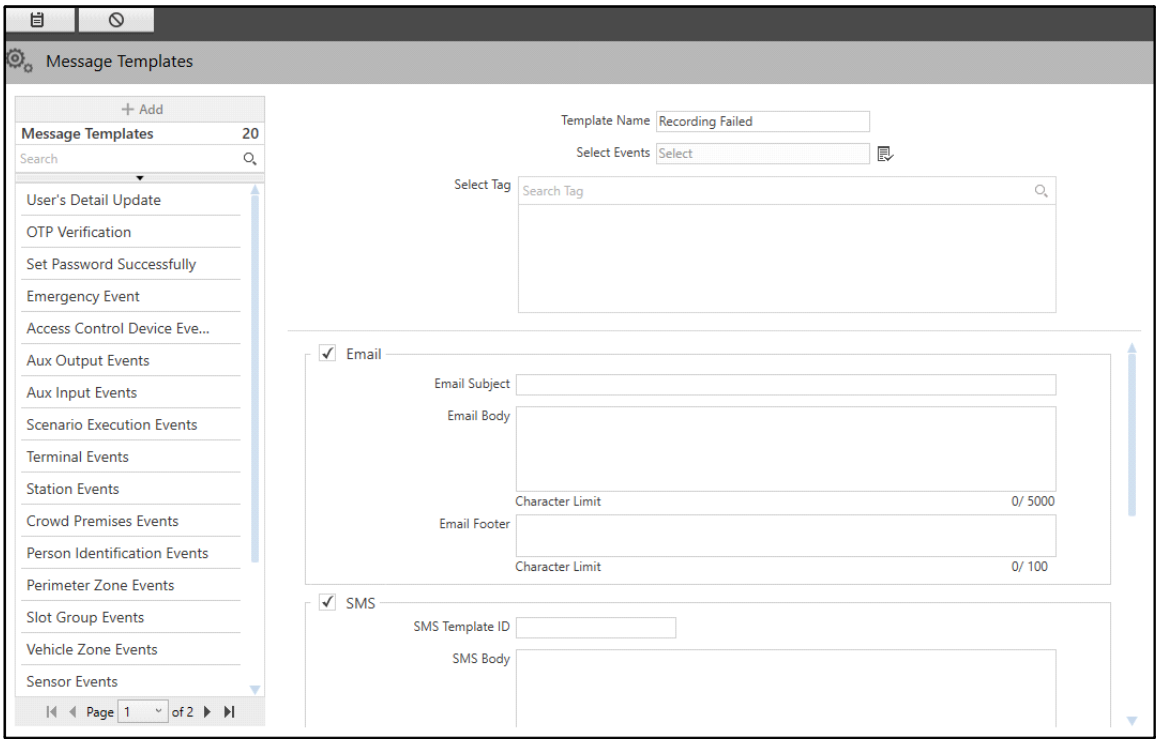
All the SMS Templates - Default as well as Custom must be registered with the desired Service Providers to enable sending the SMS. If any modifications are done in the template after registration, then the same needs to be registered again.

If you have multiple Service Providers, then make sure the required templates are registered with all the desired Service Providers. Hence for each template you will have multiple Templates IDs. Also make sure you maintain a record of all the registered Message Templates with their respective Template IDs for reference.

These pre-defined Default templates can be edited but cannot be deleted. If you wish to restore the default configuration in a Default template, click **Restore Default** under the desired section — Email/SMS/WhatsApp to restore the default configuration for that section. The configuration for the template will be restored to default.

You can also create Custom Message Templates. If the Custom template has been assigned as an action for an event and then the same is deleted/name of the template is changed/Event type is changed, then the **Default** template will be assigned in the configured scenarios automatically. To create a Custom template,

- Click **Add**.

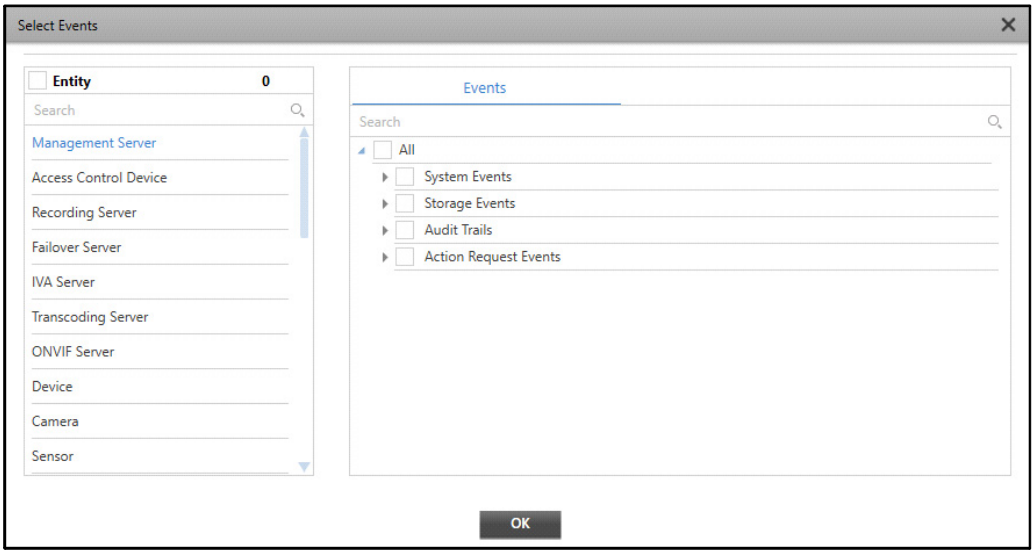


Configure the following parameters:

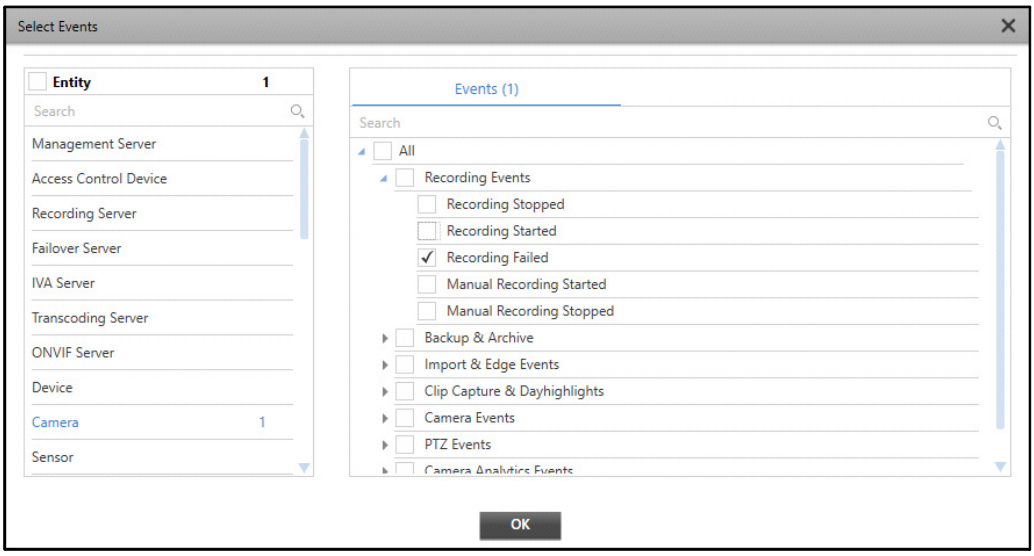
- **Template Name**: Specify a suitable name for the template. For example, Recording Failed. In Template Name, you can enter upto 50 characters. Default: Blank.

- **Select Events**: Select the desired Events for which you wish to create the Template. You can select this template when configuring actions in the desired Scenario for the same Event for which you have created the template. For details, refer to “Scenario Events With Actions”.

  - Click **Select Events** picklist. The **Select Events** pop-up appears.



- Select the desired Entity whose Events you wish to select for the template from the list. The list of all Events for the selected Entity appears in a list on the right hand side. For example, if you select Camera, all the Events of Camera appear in a list under the **Events** tab on the right hand side.



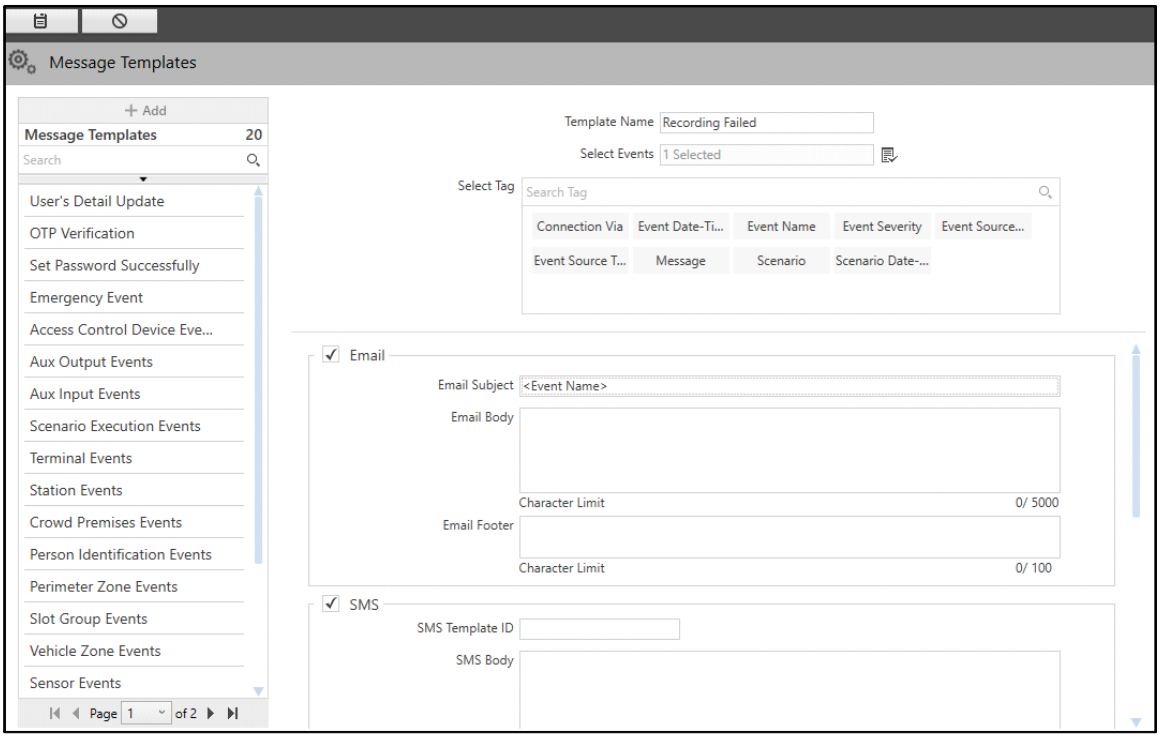
- Select the check boxes for the desired Events.
- Click **OK** to save the settings.

- **Select Tag**: The Tags appear according to the selected Event. You can add these tags to — Email Subject, Email/SMS/WhatsApp Body or Email/SMS/WhatsApp Footer.

  To select a tag,

  - Click the desired field— Subject, Body or Footer— and click on the tags that you wish to include in the Email Subject, Email/SMS/WhatsApp Body or Email/SMS/WhatsApp Footer.

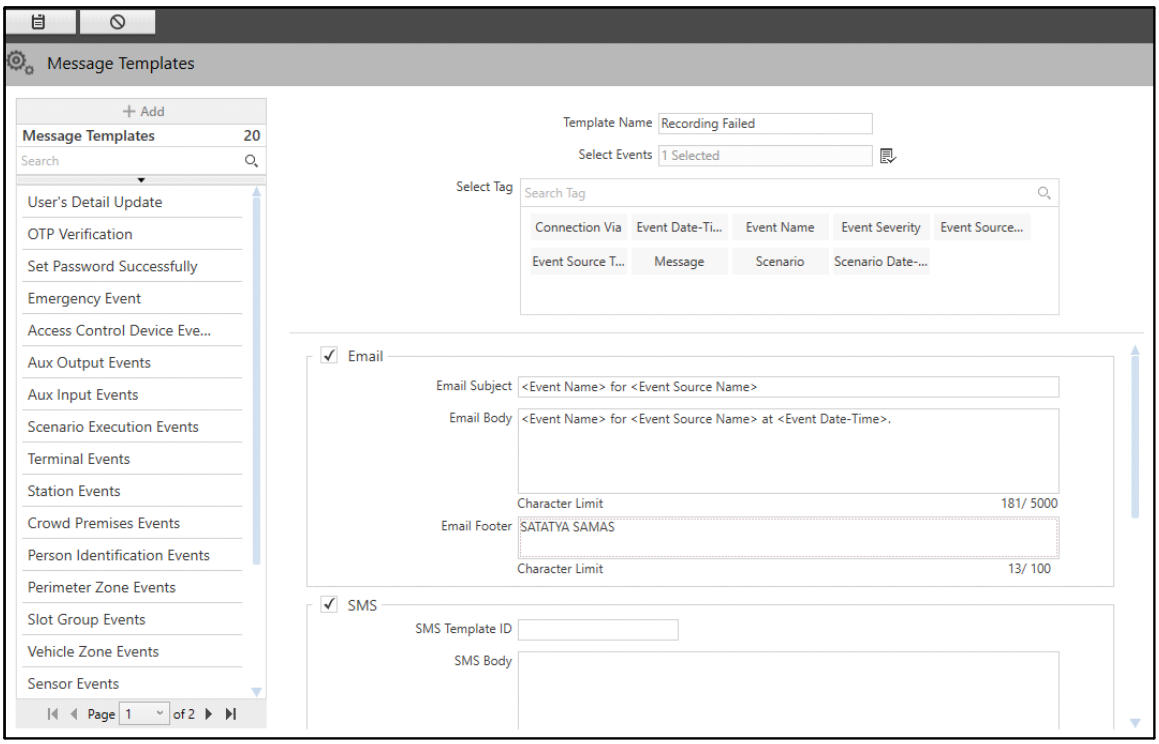
  For Example, you wish to add a tag to the Email Subject. Click the **Email Subject** text box and then click the desired tag.



The tag will appear in the Email Subject. Similarly, you can add other tags in the desired fields.

The Message Template page contains three sections — “Email”, “SMS” and “WhatsApp”.

Email



- **Email:** Select the check box to enable the Email Template configuration.

- **Email Subject:** Specify a suitable Email Subject. The tags can also be added when composing the Email Subject. In Email Subject, you can enter upto 100 characters. Default: Blank.

  If required, you can also search for the desired tags and then click on the appropriate tag to add the same along with the text.

- **Email Body:** Enter the desired text in the Email Body. The tags can also be added when composing the Email Body. In Email Body, you can enter upto 5000 characters. Default: Blank.

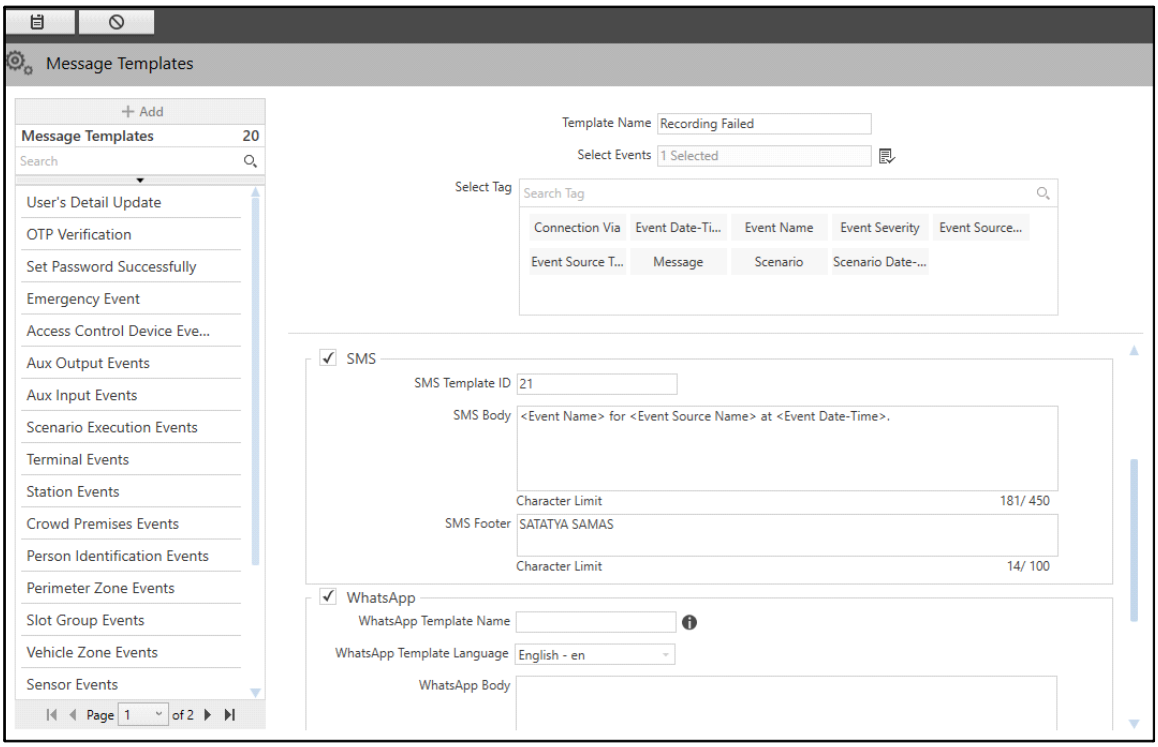
  If required, you can also search for the desired tags and then click on the appropriate tag to add the same along with the text.

- **Email Footer**: Enter the desired text in the Email Footer. The tags can also be added when composing the Email Footer. In Email Footer, you can enter upto 100 characters. Default: Blank.

  If required, you can also search for the desired tags and then click on the appropriate tag to add the same along with the text.

If any template configured in versions earlier than V6R2 are configured against any actions and you upgrade SAMAS to V6R2 or later, then the Email Footer will be visible with blank values.

SMS



- **SMS:** Select the check box to enable the SMS Template configuration.

- **SMS Template ID:** The SMS Template ID is provided by the Service Provider while registering the template. Make sure you enter the correct SMS Template ID as per the registered templates to ensure successful sending of the SMS. In SMS Template ID, you can enter upto 30 characters. Default: Blank.

If you have multiple Service Providers, then make sure the template is registered with all the desired Service Providers. Hence for each template you will have multiple Templates IDs. Also make sure you maintain a record of all the registered Message Templates with their respective Template IDs for reference.

- **SMS Body**: Enter the desired text in the SMS Body. The tags can also be added when composing the SMS Body. In SMS Body, you can enter upto 5000 characters. Default: Blank.

  If required, you can also search for the desired tags and then click on the appropriate tag to add the same along with the text.

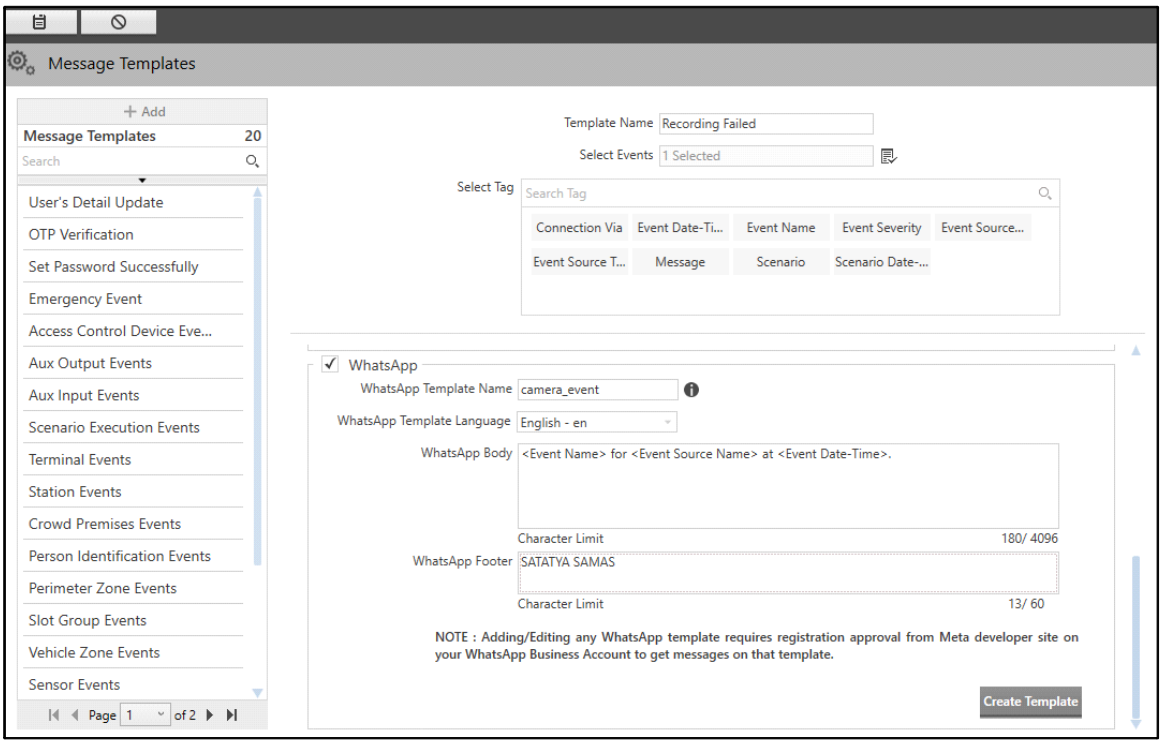
- **SMS Footer**: Enter the desired text in the SMS Footer. The tags can also be added when composing the SMS Footer. In SMS Footer, you can enter upto 100 characters. Default: Blank.

  If required, you can also search for the desired tags and then click on the appropriate tag to add the same along with the text.

If any template configured in versions earlier than V6R2 are configured against any actions and you upgrade SAMAS to V6R2 or later, then the SMS Footer will be visible with blank values.

WhatsApp

Make sure you have created your WhatsApp Business Account and configured the WhatsApp settings in the Notification Server. For details, refer to "WhatsApp Integration" and ***Configure Notification Server settings using the Notification Server Manager Utility*** in the ***SATATYA SAMAS Installation Guide***.



- **WhatsApp:** Select the check box to enable the WhatsApp Template configuration.

- **WhatsApp Template Name**: Enter the desired WhatsApp Template Name for the Template. When you add the template to your WhatsApp Business Account then this name will be displayed in the WhatsApp Business Account. Make sure you have checked the contents of the template before the same are added

to your WhatsApp Business Account. In WhatsApp Template Name, you can enter upto 512 characters. Default: Blank.



If you edit a default Message Template, the default WhatsApp Template Name assigned to selected Message template is displayed. You can change the same if required.

- **WhatsApp Template Language**: Select the desired language in which you wish to send the WhatsApp message. When you add the template to your WhatsApp Business Account it will be added in the selected language.

- **WhatsApp Body**: Enter the desired text in the WhatsApp Body. The tags can also be added when composing the WhatsApp Body. In WhatsApp Body, you can enter upto 4096 characters. Default: Blank.

  If required, you can also search for the desired tags and then click on the appropriate tag to add the same along with the text.

- **WhatsApp Footer**: Enter the desired text in the WhatsApp Footer. In WhatsApp Footer, you can enter upto 60 characters. Valid Values: A-Z a-z 0-9 -_. ()@,!$ *+[]/\:# <space>. Default: Blank. Invalid Values will lead to failure of template creation.

  The tags can also be added when composing the WhatsApp Footer. If required, you can also search for the desired tags and then click on the appropriate tag to add the same along with the text.

- Click **Create Template** if you wish to add this template in your WhatsApp Business Account.



*Make sure you have visited their official website:**https://developers.facebook.com** and read the guidelines provided for the Templates.*

Before you add any template to your WhatsApp Business Account make sure:

- *you have updated/edited the templates as per your requirement. If you have sent the template/s to your WhatsApp Account and then modify the same, you will have to manually update/edit/delete the templates from your WhatsApp Account. For smooth functioning of WhatsApp, make sure the content of the WhatsApp Templates in Message Templates and the WhatsApp Templates in your WhatsApp Account are identical.*

- *you do not have any template/s with the same name/s already created in your WhatsApp Account. If same name template/s are found in your WhatsApp Account and you select the same here, then these templates will not be sent to your WhatsApp Account.*

- *you have checked the WhatsApp Busines Policy. As per the WhatsApp Business Policy, you can create 100 templates per hour. The policies are frequently updated, hence refer to the policy details once before you move further.*

- The **Create Template** pop-up appears, with the message "**Would you like to create a WhatsApp template with an image attachment support?**"

- Click **Yes/No** as per your requirement. The message "**Your template creation request has been submitted successfully. Please check your Meta account for more details on the template status.**" appears.

Make sure you click Yes/No cautiously as,

- *If you click **Yes**, make sure you select the **Attach Snapshot** check box in the Action - "Send WhatsApp Message". If Snapshot is not enabled then a dummy image will be sent in the WhatsApp Message.*
- *If you click **No** and have selected the **Attach Snapshot** check box in Action - "Send WhatsApp Message", then the WhatsApp Message will be sent without any image.*

The names of the WhatsApp Templates in your WhatsApp Business Account appear as configured in Message Templates. The Templates will be added to your WhatsApp Business Account in the language that you have selected in Message Template.

The WhatsApp Templates created in your WhatsApp Business Account are created with category as Utility. We recommend you not to change the category for smooth functioning of this feature.

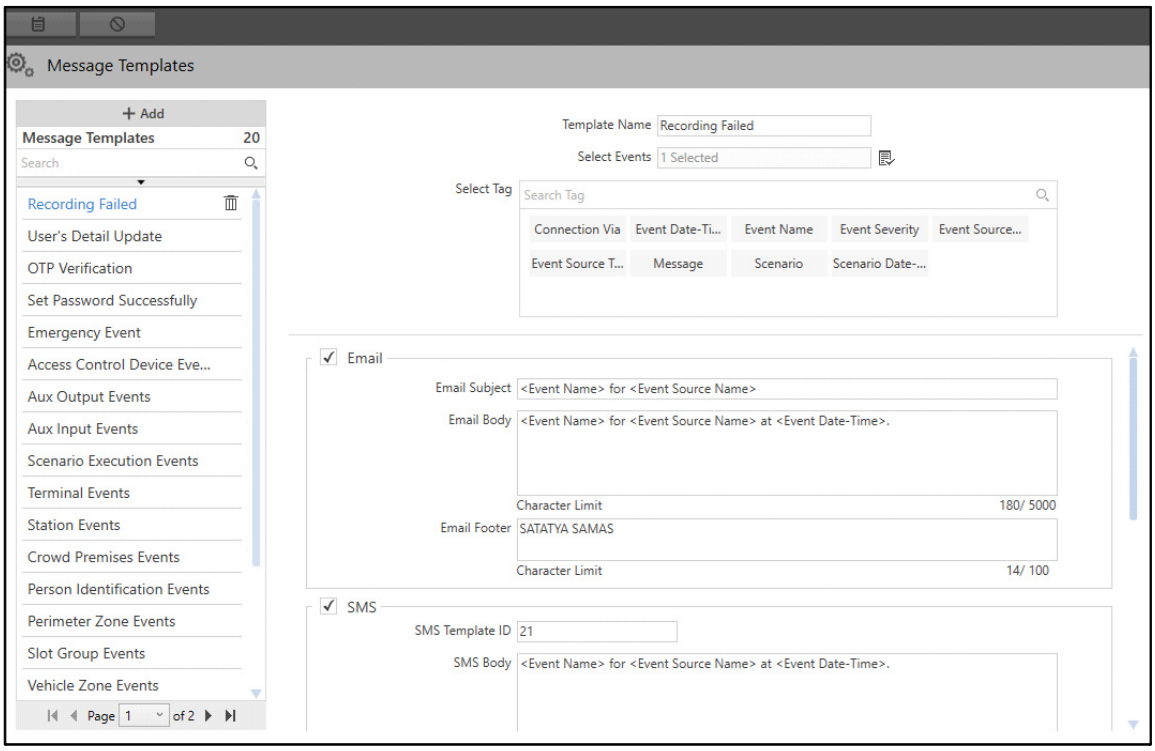
After the Templates are sent to your WhatsApp Business Account, Alerts will be sent only after these templates are approved by WhatsApp.

Since WhatsApp does not support AVI format for videos, videos cannot be sent through WhatsApp Message Templates.

- Click **Restore Default**, if you wish to assign default values to the parameters of the Template.
- Click **Save** to save the settings or **Cancel** to discard.

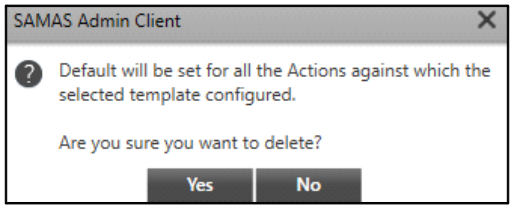
The new Message Template appears in the list on the left hand side.

You can also change the configurations of the template or delete it.



- Select the desired template from the list and edit the configurations on the right hand side.

- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired template. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

You can later assign the template in the Actions — Send Email, Send SMS or Send WhatsApp Message— when configuring the Scenario. The Email/SMS/WhatsApp notification will be sent on the Event occurrence as per the configured Action. For details, refer to “Scenario Events With Actions”.

Notification Server Logs

The logs for success or failure on sending Email/SMS/WhatsApp will be displayed in Notification Server Log.

To access the Notification Server Log,

- Right-click on the **Notification Server Manager** icon in the Tray.
- Select **Server Log** from the menu options.
- Enter the **User Name** and **Password** (same as your login credentials).
- The **Notification Server Log** pop-up window appears.
- Click the desired tab — Email, SMS, WhatsApp.
- Set the filters as per your requirement and click **Search**.
- The logs appear as per the set filter.

This is a sample Email Notification based on a template configured for Email.

From: Administrator
Subject: Recording Failed - QAPC-2
To: xyz@abc.com

ATTENTION USER!

Recording Failed at QAPC-2 on 28-Aug-2022 13:45:07.

- Matrix Team

WhatsApp Integration

In today's world as we move ahead with technology, WhatsApp has become an integral part of businesses and hence its integration with SAMAS is the need of the hour.

Integrating WhatsApp with SAMAS will enable you to send alerts on user's WhatsApp Numbers for different SAMAS Events.

To integrate WhatsApp with SAMAS, you need to follow the steps in the sequence mentioned below:

1. Create a WhatsApp Business Account. Refer to "Pre-requisites".

2. Configure the Mobile Numbers of Users, refer to "Users" for details. You can also send WhatsApp Message to Mobile Numbers which are not configured in SAMAS. These numbers can directly be configured in the "Send WhatsApp Message" action. It is mandatory that WhatsApp must be activated on the Mobile Number to receive WhatsApp Messages.

   If the registered WhatsApp mobile number and the mobile numbers to which WhatsApp Messages need to be sent are in different countries, make sure you configure the country code along with those mobile numbers (to whom the Alerts are to be sent). If the registered WhatsApp mobile number is in India (country calling code 91) but the Alerts need to be sent to number outside India, then make sure the number is configured with the country code, for example country code of the mobile number on which alert is to be sent is 1 and mobile number is 631555XXXX, then the mobile number needs to be configured as 1631555XXXX. For more details refer to ***https://developers.facebook.com/docs/whatapp/cloud-api/reference/phone-number***

3. Enable WhatsApp as well as configure the desired template parameters as per your requirement, refer to "WhatsApp" in "Message Templates" for details.

4. Add a Test Message Template manually in your WhatsApp Business Account For details, refer to "Test Message Template Creation".

5. Configure the WhatsApp parameters, refer to ***Configure Notification Server settings using the Notification Server Manager Utility*** in the ***SATATYA SAMAS Installation Guide*** for details. The WhatsApp Configuration details can be viewed from the System Report. For details, refer to "System Report".

6. Configured the "Basic Scenario" or "Advanced Scenario" as required for the desired Events. Make sure you have assigned the "Event Monitoring Rights" for these Events. For the Basic/Advanced Scenario, you must configure the "Send WhatsApp Message" action to be notified about the desired Event. For details, refer to "Configuring Actions for Events".

7. To view the details of the Alerts sent via WhatsApp, refer to "Event Log".

8. To view the details of the WhatsApp Messages sent from the Notification Server, refer to "Notification Server Logs".

Pre-requisites

To use WhatsApp for sending messages make sure you have completed the following:

Make sure you have persistent Internet connectivity.

The details mentioned below are as per the updates (Sept 2024) available on the official website of Meta.These are subject to change. To know more visit their official website: ***https://developers.facebook.com.***

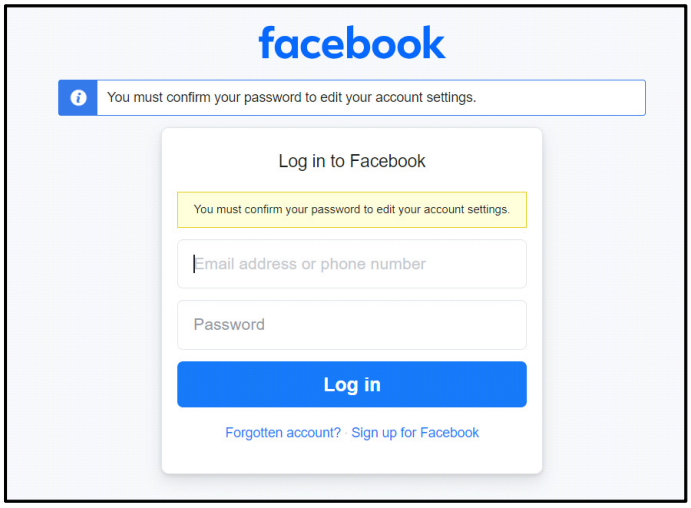
- Registered as a Meta Developer, refer to “Register as a Meta (Facebook) Developer”.
- Enabled Two- Factor Authentication for your account, refer to “Enable Two-Factor Authentication”.
- Created a Meta App, refer to “Create an App”.
- Added a Phone Number in the Meta App, refer to “Add a Phone Number”.
- Made the payment as per your requirement, refer to “Add Payment Method”.
- Created a Permanent Token for usage, refer to “Creating a Permanent Access Token”.

Register as a Meta (Facebook) Developer

To register as a Meta Developer, following the steps given below:

- To start the registration process

  Login into your Facebook Account.



Make sure your Facebook Account is Meta verified and complies to all the Terms and Conditions of Meta. To do so, access your Facebook Account Setting & privacy > Meta Account Center > Meta Verified. Make sure you follow the instructions and fulfill all the necessary Meta requirements for the same.

- Agree to the Terms and Policies.

  Click **Next** to agree to the Platform Terms and Developer Policies.

- Verify your account

  A confirmation code will be send to the phone number and email address that you provide in order to confirm that you have access to them. Your number and email will be used for important developer notifications of any changes that may impact your app.

- Select your occupation

  Select an occupation that most closely describes what you do for a living.

  The registration process is completed.

Enable Two-Factor Authentication

Two-factor authentication is a security feature that helps protect your Facebook account in addition to your password. If you set up two-factor authentication, you will be asked to enter a special login code or confirm your login attempt each time someone tries accessing Facebook from a browser or mobile device that Facebook does not recognize. You can also get alerts when someone tries logging in from a browser or mobile device that Facebook does not recognize.

Turning-on/managing two-factor authentication:

- Go to your **Security and Login Settings**.
- Scroll down to **Use two-factor authentication** and click **Edit**.
- Choose the any one of the three security method that you wish to add and follow the on-screen instructions.
  - Tapping your security key on a compatible device.
  - Login codes from a third-party authentication app.
  - Text Message (SMS) codes from your mobile phone.

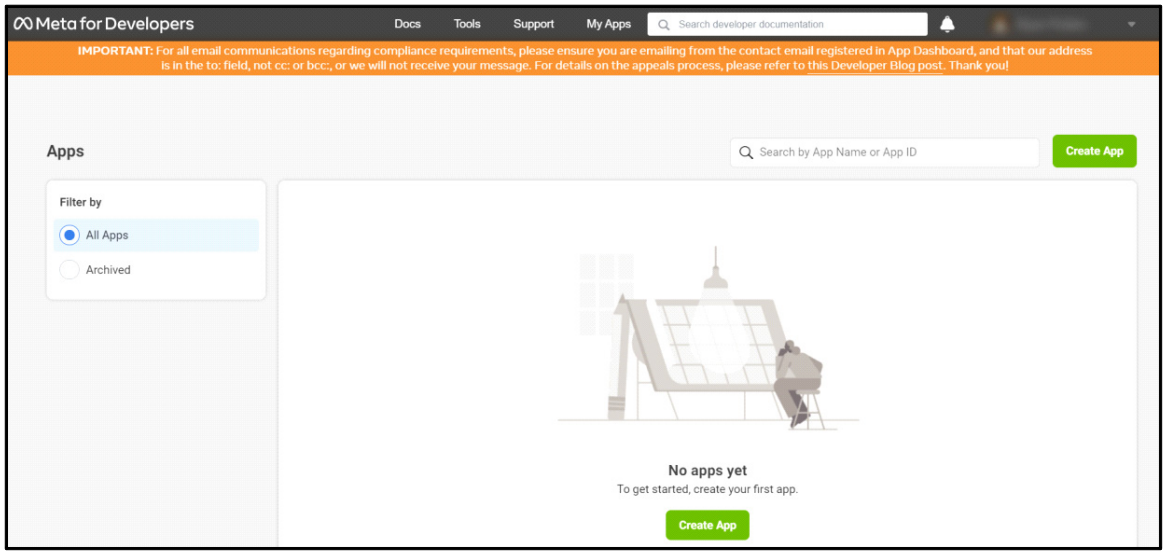
Create an App



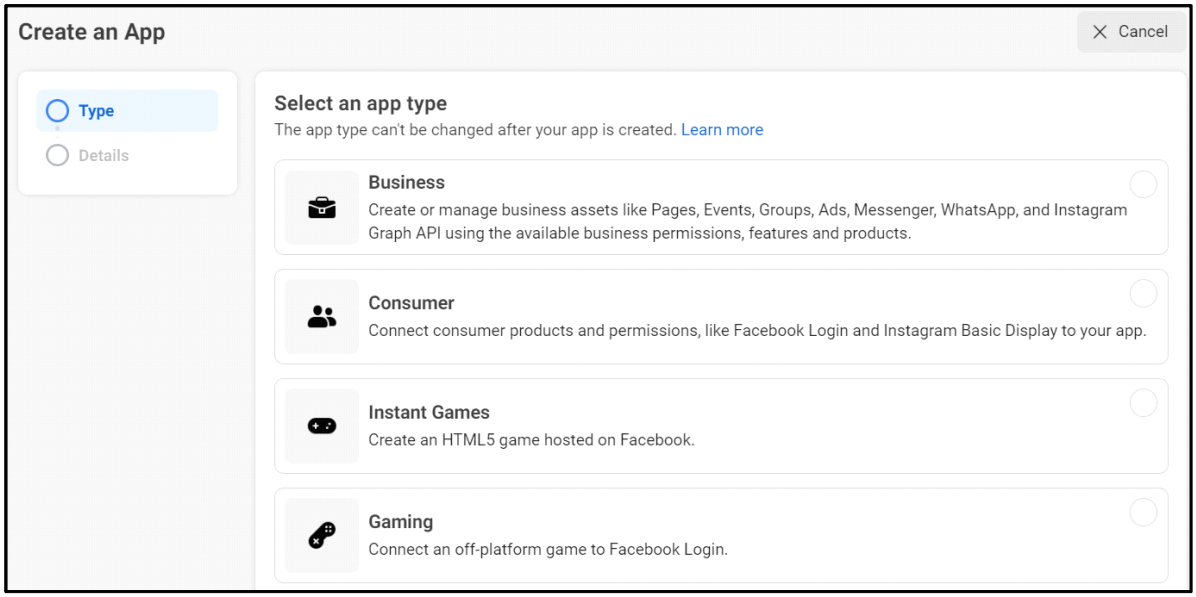
Making sure you have a developer account on Meta for Developers. You also need WhatsApp installed on a mobile device to send test message.

To create the App, following the steps mentioned below:

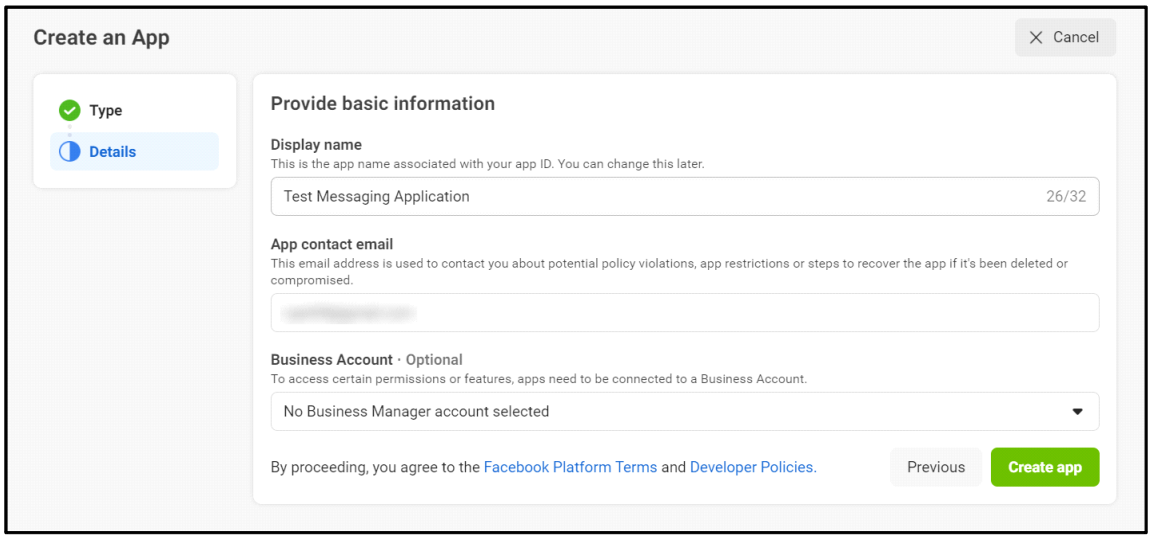
- Once you are signed in, you see the Meta for Developers App Dashboard. Click **Create App** to get started.



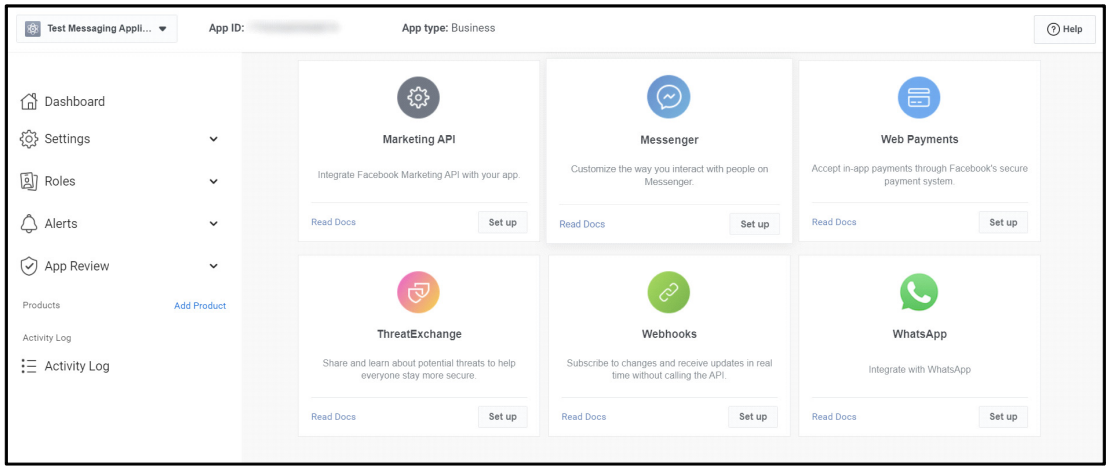
- Select **Business** as the **App Type**.



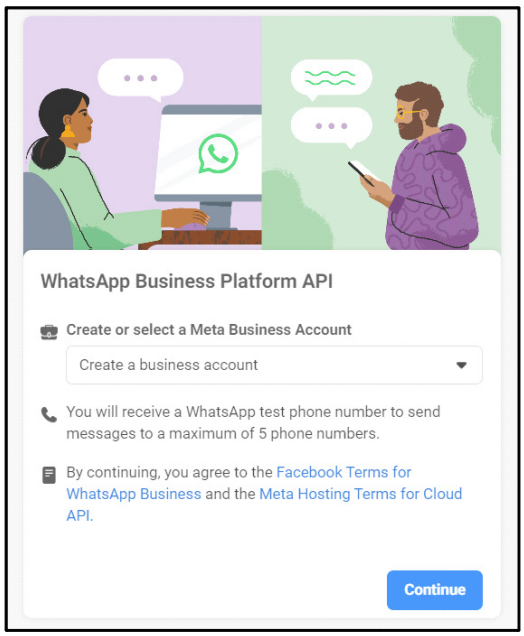
- Enter the **Display Name** for your App and an **Email Address** where you wish to receive any important developer notifications. The email address can be different from the email address associated with your Facebook account, just make sure it is valid and that you monitor it, since all important developer notifications will be sent there.



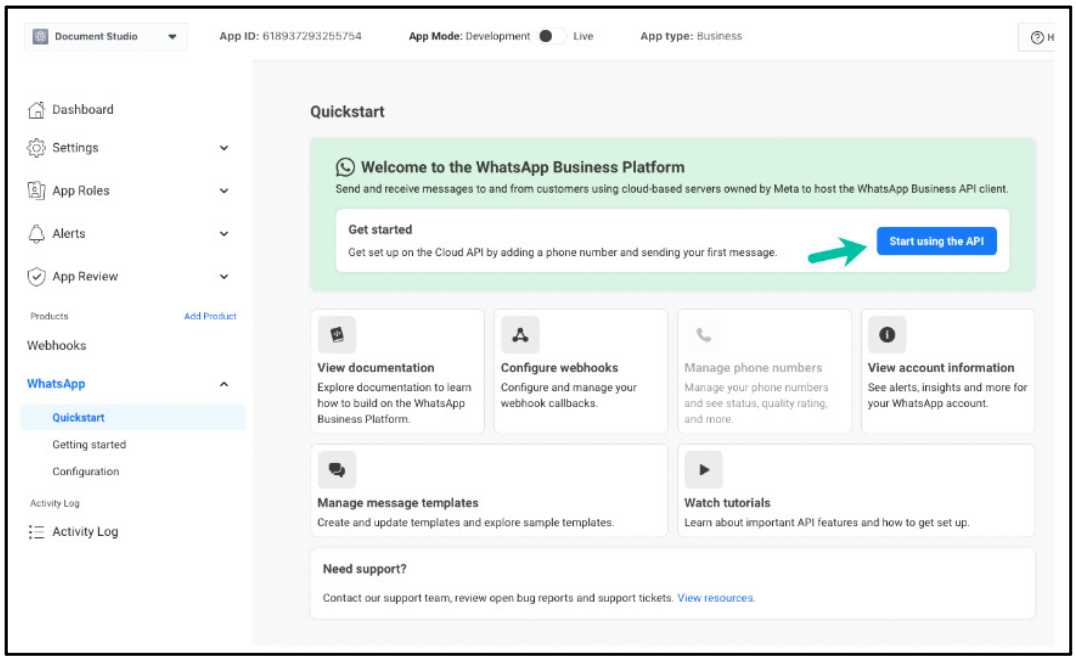
- You need to add products to your App. Scroll down until you see **WhatsApp** and click the **Set up**.



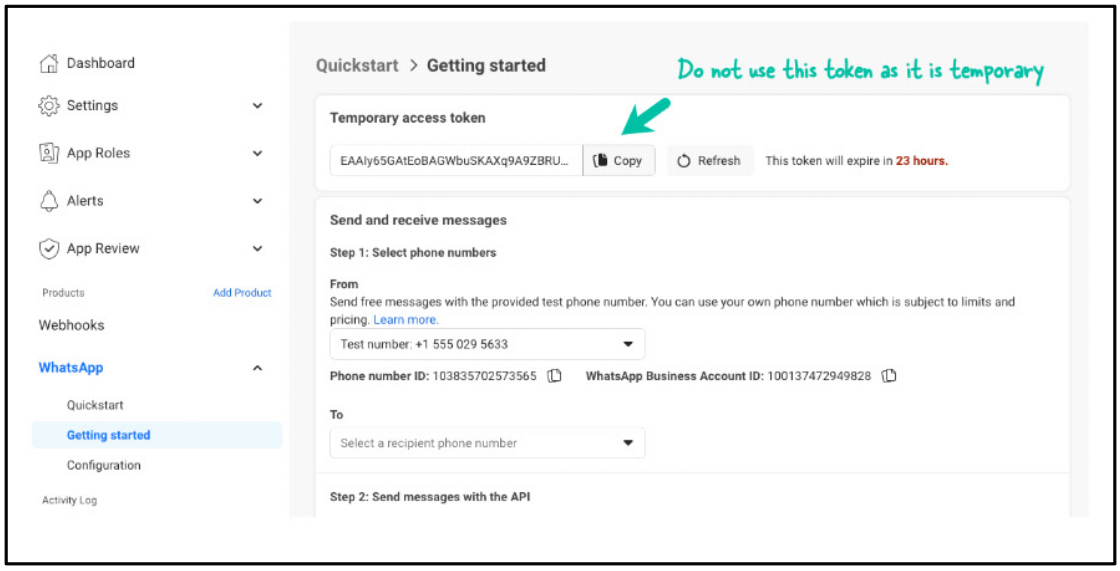
- Finally, choose an existing Meta Business Account or ask the platform to create a new one and click **Continue.**



- Click on **Start using the API** on the next screen.



Facebook will now generate a temporary access token that allows you to test your WhatsApp Cloud API integration. However, we will not use this token since it expires after 24 hours. So instead, we will generate a permanent access token. For details, refer to “Creating a Permanent Access Token”.

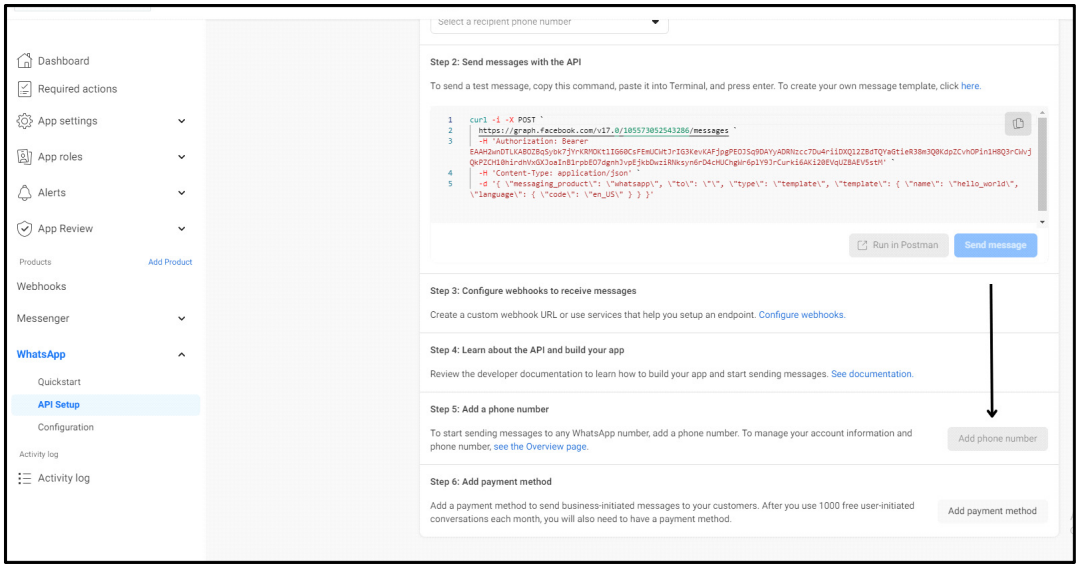


Send a message with the test number generated by WhatsApp to your Business WhatsApp number to test if your integration is a success.

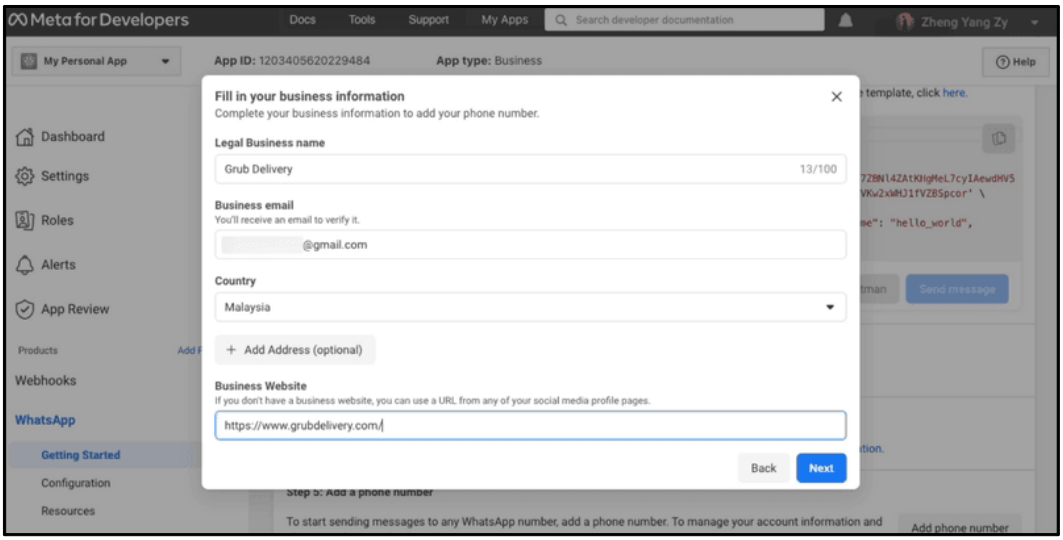
Next, you need to add your phone number to your WhatsApp Cloud API account.

Add a Phone Number

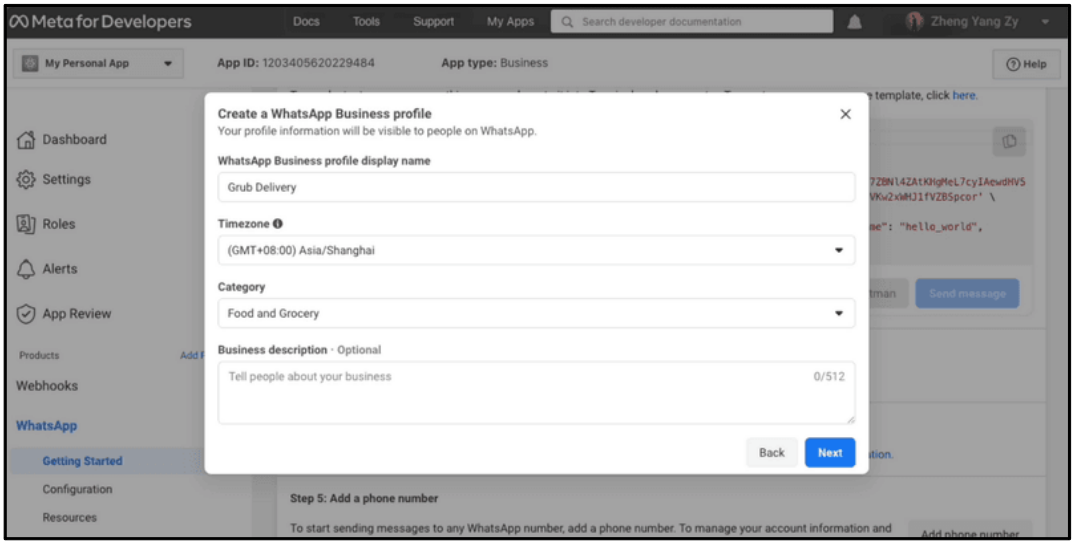
- Scroll down on the page and click **Add phone number**. You need to associate a phone number with the WhatsApp API to send messages to any WhatsApp number.



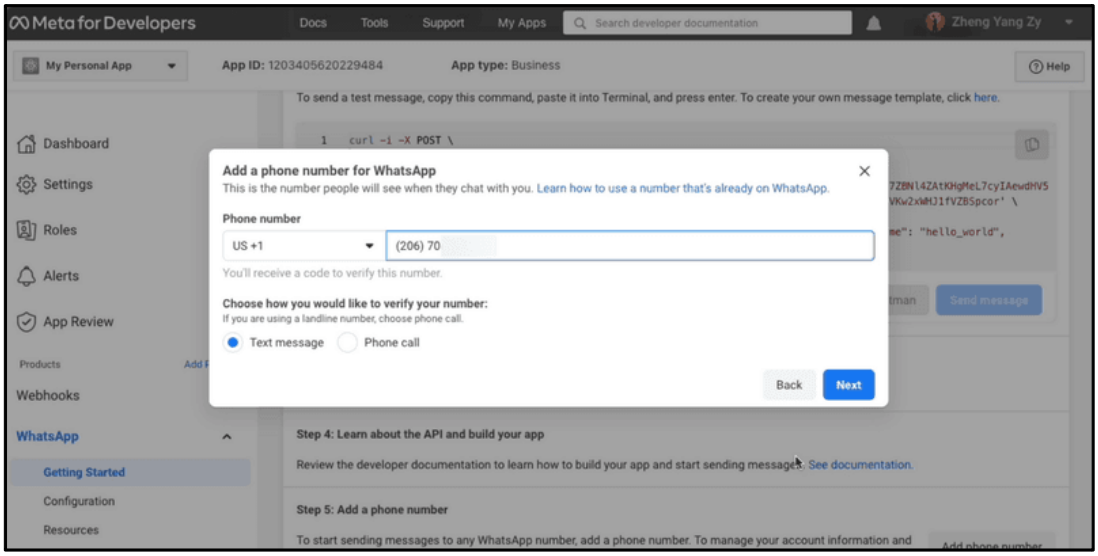
- Fill in your business information and click **Next**.



- Fill in your WhatsApp Business profile information and click **Next**.



- Add a phone number for your WhatsApp Cloud API.

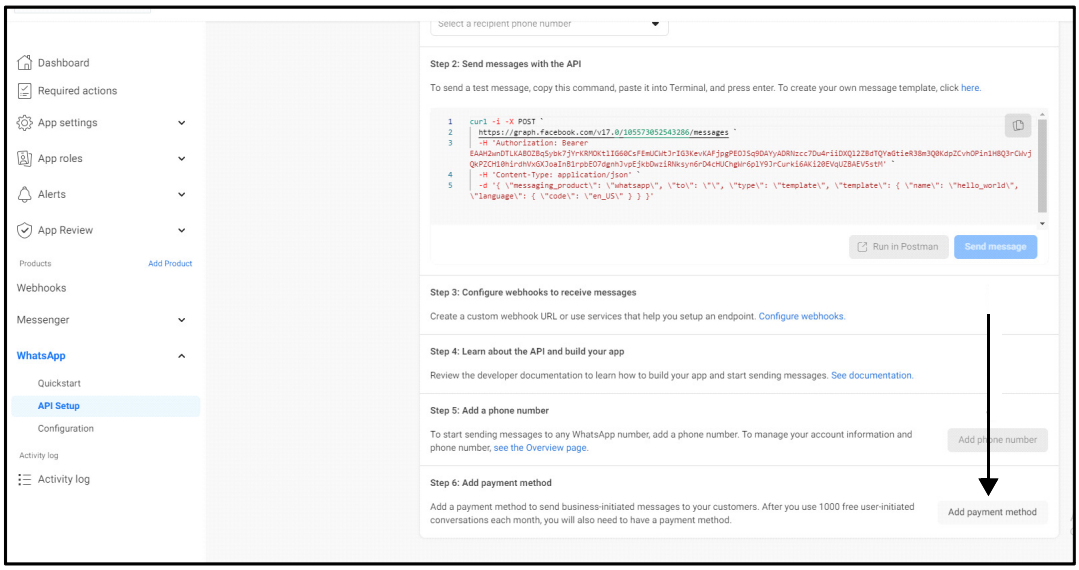


Make sure that when you are adding a number it is a new number and has never been used in WhatsApp.

- To verify the phone number you added, a 6-digit verification code will be sent to the number. Enter the verification code once you receive it.

Add Payment Method

- Click **Add payment method**.



Follow the steps and complete the payment.

Next, copy and save the **WhatsApp Business Account ID** for this phone number.

Creating a Permanent Access Token

Knowing that you need to use a bearer token in the Authorization Header of an HTTP request is helpful, but it is not enough. The only access token you have seen so far is temporary. Chances are that you want your App to access the API for more than 24 hours, so you need to generate a longer-lasting access token.

The Meta for Developers platform makes this easy. All you need to do is add a System User to your business account to obtain an access token that you can use to continue accessing the API.

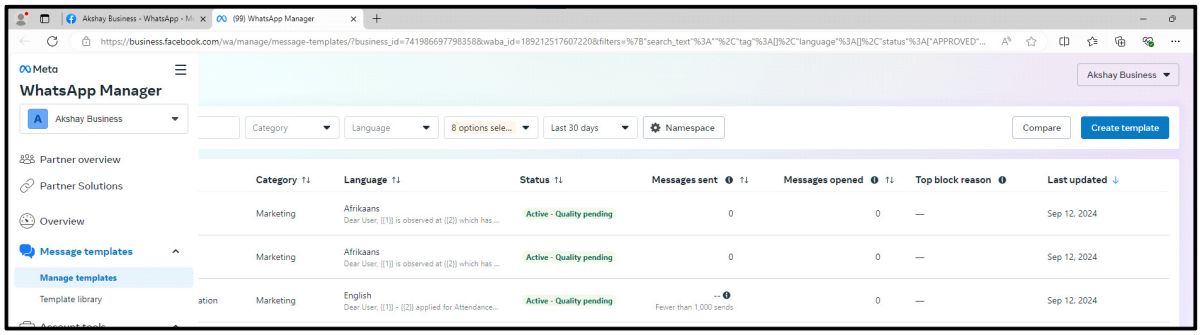
To create a system user, following the steps:

- Go to **Business Settings**.
- Select the business account your app is associated with.
- Select **Users > System Users**.
- Click **Add**.
- Configure a **Name** for the system user, choose **Admin** as the user role, and click **Create System User** to continue.
- Select the **whatsapp_business_messaging** and **whatsapp_business_management** permission.
- Click **Generate New Token** to generate a permanent access token.
- Please copy the access token and save it in your notepad as it will not be visible again on your Facebook Dashboard.

Test Message Template Creation

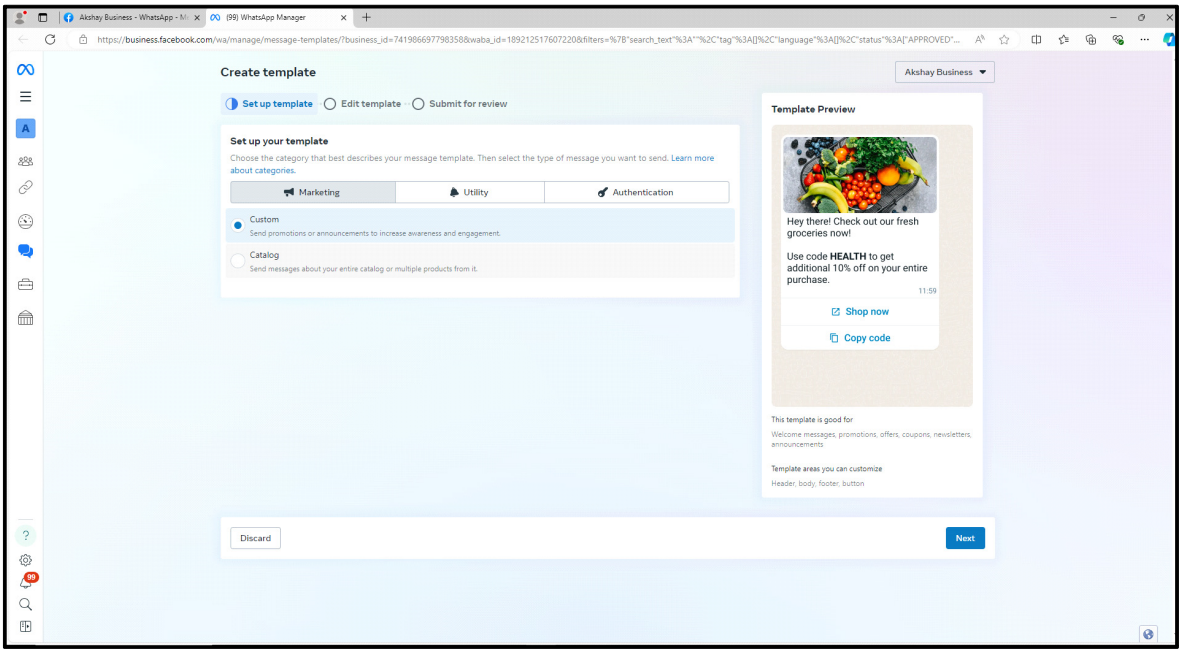
Step 1: Create a New Template

- Click **Create Template**:



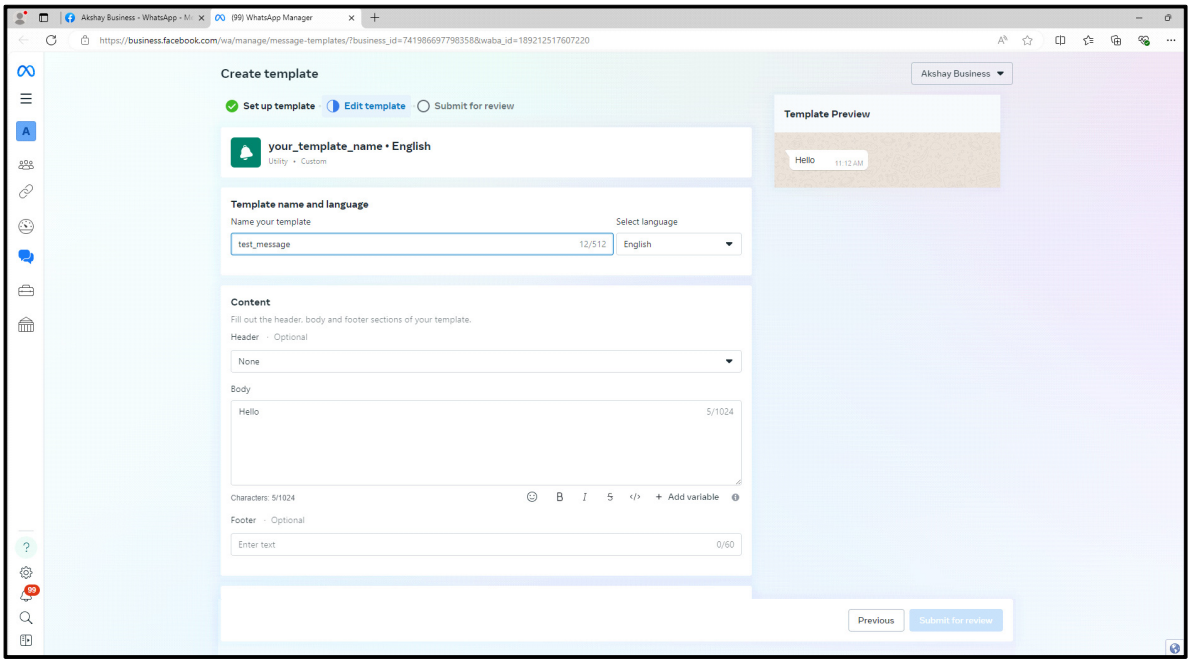
- In the **top-right corner**, you will see a button labeled **"Create Template."** Click on it to begin the template creation process.

- **Select a Category**:



  - **Selecting the Category**: For messages related to customer service or support.Recommended - Marketing / Utility.

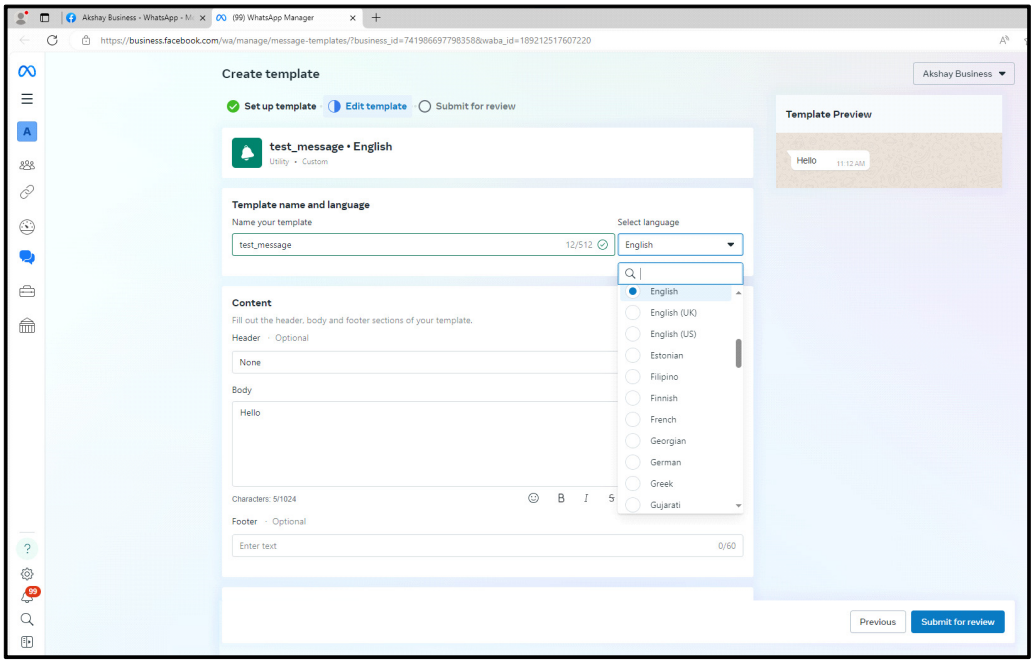
- **Name Your Template**:



  - Choose a **name** that makes it easy to identify the template's purpose. The name must:
    - Be all in **lowercase letters**.
    - Use **underscores (_) instead of spaces**.
      Example: test_message

Step 2: Define Template Content

- **Select Language**:

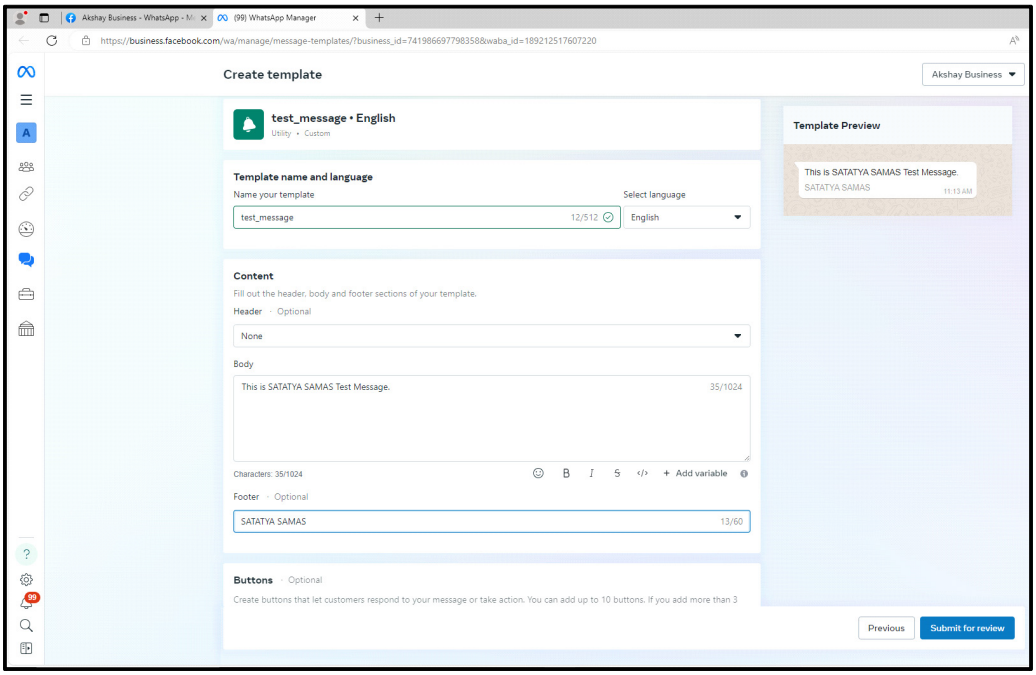


  - Choose the language for your template from the drop-down (e.g., **English**).

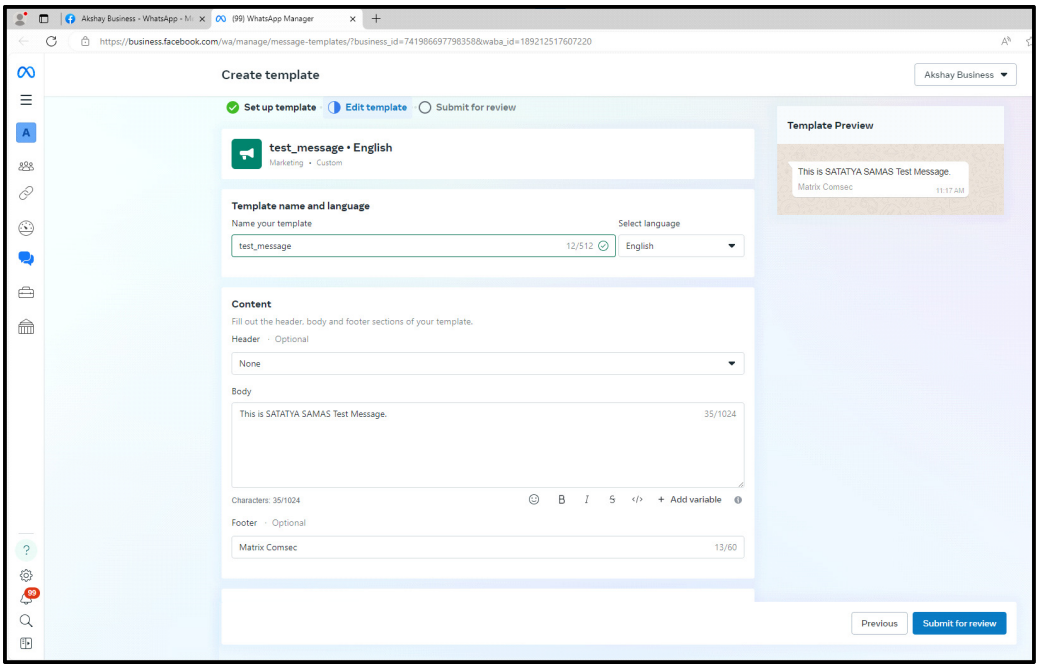
- **Choose Template Type**:

  - Since you're not using any variables, select **Standard**. This means the message will be the same for every recipient, without any placeholders.

- **Configure Template Components**:



- **Header (Optional)**:
  - Leave this blank.
- **Body**:
  - This is the main content of your message. Since you're not using variables, write a **static message** that will remain the same for all users.
  - Example: “This is SATATYA SAMAS Test Message”
- **Footer (Optional)**:



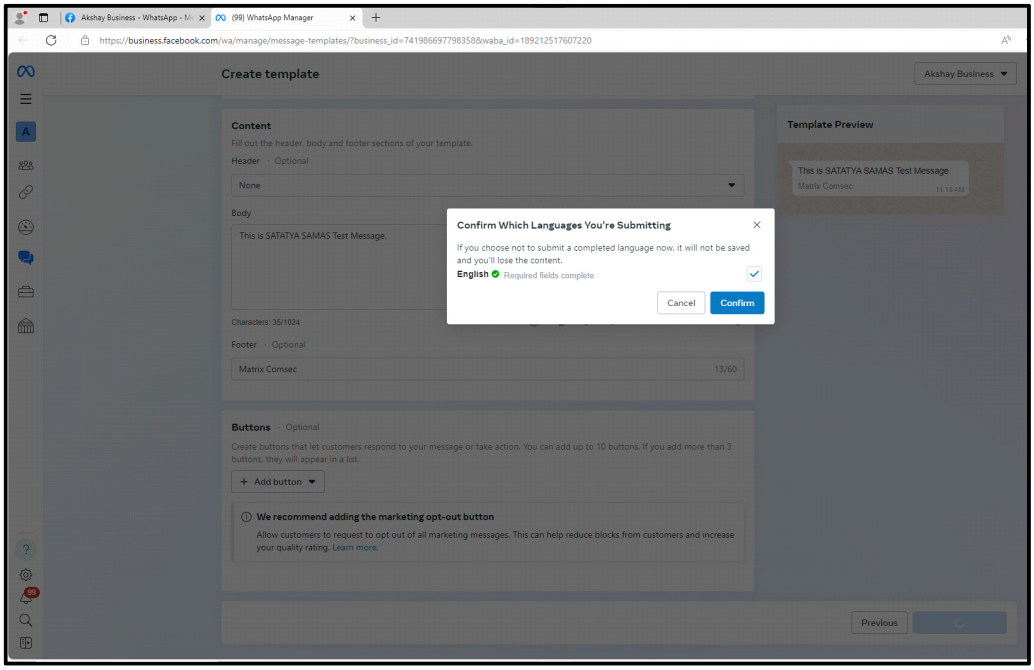
  - Add a short **footer** if needed. This could be additional info like terms of service or a support message.
- **Buttons (Optional)**:

  We do not need it so you can skip this step.

Step 3: Review and Submit

- **Review Your Template**:
  - Double-check the content you’ve entered. Since this is a **non-variable** template, ensure that:
    - The message is clear and doesn't have placeholders.
    - Any optional components (footer) are correctly added.
- **Submit the Template**:

- Once you're satisfied with the template, click **“Submit”** to send it for Meta’s approval.



Step 4: Wait for Approval

- **Approval Process**:
  - Meta will review your template to ensure it complies with WhatsApp’s policies.
  - This process usually takes **a few minutes to a couple of hours**.
- **Receive Approval Notification**:
  - Once approved, you’ll get a notification indicating that your template is ready to use.

You can now send messages using this template via the WhatsApp Business API.

File Import

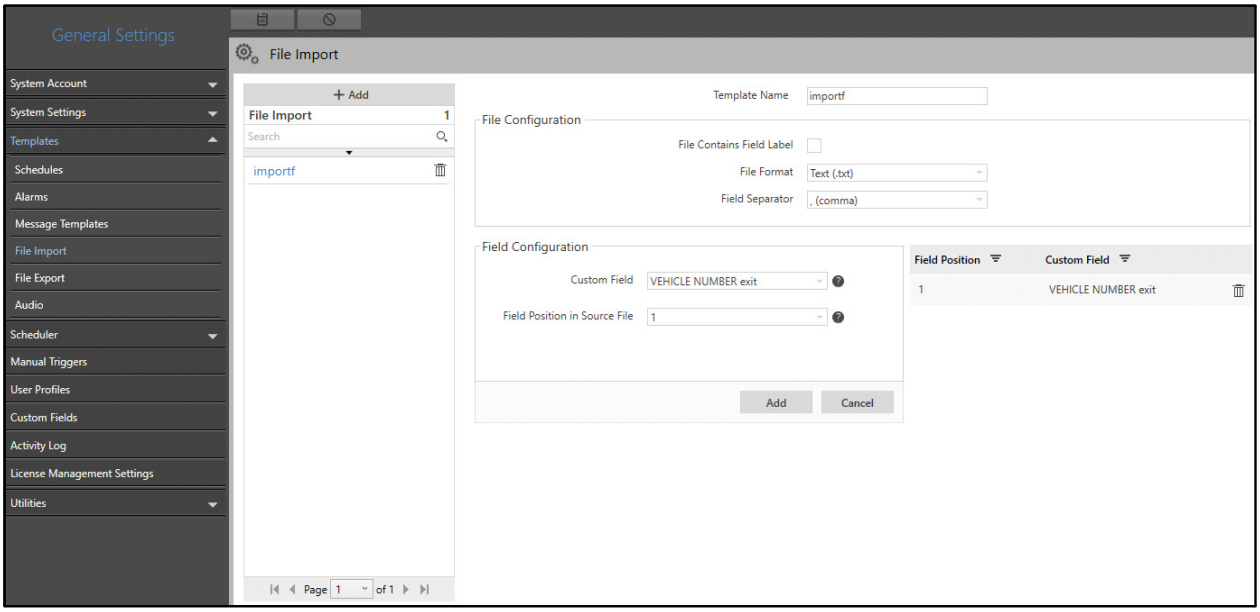
Using File Import, you can import a file containing Event related information and save it in the SATATYA SAMAS database which can be used later for generating reports. You can also import data from other third party applications and use it for report generation.

For example, if you wish to read a file and store the data in the database at 5pm daily for custom Event Report Generation, you can do so using File Import.

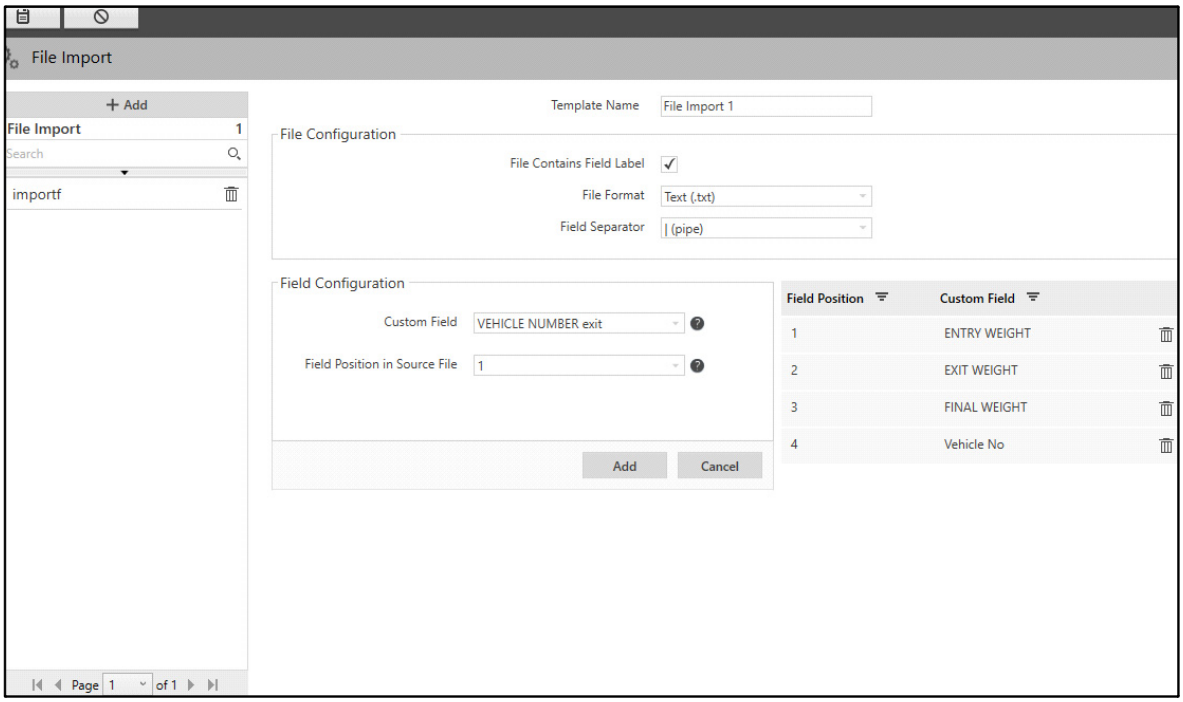
The File Import page displays the configured Import File templates. These templates can be used for generating reports. You can view and configure File Import from this page.

To configure File Import,

- Click **General Settings > Templates > File Import**.



- Click **Add**.



Configure the following parameters:

- **Template Name:** Specify a suitable name for the File Import Template. In Template Name, you can enter upto 50 characters. Default: Blank.

The File Import page contains two sections — “File Configuration” and “Field Configuration”.

File Configuration

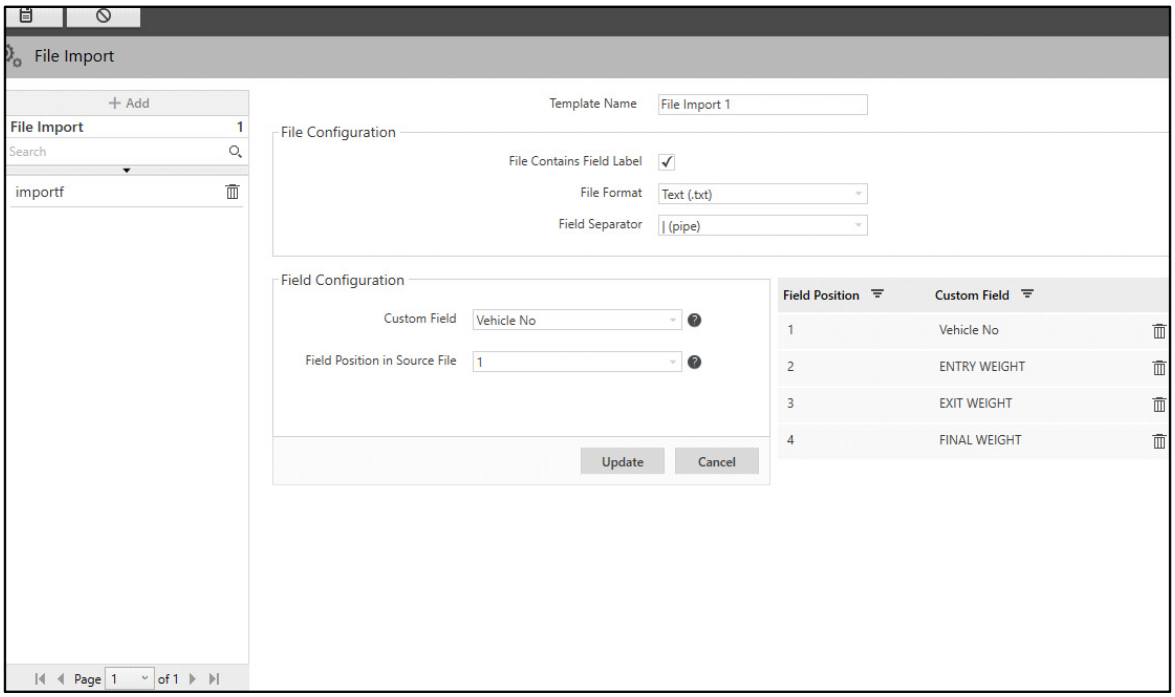
- **File Contains Field Label:** Select this check box to import data and not their field labels from an input file. If enabled, the first line is skipped and data is read from the second line. Clear the check box if the input file contains only data and no label names.
- **File Format:** Select the File Format in which you wish to import the file from the drop-down list.
- **Field Separator:** If you select the File Format as Text, then select the desired Separator — comma, colon, semi-colon or pipe. This separator will be used between the data values in the file so that they are separated and can be identified correctly.

Field Configuration

- **Custom Field:** Select the desired custom field from the drop-down list. The configured custom fields appear in this list. For details, refer to “Custom Fields”.
- **Field Position in Source File:** Select the position of the field in the import data file from the drop-down list.
- Click **Add** to add the fields or click **Cancel** to discard.

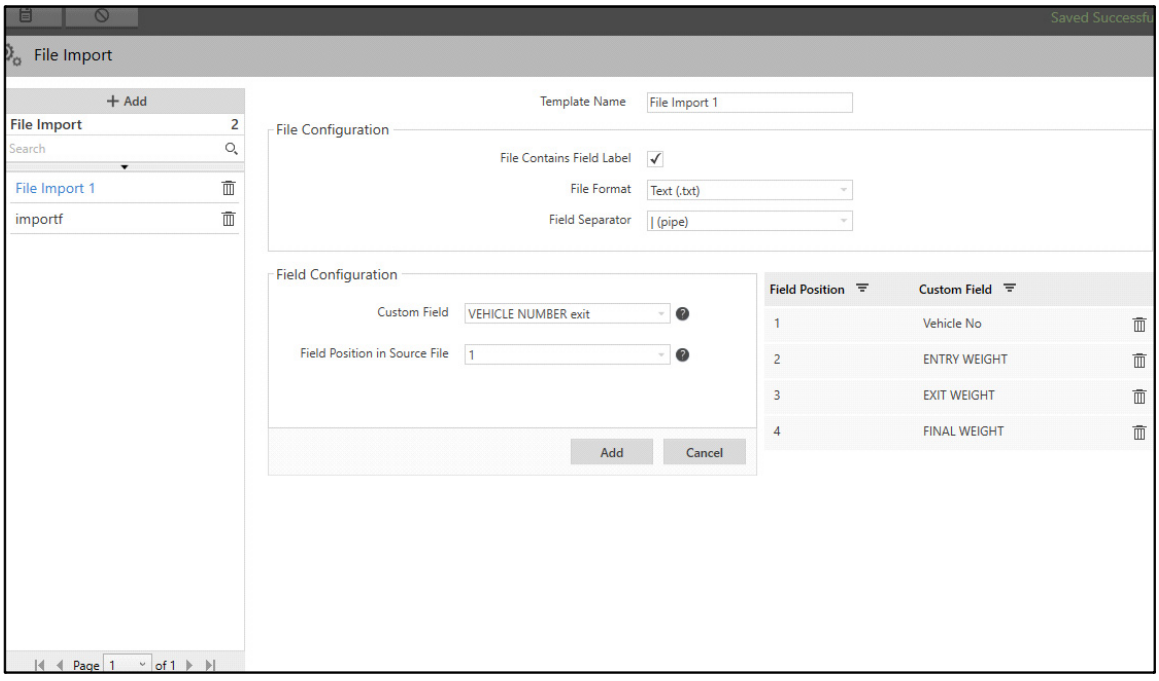
The custom fields and their position appears in the list on the right hand side.

You can also change the configurations of the fields or delete them.

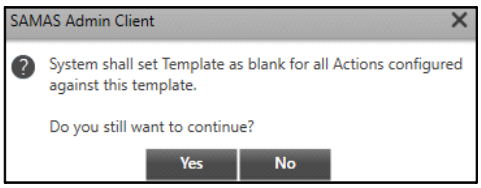


- Select the desired custom field from the list and edit the configurations on the left.
- Click **Update** to update the configurations or click **Cancel** to discard.
- Click **Delete** to delete the desired custom field.
- Click **Save** to save the settings or **Cancel** to discard.

The new File Import template appears in the list on the left hand side. You can change the configurations of the fields or delete them.



- Select the desired template from the list and edit the configurations on the right.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired template. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

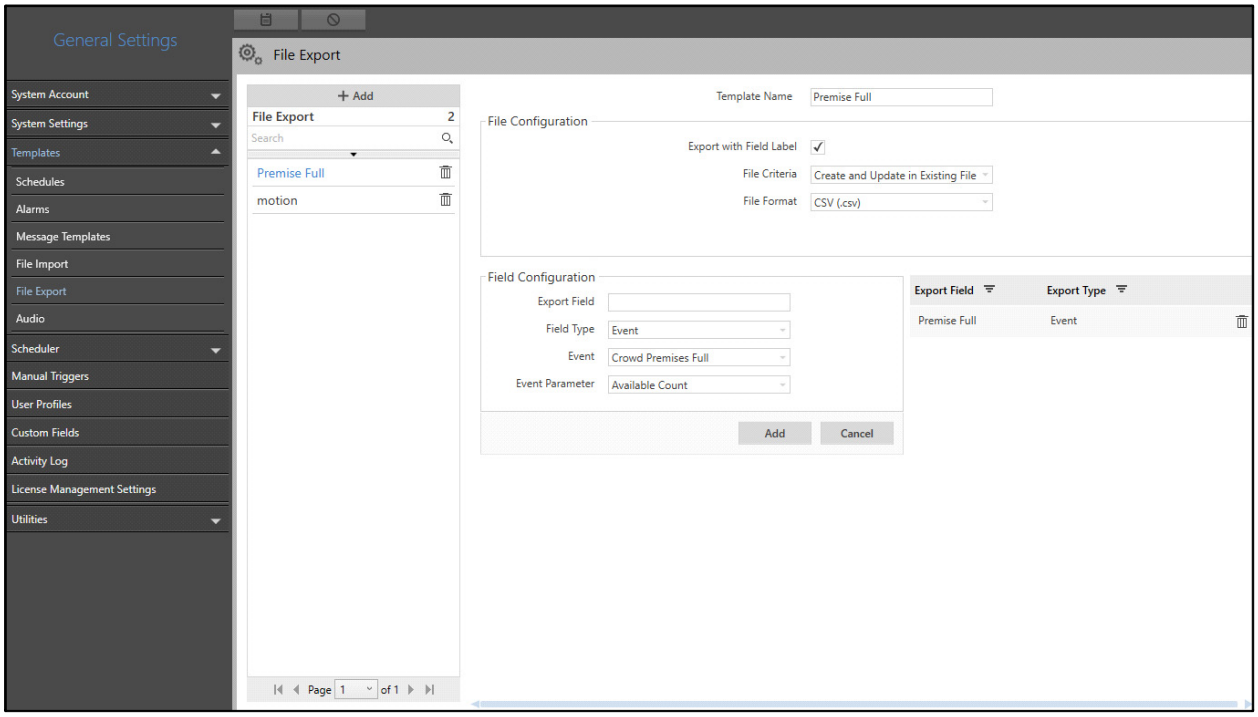
File Export

Using File Export, you can create custom templates for exporting a file containing the Event related information. This facilitates a third party application to use information provided by SATATYA SAMAS in their system and perform actions accordingly.

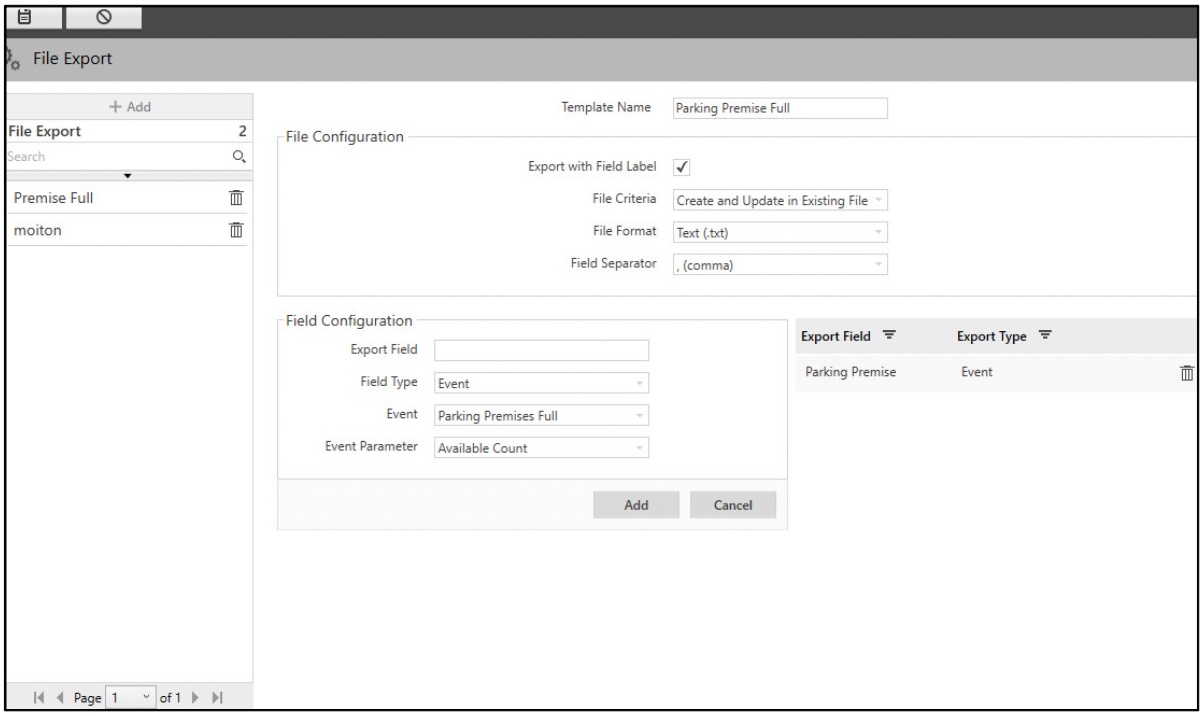
The File Export page displays the configured Export File templates. These templates can be used for generating reports. You can view and configure File Export from this page.

To configure File Export,

- Click **General Settings > Templates > File Export**.



- Click **Add**.



Configure the following parameters:

- **Template Name:** Specify a suitable name for the File Export Template. In Template Name, you can enter upto 50 characters.Default: Blank.

The File Export page contains two sections — “File Configuration” and “Field Configuration”.

File Configuration

- **Export with Field Label:** Select this check box to export the file with the field labels as specified in the **Export Field** parameter along with its value separated by the selected **Field Separator**.
- **File Criteria:** Select the File Criteria from the drop-down list — Create With Timestamp, Overwrite Existing File, Create and Update in Existing File.
- **File Format:** Select the File Format in which you wish to export the file from the drop-down list.
- **Field Separator:** If you have selected the File Format as Text, select the desired Separator — comma, colon, semi-colon or pipe. This separator will be used between the data values in the file so that they are separated and can be identified correctly.

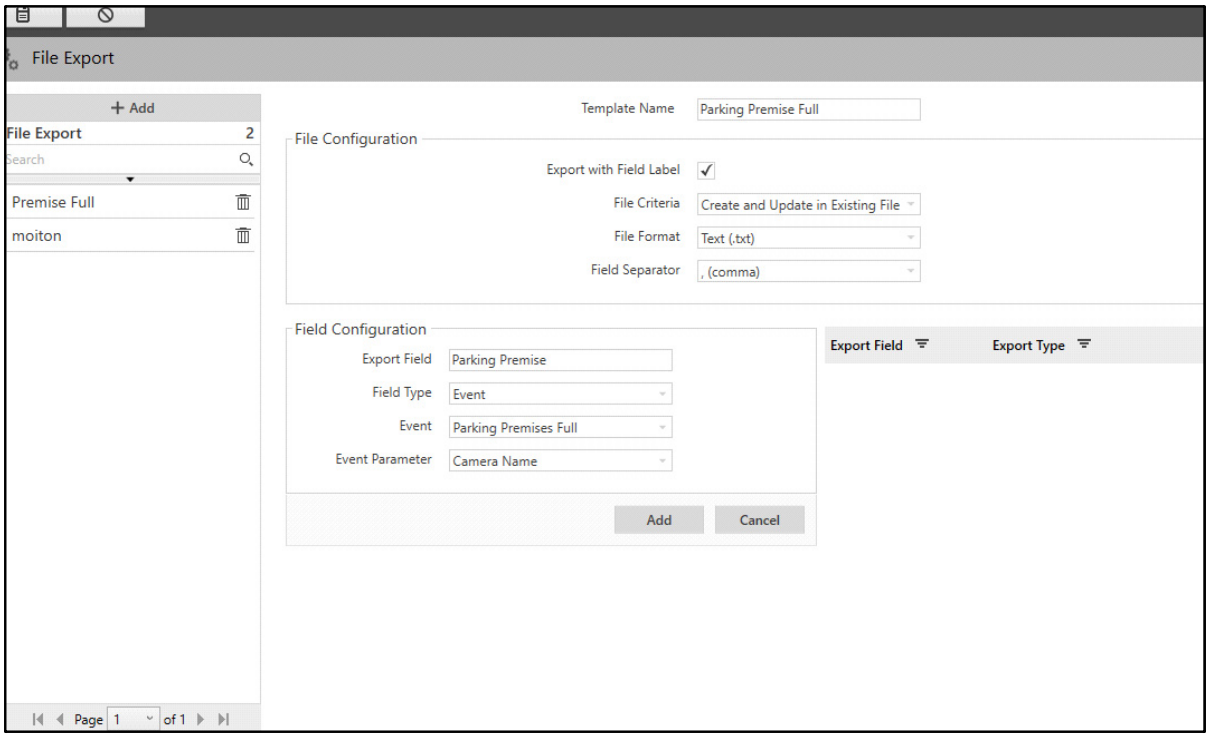
Field Configuration

- **Export Field:** Specify a suitable name for the Export Field to be inserted in the file used by the third party application for reading. In Export Field, you can enter upto 20 characters. Default: Blank.
- **Field Type:** Select the desired Field Type from the drop-down list — Event or Static.

  If you select **Event** as the Field Type, configure the following parameters:

  - **Event:** Select the desired Event from the drop-down list.

- **Event Parameter**: Select the desired Event Parameter from the drop-down list. The Event Parameters depend upon the selected Event.

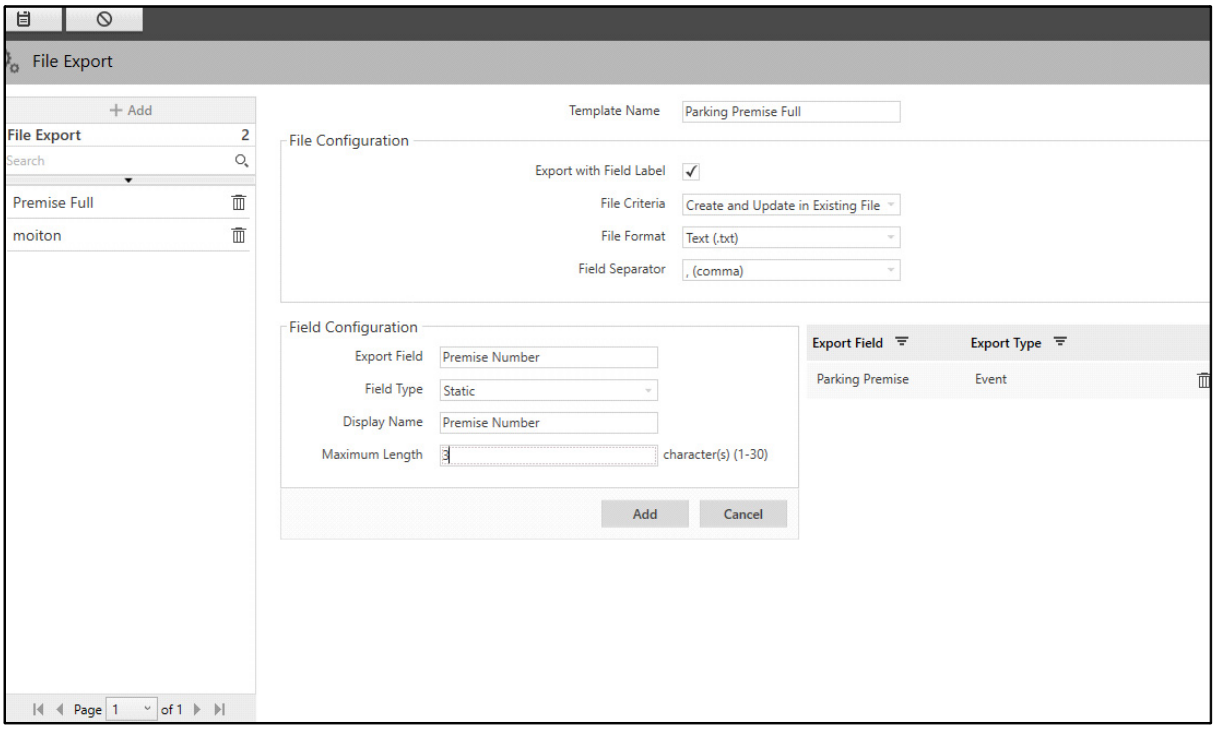


If you select **Static** as the Field Type, Configure the following parameters:

- **Display Name:** Specify a suitable Display Name. Display Name is a user friendly name given to the field for easy identification at the time of configuration of Actions for Events. For details, refer to “Configuring Actions for Events”.

  In Display Name, you can enter upto 20 characters. Default: Blank.

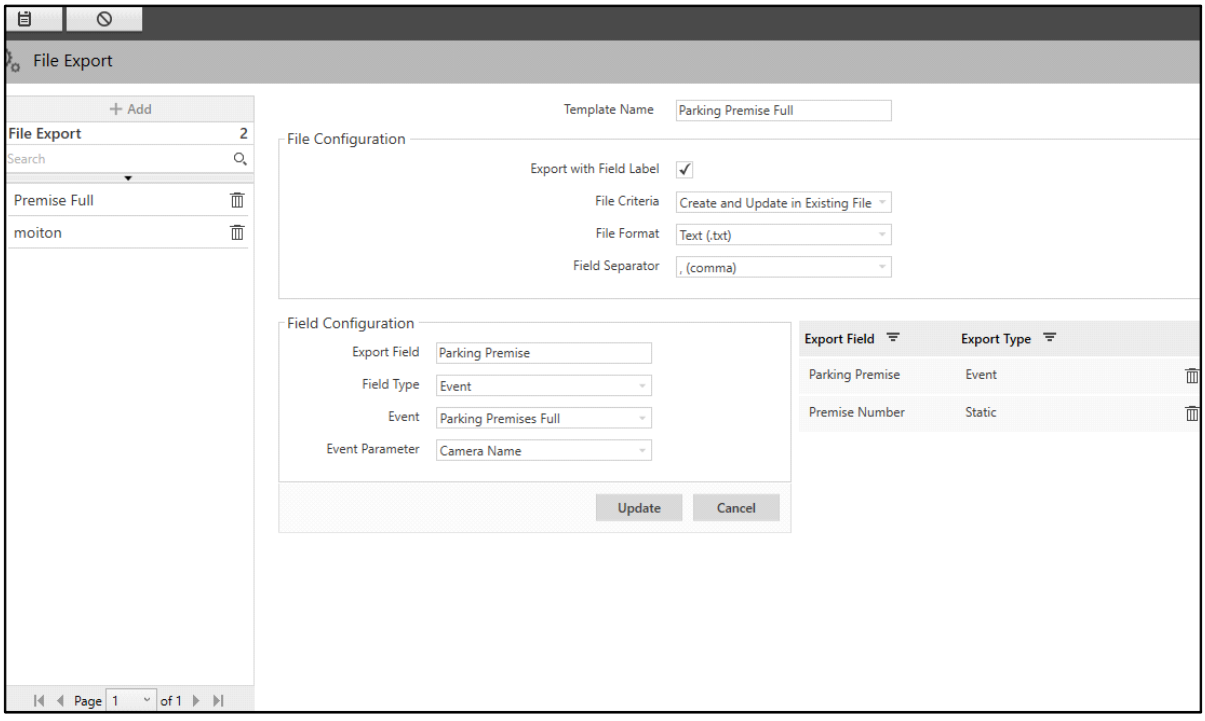
- **Maximum Length**: Specify the maximum length in terms of characters for the field value. Valid Range: 1-30. Default: Blank.



- Click **Add** to add the fields or click **Cancel** to discard.

The Export fields and their type appear in the list on the right hand side.

You can also change the configurations of the fields or delete them.

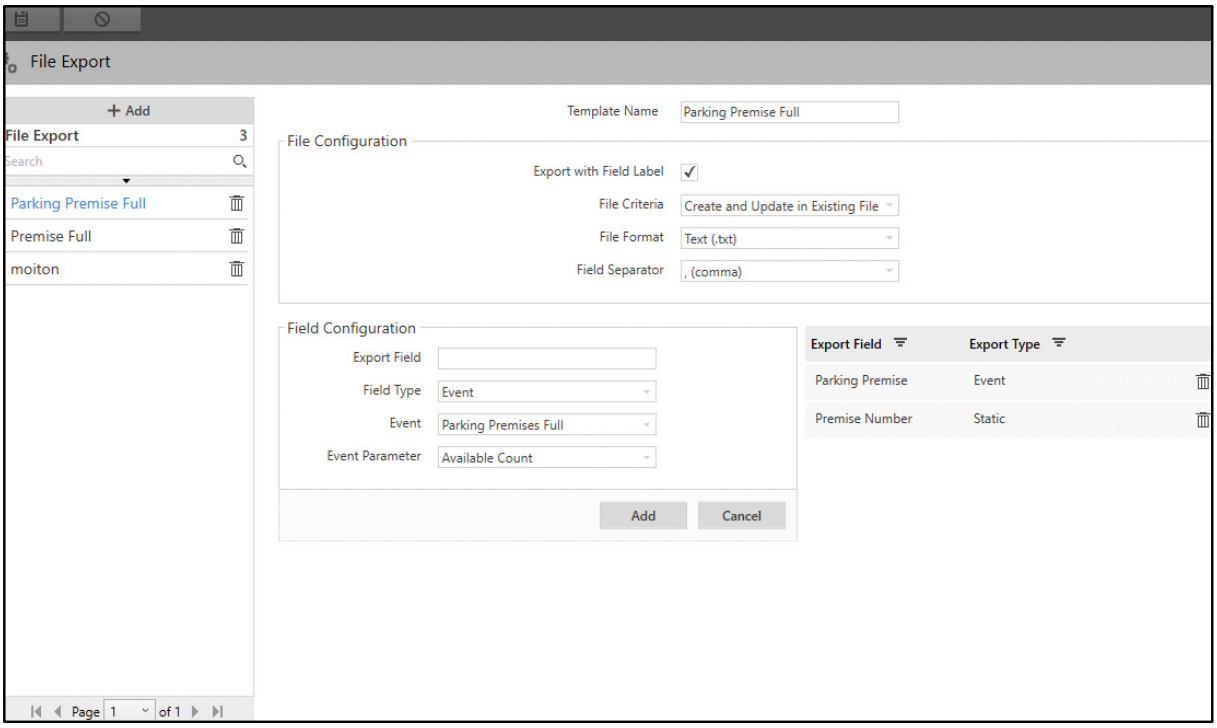


- Select the desired Export field from the list and edit the configurations on the left.
- Click **Update** to update the configurations or click **Cancel** to discard.

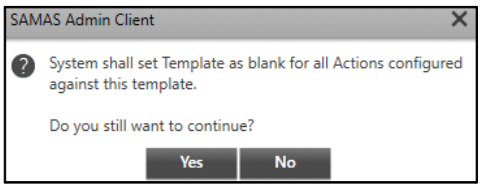
- Click **Delete** to delete the desired Export field.
- Click **Save** to save the settings or **Cancel** to discard.

The new File Export template appears in the list on the left hand side.

You can also change the configurations of the fields or delete them.



- Select the desired template from the list and edit the configurations on the right.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired template. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

Audio

Audio feature is supported in Software Release V5R6, V6R2 and onwards.

The Audio page displays the configured Audio Templates. These templates can be assigned in actions (Trigger Alarm and Live View on Event) for Events (For example, Camera Tampered) when configuring various Scenarios. You can create maximum 1000 Audio Templates by uploading .wav files. This is useful when you wish to play different audios for different scenarios which will facilitate easy identification. You can view and configure Audio Templates from this page.

Pre-Requisites for Custom Audio File

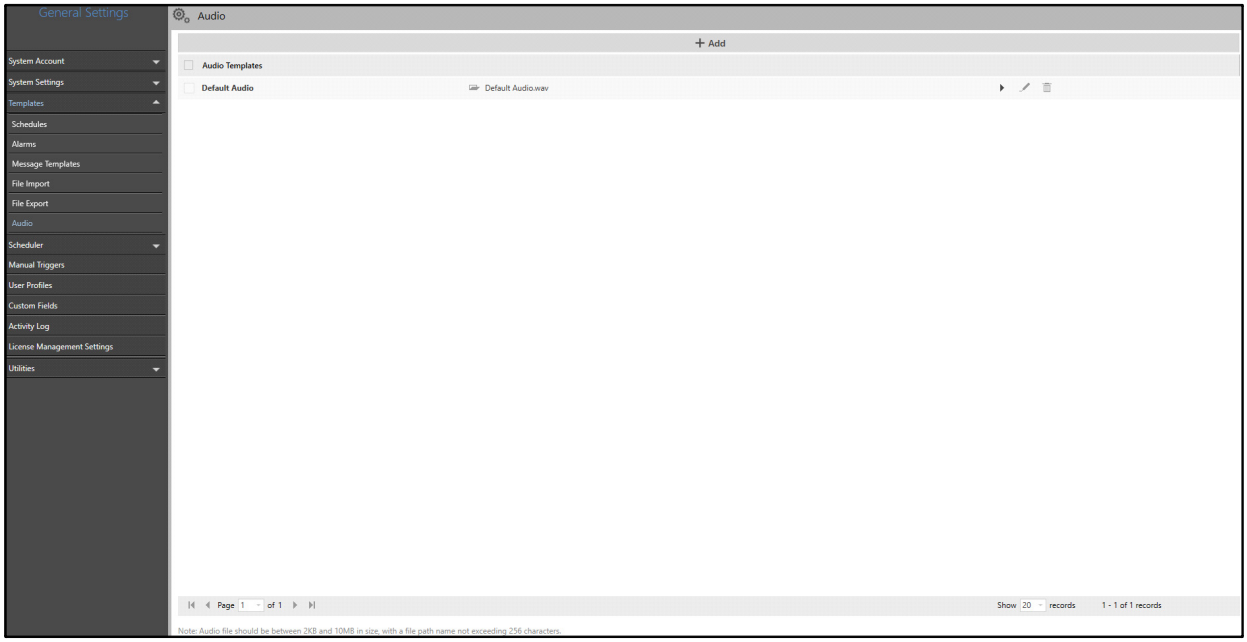
To upload a custom audio file, make sure the following pre-requisites are fulfilled:

- Audio File Format: .wav
- Audio File Size: 2KB to 10MB.
- Audio Format: Pulse-Code Modulation (PCM)
- PCM Bit Depth: 8, 16, 24 or 32 bits

To suffice these standards, you can use a reliable Audio Converter Tool to convert your custom audio files. We recommend these Audio Converter Tools— Cool Edit Pro and Microsoft Windows Sound Recorder (sndrec32).

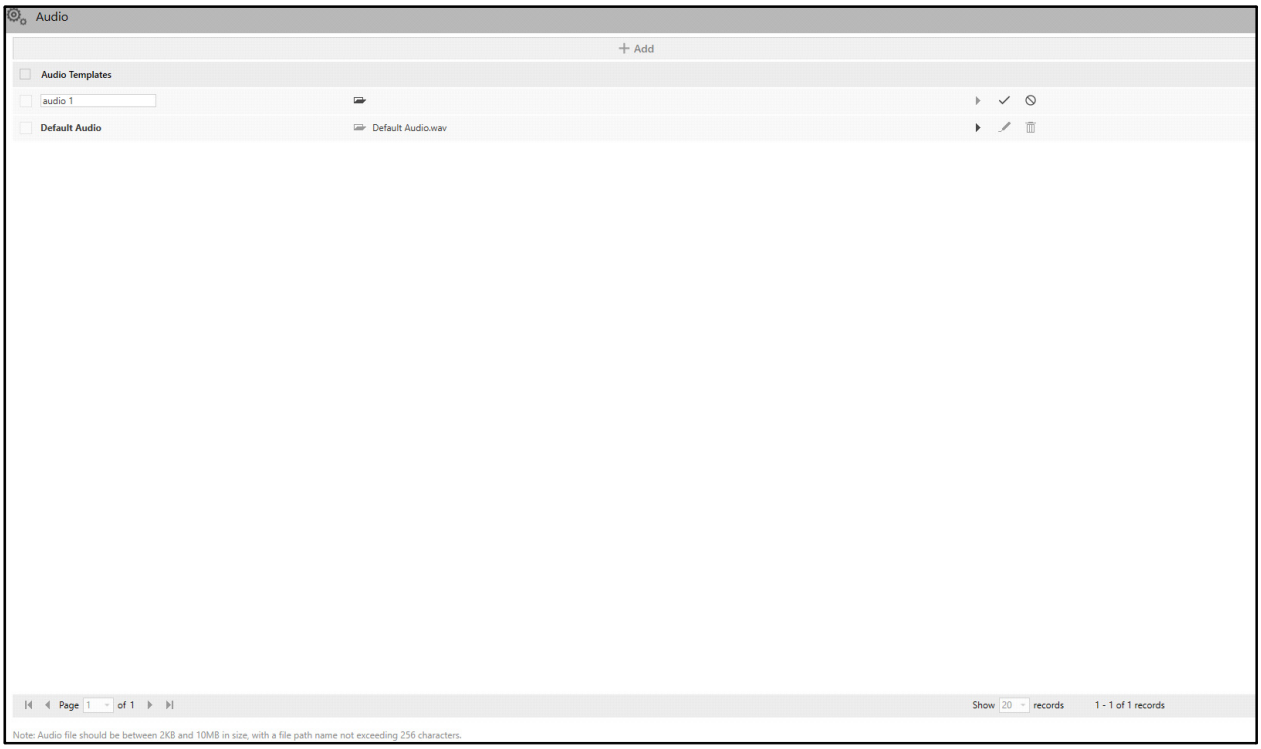
To configure Audio Templates,

- Click **General Settings > Templates > Audio**.



The Audio Template **Default Audio** is pre-configured. The configurations for this template can be changed but it cannot be deleted. However you can add Audio Templates as per your requirement.

- Click **Add**.



Configure the following parameters:

- Specify a suitable name for the Audio Template you wish to add. In Audio Template Name, you can enter upto 100 characters.Default: Blank.

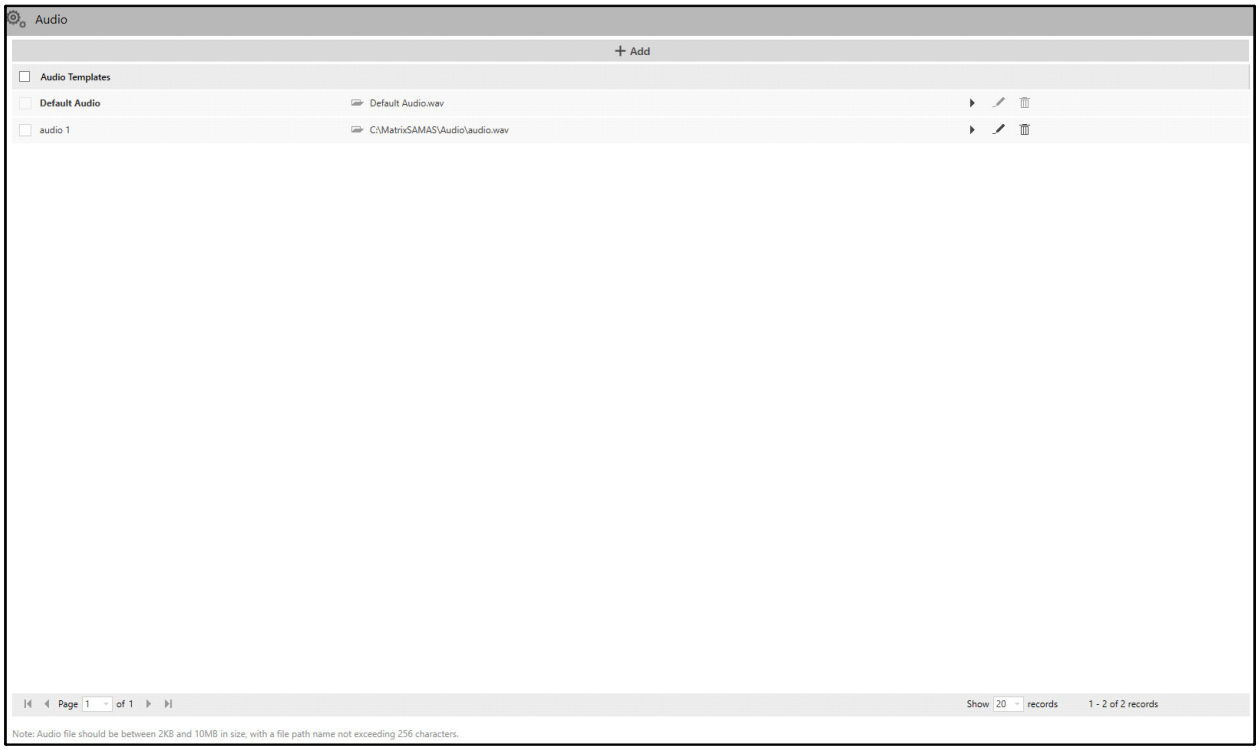
The name of the Audio file can be a maximum of 256 characters.

- **Upload**: Click **Browse** . It displays all folders which are in the drive. Select the desired audio file which you wish to upload. The uploaded audio file will be stored in the Image Storage Drive.

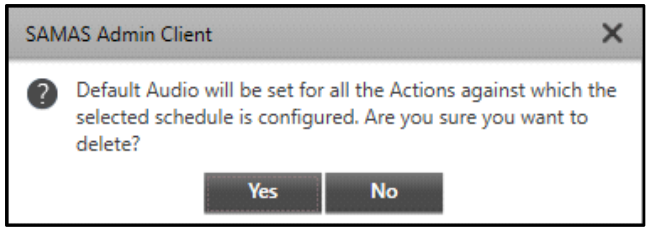
- Click **Save** to save the Audio Template or click **Cancel** to discard.

The new Audio Template appears in a list.

Each Audio Template can be played, edited or deleted.



- Click **Play** to play the desired Audio Template from the list. The icon toggles to **Stop** . Click **Stop** to stop the audio.
- Click **Edit** to edit the desired Audio Template from the list.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Audio Template. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

Scheduler

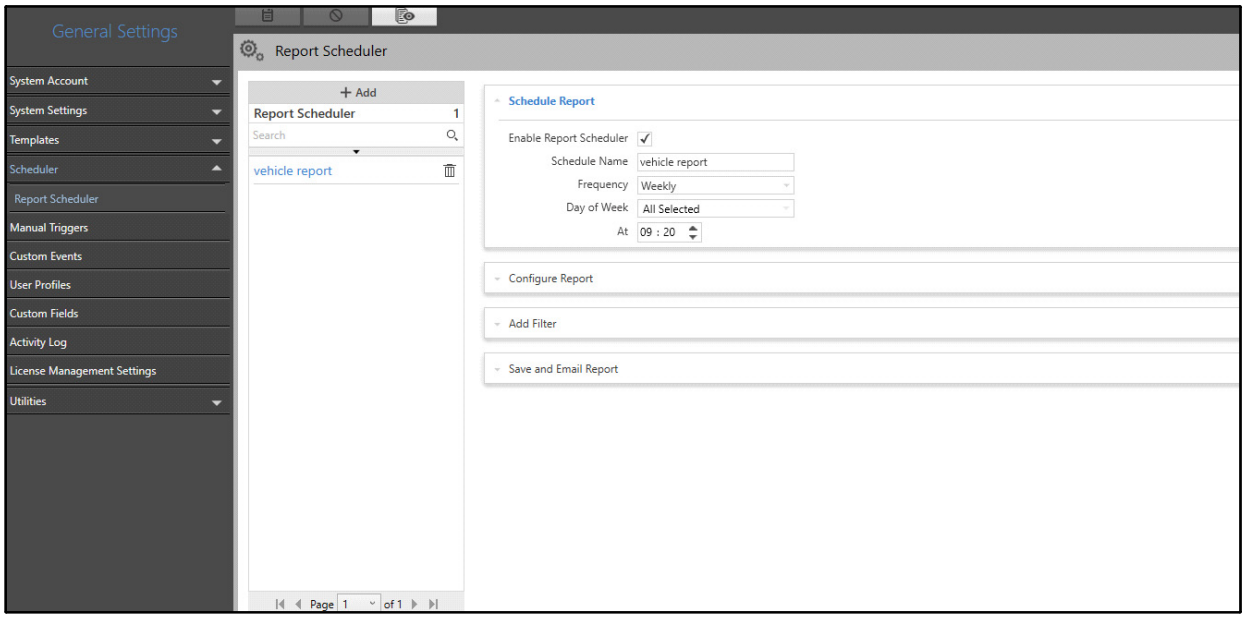
Report Scheduler

The Admin Client provides a facility to generate the reports of various SATATYA SAMAS Events from their respective modules. Apart from this, it also provides you the flexibility to create and generate customized reports using the Report Scheduler. It enables you to generate each report automatically as per the defined schedule and in the desired language. These reports can be saved at the desired location or can be sent via Email at defined time intervals.

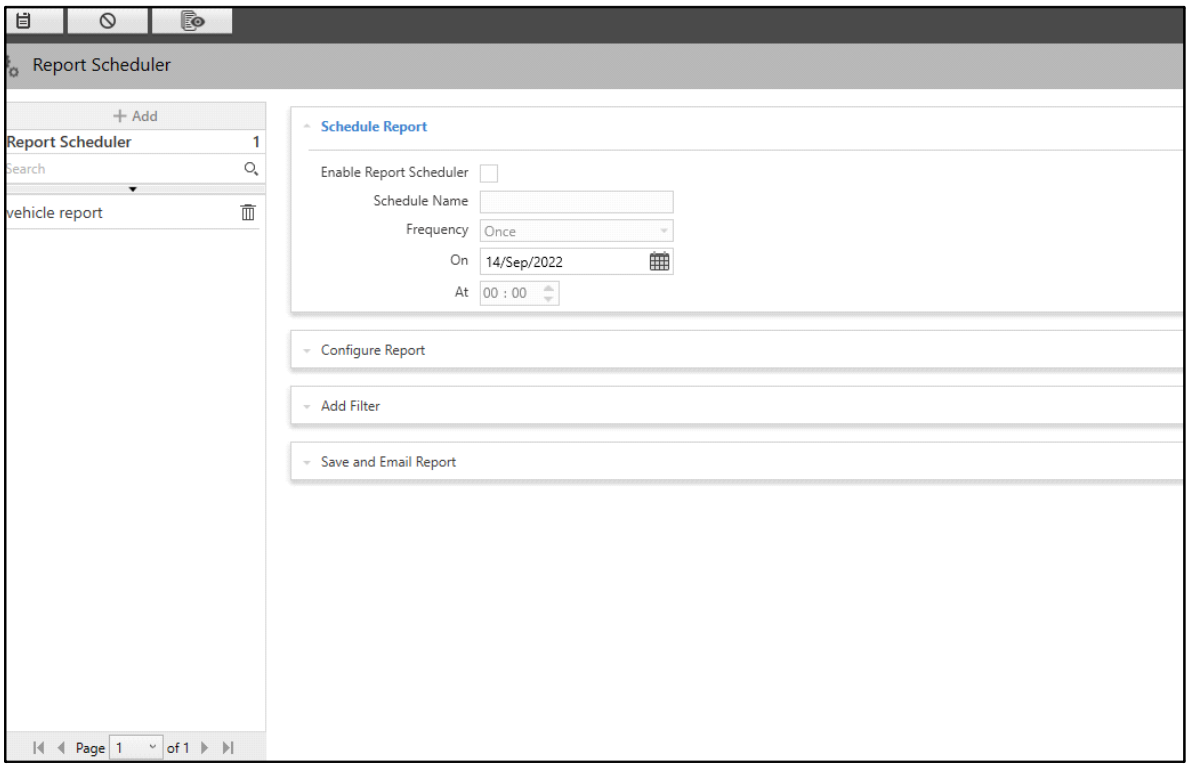
The Report Scheduler page enables you to configure parameters for Reports. You can view and configure various parameters for Report Schedule, filter and sort the data as well as store or Email the report.

To configure Report Scheduler,

- Click **General Settings > Scheduler > Report Scheduler**.



- Click **Add**.



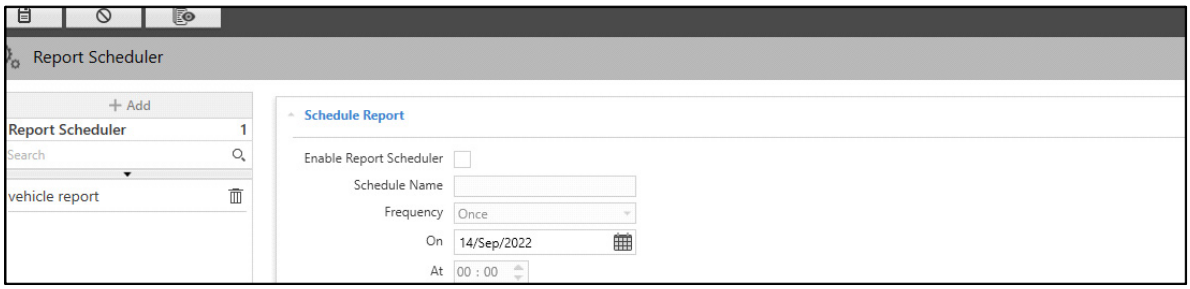
The Report Scheduler page contains four collapsible panels — “Schedule Report”, “Configure Report”, “Add Filter”and “Save and Email Report”.

Schedule Report

This panel displays the report schedule configurations. You can edit and configure the Report Schedule from this collapsible panel.

To view and edit the report schedule,

- Click the **Schedule Report** collapsible panel.



Configure the following parameters:

- **Enable Report Scheduler**: Select the check box to enable the Report Scheduler configurations.
- **Schedule Name**: Specify a suitable name for the schedule. In Schedule Name, you can enter upto 100 characters.Default: Blank.

- **Frequency**: Select the frequency at which the report must be generated automatically from the drop-down list — Yearly, Monthly, Weekly or Once.
    - **Yearly**: Select this option to generate yearly reports. Select the desired month and date from the drop-down lists.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Weekly**: Select this option to generate weekly reports. Select the desired Day of Week from the drop-down list. Select the check boxes for the days of the week on which you wish to generate the report.
    - **Once**: Select this option to generate the report once. Select the date from the calendar.
- **At**: Specify the time at which the report must be generated.

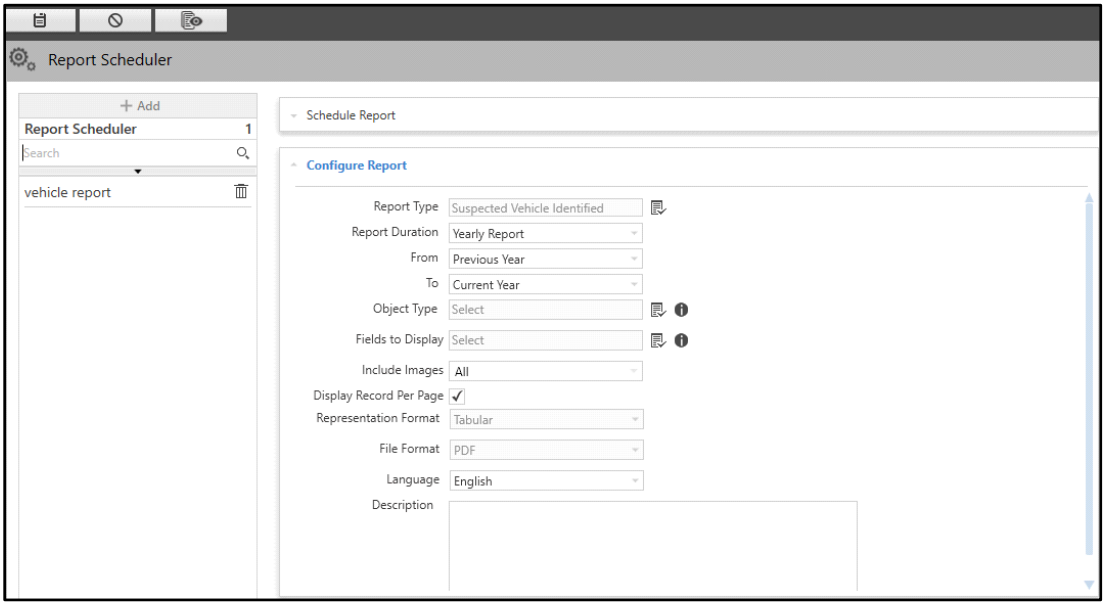
- Click **Save** to save the settings or **Cancel** to discard.

Configure Report

This panel displays the report configurations. You can edit and configure the Report parameters from this collapsible panel.

To view and edit the report configurations,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

- **Report Type**: Select the type of report you wish to generate using the **Report Type** picklist. Double-click to select the desired option.

*In the **Report Type** picklist, module-wise report types are listed. For the detailed configuration of each report type, refer to the respective modules.*

*The parameters for report configurations change as per the type of report selected in the **Report Type**. The parameter **Object Type** is applicable to Vehicle and Parking Management reports and in Evidence Reports for the events which support Object Type.*

Face Detection Report will be visible but not functional in this Software Release.It will be included in the upcoming release.

The Vehicle Counting and People Counting report types are available in IVA modules (Parking Management and Crowd Management) as well as in Servers and Devices module.

- *If selected from IVA module, the report will be generated on the basis of IVA Events.*
- *If selected from Servers and Devices, the report will be generated on the basis of Camera Events.*

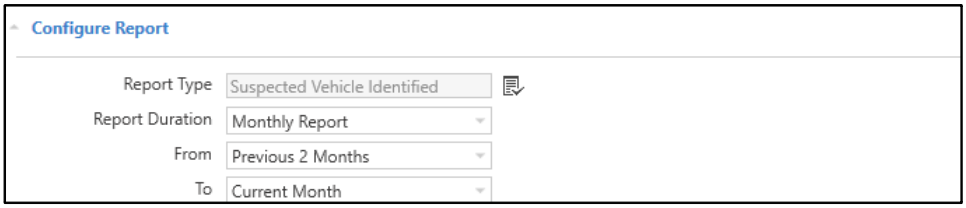
- **Report Duration**: Select the desired duration for which the report is to be generated from the drop-down list — Yearly, Monthly, Daily or Hourly.

    - On selecting **Yearly Report**, the **From** and **To** drop-down lists enable you to select the desired years. The From time duration will always be greater than the To. Select the start year and end year from the respectively From and To drop-down lists.

      For example, to view the reports from 2018 to 2020, select Previous 4 years from the From drop-down list and select Previous 2 years from the To drop-down list. The current year is taken as reference.

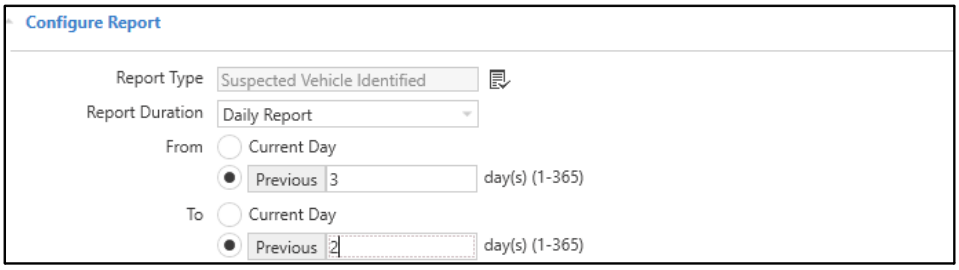


    - Similarly, on selecting **Monthly Report**, you can select the desired months from the **From** and **To** drop-down lists. The current month is taken as the reference. Monthly report configuration is the same as that of Yearly Report.

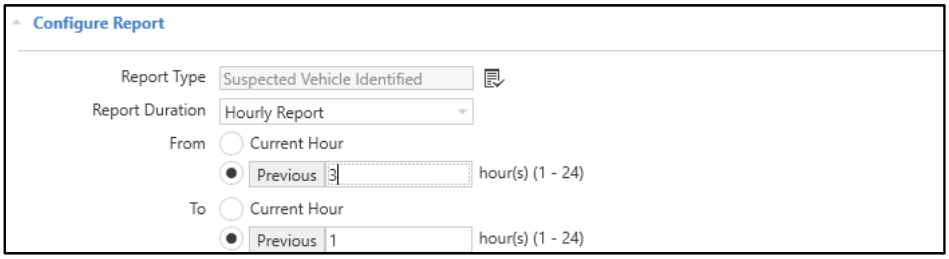


    - On selecting **Daily Report**, two radio buttons appear in the **From** and **To** fields. Specify the desired days. The From time duration will always be greater than the To. Select the **Current Day** radio button in both From and To to view the current day's report. Select the days accordingly if you want to view earlier reports.

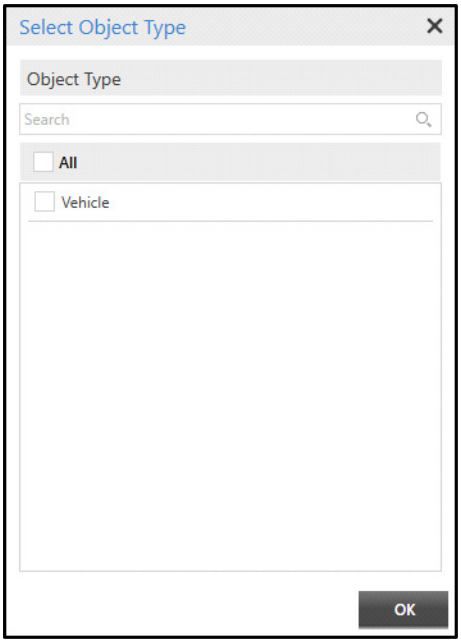
      For example, to view the reports for 7th and 8th June on 10th June, enter 3 after selecting the **Previous** radio button in From and enter 2 after selecting Previous radio button in To. The report duration considered in this case will be 7th June 00:00 hrs to 8th June 23:59 hrs. Always, the current day is taken as reference.



- Similarly, on selecting **Hourly Report**, the **Current Hour** and **Previous** radio buttons appear in **From** and **To** fields. The current hour is taken as the reference. Hourly Report configuration is the same as that of the Daily Report.

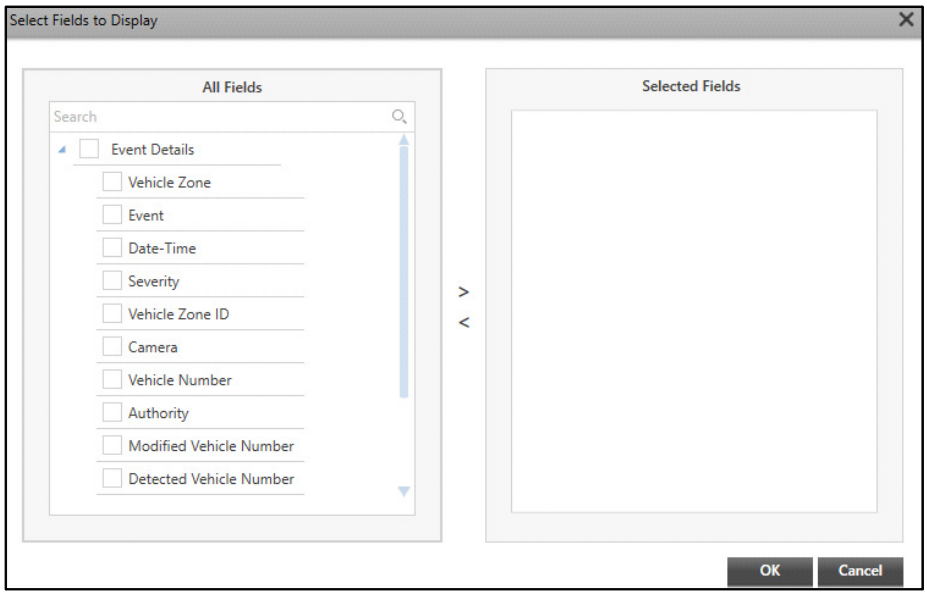


- **Object Type**: Select the desired Object Type which should be displayed in the report using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



- Select the **Vehicle** check box. Click **OK**.
- **Fields To Display:** Select the desired fields to be displayed in the report using the **Fields to Display** picklist.

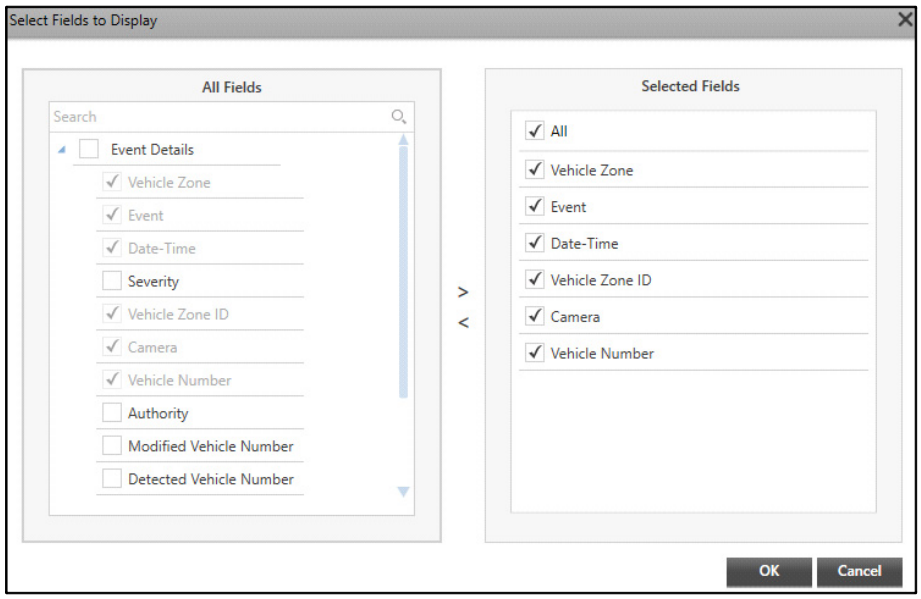
- Click the **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



- The fields that appear here depend on the type of report you have selected under **Report Type**. Select the check boxes of the fields you wish to include in the report from the **All Fields**.

- Click the right arrow button to add those fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

- To remove fields, select the check boxes of the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields from the Selected Fields list.



- Click **OK** to confirm or click **Cancel** to discard.



- **Include Images**: Select the check boxes of the desired images to be included in the report from the drop-down list. This drop-down list changes as per the selected report type to include images relevant to the report.
- **Display Record Per Page**: Select the check box to display each record for the selected fields on a new page.
- **Representation Format**: Select the format in which the report is be generated from the drop-down list.
- **Graph Type**: If you have selected Graph as the Representation Format, select the Graph Type from the drop-down list.
- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.
- **Description**: Enter the desired description of the report you wish to generate. In Description, you can enter upto 2000 characters. Default: Blank.

- Click **Save** to save the settings or **Cancel** to discard.

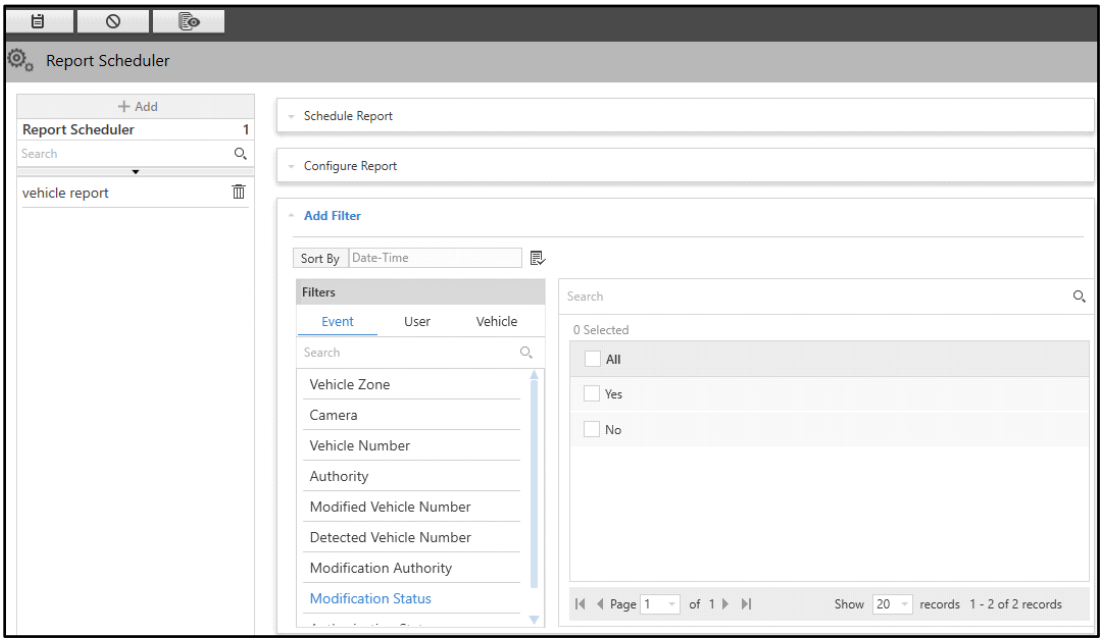
Add Filter

This panel allows you to add filters for the Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters. You can view and edit the filters from this collapsible panel.

*Add Filter panel is available only for Parking Management, CREAM and Vehicle Management Module entities, selected from Configure Report section. The parameters under **Add Filter** change as per the type of report selected in **Report Type.***

To view and edit the filters,

- Click the **Add Filter** collapsible panel.

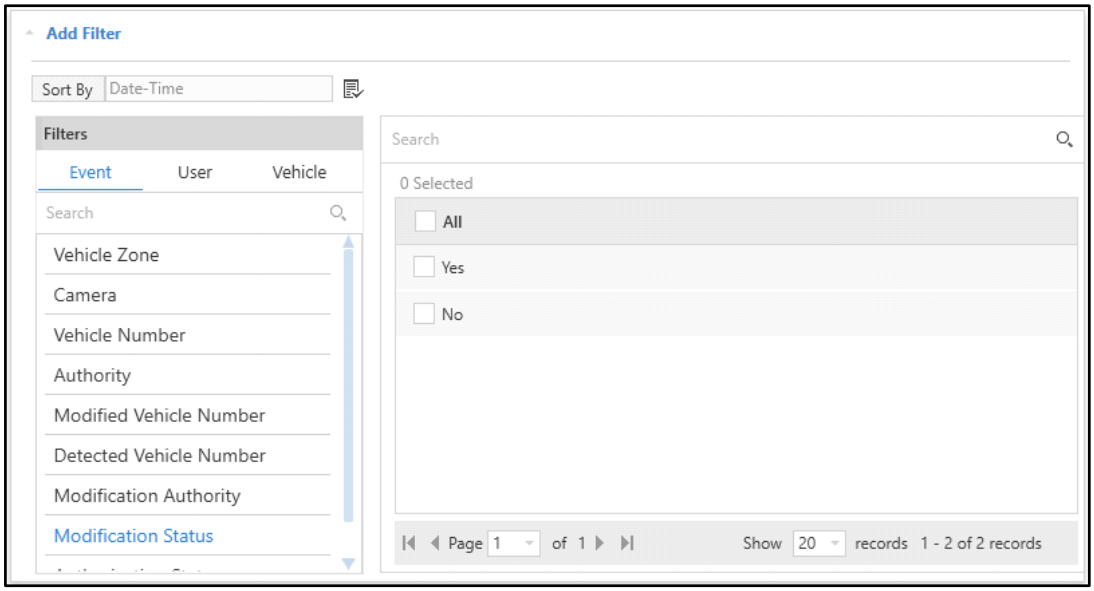


Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data from Event Details, User Details or Vehicle Details using the **Sort By** picklist. Double-click to select the desired option. By default, the sorting is done as per the Date and Time of the Event Occurrence. The parameters that appear here depend on the type of report you have selected in **Report Type**.

- **Filters**: You can get the desired data for the report using Filters. The Filters section contains three tabs — Event, User and Vehicle. Select the desired tab to view the associated parameters.

  - Click the desired parameter to view the associated entities with the selected Event. For example, if you select Camera, all the cameras associated with the selected Event are displayed on the right hand side. Select the desired entities to include in the report.



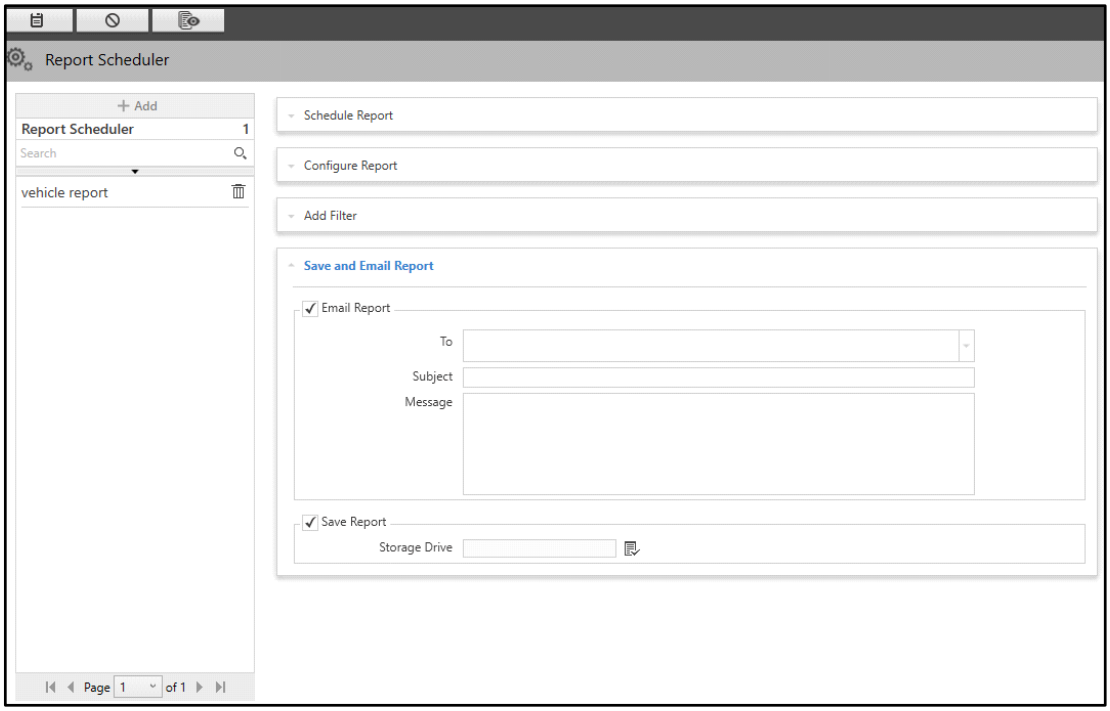
- Click **Save** to save the settings or **Cancel** to discard.

Save and Email Report

This panel displays the configurations for emailing and saving the report. You can edit and configure the Email and Storage parameters from this collapsible panel. It is mandatory to either select the **Email Report** option or the **Save Report** option.

To view and edit the Save and Email Report configurations,

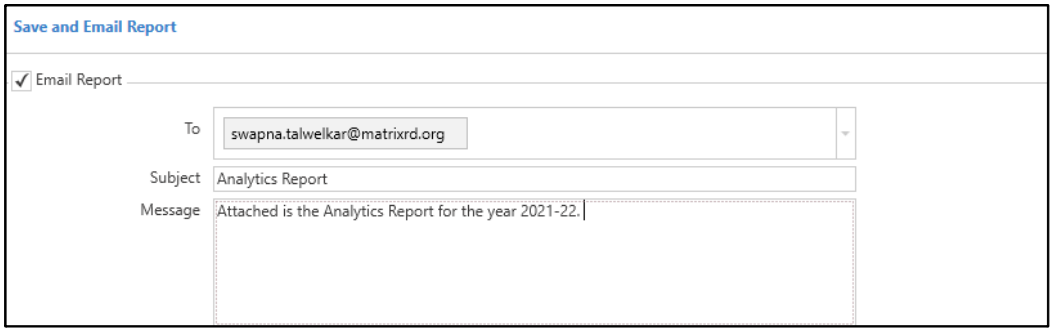
- Click the **Save and Email Report** collapsible panel.



The Save and Email Report panel contains two sections — “Email Report” and “Save Report”.

Email Report

- Select the **Email Report** check box to enable the Email Report configurations.



Configure the following parameters:

- **To**: Specify the Email Address of the users to whom the report is to be sent. This field is mandatory. In To, you can enter upto 100 characters. Default: Blank.
- **Subject**: Specify a suitable subject line for the Email. In Subject, you can enter upto 100 characters. Default: Blank.
- **Message**: Enter the message body for the Email. In Message, you can enter upto 500 characters. Default: Blank.

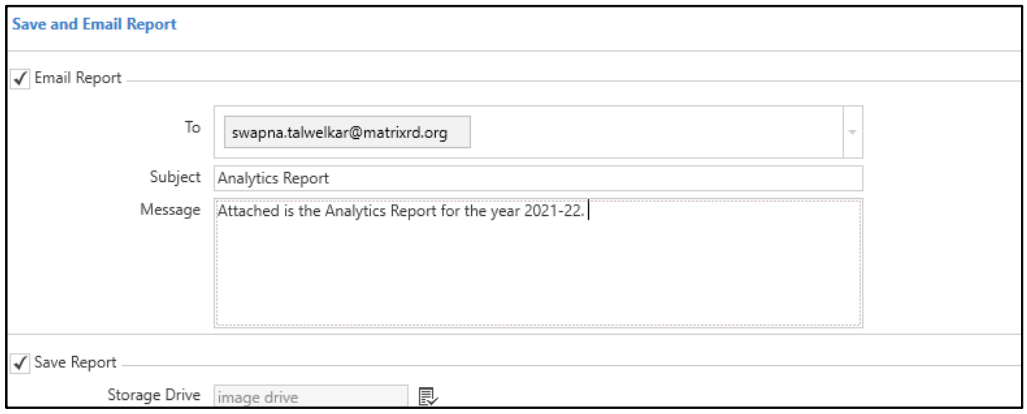
Maximum report size to be mailed is 25 MB.

If the multiple reports are formed or the file size exceeds 25 MB, the files will be automatically zipped and mailed. Else, the email will be sent without the report.

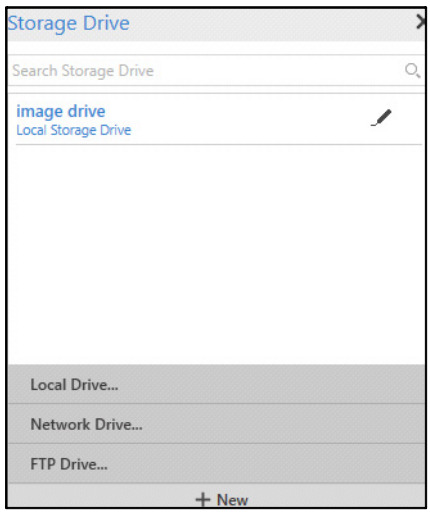
Management Server and Notification Server both should be online for generating reports and sending them in email via Report Scheduler. When offline, the reports will not be generated and emailed.

Save Report

- Select the **Save Report** check box to enable the Save Report configurations.



- **Storage Drive:** Select the storage drive where you wish to store the report using the **Storage Drive** picklist.
  - Click **Storage Drive** picklist. The **Storage Drive** pop-up appears.



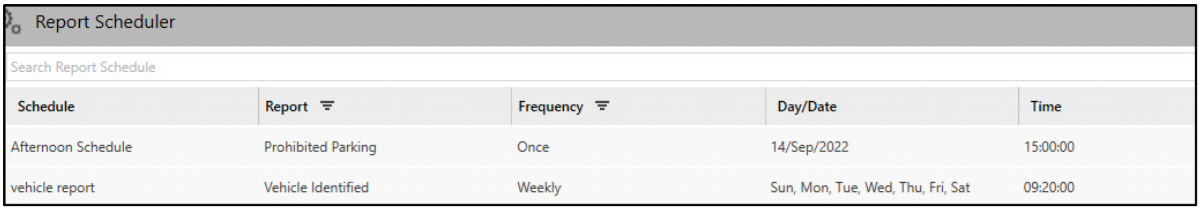
- Double-click to select the desired Storage Drive from the list. You can edit an existing drive by clicking **Edit** . You can also configure a new Storage Drive by clicking **New**. The process of adding a new Storage Drive to Management Server is similar to the Recording Server. For details, refer to “Storage”.

Storage Drive should be connected with the Management Server when the report is scheduled to save in the defined storage drive via Report Scheduler. If not, reports will not be saved.

- Click **Save** to save the settings or **Cancel** to discard.

Once all the configurations are done, you can view all the configured Report Schedules.

- Click **View All** .



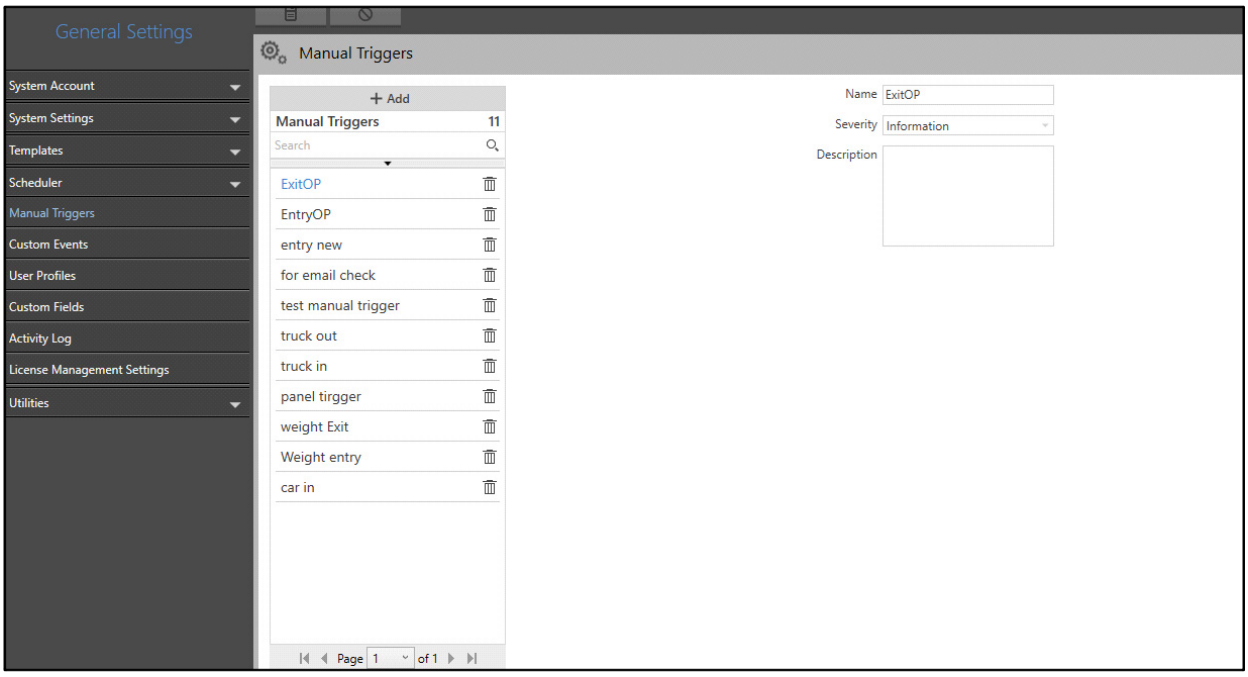
All the configured report schedules appear in a list. These Report Schedule details are displayed — Schedule, Report, Frequency, Day/Date and Time. You can also search for a Report Schedule using the **Search Report Schedule** search bar.

Manual Triggers

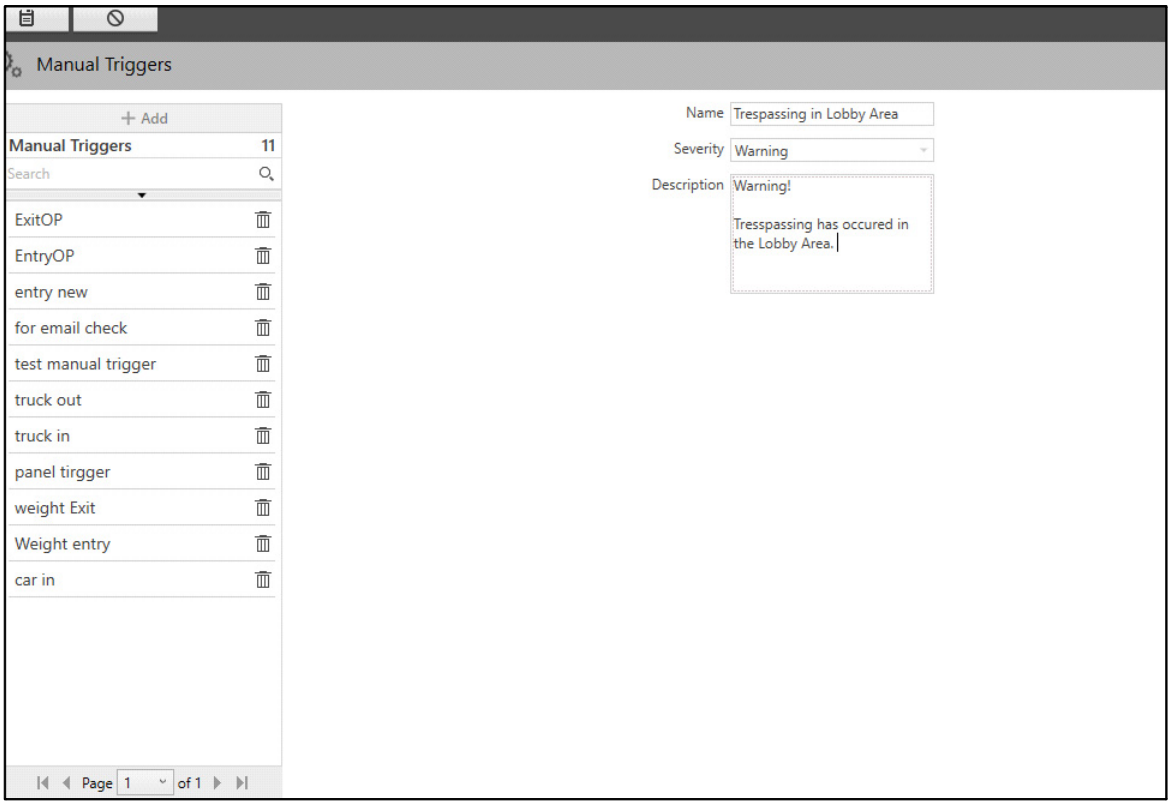
The Manual Triggers page displays the configured Manual Triggers. Manual Triggers are user-defined Events. These can be used for manually triggering specific actions like Trigger Alarm using the Smart Client. You can view and configure Manual Triggers from this page.

To configure Manual Triggers,

- Click **General Settings > Manual Triggers**.



- Click **Add**.

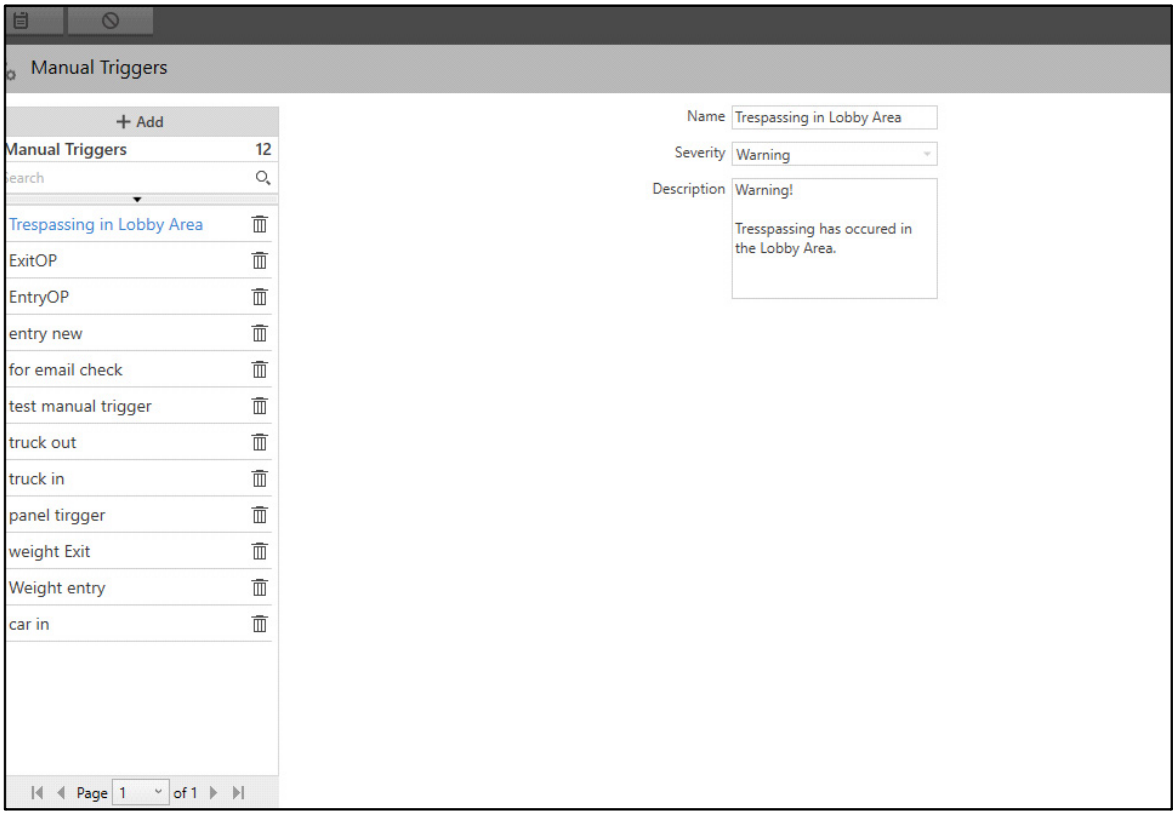


Configure the following parameters:

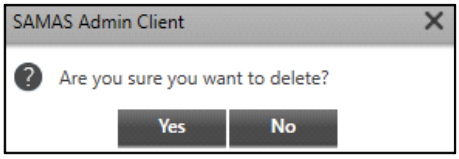
- **Name:** Specify a suitable name for the Manual Trigger. For example, Trespassing in the Lobby Area. In Name, you can enter upto 50 characters. Default: Blank.
- **Severity**: Select the Severity level from the drop-down list — Information, Warning, Error or Critical.
- **Description**: Enter the desired text in the Description box related to the Event. In Description, you can enter upto 200 characters. Default: Blank.

- Click **Save** to save the settings or **Cancel** to discard.

The new Manual Trigger appears in a list on the left hand side. You can change the configurations of the Manual Trigger or delete it.

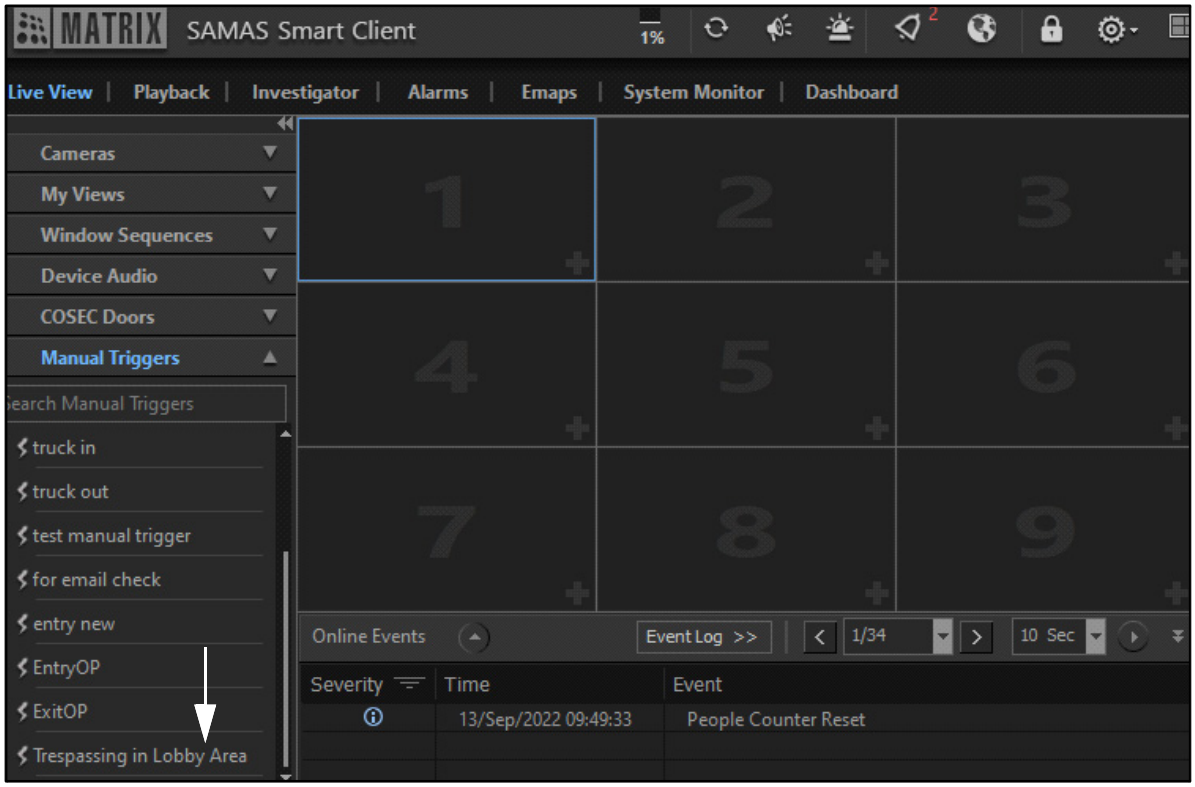


- Select the desired Manual Trigger from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Manual Trigger. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

After the Manual Trigger has been configured, you can trigger the Event manually from the **Smart Client > Live View > Manual Triggers**.


MATRIX
SAMAS Smart Client
1%
Live View
Playback
Investigator
Alarms
Emaps
System Monitor
Dashboard
Cameras
My Views
Window Sequences
Device Audio
COSEC Doors
Manual Triggers
earch Manual Triggers
truck in
truck out
test manual trigger
for email check
entry new
EntryOP
ExitOP
Trespassing in Lobby Area
1
2
3
4
5
6
7
8
9
Online Events
Event Log >>
1/34
10 Sec
Severity
Time
Event
13/Sep/2022 09:49:33
People Counter Reset

Custom Events

Custom Events feature is supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.

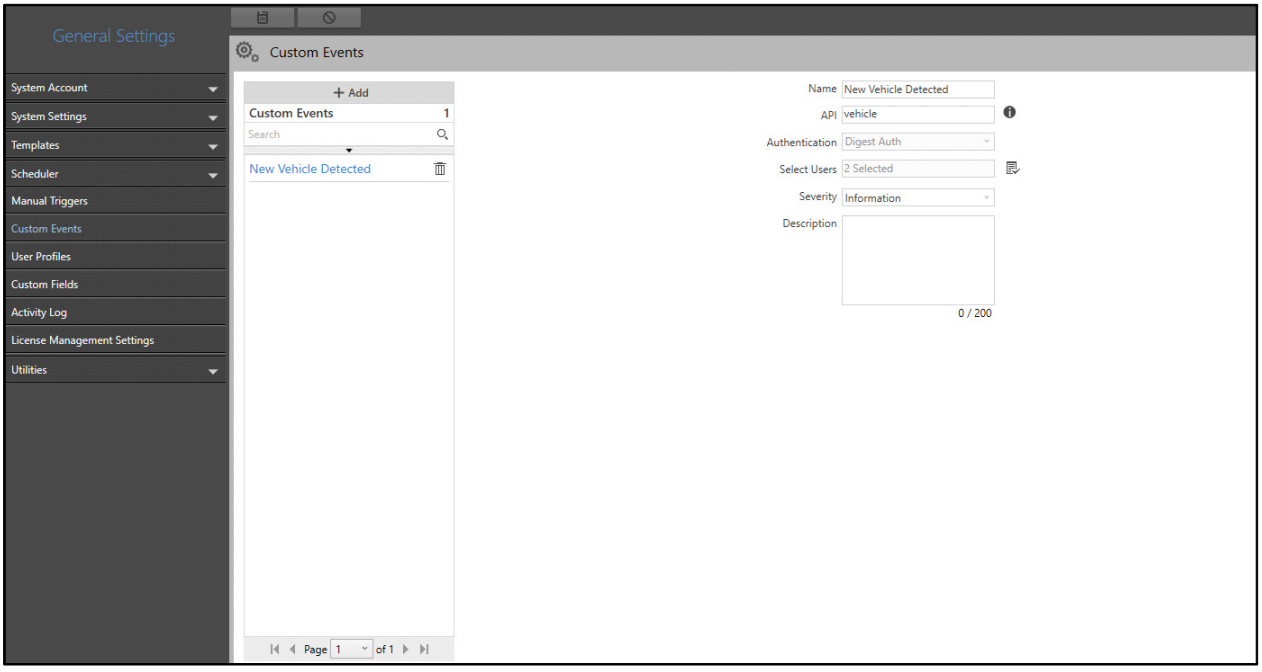
From Software Release V6R4 and onwards, if Management Server is running on SSL Mode, only HTTPs API requests will be accepted over SAMAS HTTP API Port configured under SSL section of Management Server Manager.

The Custom Events page displays the configured Custom Events. Custom Events are user-defined Events. These Events can be triggered using the API of third party applications. You can also configure actions for the Custom Events. You can view and configure Custom Events from this page.

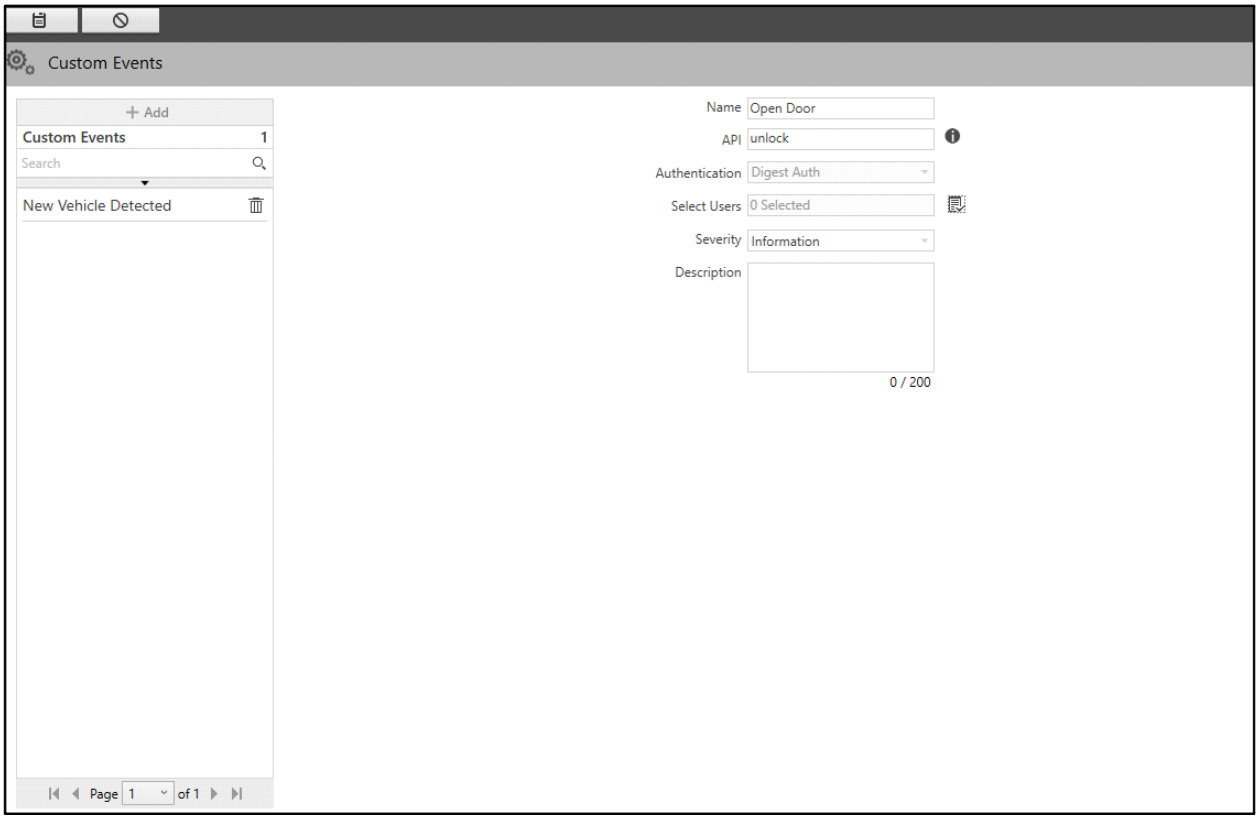
Please note that before you trigger API from the third party application, you need to configure the Management Server IP and SATATYA SAMAS TCP and HTTP Port in the third party application.

To configure Custom Events,

- Click **General Settings > Custom Events**.



- Click **Add**.



Configure the following parameters:

- **Name:** Specify a suitable name for the new Event. For example, Open Door Event. In Name, you can enter upto 50 characters. Default: Blank.
- **API**: Specify a unique Third Party API to trigger the Custom Event. In API, you can enter upto 500 characters. Default: Blank.

  You can enter the third party HTTP/HTTPs and TCP API. The API entered in this field gets appended with the Management Server's IPv4/IPv6 Address and SATATYA SAMAS HTTP Port in the format as shown when you hover the cursor over the Information icon.

  For example, you enter the third party API as **trigger** in the API field, the HTTP API will be formed as; http://192.168.104.24:8300/trigger where, 192.168.104.24 is MS IP Address and 8300 is SAMAS HTTP API Port.

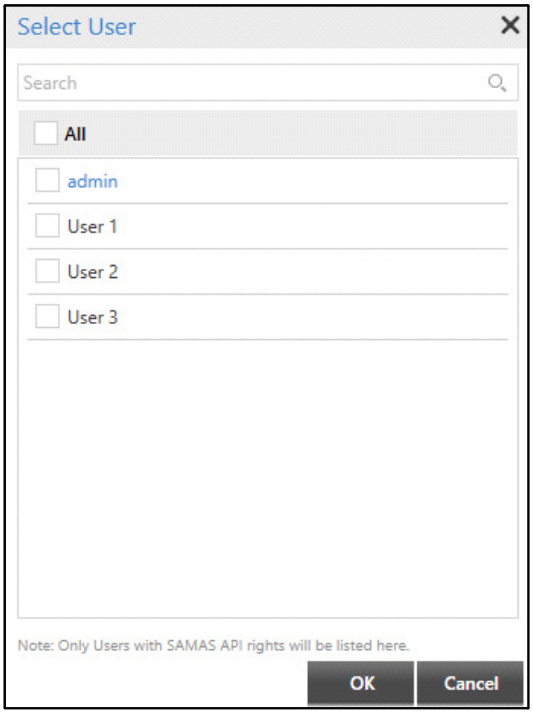
  If you have configured SAMAS HTTP API Port under SSL section of Management Server Manager, then the HTTPs API will be formed as; https://192.168.104.24:7300/trigger.
- **Authentication**: It is un-editable and displays **Digest Auth**. In this case, you will need to enter the valid login credentials when you fire the API.

When you upgrade SAMAS to V6R4 and later:

- *It is mandatory that Users have been granted **SAMAS API** "Application Rights"to be able to fire API successfully.*
- *The custom events configured before upgrade will display Authentication as **No Auth**. If you select **Digest Auth** and save the configuration, you cannot change the Authentication again.*
- *If the Authentication is selected as **No Auth**, then no authentication will be required when firing the API.*
- *"Password Validity", "Account Lockout Policy" and "IP Blocking Policy" are applicable to Custom Event. If any invalid attempts are made to fire API, the same will be logged under "Event Log".*

- **Select Users**: Select the desired users to whom you wish to grant Custom Events rights. Only those users who have SAMAS API right will appear in this list.

  - Click **Select Users** picklist. The **Select User** pop-up appears.



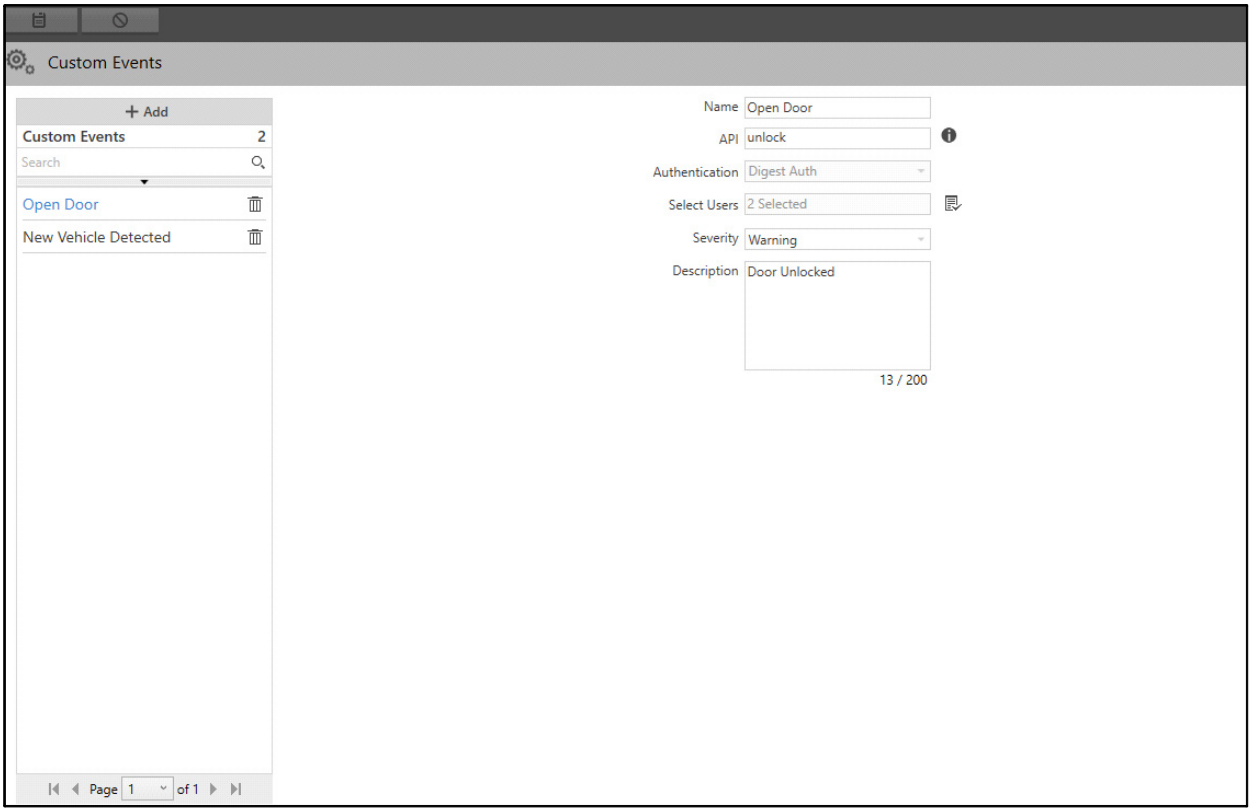
  - Select the check boxes for the desired users. Click **OK**.

- **Severity**: Select the Severity level from the drop-down list — Information, Warning, Error and Critical.

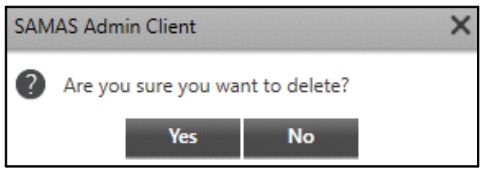
- **Description**: Enter the desired text in the Description box related to the Event. In Description, you can enter upto 200 characters. Default: Blank.

- Click **Save** to save the settings or **Cancel** to discard.

The new Custom Event appears in a list on the left hand side. You can change the configurations of the Custom Event or delete it.



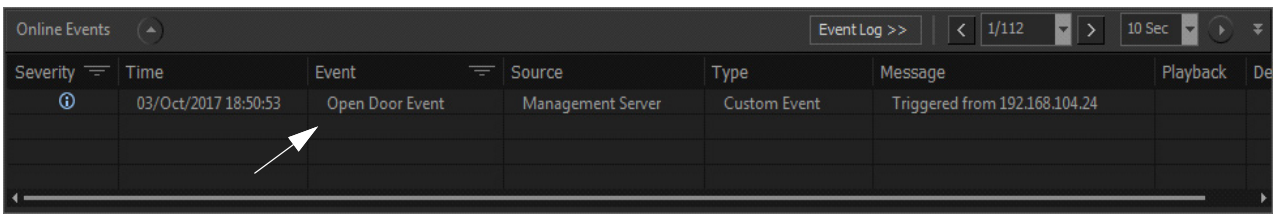
- Select the desired Custom Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Custom Event. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

Consider a Scenario, where on triggering the API from the third party application leads to opening of the door.

When the API is triggered from a third party application, it is matched with the API configured in the Custom Event (Admin Client). If the API matches, the door opens. The Event generated can be viewed in the Smart Client.



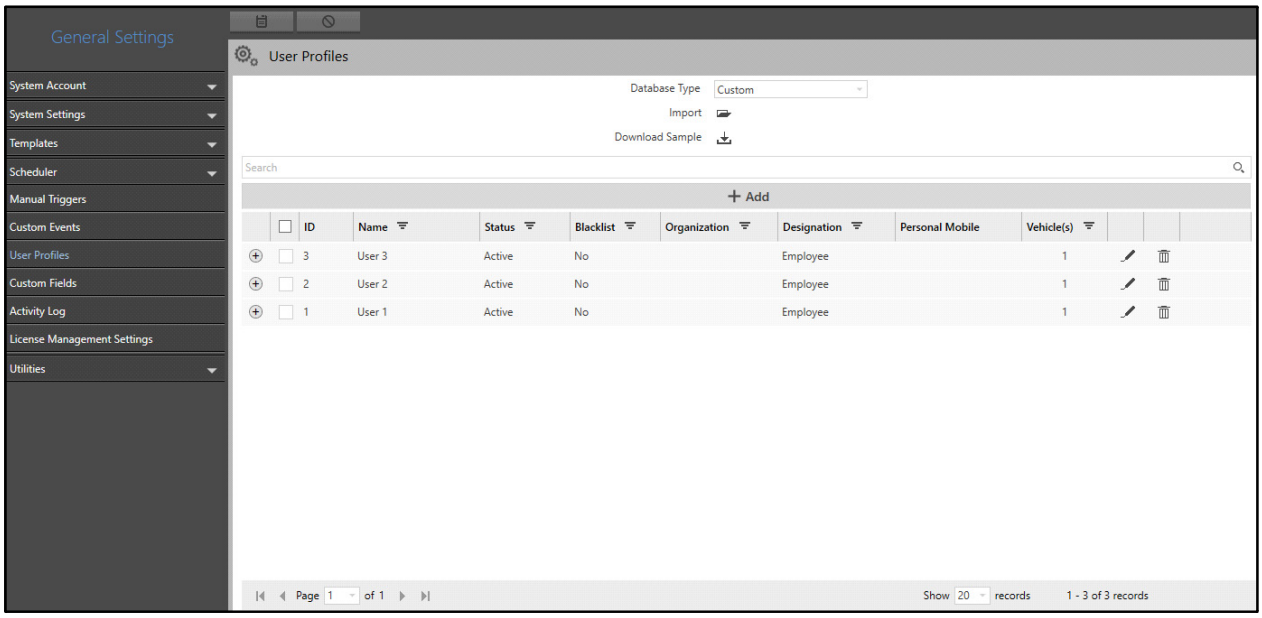
User Profiles

The User Profile page enables you to configure parameters related to the details of a user and vehicle in the database. You can view and configure User Profiles from this page. This data helps to allow only the authorized users to access various areas of the premises. There are two types of databases from which a user can be authorized. These are — COSEC and Custom (SATATYA SAMAS local database).

User Profile searches for the user details of the identified Vehicle Number from the COSEC Server or from SATATYA SAMAS database. It then intimates the Smart Client user, whether to allow or deny the identified user. If the user is not found, appropriate action needs to be taken.

To configure User Profiles,

- Click **General Settings > User Profiles**.



Configure the following parameters:

- **Database Type:** Select the database from which the identified user is to be searched. You can select **Custom** or **COSEC**.

  If **COSEC** is selected, the user details are fetched from the COSEC Server database and accordingly actions are taken for authorizing a user.

  If **Custom** is selected, user details are fetched from the SATATYA SAMAS database. You can insert user data manually in the database or import an excel sheet directly.

  If you have selected **Custom** as the Database Type, configure the following parameters:

  The data in the Custom database can be imported using the Import option or you can enter the details manually using the Add option.

Using Import option:

To use this option, you must first download the sample file. Update the desired details and then import the updated file.

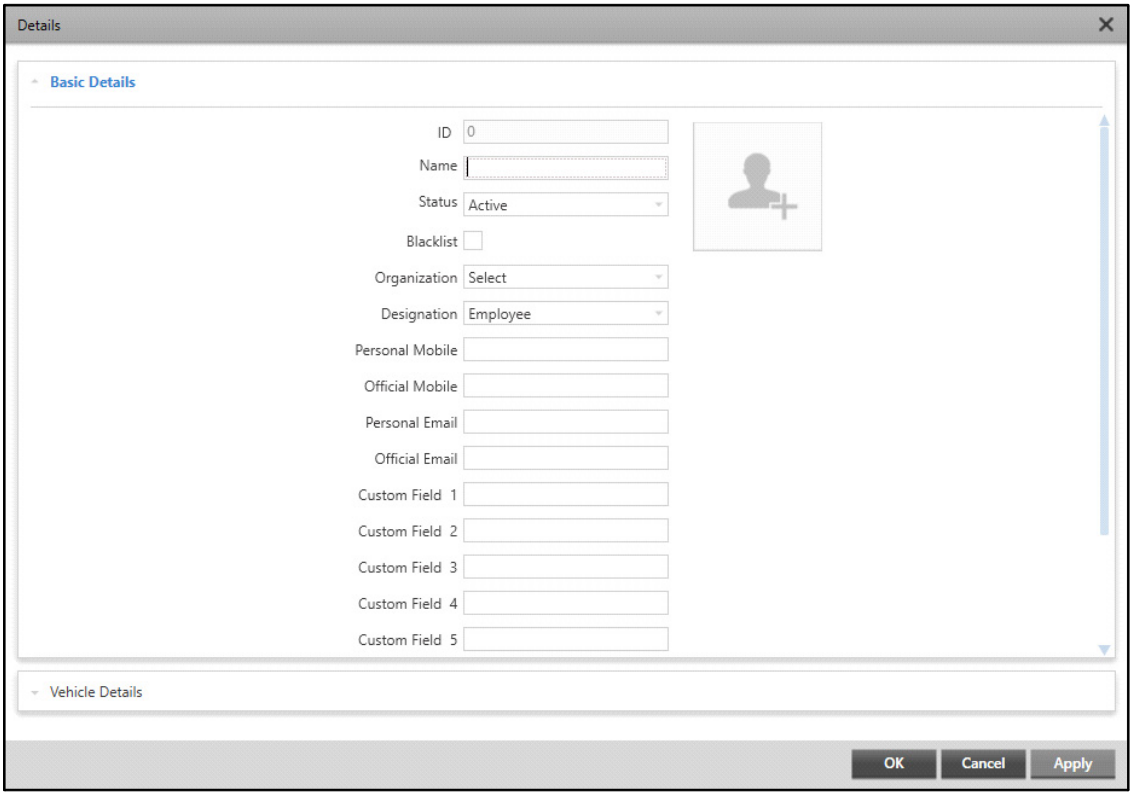
- **Import:** Before you import the file, you need to **Download Sample** file. Update the details of the Users as per the fields in this file. Now, click to import the file you have saved with the updated details. The maximum file size supported is 25MB.

- **Download Sample:** Click to download the sample database file. Enter the details of the User and Vehicle in this excel file. Once you have updated all the user details, save this file. You can now import this file.

Using Add option:

If you do not wish to use the Import option, you can also update the database manually.

- Click **Add**. The **Details** pop-up appears.



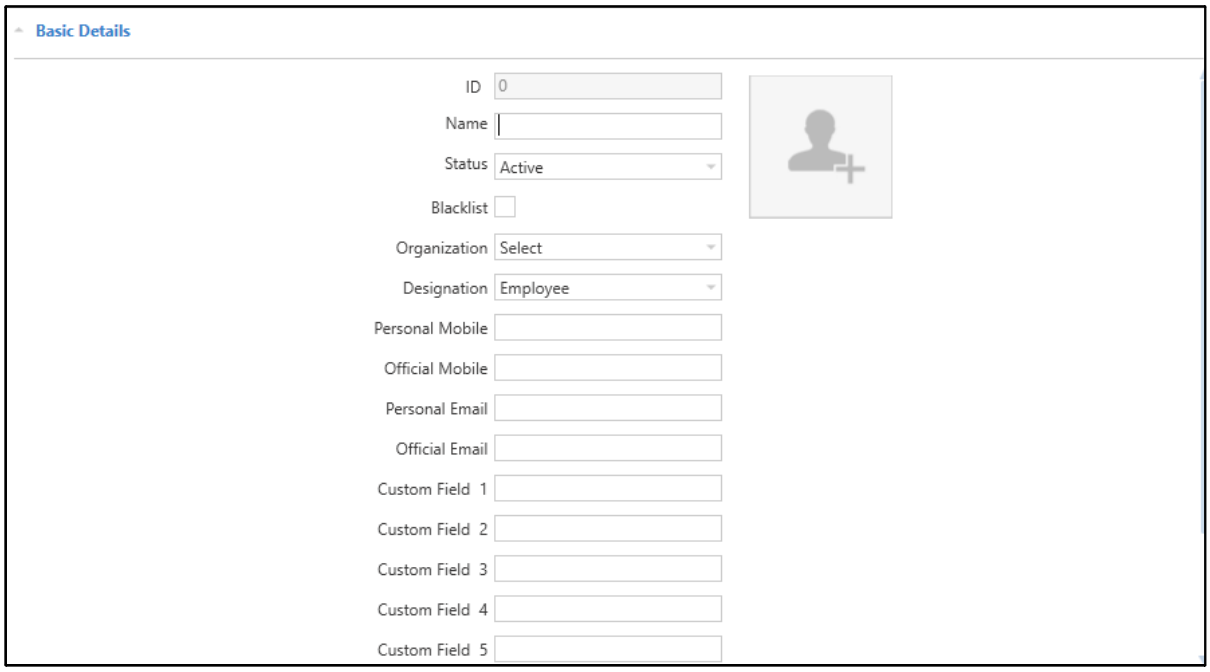
The Details pop-up contains two collapsible panels — “Basic Details” and “Vehicle Details”.

Basic Details

This panel displays the configurations for Basic Details. You can add or edit the user’s Basic Details from this collapsible panel.

To add or edit the Basic Details,

- Click the **Basic Details** collapsible panel.



Configure the following parameters:

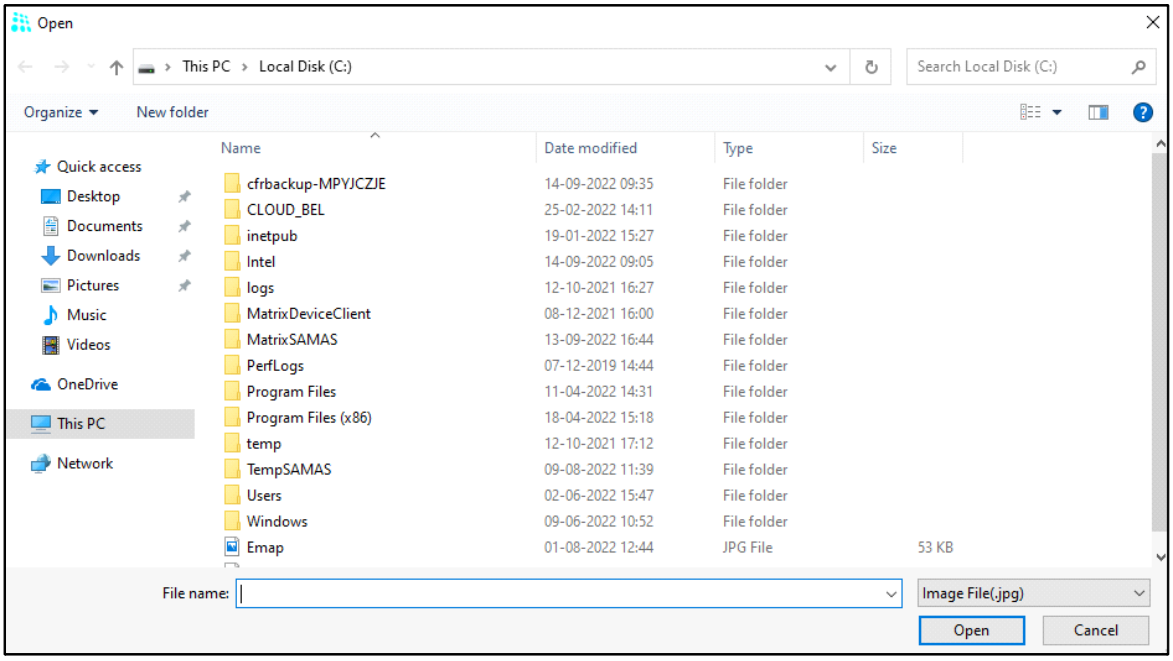
- **ID**: This is a non-configurable field that will generate a unique numeric ID in ascending order for each configured user. It shows 0 value while configuring the user profile.
- **Name**: Specify the name of the user. In Name, you can enter upto 50 characters. Default: Blank.
- **Status**: Select the status of the user from the drop-down list — Active or Inactive.
- **Blacklist**: Select the check box if you wish to blacklist the user. If the check box is enabled, the status is set to Inactive automatically.
- **Organization**: Select the Organization with which the user is associated from the drop-down list. You can configure Organization from the User Attributes section. For more details, refer to “Organization”.
- **Designation:** Select the Designation of the user from the drop-down list. You can configure designation from the User Attributes section. For more details, refer to “Designation”.
- **Personal Mobile**: Specify the Personal Mobile Number of the user. In Personal Mobile, you can enter upto 15 characters. Default: Blank.
- **Official Mobile**: Specify the Official Mobile Number of the user. In Official Mobile, you can enter upto 15 characters. Default: Blank.
- **Personal Email**: Specify the Personal Email Address of the user. In Personal Email, you can enter upto 100 characters. Default: Blank.
- **Official Email**: Specify the Official Email Address of the user. In Official Email, you can enter upto 100 characters. Default: Blank.
- **Custom Field:** User Custom fields are used to add extra user information as per your requirement in the User Profile. In Custom Field, you can enter upto 50 characters. Default: Blank.

For example, for a user you wish to configure the User Profile with Aadhar Card Number and Date of Birth. You can utilize two custom fields and configure the display name as per your requirement from the User Attributes section in Utilities. For more details, refer to “User Attributes”.

- **Remarks**: Enter the remarks for the user, if required. In Remarks, you can enter upto 200 characters. Default: Blank.

Once these configurations are done, you need to add a profile picture of the user.

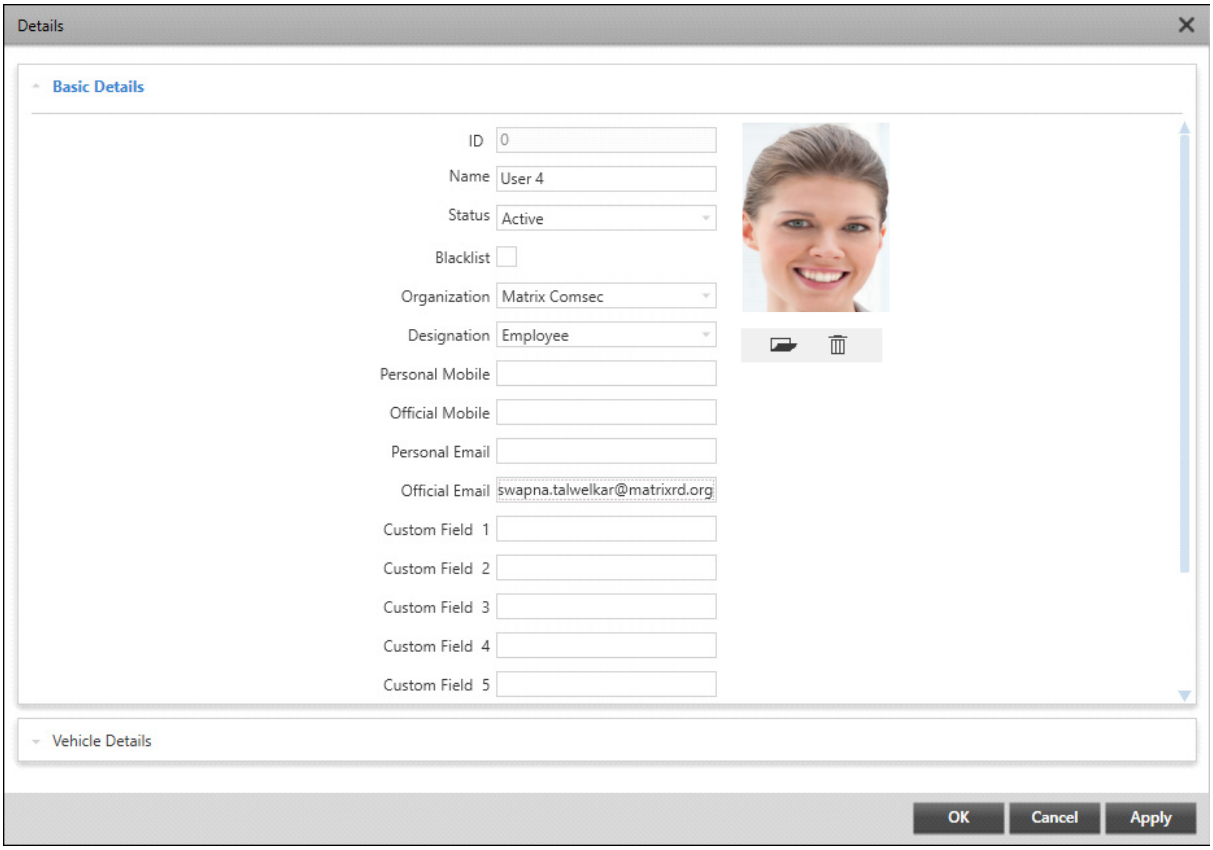
- Click **Add** . The **Open** pop-up appears.



- Select the desired image to be uploaded.
- Click **Open** to upload the image or **Cancel** to discard.

*The size of the User image can be of upto **50kb** and formats supported are **.jpg** or**.bmp**.*

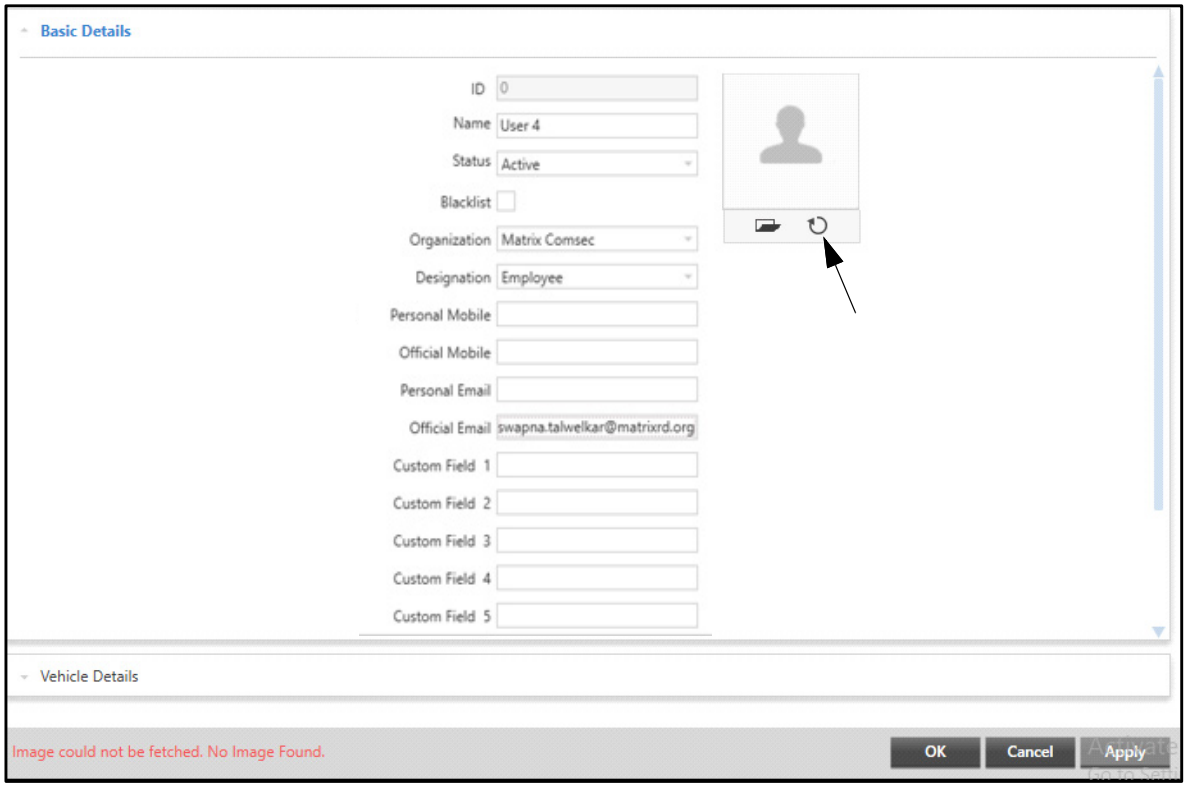
The Profile picture appears along with the configured details. You can browse another picture or delete it.



- Click **Browse** to select another picture from the desired path.
- Click **Delete** to delete the profile picture.

The image uploaded for profile picture will be saved into the Image Storage Drive. If due to any reason the image upload fails, a notification will be send for the same with a validation message.

When you wish to edit the Profile of any previously enrolled user, the MS will try to fetch the profile picture of that particular user from Image Storage Drive. If due to any reason, the MS is unable to fetch the image from drive, an option for retry appears.



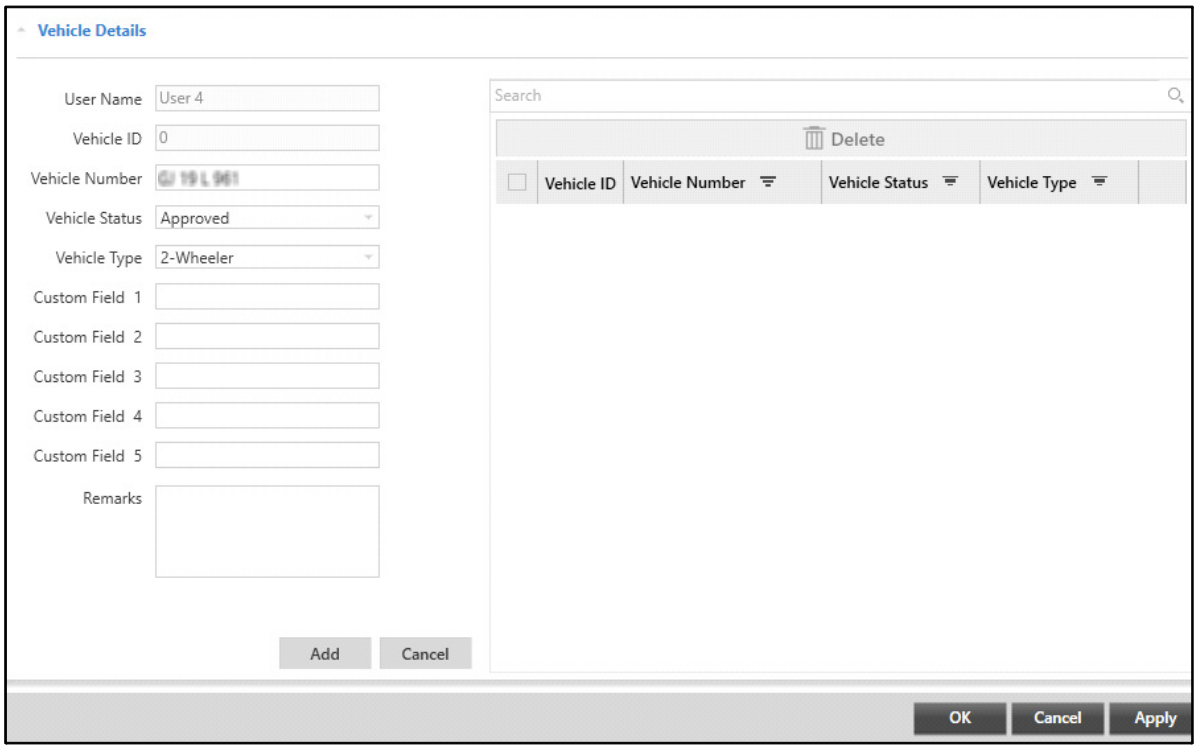
- Click **Retry** for the MS to try once again to fetch the User image from the configured Image Storage Drive.
- Click **Apply** to save the Basic Details and the Profile Picture.

Vehicle Details

This panel displays the configurations for Vehicle Details. You can add or edit the user's Vehicle Details from this collapsible panel.

To add or edit the Vehicle Details,

- Click the **Vehicle Details** collapsible panel.



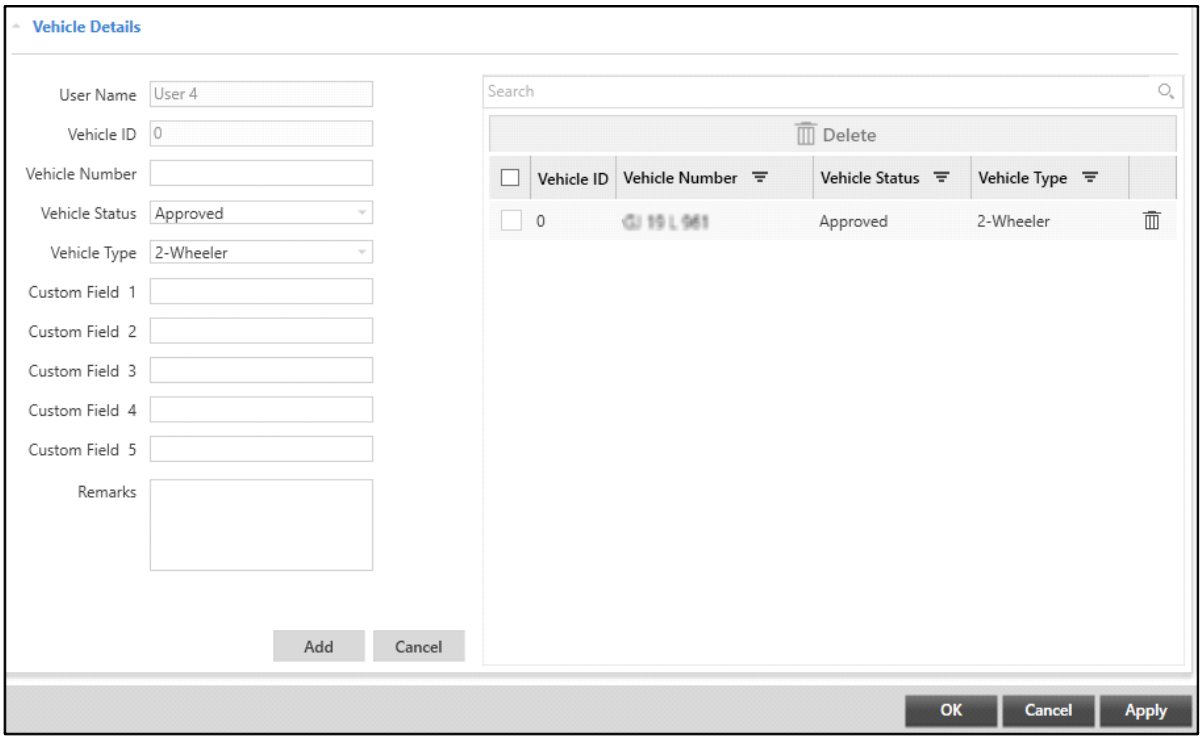
Configure the following parameters:

- **User Name**: The User Name is non-configurable. It is fetched from the Basic Details.
- **Vehicle ID**: This is a non-configurable field that will generate a unique numeric ID in ascending order for each configured vehicle. It shows 0 value while configuring the vehicle details.
- **Vehicle Number**: Specify the License Plate Number of the user's vehicle. In Vehicle Number, you can enter upto 50 characters. Default: Blank.
- **Vehicle Status**: Select the Vehicle Status to be assigned to the vehicle from the drop-down list.
- **Vehicle Type**: Select the type of vehicle from the drop-down list. You can configure vehicle type from the Vehicle Attributes section. For more details, refer to "Vehicle Attributes".
- **Custom Fields**: Vehicle Custom fields are used to add extra vehicle information as per your requirement in Vehicle details of the User Profile. In Custom Fields, you can enter upto 50 characters. Default: Blank.

  For example, a user wants to configure Vehicle Details with Vehicle Model. You can utilize one custom field and configure the display name as per your requirement from the Vehicle Attributes section in Utilities. For more details, refer to "Vehicle Attributes".
- **Remarks**: Enter the remarks for the user's vehicle, if required. In Remarks, you can enter upto 200 characters. Default: Blank.

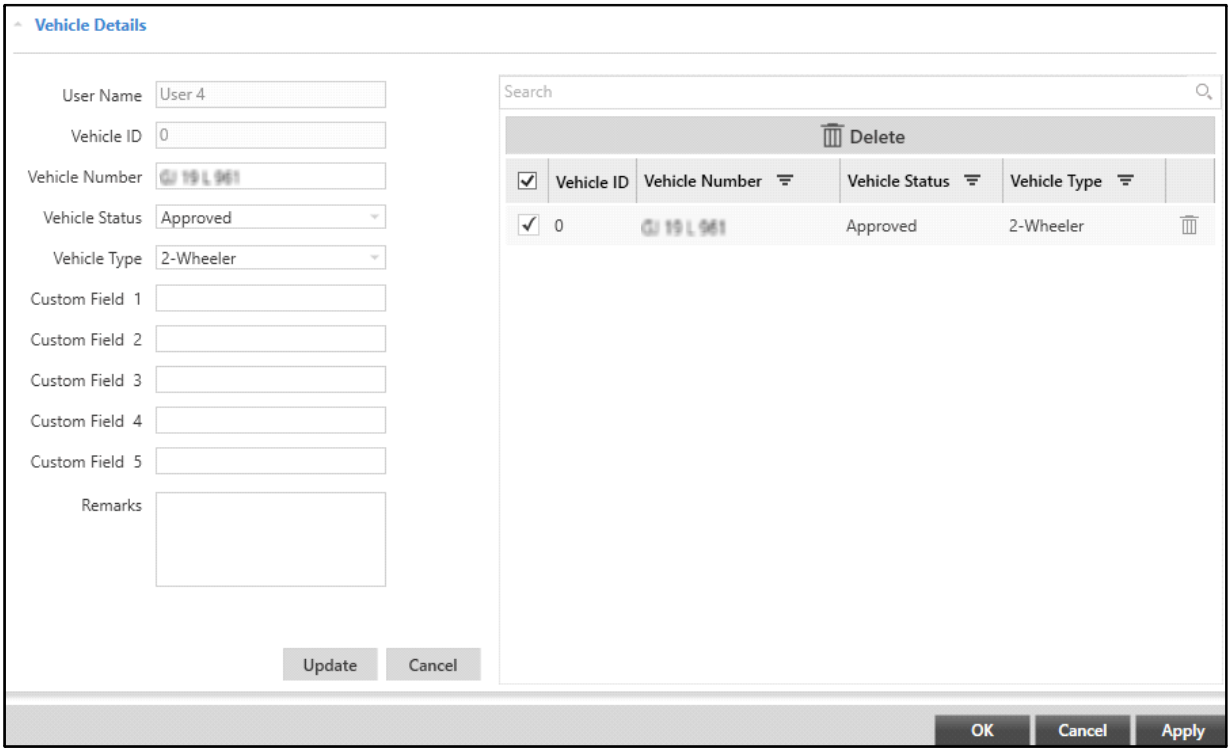
- Click **Add** to add the Vehicle Details or click **Cancel** to discard.

  The added Vehicle Details appear in a list on the right hand side. You can change the Vehicle Details or delete it.



- To edit, select the check box of the Vehicle ID that you wish to edit. Edit the configurations on the left hand side as per your requirement.

- Click **Update** to update the configurations or click **Cancel** to discard.



- To delete, click **Delete** against the desired Vehicle ID.

- You can filter the records. To do so, click **Filter** of the respective parameter — Vehicle ID, Vehicle Number, Vehicle Status, Vehicle Type.

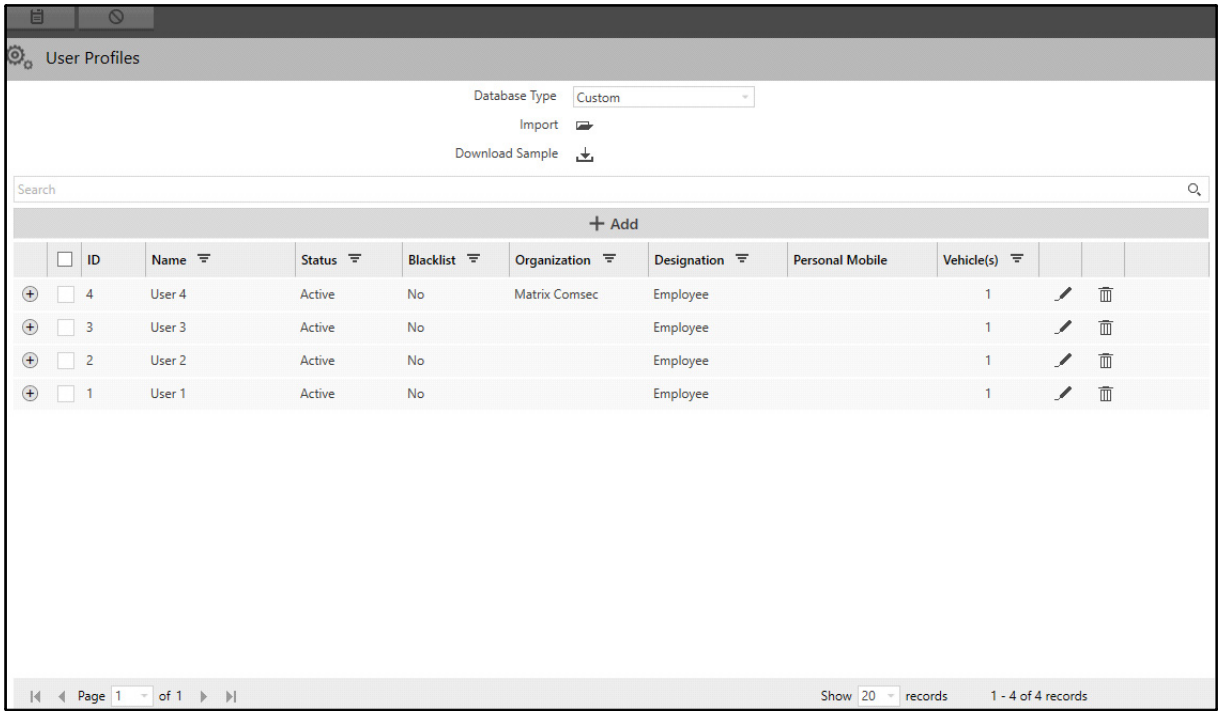
  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER** of the desired parameter.

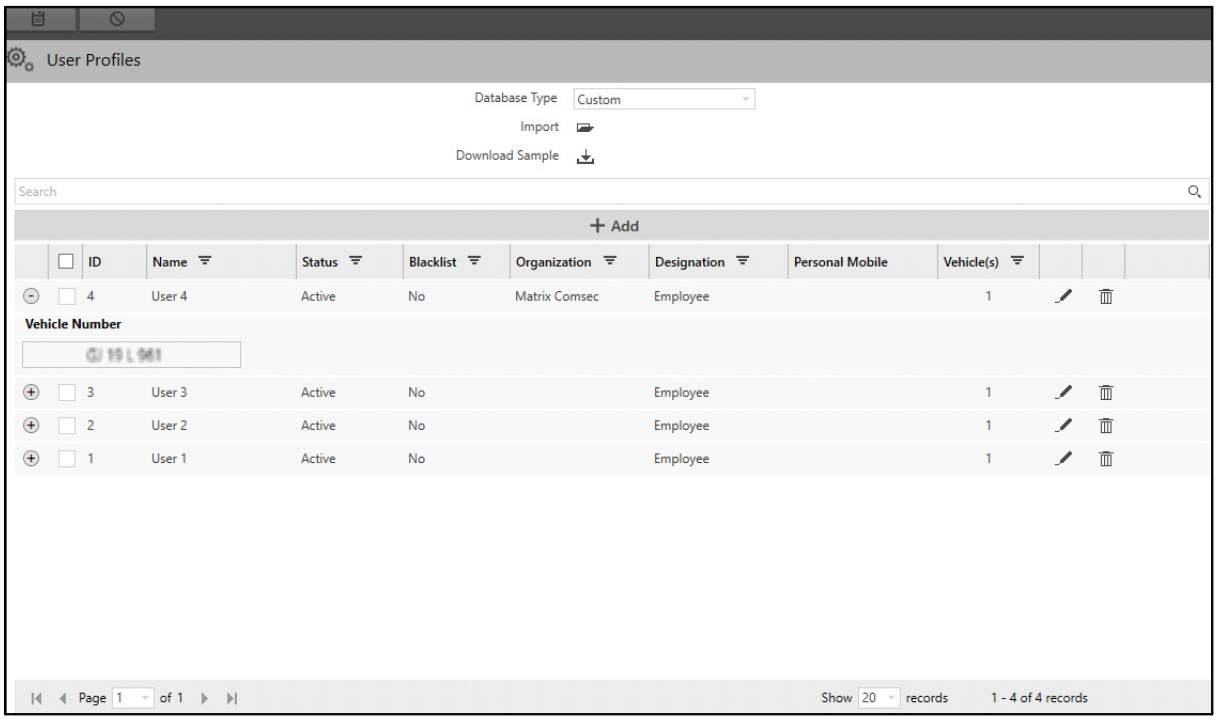
- You can also **Sort** records. To do so, click on the desired option — Vehicle ID, Vehicle Number, Vehicle Status, Vehicle Type in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

- Click **Apply** to save the Vehicle Details and click **OK** to close the pop-up.

The configured User and Vehicle Details appear in a list on the User Profiles page.



- Click **Show Vehicle Number** to view the Vehicle Number configured against the User Profile.



- Click **Edit** to edit the desired User Profile.
- Click **Delete** to delete the desired User Profile.
- You can filter the records. To do so, click **Filter** of the respective parameter — ID, Name, Status, Blacklist, Organization, Designation, Vehicle(s).

  Select the check box of the desired option and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER** of the desired parameter.

- You can also **Sort** records. To do so, click on the desired option — ID, Name, Status, Blacklist,

  Organization, Designation, Personal Mobile, Vehicle(s) in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

- Click **Save** to save the settings or **Cancel** to discard.

Custom Fields

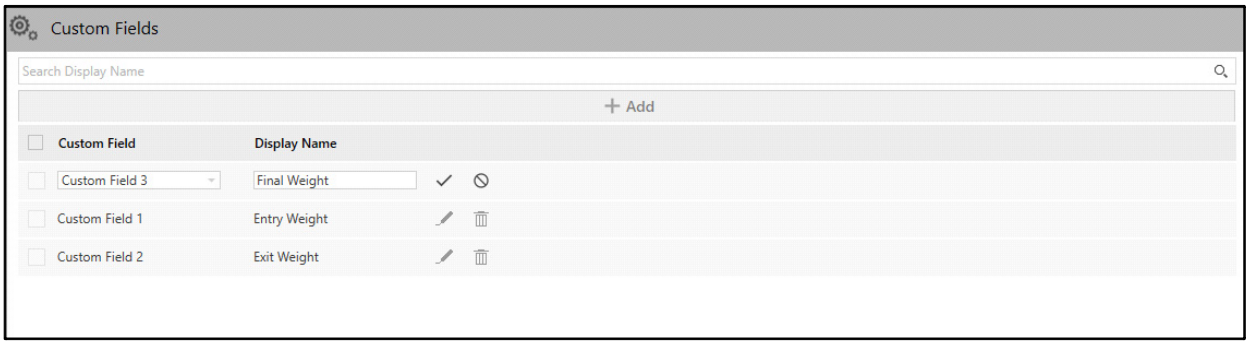
The Custom Fields page displays the configured Custom Fields. Custom Fields is a feature that enables the third party application or user to manually insert the user defined data in SATATYA SAMAS database. This database can be used for generating various reports based on the data collected by Admin Client and user data received from Smart Client. You can create upto 101 Custom Fields. You can view and configure Custom Fields from this page.

To configure Custom Fields,

- Click **General Settings > Custom Fields**.



- Click **Add**.

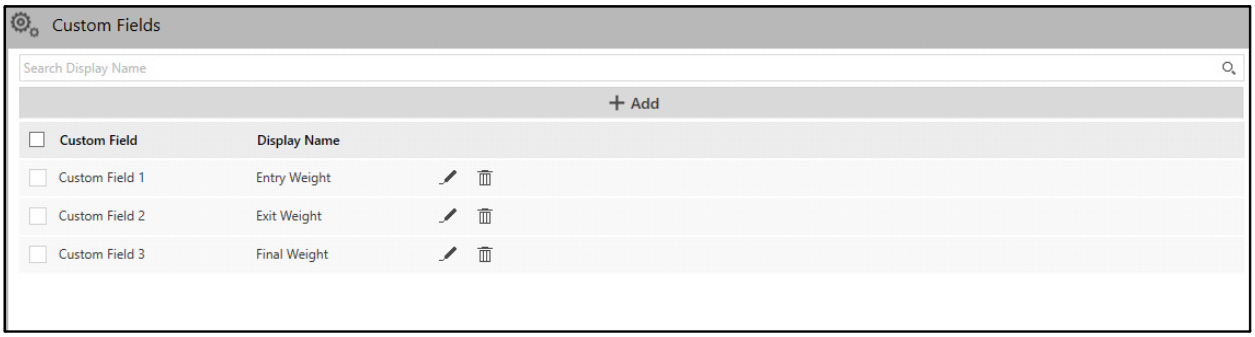


  Configure the following parameters:

  - **Custom Field**: Select the Custom Field from the drop-down list. The **SAMAS Mapping Field** is a default field.
  - **Display Name**: Specify a suitable name for the Custom Field. In Display Name, you can enter upto 50 characters. Default: Blank.

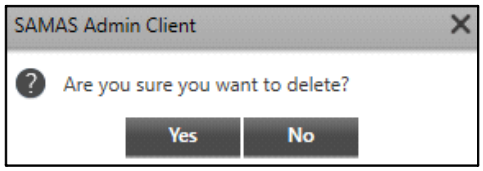
- Click **Save** ✓ to save the details or click **Cancel** ⊘ to discard.

The new Custom Field appears in the list. You can change the configurations of the Custom Field or delete it.



You can search for the desired Custom Field using the Search Bar. Enter the Display Name keyword to search the Custom Fields.

- Click **Edit** to edit the desired Custom Field from the list.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Custom Field. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

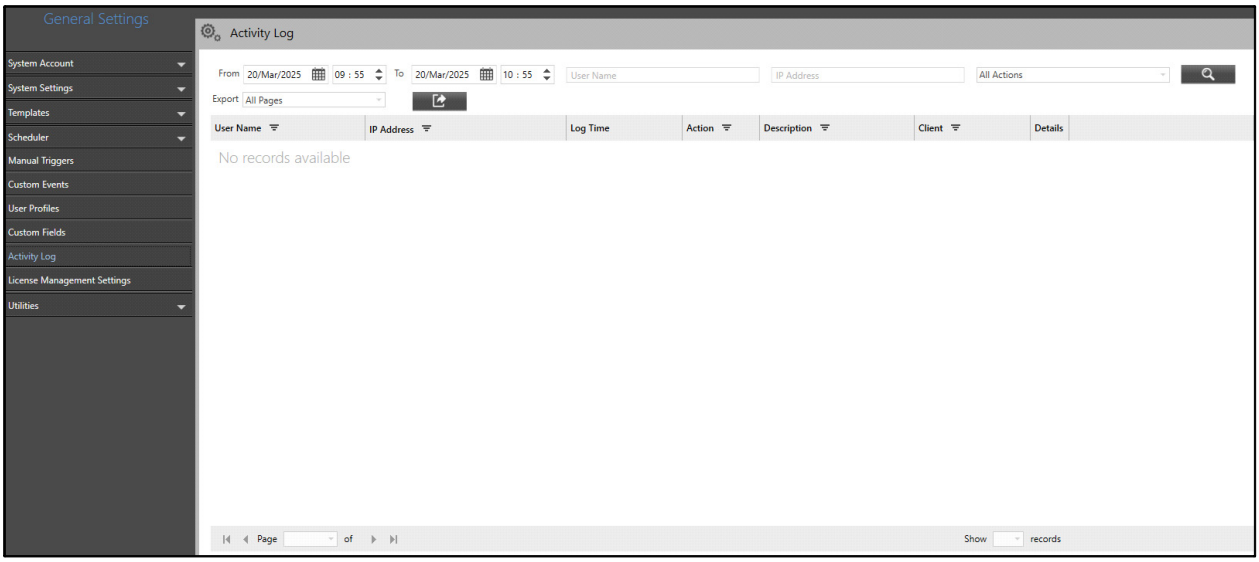
Activity Log

Activity Log is a feature that monitors and logs all the activities of the entire application, helping the users to view and check every activity in the system at any given time. Activity Log has a buffer capacity of 500 records which are stored using the FIFO method.

The Activity Log page displays the logs for all the users of the Admin Client. You can search and filter different logs from this page.

To configure Activity Log,

- Click **General Settings > Activity Log**.



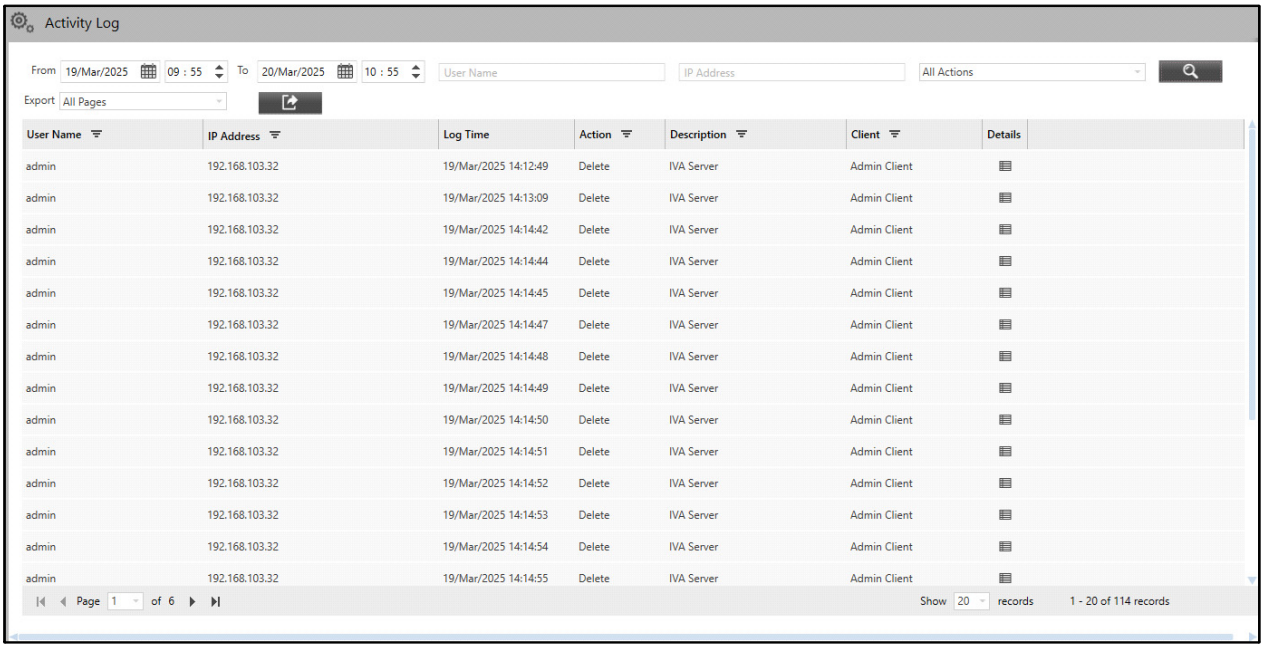
Configure the following parameters:

- **From**: Select the date from which you wish to view the Activity Log from the calendar and specify the time.
- **To**: Select the date till which you wish to view the Activity log from the calendar and specify the time.
- **User Name**: Specify the User Name of the user whose logs you wish to view. In User Name, you can enter upto 50 characters. Default: Blank.
- **IP Address**: Specify the IPv4/IPv6 Address of the user whose logs you wish to view. In IP Address, you can enter upto 39 characters. Default: Blank.
- **Actions**: Select the type of action for which you wish to view the Activity Logs from the drop-down list—All Actions, Add, Update or Delete.

- Click **Search** . The list of all the activities as per the set configuration appear.

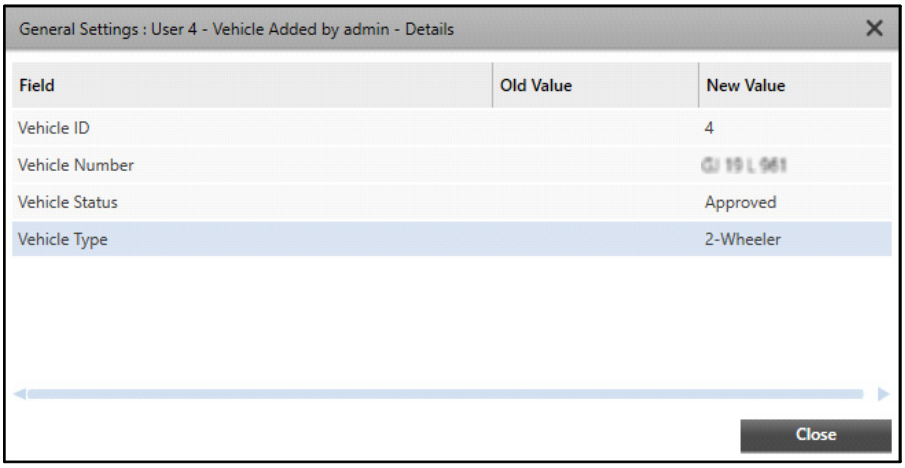
Sensitive Transactions include — Clips exported from Playback and Investigator using the Smart Client. Sensitive Transactions will be displayed in the Activity Log for a user if ***Re-authenticate on Sensitive Transaction*** *is enabled for that user.*

Passwords displayed will appear masked.



Each log displays the details — User Name, IP Address, Log Time, Action, Description, Client and Details.

- To view additional details, click **Details** corresponding to the desired log. The following pop-up appears.

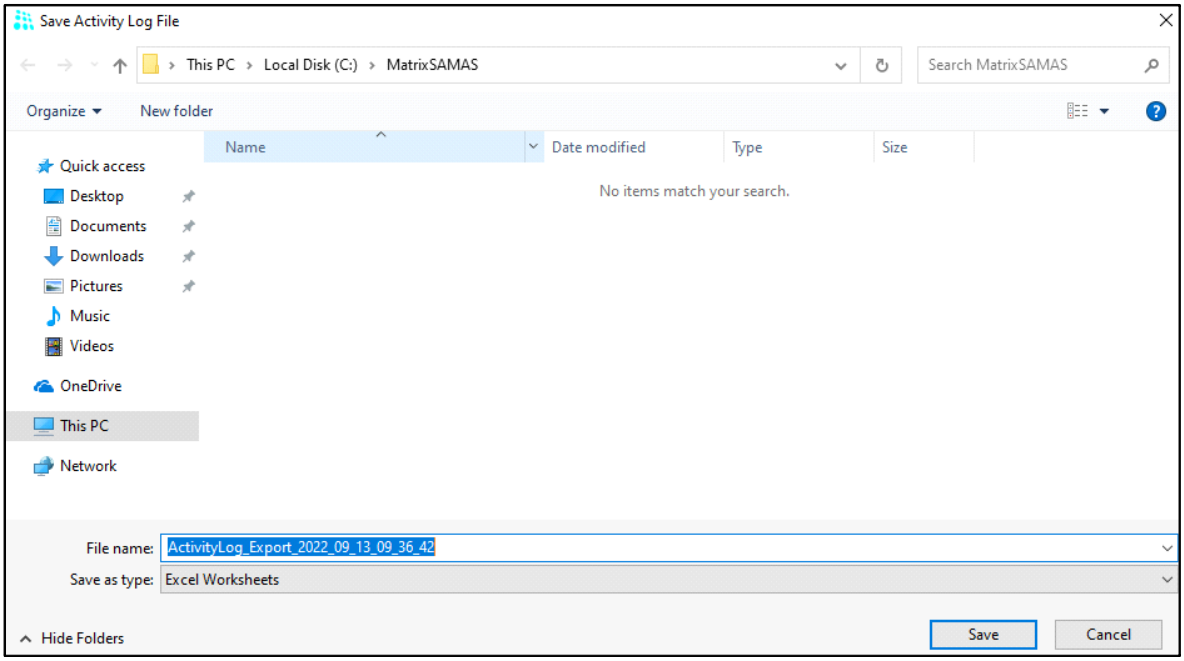


- Click **Close** to close the pop-up.

The Name of the pop-up and the details displayed vary from log to log. It depends on the type of action (Add, Update or Delete) and the activity.

You can also export the Activity Logs. To do so,

- Select the pages that you wish to export from the **Export** drop-down list.
- Click **Export** . The **Save Activity Log File** pop-up appears.



- Select the desired folder where you wish to save the Activity Log file and specify the file name.
- Click **Save** to save the file or click **Cancel** to discard.

License Management Settings

The License Key may be a Virtual Key or a Dongle Key. From the License Management Settings page:

- you can manage the upgradation/registration of these keys.
- view the details of the activated license under Existing License Profile.

Make sure the login user has atleast View and Edit rights of General Settings Module. For details refer to "Configuration Rights" in "User Groups".

If you have opted for Service Based/Device Based License Key, then the Dongle will have only the GENERIC license, all other license vouchers need to be purchased. These need to be purchased as per your requirement. Once ordered, you will receive keys in the form of a PDF file.

If you have opted for Virtual License or you wish to migrate from Dongle License to Virtual License, then you need to purchase the MATRIX VIRTUAL DONGLE300 Key as well as other vouchers as per your requirement.Once ordered, you will receive keys in the form of a PDF file. You may receive a single PDF will the Generic Key as well as the vouchers activated or you may receive separate PDFs — Generic Key PDF and then other PDFs as per the order placed.

For the details regarding the various licenses that can be purchased, refer to "Supported Licenses".

After you have received the License Key PDF as per your requirement, you need to register/update the same. For details, refer to the relevant link — "Virtual License Key" or "Dongle License Key".

Virtual License Key

If you have opted for Virtual License for the first time or opted to migrate from Dongle License to Virtual License, you need to make sure you have purchased the Licenses — MATRIX VIRTUAL DONGLE300 Key and the SATATYA SAMAS PLT Key (as well as the Module licenses need to be purchased as per your requirement). You may receive a single PDF or multiple PDFs for these keys.

For Virtual License, you need to have:

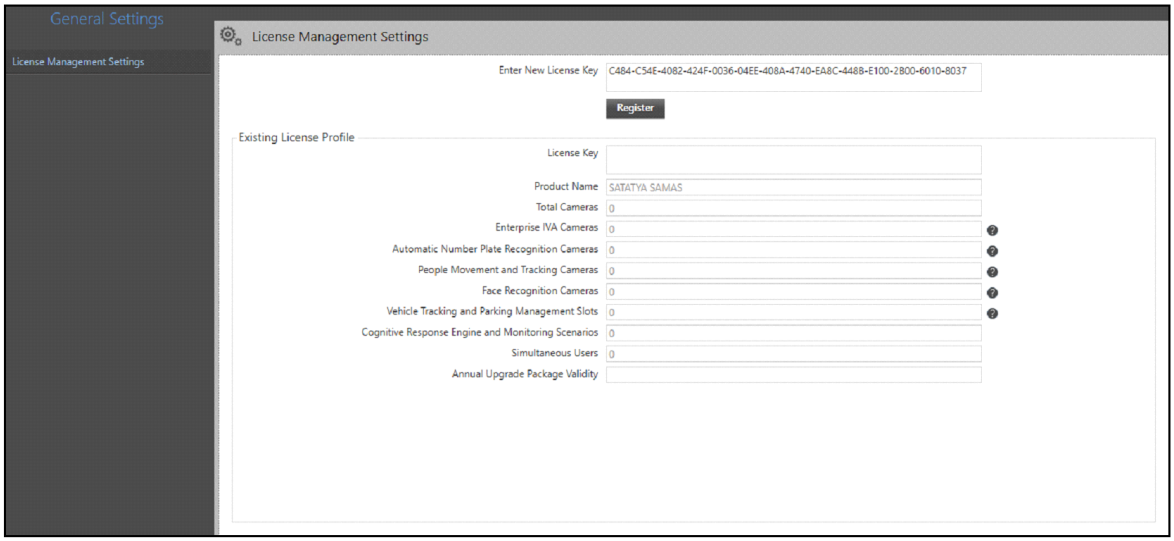
- a persistent Internet connection with good speed (where Management Server is running).
- License Key PDFs are kept handy for activation.

The SAMAS communicates with the Virtual License Manager (VLM) for registration, updation as well as re-registration. If the connectivity is established, the further process continues. For details refer to:

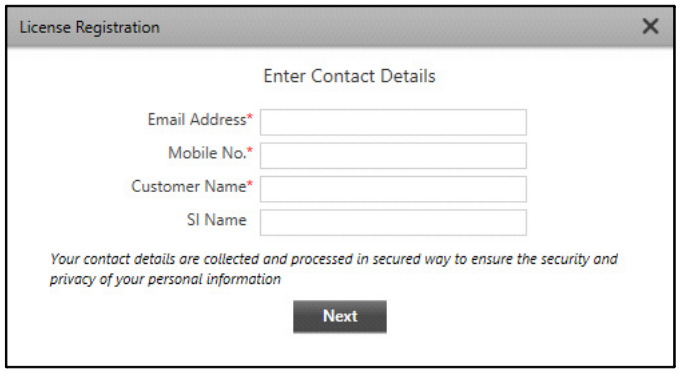
- "Registering the Virtual License Key"
- "Updating the Virtual License Key"
- "Updating the Contact Details"
- "Re-registering the Virtual License Key"

Registering the Virtual License Key

- Click **General Settings > License Management Settings**.
- **Enter New License Key:** Enter the Generic Virtual License Key / migrated Virtual License Key received in the PDF here. To do so,
  - Open the Generic Virtual License Key PDF / migrated Virtual License Key PDF file and select the key.
  - Drag and drop the same onto this field.



- Click **Register**. The **License Registration** pop-up appears.

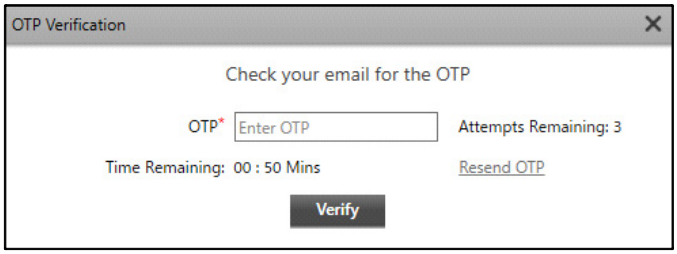


Configure the following parameters:

- **Email Address:** Enter the Email ID of the Client. Make sure it is genuine as the Alerts/Notifications as well as authentication OTP will be sent on this Email ID. In Email Address, you can enter upto 100 characters. Default: Blank.
- **Mobile No.:** Enter the Mobile Number of the Client. In Mobile No., you can enter upto 20 characters. Default: Blank.
- **Customer Name:** Enter the Customer Name. In Customer Name, you can enter upto 30 characters. Default: Blank.

- **SI Name:** Enter the name of the SI. In SI Name, you can enter upto 30 characters. Default: Blank.
- Click **Next**.

The **OTP Verification** pop-up appears and an OTP is sent to your Email ID.



- **OTP:** Check your Email ID for the OTP and enter the same here. In OTP, you can enter upto 6 characters. Default: Blank.

As soon as the system sends the first OTP, the Time Remaining timer begins. The Attempts Remaining are displayed.
In case you do not receive the first OTP, you can click Resend OTP only after the Time Remaining timer expires.
When you click Resend OTP, the OTP is sent again to the Email ID and the Time Remaining timer begins once again and number of Attempts Remaining is updated.

- Click **Verify**.

Once the Generic Virtual License Key or the Key PDF with all the desired vouchers activated is authenticated and registered successfully, the **License Activation Successful** message appears.

Once the License is activated, you are logged-out and re-directed to the Login page.

This registered Virtual License Key details are displayed in License Key under “Existing License Profile”.

SAMAS then checks the availability of the VLM Server at regular intervals (make sure you have a persistent Internet connection where Management Server is running) and if it is unable to reach the VLM Server, then the event — Virtual License Validation Failed — will be generated. To send this event notification as SMS/Email/Push Notification to the selected user’s Email ID/Mobile Number/Mobile Client (SATATYA VISION), make sure the desired scenario and action is configured as follows:

- Select Event Source Type as Management Server.
- Select Event as Virtual License Validation Failed.
- Select Action as per your requirement. We recommend you to configure Send SMS/Send Email/Push Notification as Actions, if required.

For details, refer to “Basic Scenario”.

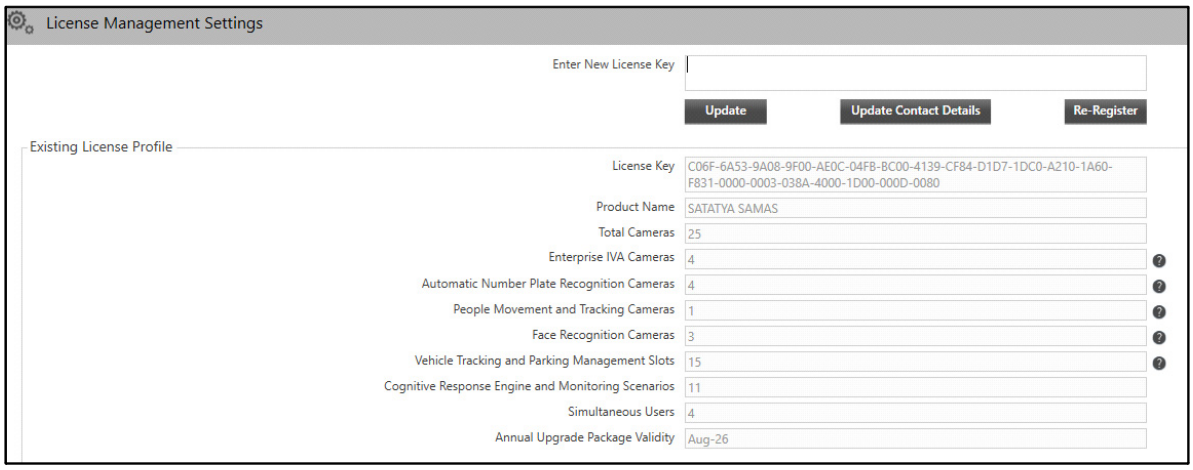
The Virtual License Validation Failed Event will appear in the Event Log as well as in the Smart Client.

If you encounter an error “License Key not Valid. Please Register Again”, you will need to register your Virtual License Key again. Make sure the registration process is initiated from the same PC from where the Virtual License was originally registered. If you have the latest Virtual License Key, enter the same to restore system functionality. If you do not have the latest key, you may use the last Virtual License Key you possess for registration. You can contact your System Integrator (SI) or Matrix Support Team to obtain the latest key. Once you receive the latest Virtual License Key, update it in the system to ensure normal operation.

If you do not have any Virtual License Key, please contact Matrix Technical Support Team to retrieve your Virtual License Key.

Existing License Profile

The Existing License Profile displays the following license details — Product Name, Total Cameras, Enterprise IVA Cameras, Automatic Number Plate Recognition Cameras, People Movement and Tracking Cameras, Face Recognition Cameras[2], Vehicle Tracking and Parking Management Slots, Cognitive Response Engine and Monitoring Scenarios, Simultaneous Users and Annual Upgrade Package Validity.



Make sure the following pre-requisites are fulfilled to configure **Object Detection** and **Face Detection**:

- GPU is affixed in the PC where IVA Server and Smart Client are installed. The required GPU is NVIDIA RTX[3].
- If you have multiple GPU affixed in your PC, make sure NVIDIA RTX is affixed at the first position.
- GPU Model is created using the SATATYA SAMAS GPU Model Creator Utility (Applicable only to Object Detection). For more details, refer to SATATYA SAMAS Installation Guide.

If you are upgrading SAMAS to V6R5 and later, make sure you upgrade the latest drivers for the affixed GPU to ensure successful GPU Model Creation.

The IVA Server uses the GPU Model for Object Detection. If the IVA Server fails to load the GPU Model library for some reason, then an event for the same will be displayed in Event Log as well as the event detection will fail.

2. *This License is not available in the current Software Release. These will be included in the upcoming release.*
3. *Recommended GPU is NVIDIA GeForce RTX-3050.*

Updating the Virtual License Key

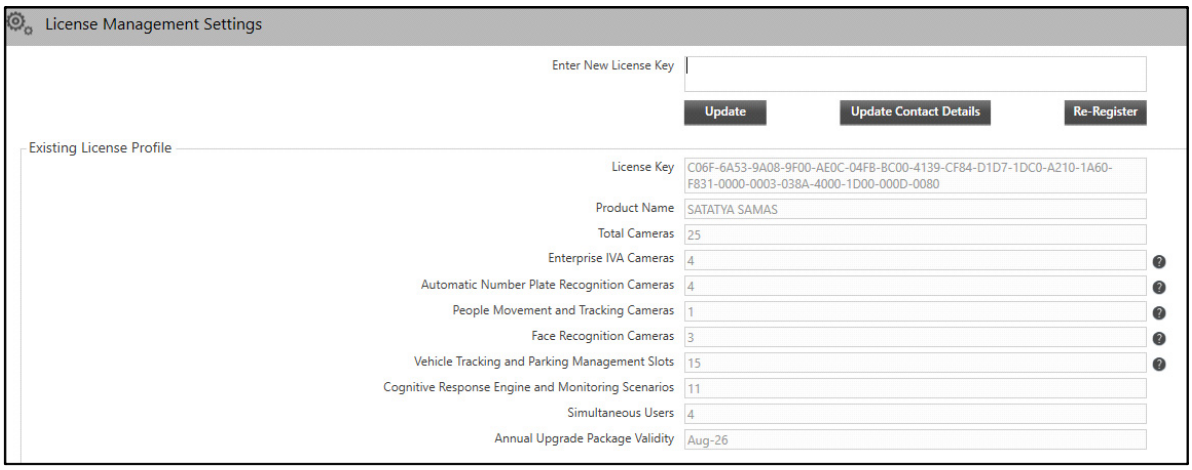
You need to Update the existing keys in the following scenarios:

- after registering the Generic Virtual License Key you need to update this key with the SAMAS PLATFORM Key.
- if you have purchased new vouchers to add on to your existing license, then you can update your existing key.

These keys are received in the form of PDF against your Purchase Order.

- Click **General Settings > License Management Settings**.

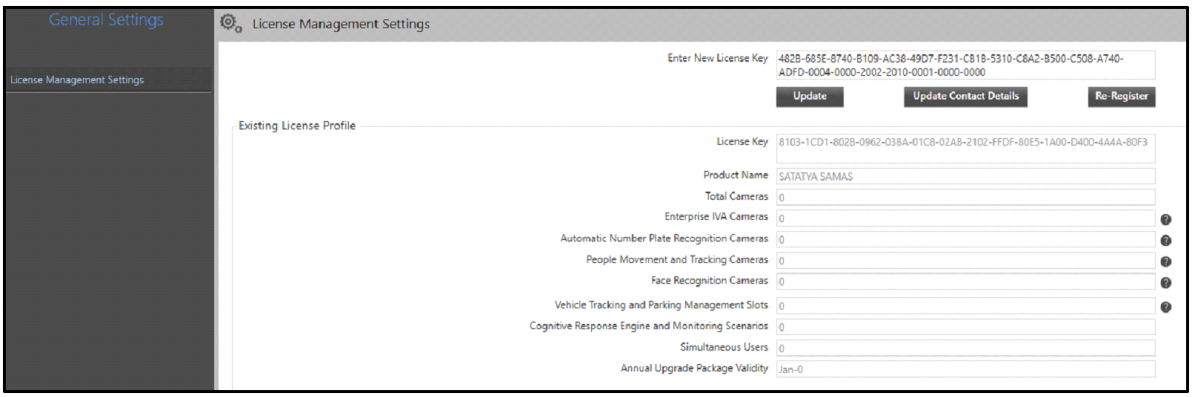
  - **License Key** under **Existing License Profile:** Displays the Generic Virtual License Key (in case you have activated the Virtual License for the first time).



  - **Enter New License Key:** If you have purchased new vouchers for additional features, you will receive a new License Key PDF. You need to update the existing key with this new key. To do so,

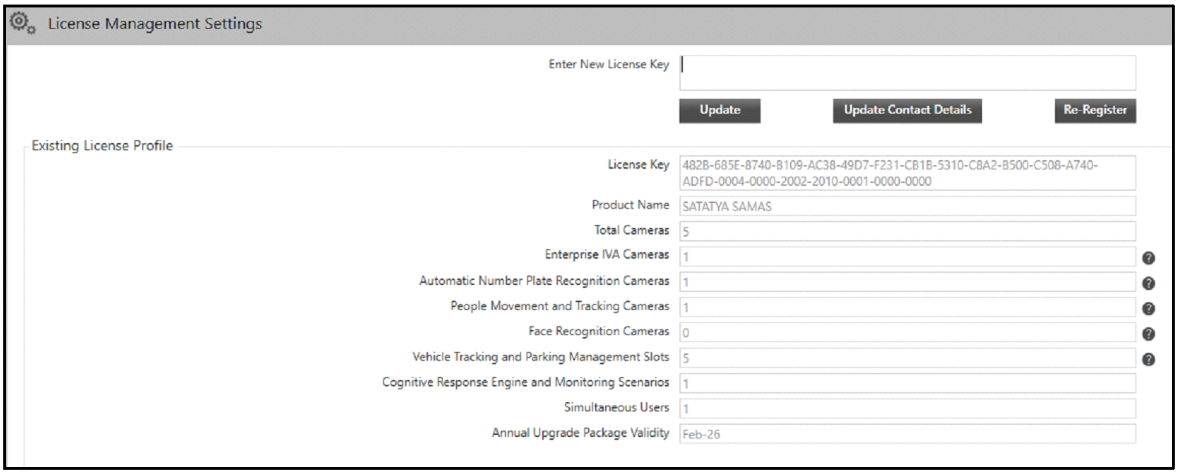
  - Open the License Key PDF file and select the key.

  - Drag and drop the same onto this field.



  - Click **Update**.

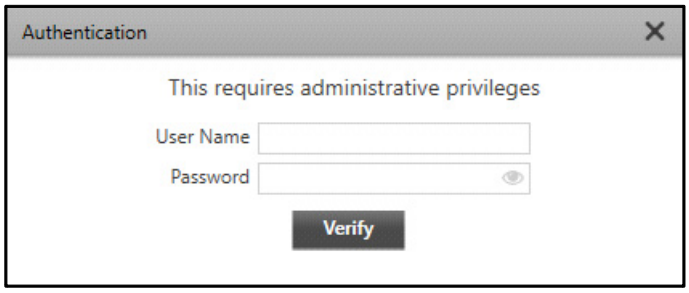
Now, this new key is displayed as the **License Key** under “Existing License Profile” and the License activation details are also updated as per the key.



Updating the Contact Details

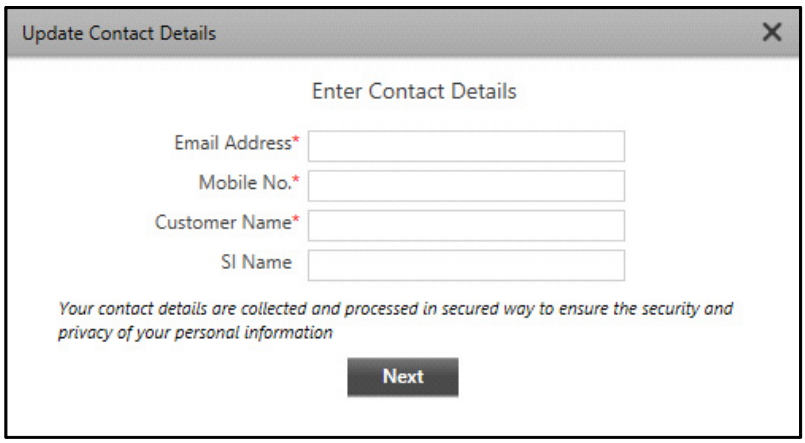
There may be certain instances — the personnel managing the IT may have left, Mobile Number is discontinued, etc — where-in, you need to update the contact details so that you continue receiving the alerts/OTPs. To do so,

- Click **General Settings > License Management Settings**.
- Click **Update Contact Details**.
    - The **Authentication** pop-up appears.



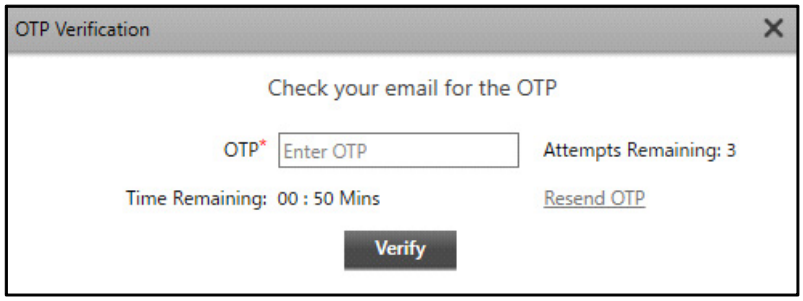
- **User Name:** Enter the User Name, for example sa. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password:** Enter the Password, for example admin. In Password, you can enter upto 12 characters. Default: Blank.
- Click **Verify**.

The **Update Contact Details** pop-up appears.



- Fill-in the updated details as per your requirement.

  Click **Next**. The **OTP Verification** pop-up appears and an OTP is sent to your Email ID.



- **OTP:** Check your Email ID for the OTP and enter the same here. In OTP, you can enter upto 6 characters. Default: Blank.

  Click **Next**. The **Contact Details are Updated Successfully**, message appears.

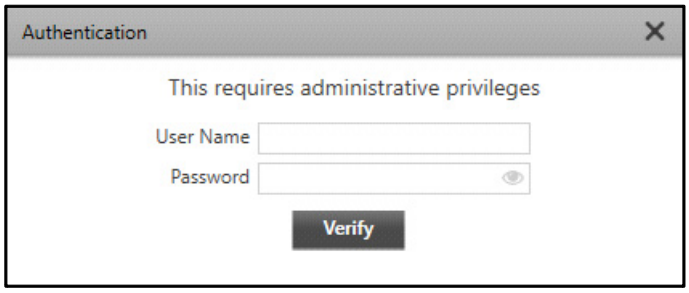
Re-registering the Virtual License Key

If you wish to migrate from a lower configuration SAMAS Server PC to a higher configuration Server PC or your PC needs to undergo maintenance, that is you are changing your PC but the Admin Client database backup is available, then you need to Re-register the Virtual License Key, so that Virtual License validation can be re-initiated.

If your SAMAS Server PC crashes and the Admin Client database backup is not available, then you need to contact the Matrix Technical Support Team for registering your Virtual License Key.

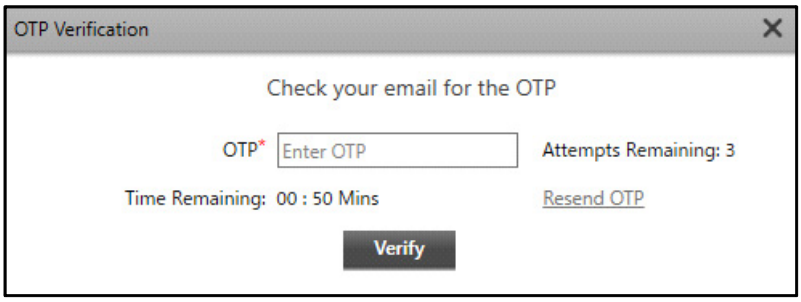
To Re-register the Virtual License Key,

- Click **General Settings > License Management Settings**.
- Click **Re-register**. The **Authentication** pop-up appears.



- **User Name:** Enter the User Name, for example sa. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password:** Enter the Password, for example admin. In Password, you can enter upto 12 characters. Default: Blank.
- Click **Verify**.

  The **OTP Verification** pop-up appears and an OTP is sent to your Email ID.



- **OTP:** Check your Email ID for the OTP and enter the same here. In OTP, you can enter upto 6 characters. Default: Blank.
- Click **Next**. The **License Re-registered Successfully**, message appears.

Once the License is re-registered, you are logged-out and re-directed to the Login page.

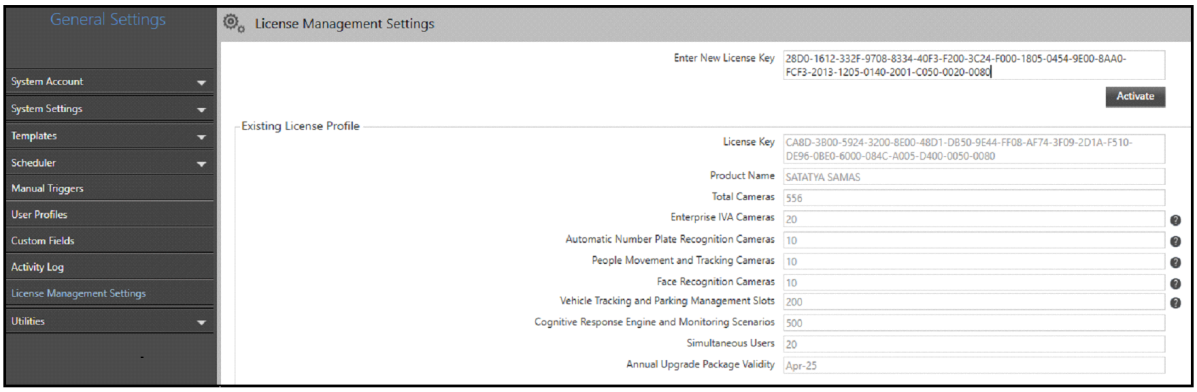
- *If the internet connectivity is not available or lost at any given point, SAMAS will close any open pop-up and you will be re-directed to the License Management Settings page. You need to restart the registration process.*
- *If you close the pop-up or the Admin Client or your PC restarts or you refresh, then no previous request initiated information will be retained by SAMAS.*
- *If at any point of time there exists any ongoing license registration/ verification/ new key updation or contact updatation process, then please wait for some time if you receive the same message again and again.Then retry after sometime.*

Dongle License Key

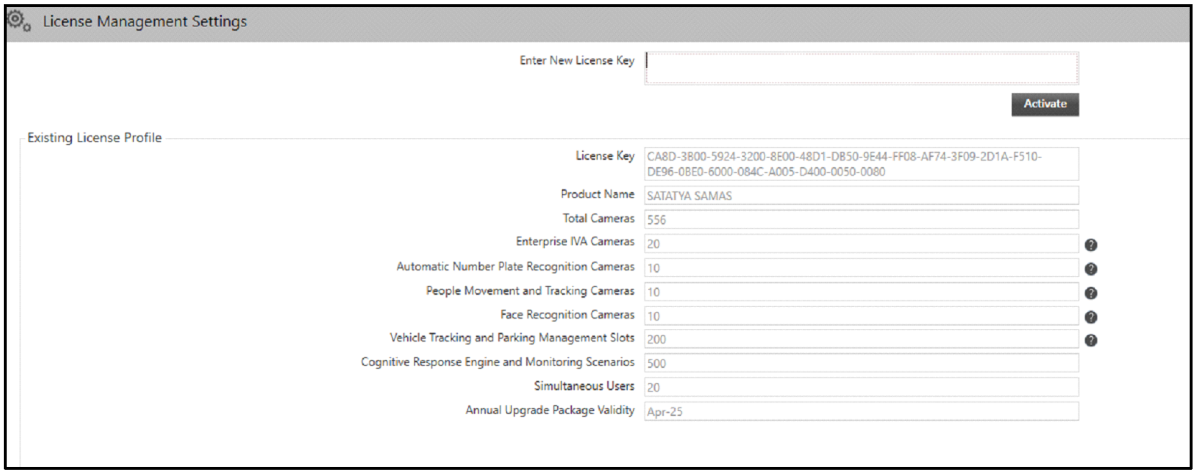
You can view the details of the your License as well as update your license. For details refer to “View Existing License Details” and “Update License Key”.

View Existing License Details

- Click **General Settings > License Management Settings**.
- If you have a license, the details of the same are displayed under **Existing License Profile**.



The Existing License Profile displays the following license details — Product Name, Total Cameras, Enterprise IVA Cameras, Automatic Number Plate Recognition Cameras, People Movement and Tracking Cameras, Face Recognition Cameras[4], Vehicle Tracking and Parking Management Slots, Cognitive Response Engine and Monitoring Scenarios, Simultaneous Users and Annual Upgrade Package Validity.



Make sure the following pre-requisites are fulfilled to configure **Object Detection** and **Face Detection**:

- GPU is affixed in the PC where IVA Server and Smart Client are installed. The required GPU is NVIDIA RTX[5].
- If you have multiple GPU affixed in your PC, make sure NVIDIA RTX is affixed at the first position.
- GPU Model is created using the SATATYA SAMAS GPU Model Creator Utility (Applicable only to Object Detection). For more details, refer to SATATYA SAMAS Installation Guide.

---

4. This License is not available in the current Software Release.These will be included in the upcoming release.
5. Recommended GPU is NVIDIA GeForce RTX-3050.

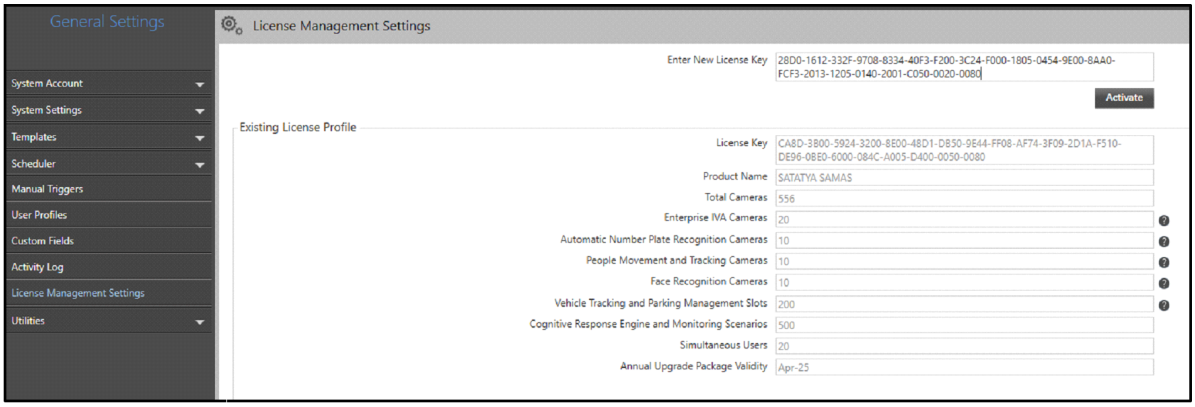
If you are upgrading SAMAS to V6R5 and later, make sure you upgrade the latest drivers for the affixed GPU to ensure successful GPU Model Creation.

The IVA Server uses the GPU Model for Object Detection. If the IVA Server fails to load the GPU Model library for some reason, then an event for the same will be displayed in Event Log as well as the event detection will fail.

Update License Key

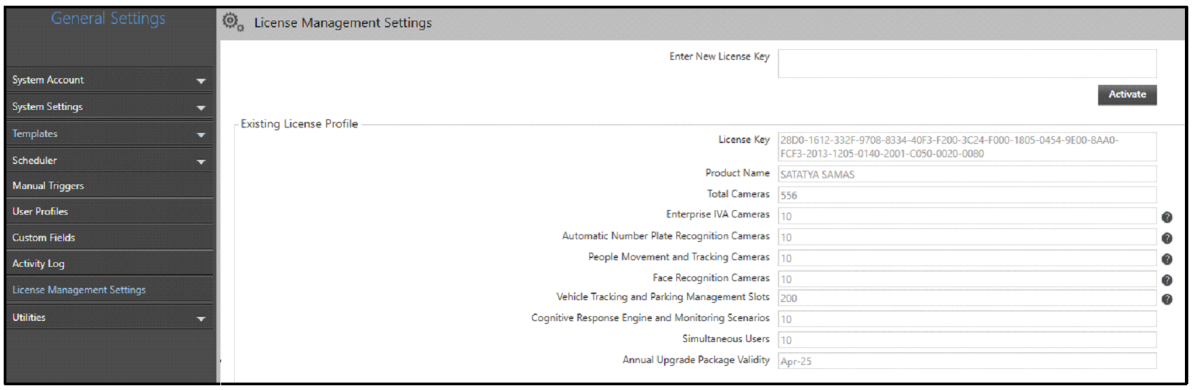
If you wish to Update a License, make sure your AUP has not expired.

- Click **General Settings > License Management Settings**.
- **Enter New License Key:** If you have purchased new vouchers for additional features, you will receive a new License Key PDF. You need to update the existing key with this new key.To do so,
  - Open the License Key PDF file and select the key.
  - Drag and drop the same onto this field.



- Click **Activate**.

Now, this new key is displayed as the License Key under Existing License Profile and the License activation details are updated as per the key.

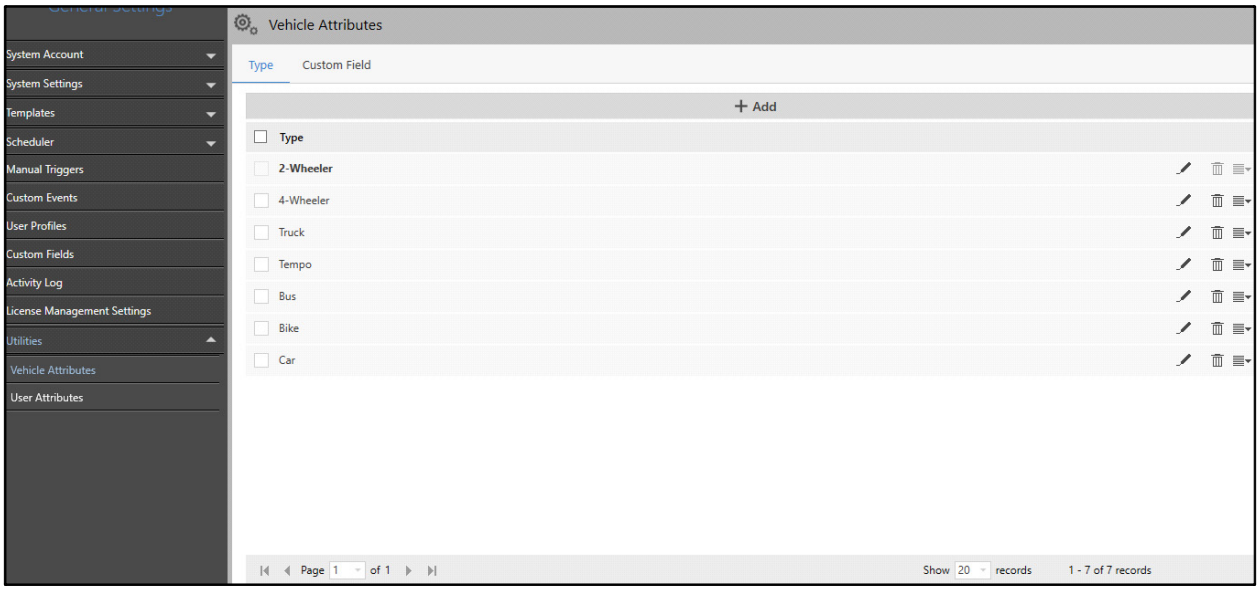


Utilities

The General Settings module enables you to configure Utilities, wherein you can add Vehicle Attributes and User Attributes. You can add Custom Fields for both. These attributes are useful when you configure User Profiles.

To configure Utilities,

- Click **General Settings > Utilities**.



The Utilities section contains two pages — “Vehicle Attributes” and “User Attributes”.

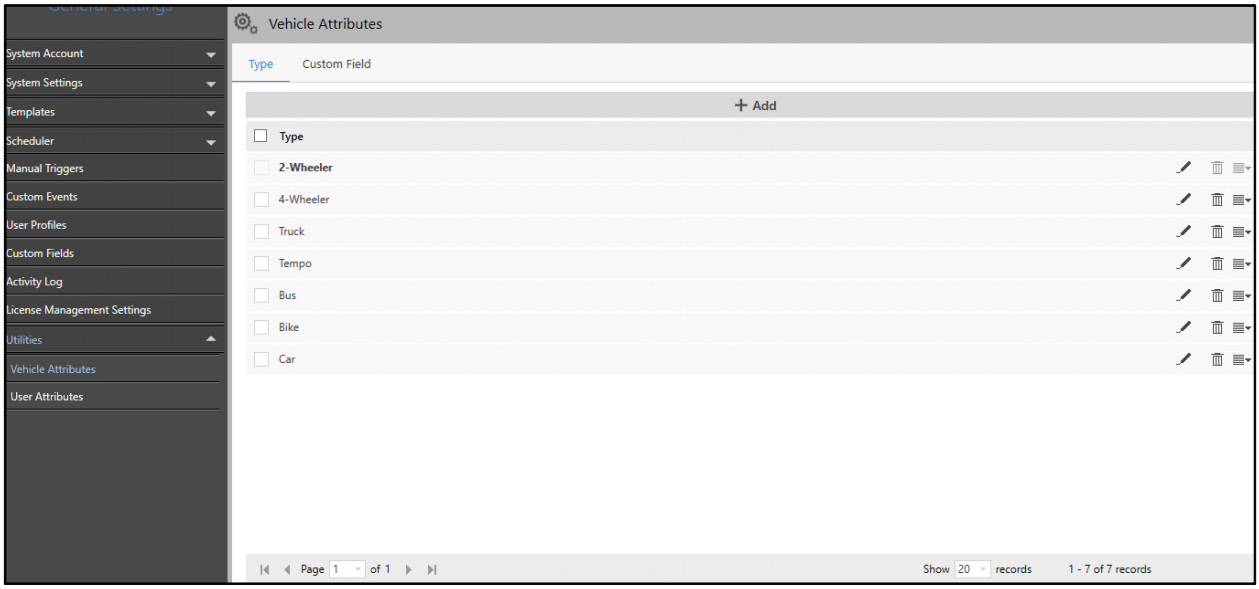
Vehicle Attributes

Vehicle Attributes allows you to configure various types of vehicles, such as 2-Wheeler, 4-Wheeler etc. Custom Fields allow you to configure the desired customized fields as per your requirement. Vehicle attributes created here will be available for selection while configuring Vehicle Details in the User Profile section.

The Vehicle Attributes page displays the configured Vehicle Attributes. You can add, view and configure the Vehicle Attributes from this page.

To configure Vehicle Attributes,

- Click **General Settings > Utilities > Vehicle Attributes**.



The Vehicle Attributes page consists of the following tabs.

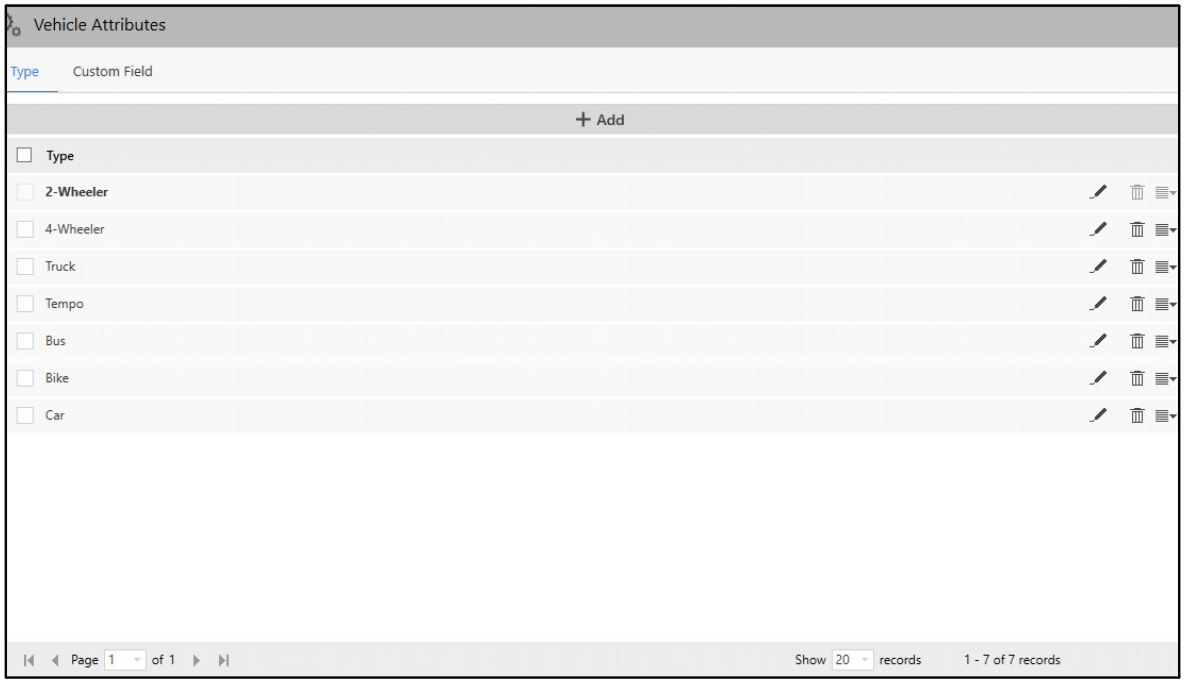
- "Type"
- "Custom Field"

Type

This tab enables you to configure the type of vehicle. All the configured Vehicle Attribute types appear under this tab.

To add, view or edit Type,

- Click the **Type** tab.

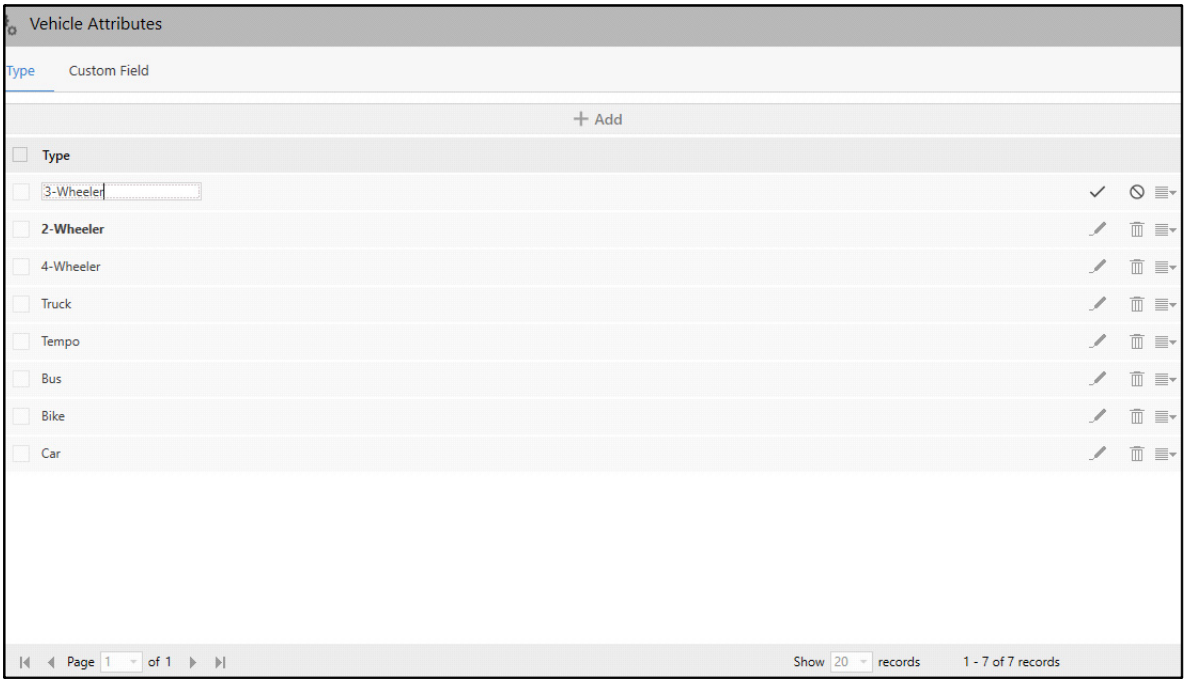


The following are the pre-defined types of vehicle. You can modify or delete them as per your requirement.

- 2-Wheeler
- 4-Wheeler
- Truck
- Tempo
- Bus
- Bike
- Car

You can also add a custom type. To do so,

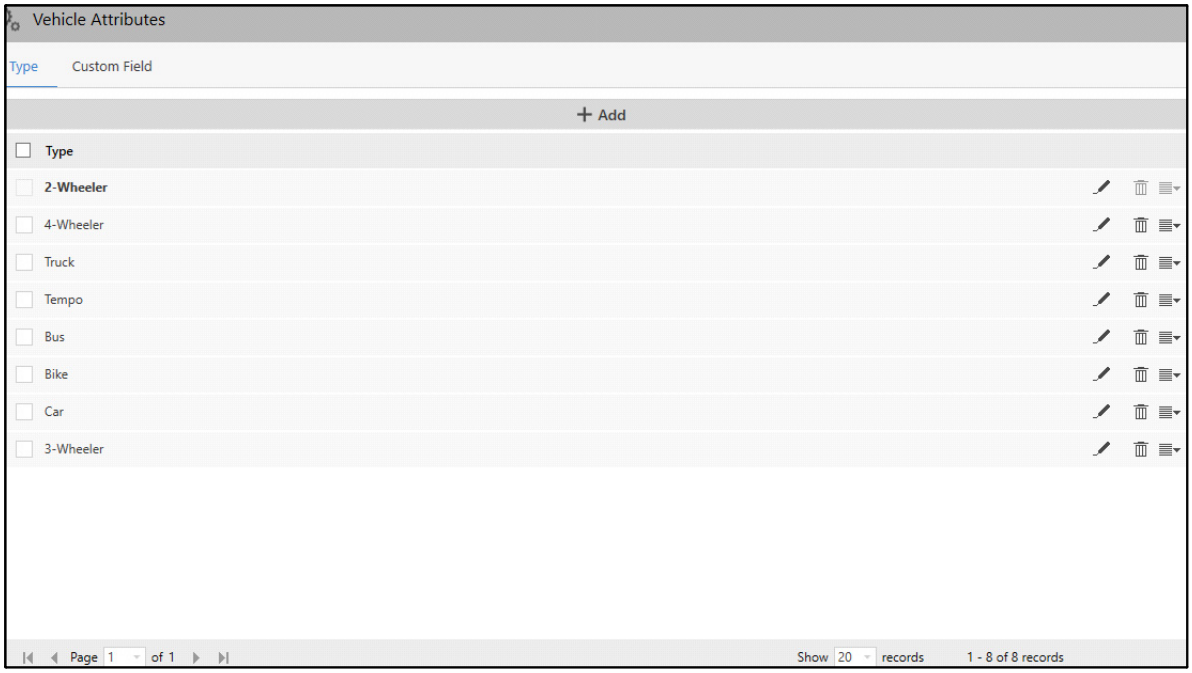
- Click **Add**.



- Specify a suitable name for the type of vehicle you wish to add. In Name, you can enter upto 30 characters. Default: Blank.
- Click **Save** to save the details or click **Cancel** to discard.

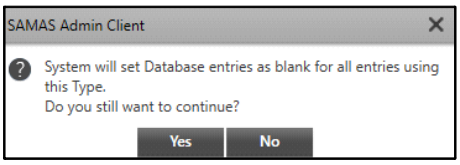
The new Vehicle Attribute Type appears in a list.

Each Type can be edited, deleted or can be set as Use as Default.

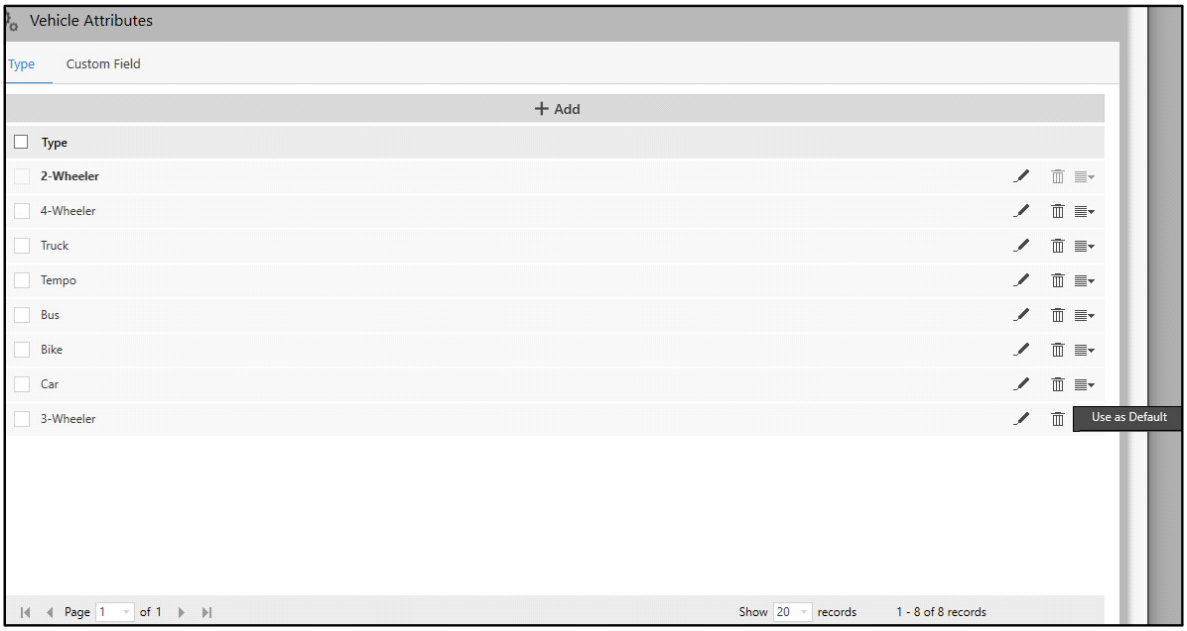


- Click **Edit** to edit the desired Type from the list.

- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Type. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.
- Click **Actions** of the desired Type. The **Use as Default** option appears.



- Select **Use as Default** if you wish to use this Type as default.

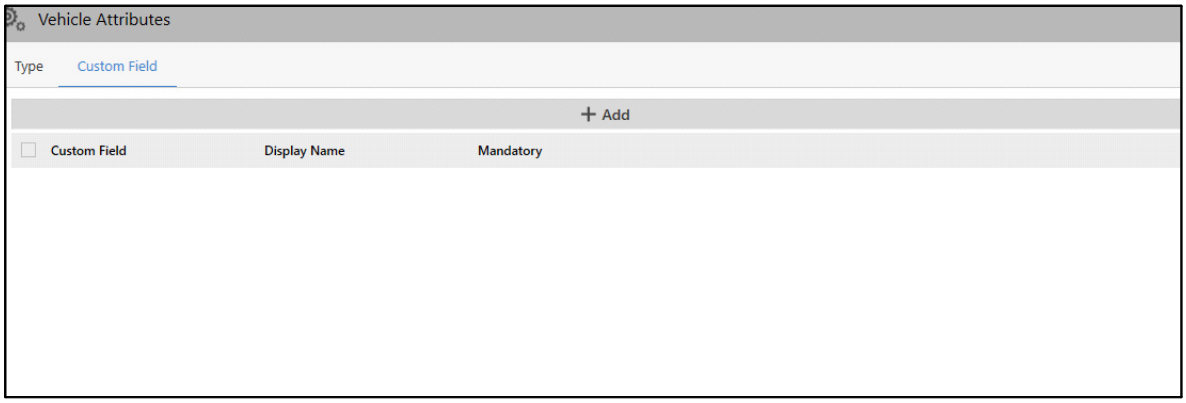
The Vehicle Attribute Type set as default cannot be deleted.

Custom Field

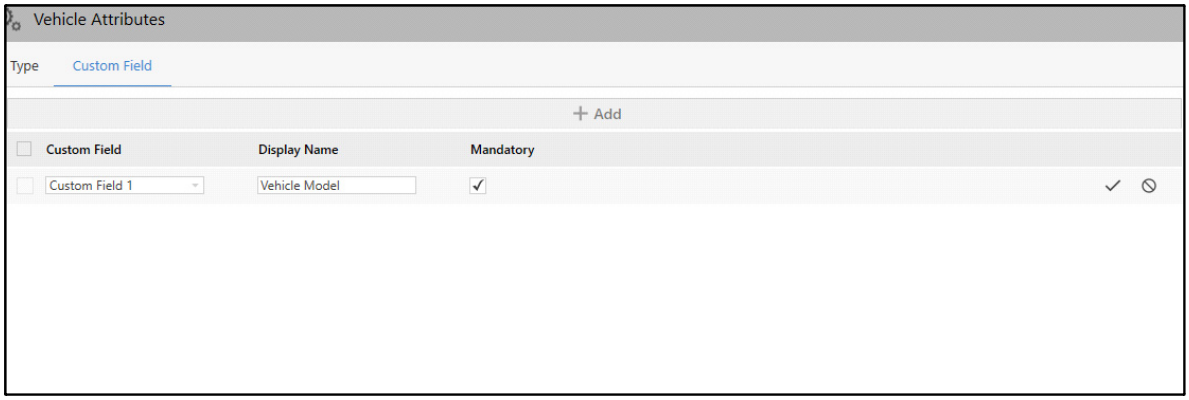
This tab enables you to configure Custom Fields. All the configured Custom Fields appear under this tab.

To add, view and configure Custom Fields,

- Click the **Custom Field** tab.



- Click **Add**.



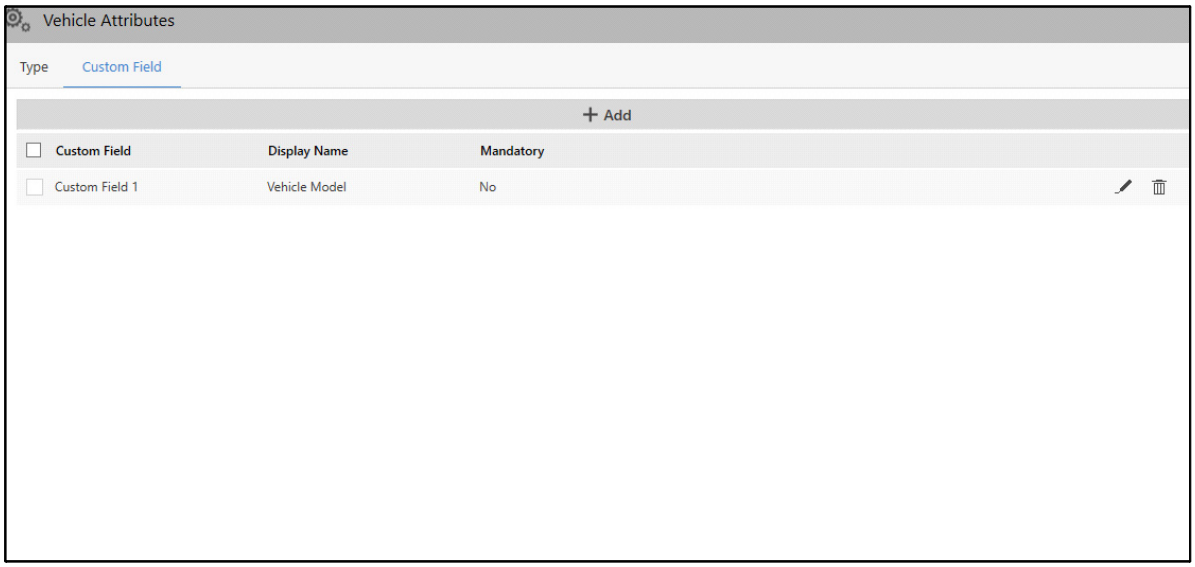
Configure the following parameters:

- **Custom Field**: Select the Custom Field number from the drop-down list.
- **Display Name**: Specify a suitable name for the Custom Field. In Display Name, you can enter upto 55 characters. Default: Blank.
- **Mandatory**: Select the check box if you wish to make this field mandatory while configuring User Profiles.

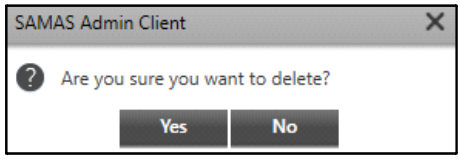
- Click **Save** to save the details or click **Cancel** to discard.

The new Custom Field appears in a list.

You can edit the configuration or delete the desired Custom Field.



- Click **Edit** to edit the desired Custom Field from the list.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Custom Field. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

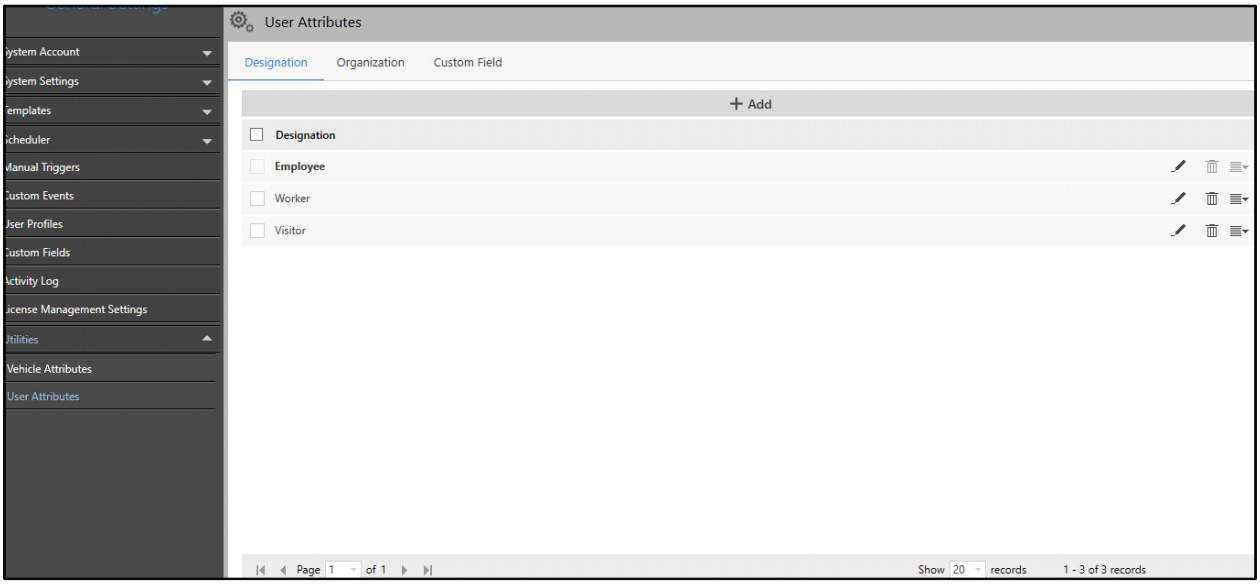
User Attributes

User Attributes allows you to configure various Designations, such as Employee, Worker etc. It also allows you to configure various Organization names, such as Matrix Comsec. User attributes created here will be available for selection while configuring the Basic Details in the User Profile section.

The User Attributes page displays the configured User Attributes. You can add, view and configure the User Attributes from this page.

To configure User Attributes,

- Click **General Settings > Utilities > User Attributes**.



The User Attributes page consists of the following tabs.

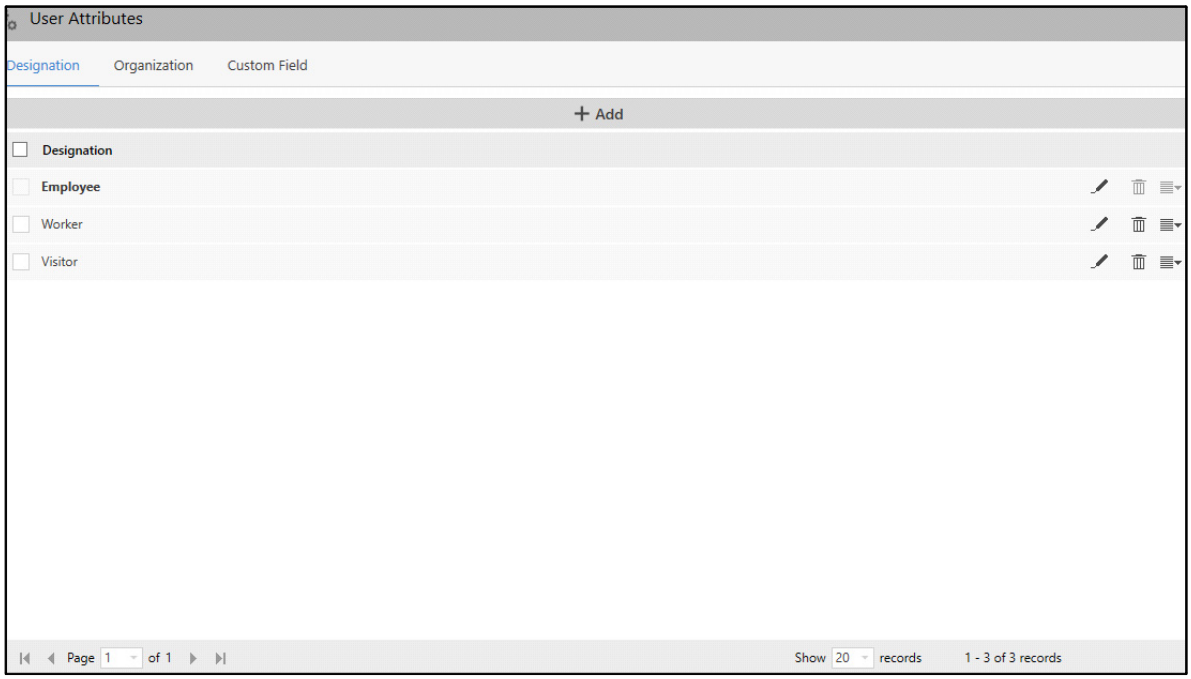
- “Designation”
- “Organization”
- “Custom Field”

Designation

This tab enables you to configure the different Designations. All the configured Designations appear under this tab.

To add, view or edit Designation,

- Click the **Designation** tab.

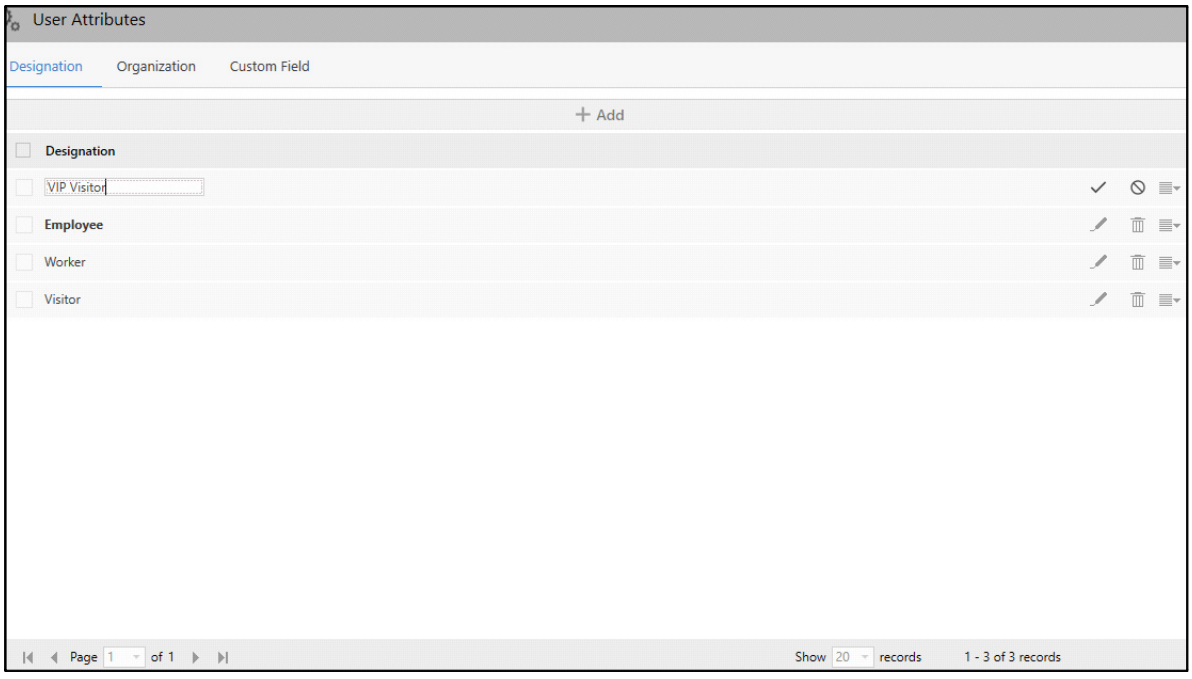


The following are the pre-defined user attributes. You can edit or delete them as per your requirement.

- Employee
- Worker
- Visitor

You can also add custom a Designation.

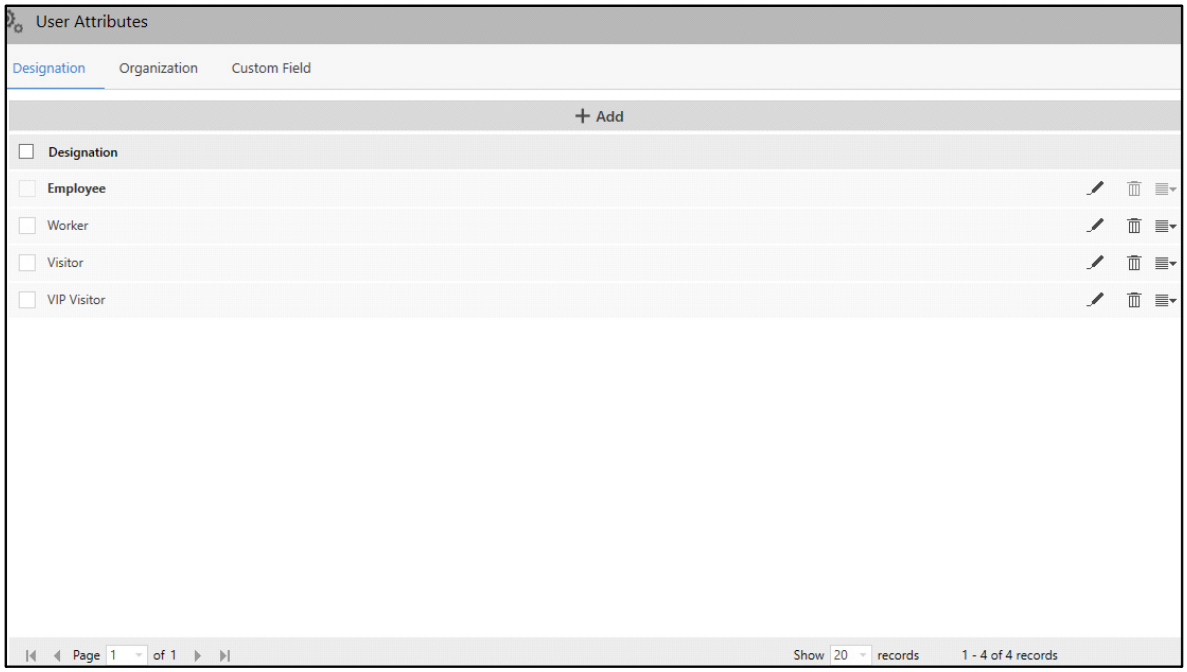
- Click **Add**.



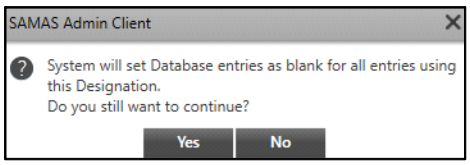
- Specify a suitable name for the Designation. In Designation, you can enter upto 30 characters. Default: Blank.
- Click **Save** to save the details or click **Cancel** to discard.

The new Designation appears in a list.

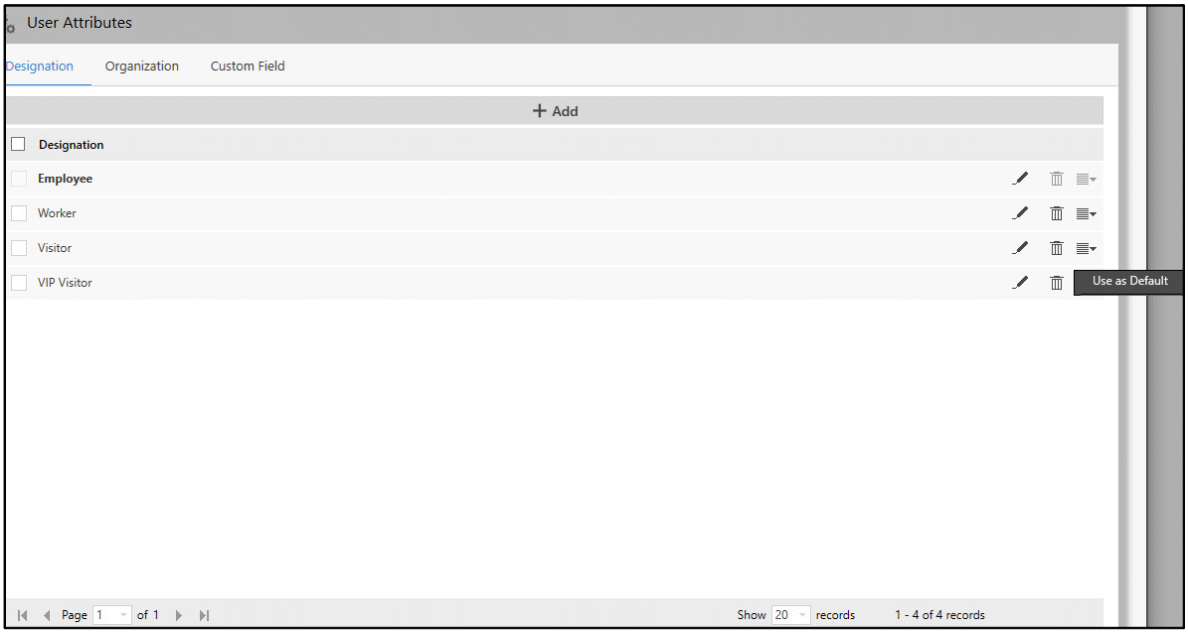
Each Designation can be edited, deleted or set as Use as Default.



- Click **Edit** to edit the desired Designation from the list.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Designation. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.
- Click **Actions** of the desired Designation. The **Use as Default** option appears.



- Select **Use as Default** if you wish to use this Designation as default.

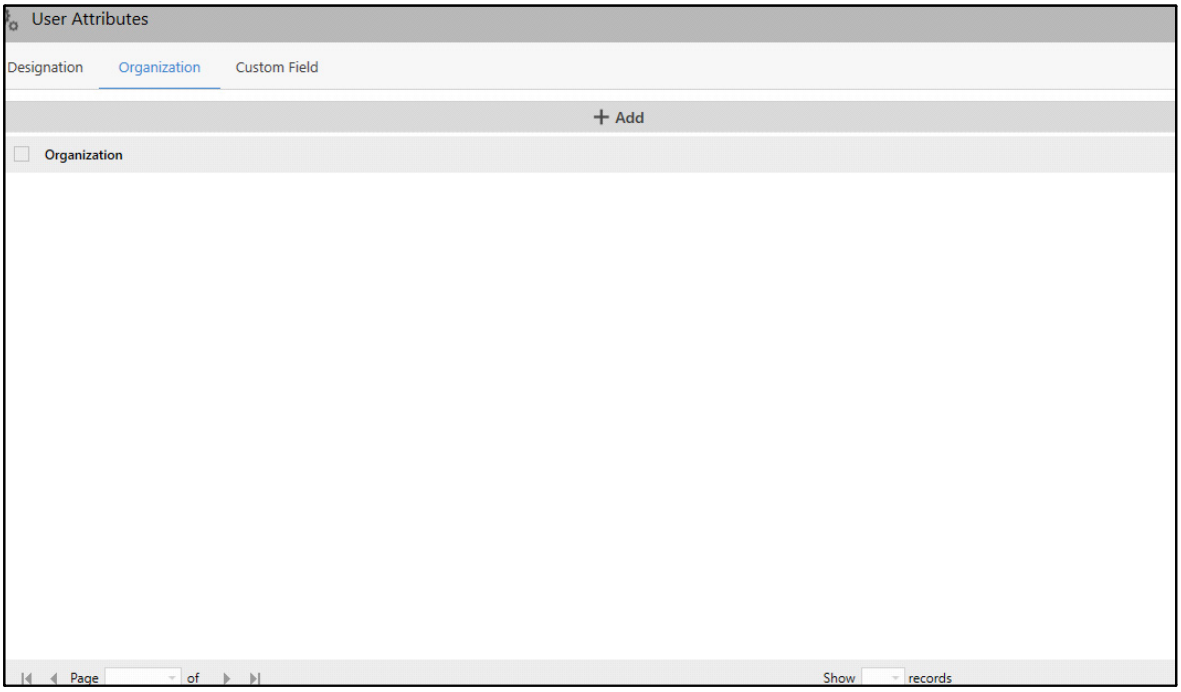
The Designation set as default cannot be deleted.

Organization

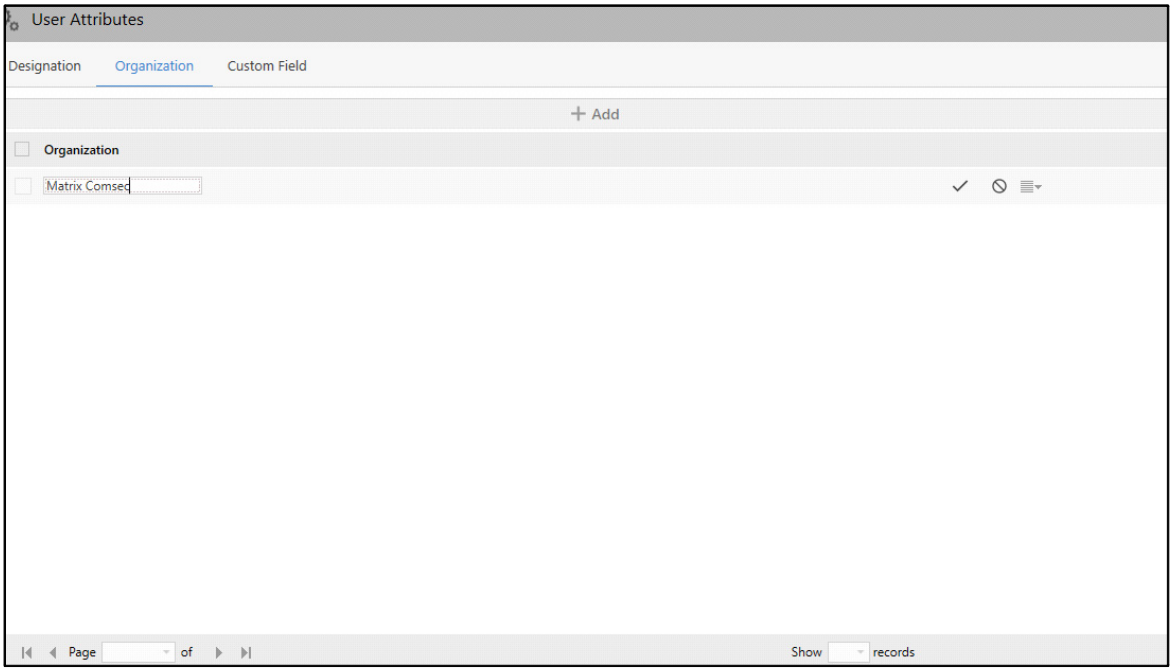
This tab enables you to configure the different Organizations. All the configured Organizations appear under this tab.

To add, edit or view Organization,

- Click the **Organization** tab.



- Click **Add**.

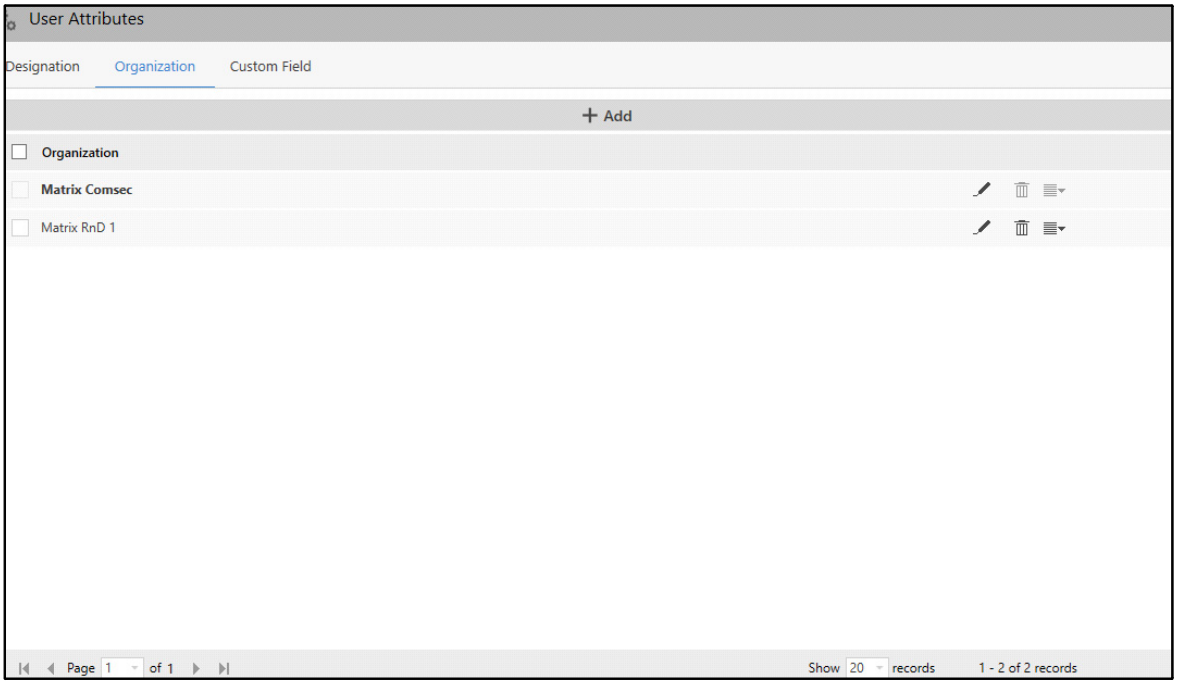


- Specify a suitable name for the Organization. In Organization, you can enter upto 50 characters. Default: Blank.
- Click **Save** to save the details or click **Cancel** to discard.

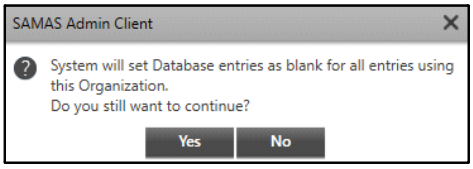
The new Organization appears in a list.

If only one Organization is added then the options — Actions and Delete are not applicable.

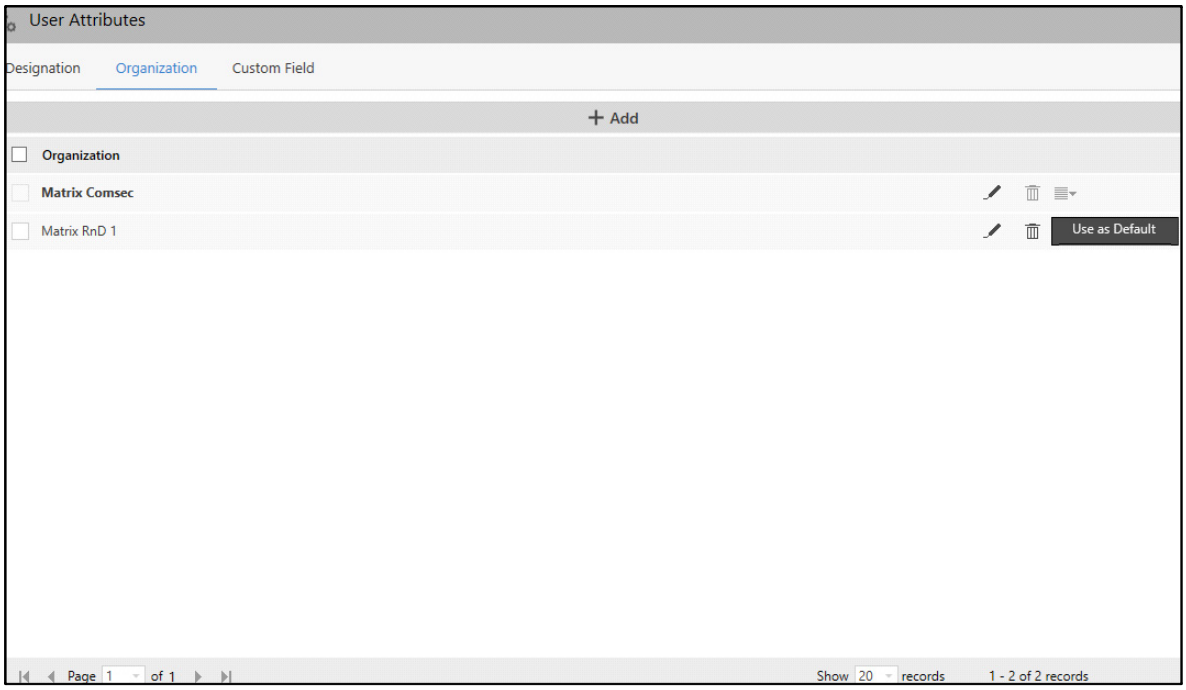
Each Organization can be edited, deleted or set as Use as Default.



- Click **Edit** to edit the desired Organization from the list.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Organization. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.
- Click **Actions** of the desired Organization. The **Use as Default** option appears.



- Select **Use as Default** if you wish to use the Organization as default.

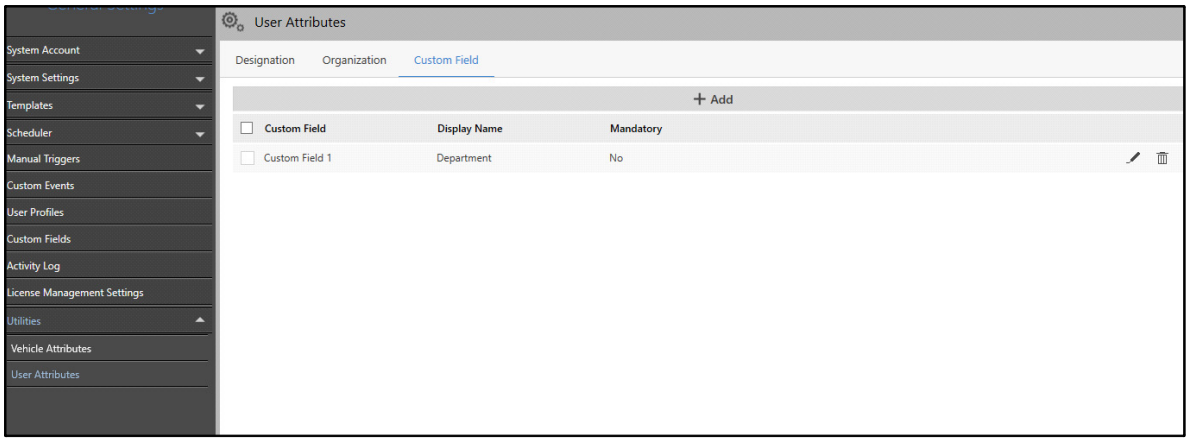
The Organization set as default cannot be deleted.

Custom Field

This tab enables you to configure different Custom Fields. All the configured Custom Fields appear under this tab.

To add, view and configure Custom Fields,

- Click the **Custom Field** tab.



The configurations of Custom Fields for User Attributes are similar to the Vehicle Attributes. For details, refer to “Custom Field”.

CHAPTER 5

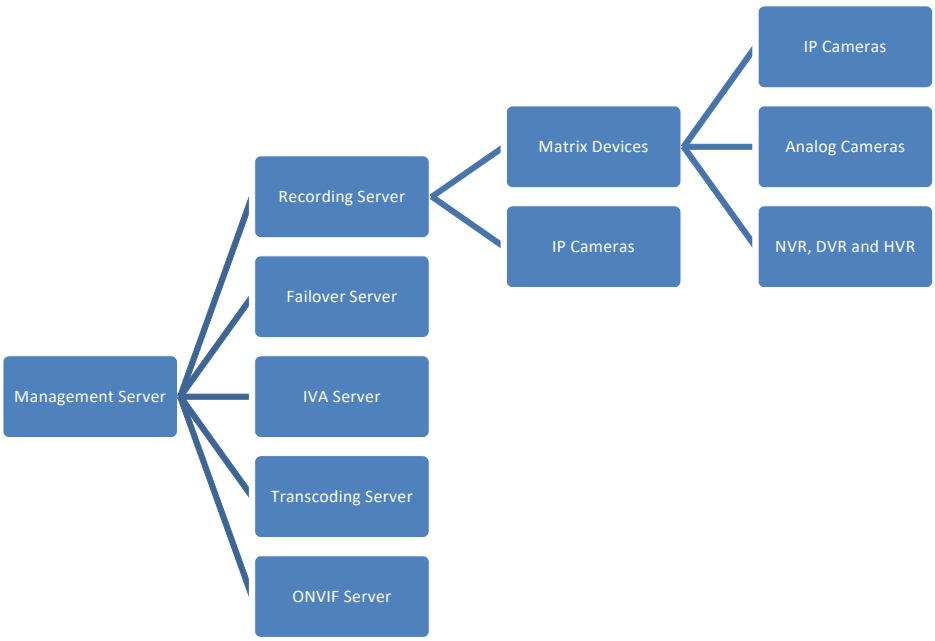
Servers & Devices

The Servers & Devices module enables you to add and configure the basic component entities of the SATATYA SAMAS based on a pre-defined hierarchical relationship. To know about the physical components of SATATYA SAMAS, refer to "System Components".

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

The Server/Physical Devices Hierarchy

The following figure represents the basic Server-Device relationship in SATATYA SAMAS, which is important to understand before you begin adding new devices to the system.



The **Management Server** is a default entity created by the Admin Client at the first login. This is the same Management Server for which IPv4/IPv6 Address and Port number were entered while logging into the Admin Client.

SATATYA SAMAS has the following components in addition to Management Server— Recording Server, Failover Server, IVA Server, Transcoding Server and ONVIF Server. All of the Servers communicate with the Management

Server and perform specific functions. To know more about their functions, refer to “System Components”. To install the Servers, refer to the **SATATYA SAMAS Installation Guide**.

The Matrix Devices consist of IP Cameras and Video Recorders — Network Video Recorder (NVR), Digital Video Recorder (DVR) and Hybrid Video Recorder (HVR). You can add Matrix Devices (NVR, DVR and HVR) and IP Cameras to the Recording Servers. You can add IP Cameras to the Matrix Devices (NVR and HVR). You can add the Analog Cameras to the Matrix Devices (HVR and DVR). The Recording Server communicates with these devices and records video streams.

Servers and Devices Icon Representation

In Admin Client, the following icons of Servers and devices appear.

Icons	Description
Server Status Icons	
	Recording Server is Connected
	Recording Server is Disconnected
	Failover Server is Connected
	Failover Server is Disconnected
	IVA Server is Connected
	IVA Server is Disconnected
	Transcoding Server is Connected
	Transcoding Server is Disconnected
	ONVIF Server is Connected
	ONVIF Server is Disconnected
Recording Server (RS) Device Icons	
	Device is disconnected from RS
	Device is connected with RS
	Device is kept under maintenance
	Device is disconnected from RS, while it is connected with FoS
Failover Server (FoS) Devices Icons	

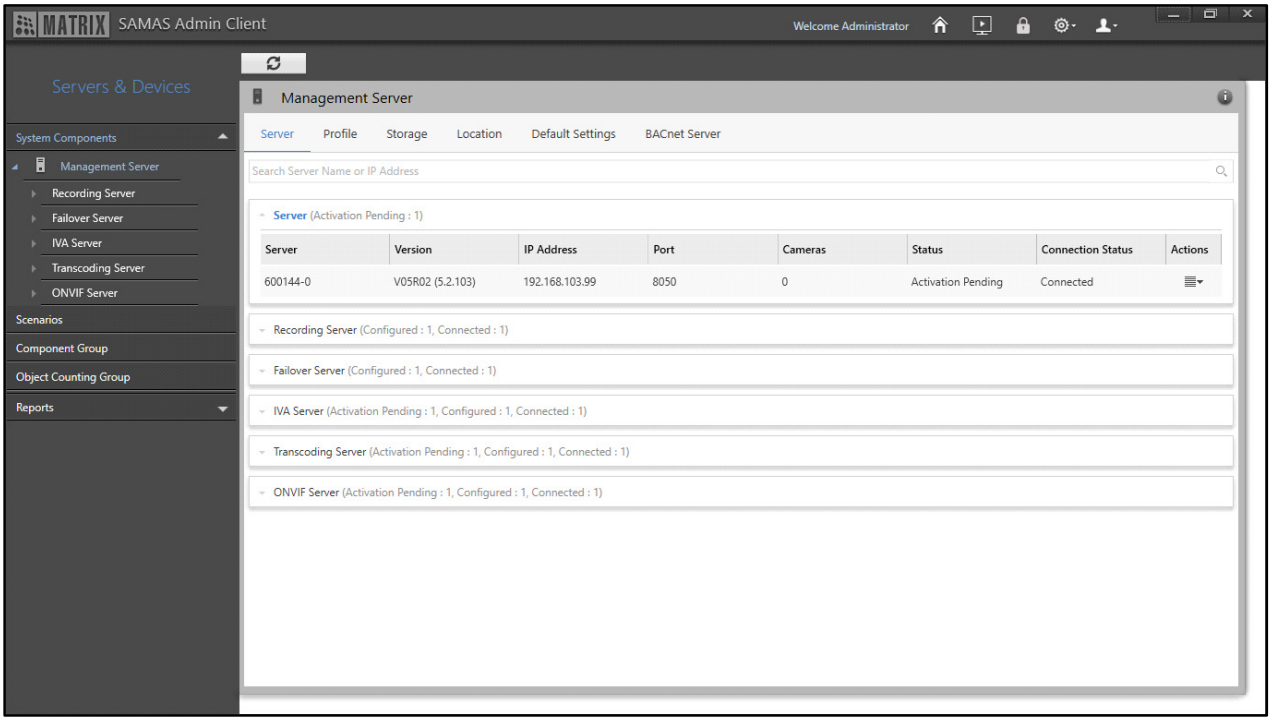
Icons	Description
	Device is connected via FoS and disconnected from RS. ***Note:*** *In this case, RS will be disconnected.*
	Device is connected via RS and not via FoS.
	Device is neither connected via RS nor FoS.
Server Version Mismatch Icons	
	FoS version mismatch (Connected)
	FoS version mismatch (Disconnected)
	IVA Server version mismatch (Connected)
	IVA Server version mismatch (Disconnected)
	Recording Server version mismatch (Connected)
	Recording Server version mismatch (Disconnected)
	Transcoding Server version mismatch (Connected)
	Transcoding Server version mismatch (Disconnected)
	ONVIF Server version mismatch (Connected)
	ONVIF Server version mismatch (Disconnected)
Mobile Camera Icons	
	Mobile Camera is connected with RS It will be enabled only when the Push Video feature is being accessed from the associated Mobile Client.
	Mobile Camera is disconnected from RS
	Mobile Camera is connected via FoS and not via RS. It will be enabled only when the Push Video feature is being accessed from the associated Mobile Client.
	Mobile Camera is disconnected from FoS

The Servers & Devices module enables you to configure the various Servers, Devices and Cameras.

The IPv4/IPv6 Address of all the Servers will be displayed under respective Server's collapsible Panel.

To configure Servers & Devices,

- Click **Servers & Devices**.



The Servers & Devices module contains these sections and pages — System Components, Scenarios, Component Group, Object Counting Group and Reports.

If you have enabled Secure Communication, all the servers communicate with each other after validating the SSL Certificate. If the certificate is found to be expired or is unavailable, then also they will still communicate with each other via untrusted/expired certificate or even if the certificate is not available. Such events will be logged in the "Event Log".

When the selected certificate is unavailable for Management Server, License Server and Recording Server/ Failover Server, then the SAMAS Default Certificate will be used for communication. Such events will be logged in the "Event Log".

Refer to the following links for the configuration details of different Servers.

- "Management Server"
- "Recording Server"
- "Failover Server"
- "IVA Server"
- "Transcoding Server"

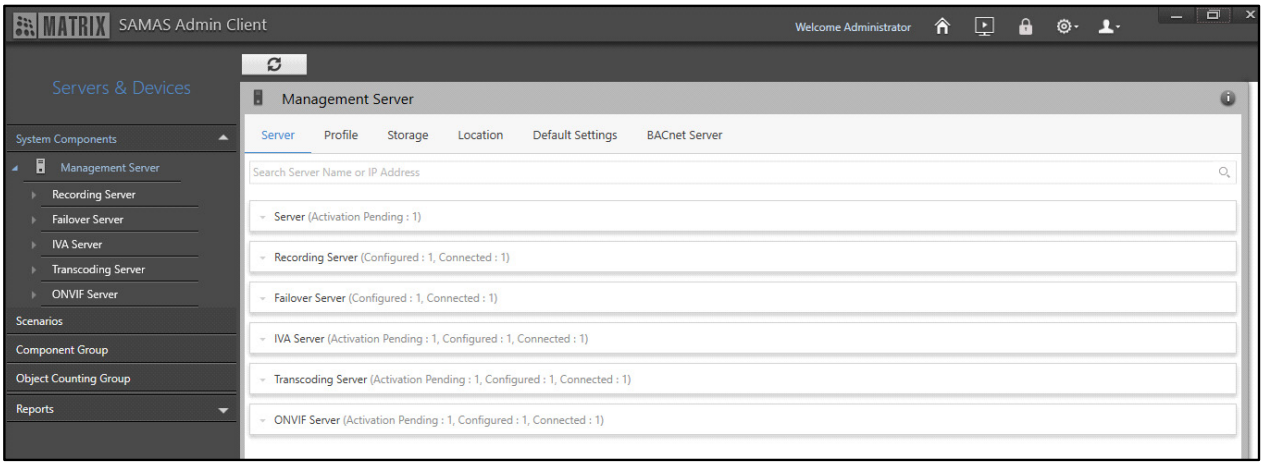
- “ONVIF Server”

Management Server

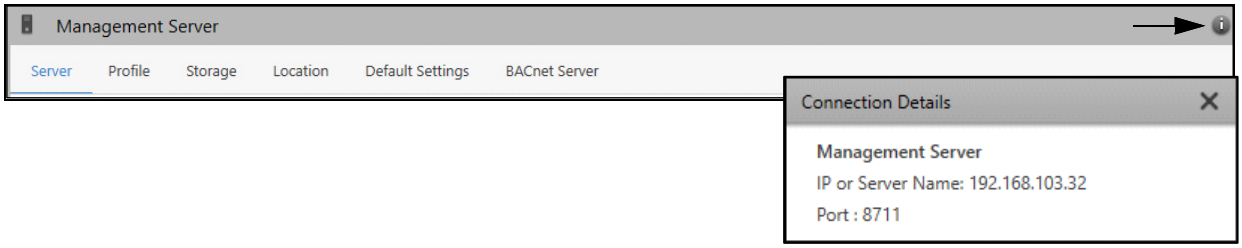
The Management Server manages all the entities of the SATATYA SAMAS. The Management Server page displays various Servers and their status. The requests of Servers received by the Management Server also appear on this page. You can view and configure different Servers from this page.

To configure Management Server,

- Click **Servers & Devices > System Components > Management Server**.



- To view the **Connection Details** of the Management Server, click **Connection Details** at the top right corner of the Management Server page. It displays the Management Server Name, IP (IPv4/IPv6) or Server Name and Port.



The Management Server contains the following tabs:

- “Server”
- “Profile”
- “Storage”
- “Location”
- “Default Settings”
- “BACnet Server”

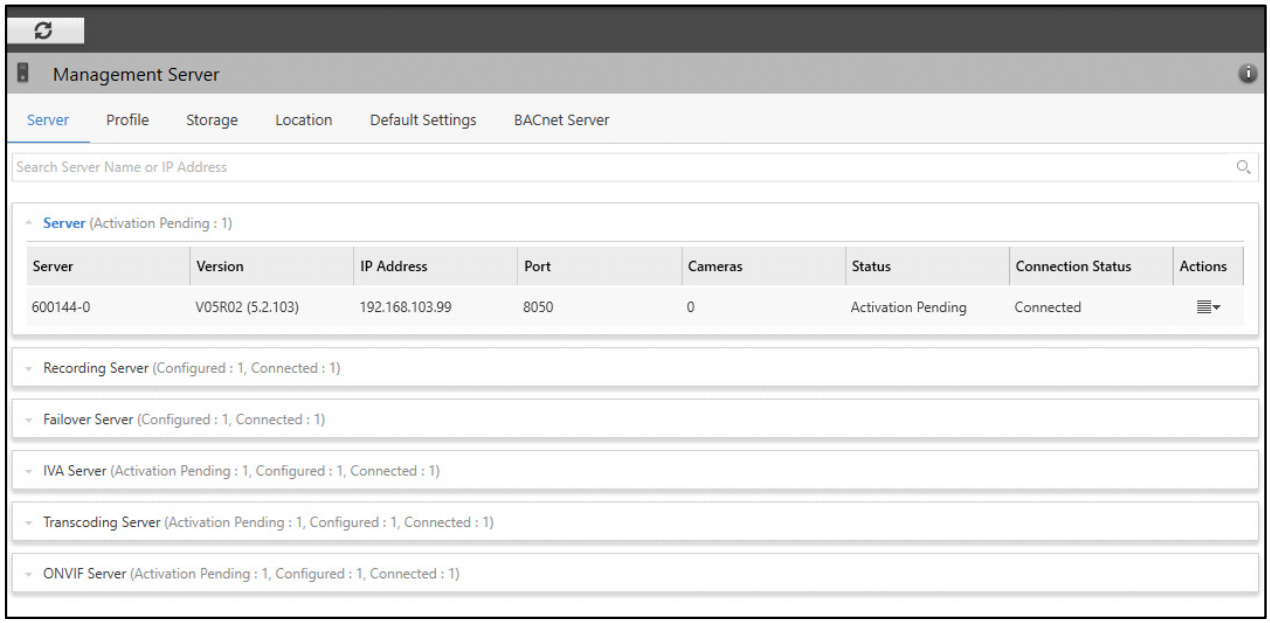
Server

All the Servers send their activation requests to the Management Server. This tab enables you to view the activation requests of various Servers. You can activate and configure Servers from this page. You can also assign a server as Recording Server or Failover Server from this page.

The names of the Servers — Recording, Failover— whose activation requests are pending are the names of the PC on which the respective Servers are installed. After Activation the names can be edited from their respective Profiles. Refer to "Profile" in "Recording Server Configuration" and "Profile" in "Failover Server Configuration".

To configure Servers,

- Click the **Server** tab.



The Server tab contains six collapsible panels — Server, Recording Server, Failover Server, Transcoding Server, IVA Server and ONVIF Server.

The entries under each collapsible panel can be sorted. To do so, click on the desired parameter in the header row.

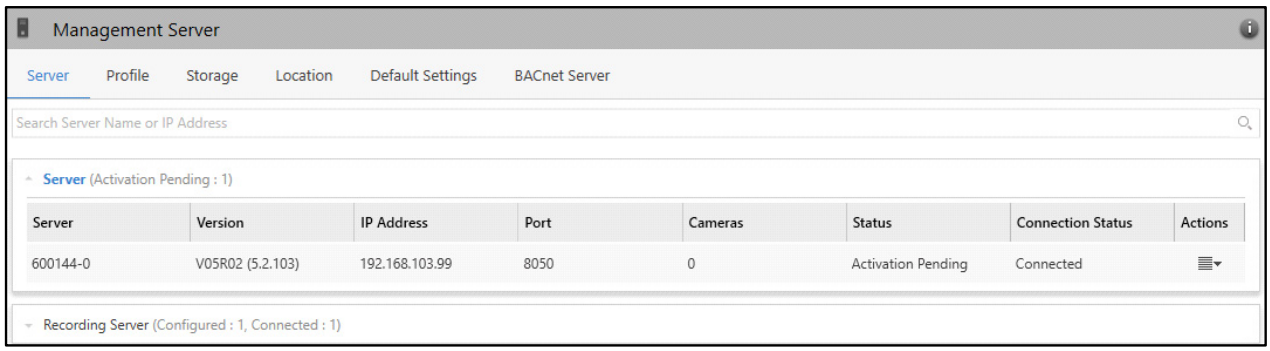
An arrow ▲ icon appears. Click on it. Entries can be sorted in ascending or descending order.

Assigning Server as Recording Server or Failover Server

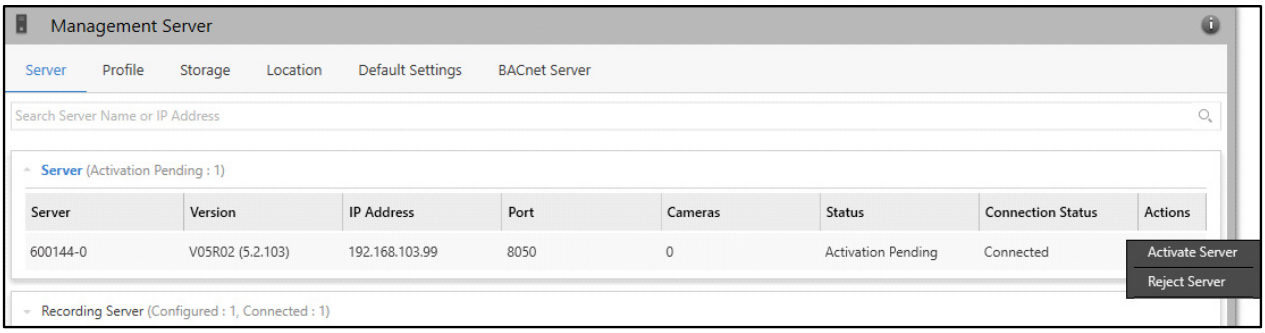
The Server collapsible panel displays the pending activation requests of different Servers. You can activate the Servers from this collapsible panel. The servers in the Server collapsible panel can be assigned as Recording Server or Failover Server.

To activate the Servers,

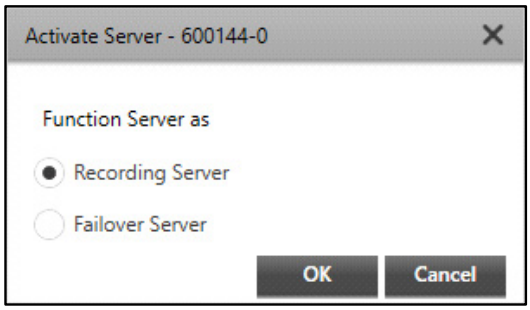
- Click the **Server** collapsible panel.
- To activate the requesting Server, click **Actions** .



- Click **Activate Server.** If you do not wish to activate it, click **Reject Server**.

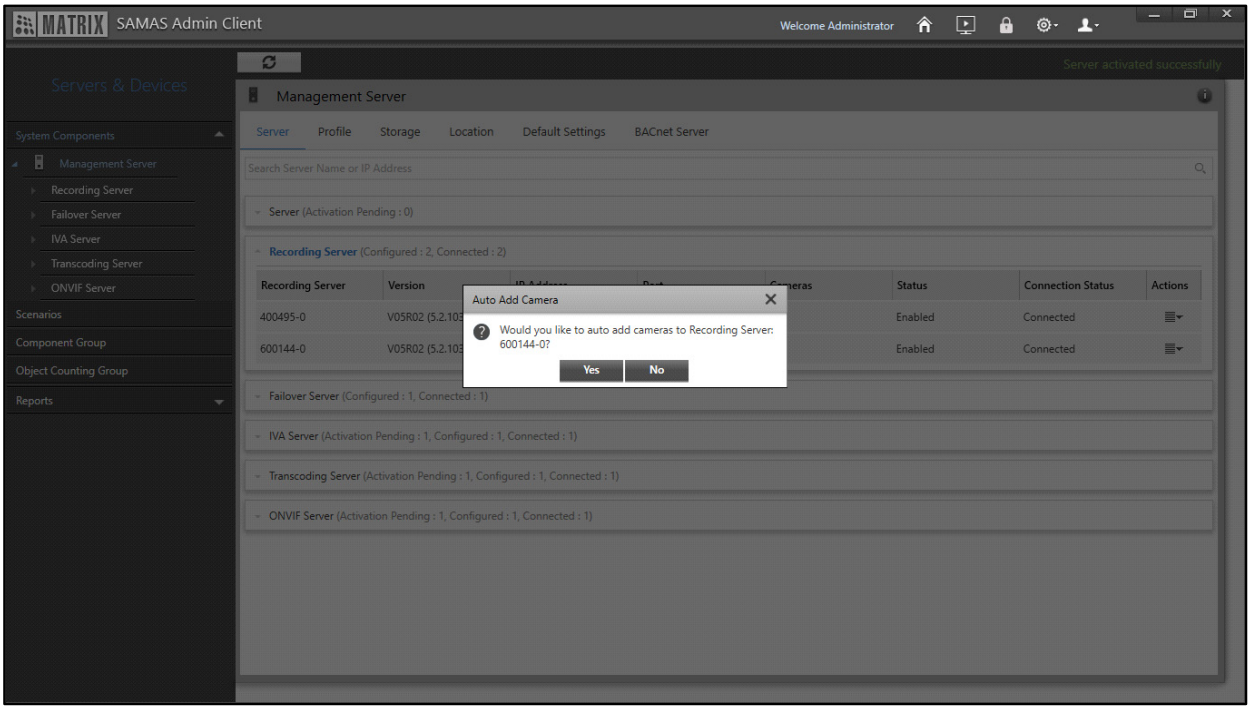


- The **Activate Server** pop-up appears once the Server is activated. You can select the Server to function as either **Recording Server** or **Failover Server**.

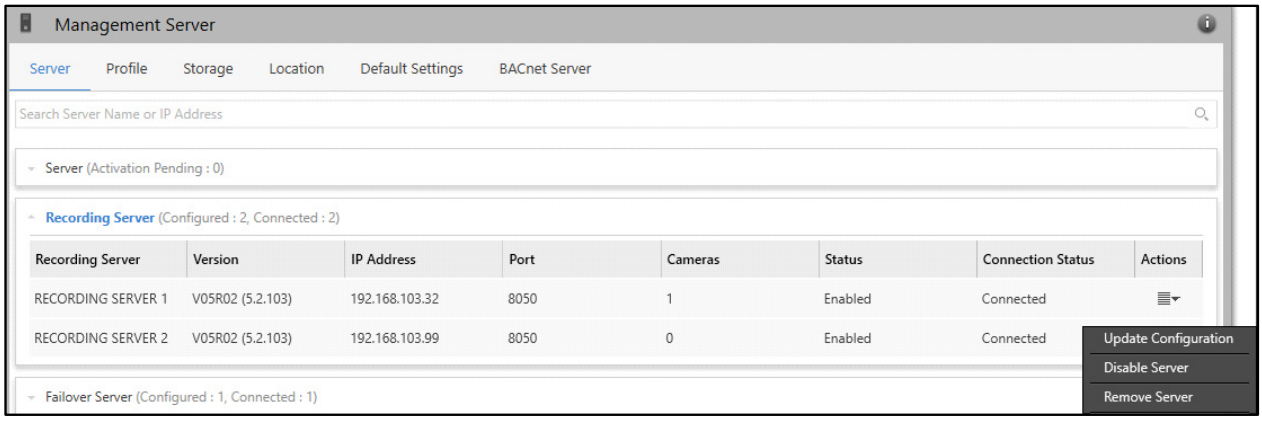


According to the function you select, the Server will be displayed under the respective collapsible panel — Recording Server or Failover Server collapsible panel.

- The **Auto Add Camera** pop-up appears automatically once you activate the Server as Recording Server.



- Click **Yes** to add the cameras. For more details, refer to “Auto Adding Devices/Cameras while activating the Recording Server”.
- If you click **No**, you can add devices later-on also. For details, refer to “Devices”.
- To make changes in the activated Server’s configuration — Recording/Failover, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.



*Once a Recording Server is removed, all its configured devices will get deleted. The removed Recording Server shall, however, appear in the Server list with the **Activation Pending** status (on restarting the Recording Server) and can be activated again, as required. To permanently remove a Recording Server, you must uninstall it.*

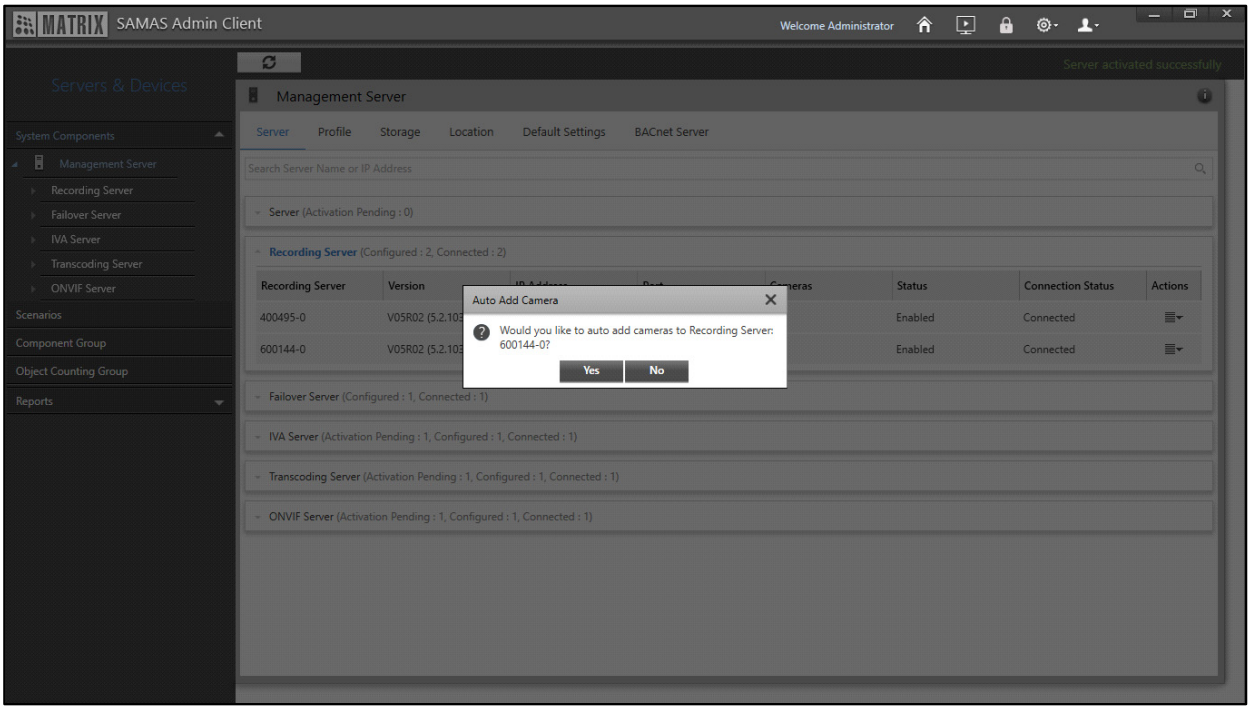
Auto Adding Devices/Cameras while activating the Recording Server

To avoid the hassle of manually adding and configuring network cameras one at a time, there is an option to automatically search the network, add and configure all detected IP cameras at once. Any IP cameras in the local

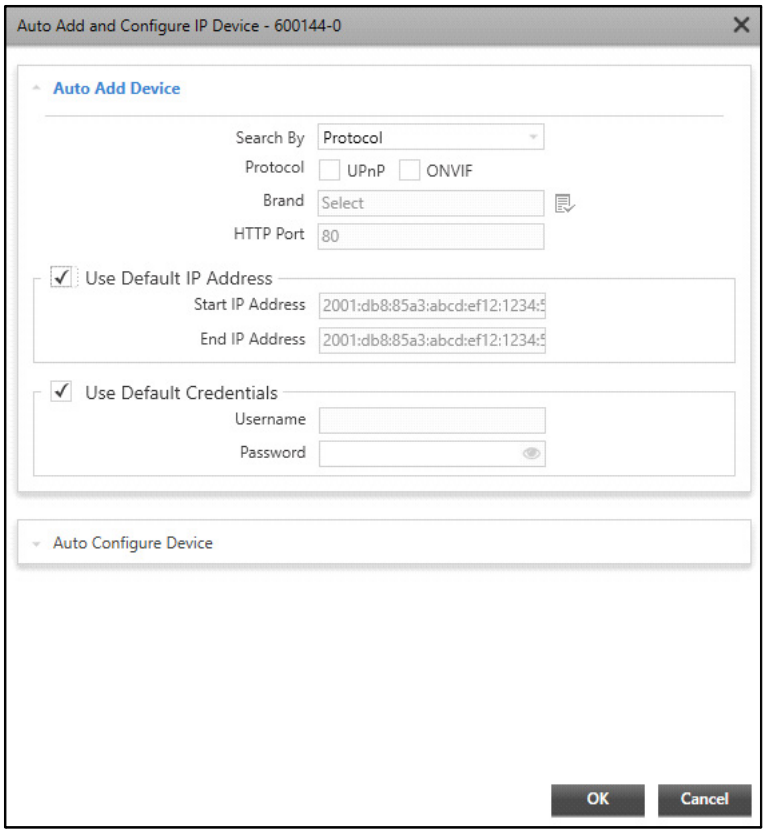
network of the Recording Server are discovered on activation of the Recording Server and the you are prompted to auto add them.

The names of the Recording Servers whose activation requests are pending are the names of the PC on which the respective Servers are installed. After Activation the names can be edited from their respective Profiles.

- The **Auto Add Camera** pop-up appears when you configure a server as Recording Server from the **Server** collapsible panel on the **Management Server** page.



- Click **Yes**. The **Auto Add and Configure IP Device** pop-up appears.



The **Auto Add and Configure IP Device** pop-up contains two collapsible panels —"Auto Add Device" and "Auto Configure Device"

Make sure the IP Address Range configured is either IPv4 or IPv6 in both "Auto Add Device" and "Auto Configure Device".

Configure the following parameters:

Auto Add Device

- **Search By:** Select the search mode from the Search By drop-down list options — Protocol or Brand. If you select **Protocol**, select the desired protocol— **UPnP**, **ONVIF** or you can also select both the check boxes.

  If you select **Brand**, select the device brand from the **Brand** picklist. Double-click to select the desired option.

Only Matrix Cameras will be fetched by UPnP Protocol.

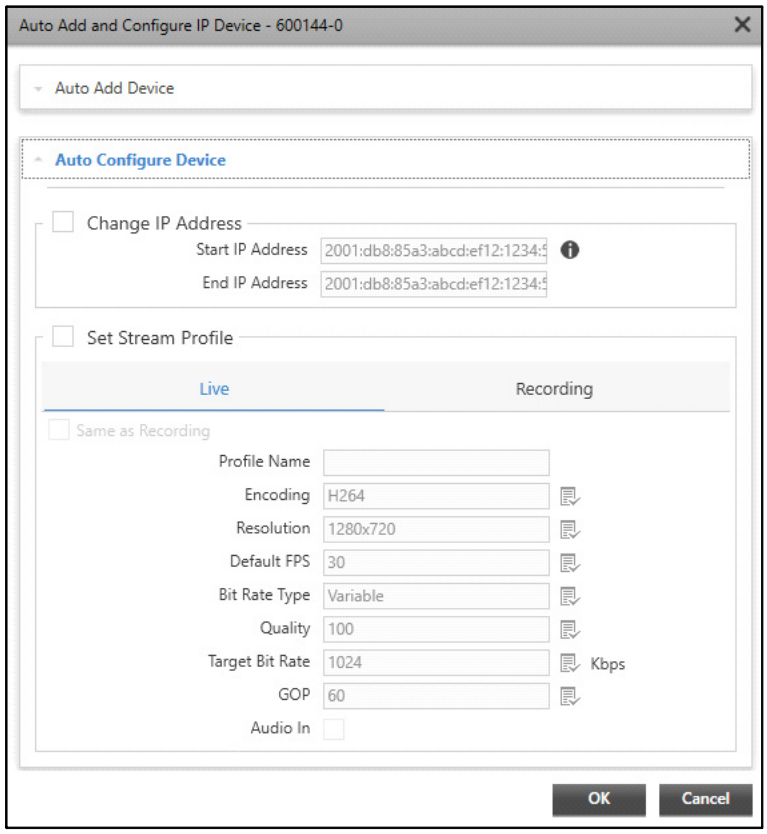
- **HTTP Port:** If you have selected **Search By** as **brand**, specify the HTTP Port. Valid Range: 1-65535. Default: 80.

- **Use Default IP Address:** Select this check box to search the cameras using Default IP Range. The Default IP Range will be in the range of the Recording Server network. If this check box is not selected, then user-defined IP Range can be specified in Start/End IP Address using which cameras will be searched.

- **Start IP Address**: Specify the Start IPv4/IPv6 Address if you wish to search the cameras in a specific IP range. In Start IP Address, you can enter upto 39 characters. Default: 192.168.1.1
- **End IP Address**: Specify the End IPv4/IPv6 Address of the IP range in which you wish to search the cameras. In End IP Address, you can enter upto 39 characters. Default: 192.168.1.254
- **Use Default Credentials:** Select this check box to add the cameras using default credentials for authentication.

  If you wish to specify user-defined credentials in User Name and Password field for authentication, make sure you clear the **Use Default Credentials** check box.
- **User Name**: Specify the User Name to search the cameras using user-defined credentials. In User Name, you can enter upto 100 characters. Default: Blank.
- **Password**: Specify the Password for authentication. In Password, you can enter upto 100 characters. Default: Blank. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

Auto Configure Device



- **Change IP Address**: Select the check box to enable changing the IP Addresses of all the discovered cameras. This may be useful especially in instances when all the added cameras are of a particular brand and have the same IP Address. In such cases, system will identify only a single IP Address and only one camera will be added, unless different IP Addresses are assigned to all the cameras.

Make sure the cameras support IPv4/IPv6 Addressing Mode before changing the IP Address.

- **Start IP Address**: Specify the Start IPv4/IPv6 Address for the IP range. In Start IP Address, you can enter upto 39 characters. Default: Depends on the subnet of the PC where Recording Server is installed.

- **End IP Address**: Specify the End IPv4/IPv6 Address for the IP range. In End IP Address, you can enter upto 39 characters. Default: Depends on the subnet of the PC where Recording Server is installed.

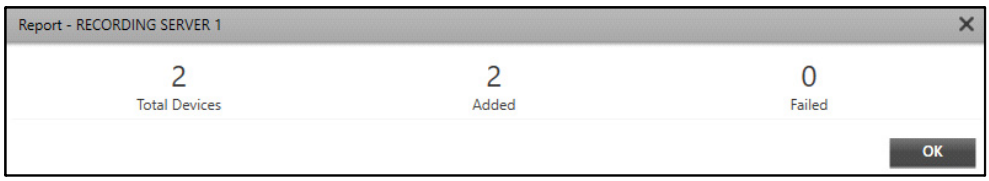
- **Set Stream Profile**: Select the check box to set user-defined stream profile settings. To set the Stream Profile, refer to "Camera Configuration".

*If **Set Stream Profile** is disabled, Live stream and Recording stream will be set as per default stream profile settings.*

- You can define Stream Settings separately under the **Live** and **Recording** tabs. You can also replicate settings of **Live** tab to **Recording** tab and vice-versa. Select **Same as Recording** check box under **Live** tab or **Same as Live** under **Recording** tab**.**

- Click **OK** to add all cameras with the above configuration. Click **Cancel** to discard.

Once the cameras are added in the Recording Server, a Report for the same appears.



- Click **OK**. The added cameras appear under the Recording Server. For details, refer to "Devices".

Activating Server as IVA Server

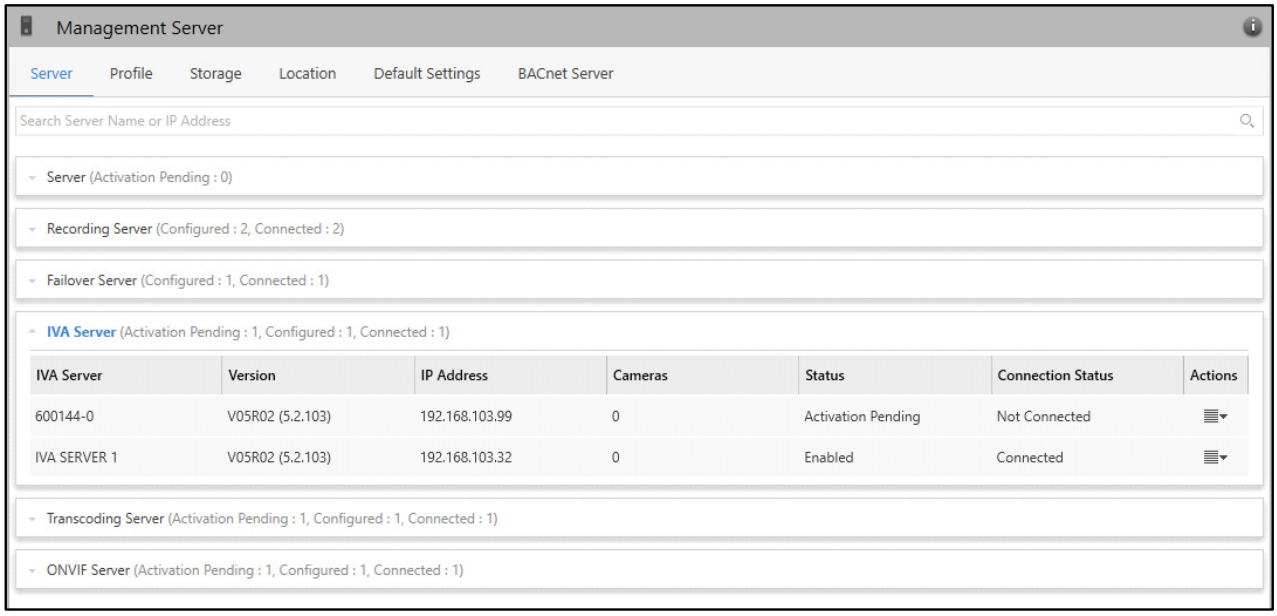
The IVA Server collapsible panel displays the pending activation requests of the IVA Servers. You can activate the IVA Servers from this collapsible panel.

To activate the Servers,

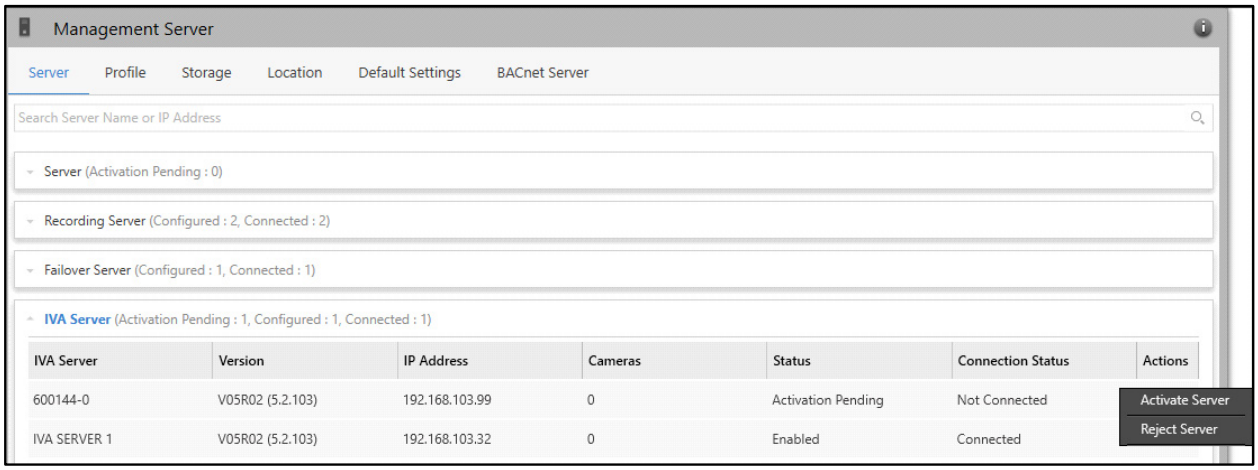
- Click the **IVA Server** collapsible panel.

The names of the IVA Servers whose activation requests are pending are the names of the PC on which the respective Servers are installed. After Activation the names can be edited from their respective Profiles. Refer to "Profile" in "IVA Server Configuration".

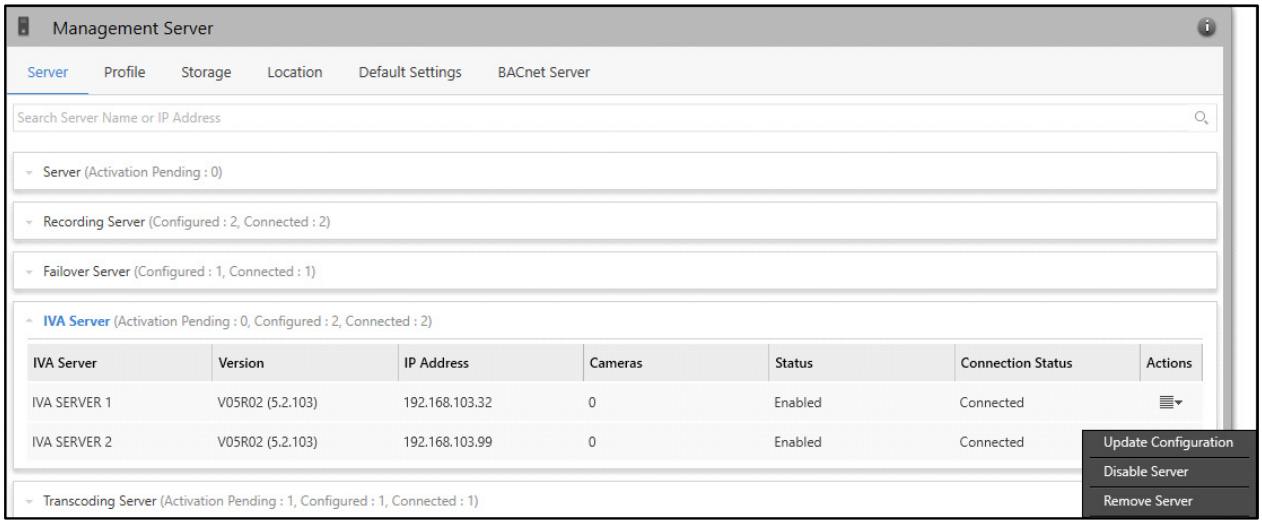
- To activate the requesting server, click **Actions** .



- Click **Activate Server**. If you do not wish to activate it, click **Reject Server**.



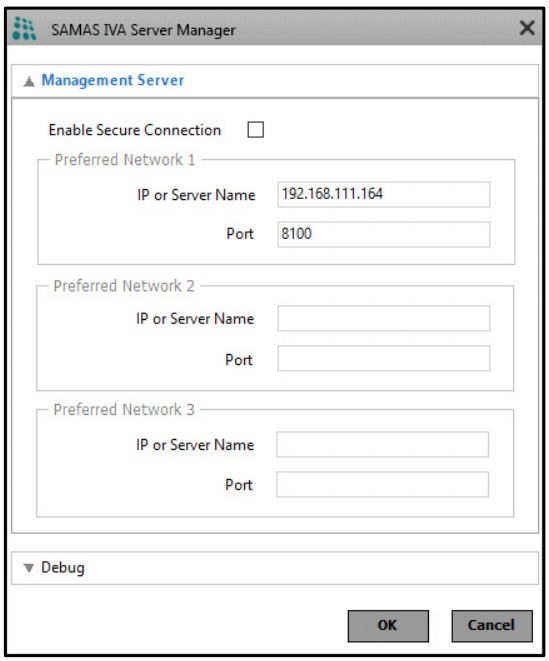
- To make changes in the activated server's configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.



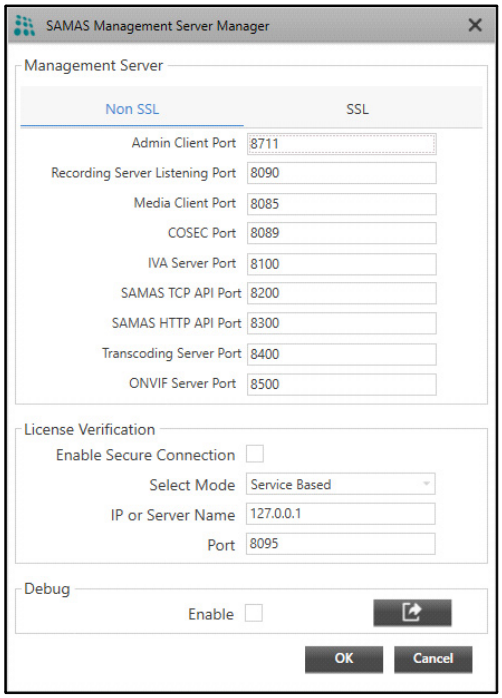
- *The Cameras can be added to the IVA Server only if the Cameras are added to the respective Recording Servers.*
- *One camera cannot be added in two IVA Servers.*
- *Make sure you have enabled the IVA Server, before adding cameras to it.*

For example, IVA Server (192.168.103.99) has requested to connect to the MS (192.168.111.164). To connect the server, the IP Address (192.168.111.164) and Port (8100) of MS must be specified in IVA Server Manager of PC (192.168.103.99).

Settings in PC (192.168.103.99, IVA Server)



Settings in PC (192.168.111.164, MS)



Activating Server as Transcoding Server

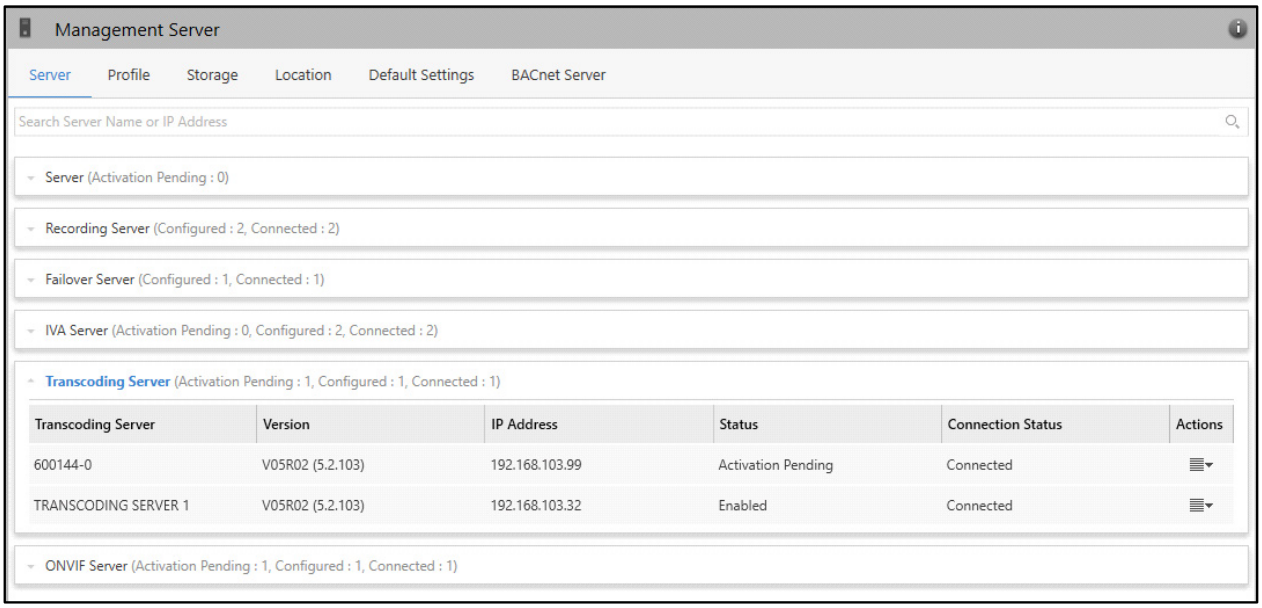
The Transcoding Server collapsible panel displays the pending activation requests of the Transcoding Servers. You can activate the Transcoding Servers from this collapsible panel.

To activate the Servers,

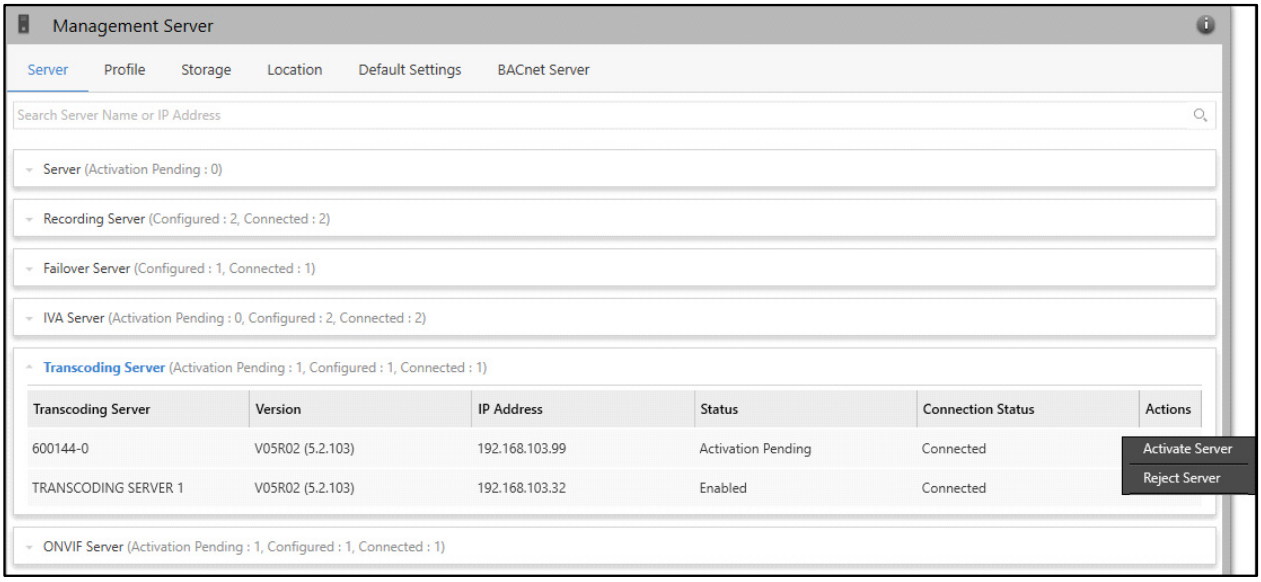
- Click the **Transcoding Server** collapsible panel.

The names of the Transcoding Servers whose activation requests are pending are the names of the PC on which the respective Servers are installed. After Activation the names can be edited from their respective Profiles. Refer to "Profile" in "Transcoding Server Configuration".

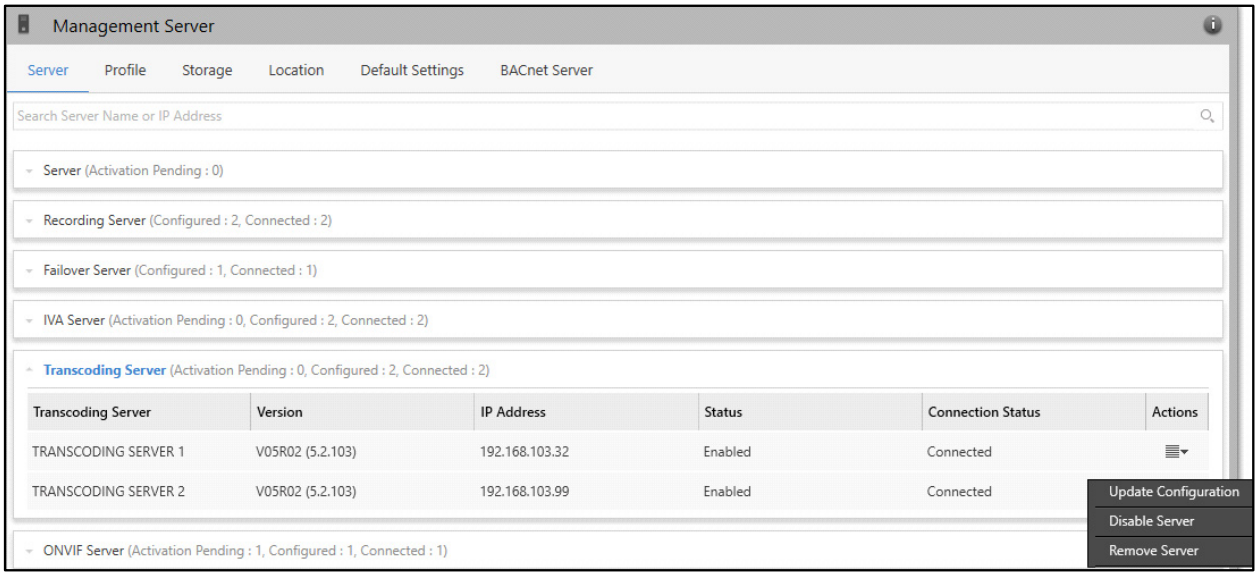
- To activate the requesting server, click **Actions** .



- Click **Activate Server**. If you do not wish to activate it, click **Reject Server**.

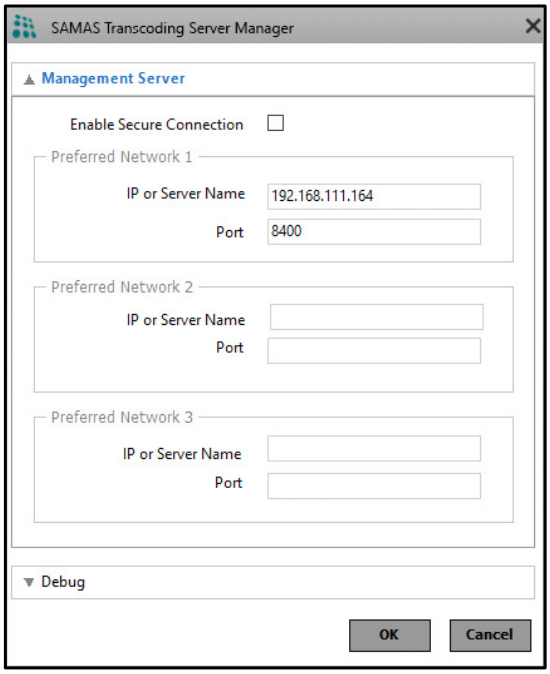


- To make changes in the activated server's configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.

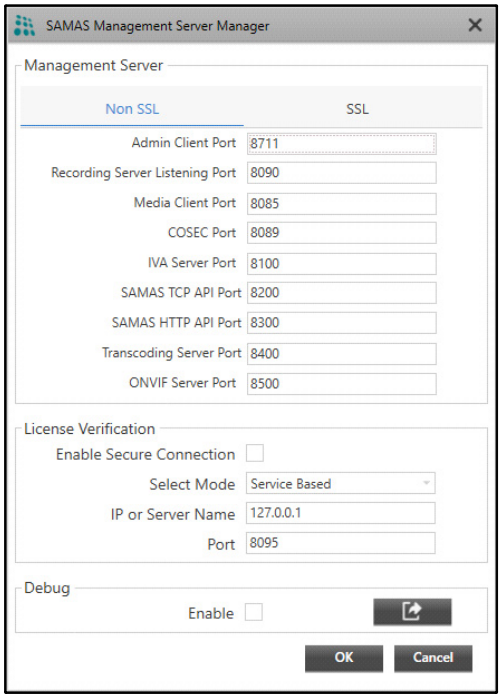


For example, Transcoding Server (192.168.103.99) has requested to connect with the MS IP (192.168.111.164). To connect, the IP Address (192.168.111.164) and Port (8400) of MS must be specified in Transcoding Server Manager (192.168.103.99).

Settings in PC (192.168.103.99, Transcoding Server)



Settings in PC (192.168.111.164, MS)



Activating Server as ONVIF Server

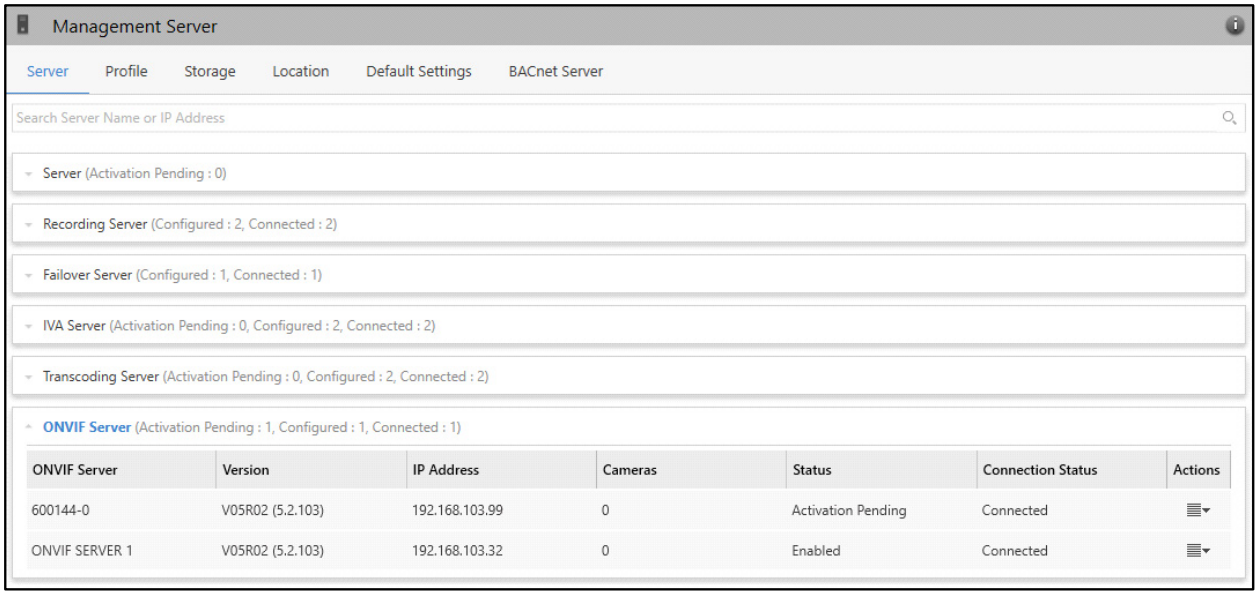
The ONVIF Server collapsible panel displays the pending activation requests of ONVIF Servers. You can activate the ONVIF Servers from this collapsible panel.

To view and activate the Servers,

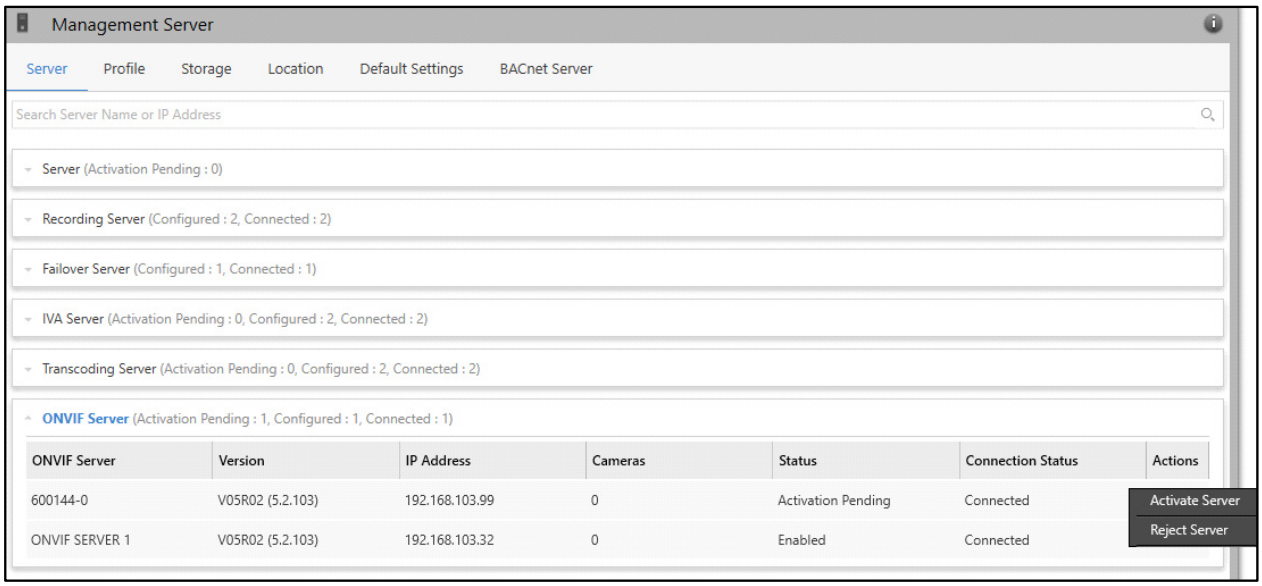
- Click the **ONVIF Server** collapsible panel.

The names of the ONVIF Servers whose activation requests are pending are the names of the PC on which the respective Servers are installed. After Activation the names can be edited from their respective Profiles. Refer to "Profile" in "ONVIF Server Configuration".

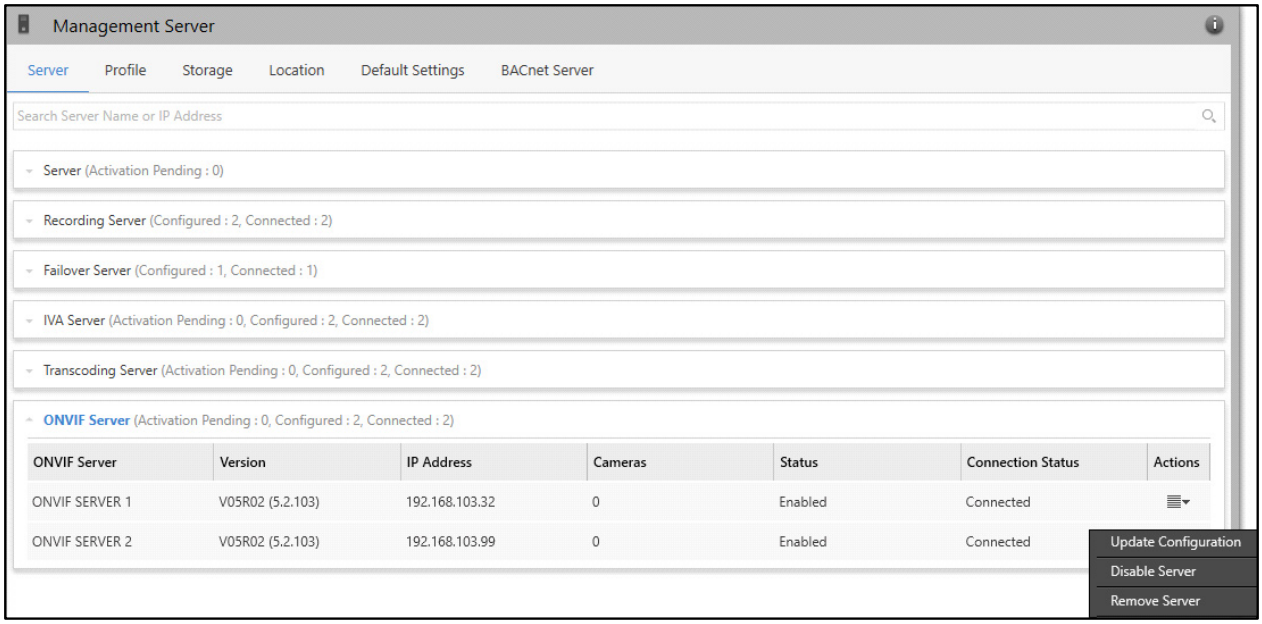
- To activate the requesting server, click **Actions** .



- Click **Activate Server**. If you do not wish to activate it, click **Reject Server**.

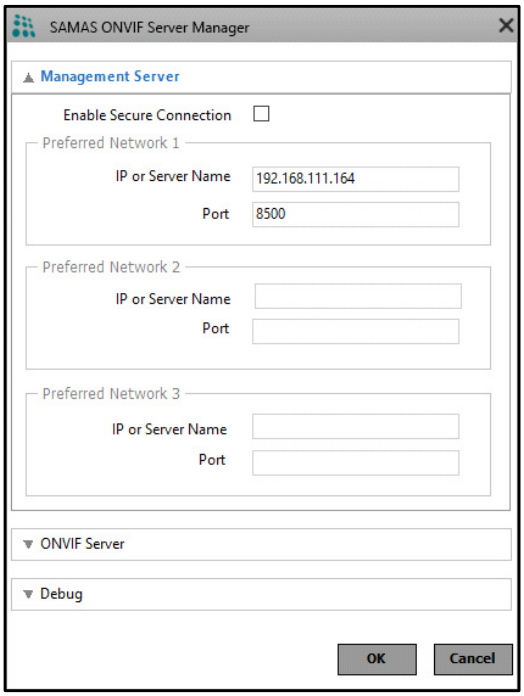


- To make changes in the activated server's configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.

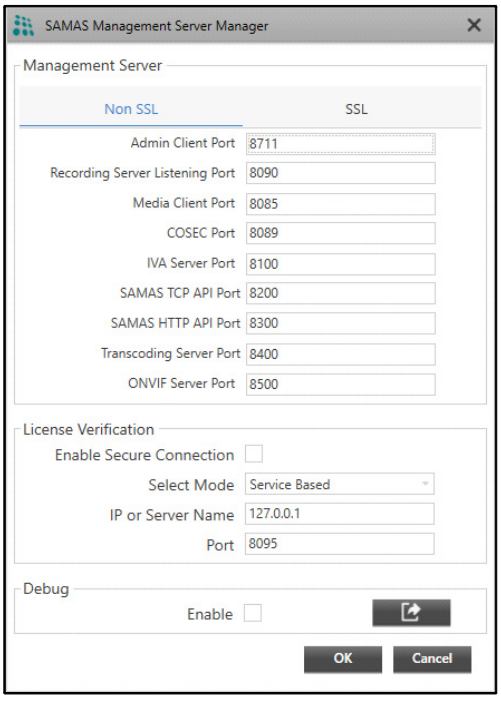


For example, The request from ONVIF Server (192.168.103.99) is sent to the MS IP (192.168.111.164). For this the IP Address (192.168.111.164) and Port (8500) of MS is specified in ONVIF Server Manager (192.168.103.99).

Settings in PC (192.168.103.99, ONVIF Server)



Settings in PC (192.168.111.164, MS)

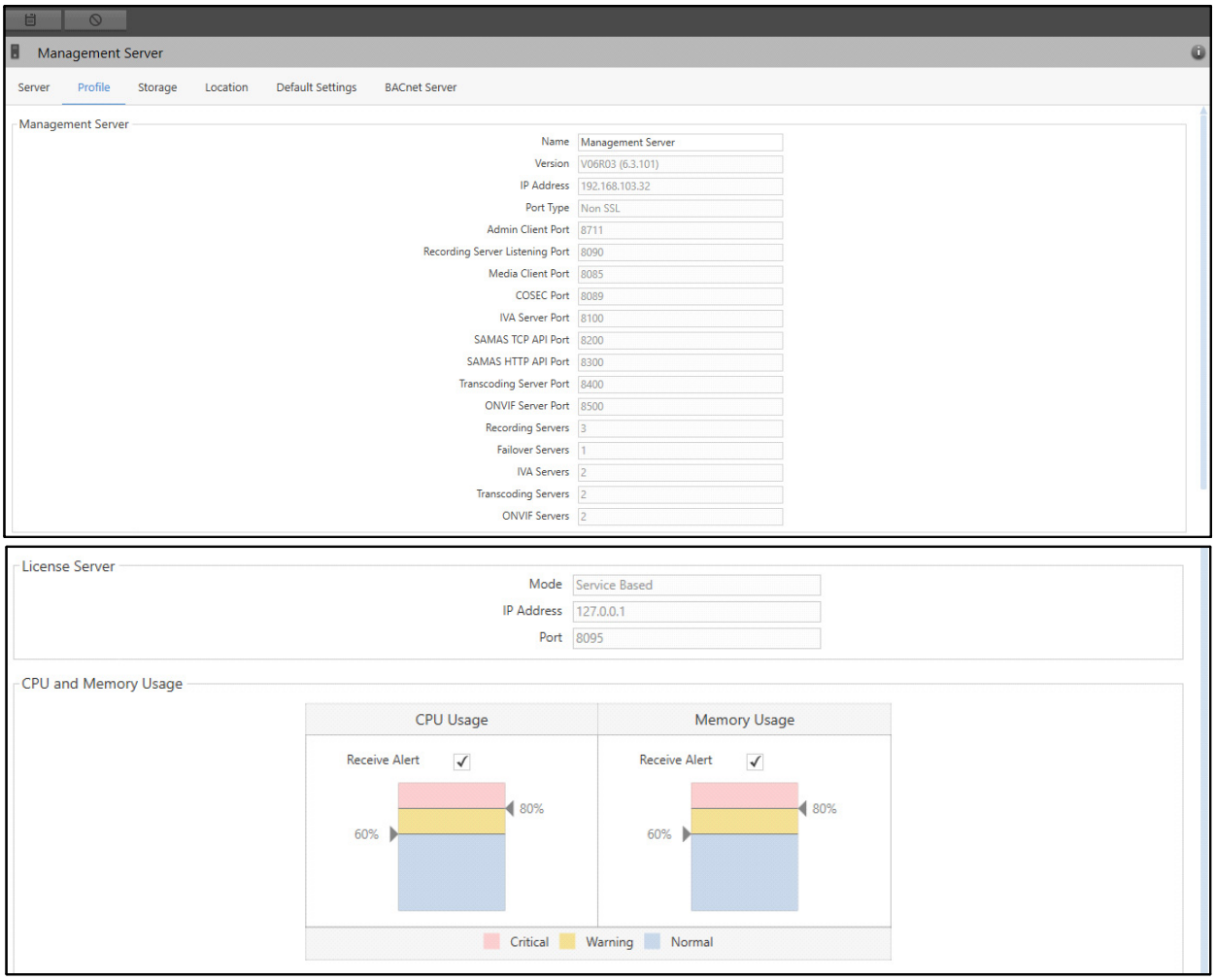


Profile

This tab enables you to view the Profile of the Management Server.

To configure Profile settings,

- Click the **Profile** tab.



This tab contains these sections — “Management Server”, “License Server” and “CPU and Memory Usage”.

Management Server

This section displays the details of the Management Server like IPv4/IPv6 Address, Version, Port Settings and the subsequent number of servers assigned. You can only assign a Name to the Management Server.

- **Name**: Specify a name for the Management Server. In Name, you can enter upto 50 characters. Default: Management Server.
- Click **Save** to save the settings or **Cancel** to discard.

License Server

This section displays the selected Mode for license verification, IPv4/IPv6 Address/MAC Address and Port number of the License Server.

CPU and Memory Usage

This section displays the CPU and Memory Usage configurations.

- **Receive Alert**: This check box is selected by default, to receive alerts when the Management Server crosses the set threshold value under **CPU Usage** and **Memory Usage**. We recommend you not to clear this check box.

- **Critical, Warning and Normal Threshold Values:** The Critical, Warning and Normal Threshold Values for CPU and Memory Usage can be configured by dragging the pointer or tapping on the empty area. Valid Range: 0-100%. Default: Warning: 60, Critical: 80.

  In the Smart Client,
  - the CPU Usage/Memory Usage Exceeded pop-ups appear with a yellow boundary.
  - the CPU Usage/Memory Usage Critical pop-ups appear with a red boundary.
  - the CPU Usage/Memory Usage Critical event is highlighted in red color under Online Events.

  For example, in the above screen the CPU Usage and Memory Usage thresholds are configured as 60% for Warning and 80% for Critical respectively. Hence, you will receive an alert when the CPU Usage or the Memory Usage goes beyond 60% and 80%, that is when it crosses the Warning and Critical limit as well as when it comes back to its Normal limit again.

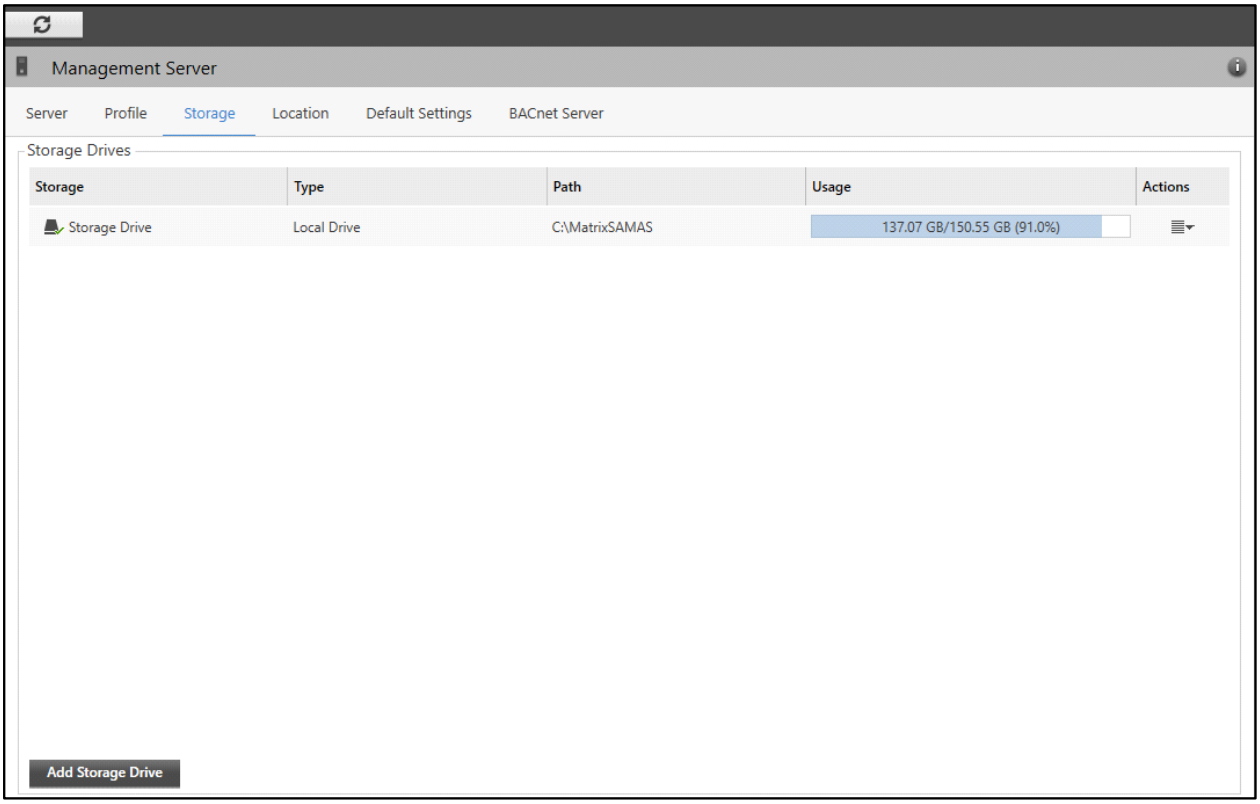
- Click **Save**  to save the settings or **Cancel**  to discard.

Storage

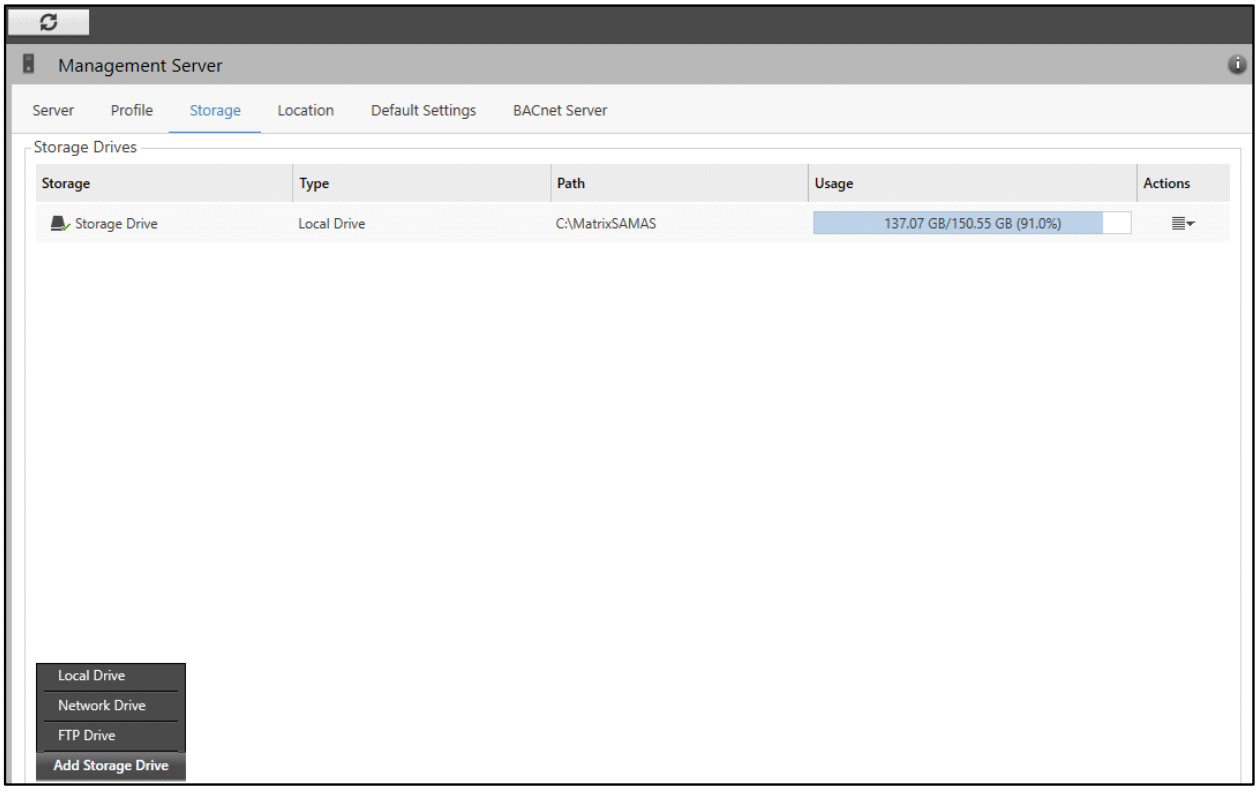
This tab enables you to define the storage drive path where all the data can be saved. The storage path can be defined here by adding the Storage Drive to save the data at the defined path to be accessed later.

To add a Storage Drive,

- Click the **Storage** tab. The Storage Drive as configured with the Management Server during the installation of the Admin Client appears by default. You can only delete the default Storage Drive.



- Click **Add Storage Drive**. You can either add Local Drive, Network Drive or FTP Drive.

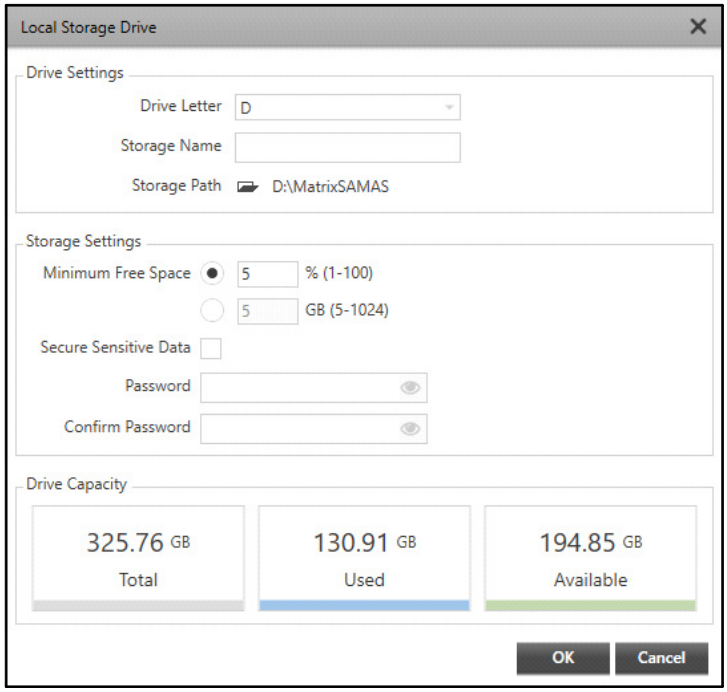


Refer to the following links for detailed configuration of each type of drive.

- “Local Drive”
- “Network Drive”
- “FTP Drive”

Local Drive

- Click **Add Storage Drive > Local Drive.**
- The **Local Storage Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Drive Letter:** Select a drive from the drop-down list where you wish to store the records.
- **Storage Name:** Specify a unique name. The configured Local Drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.
- **Storage Path:** Browse a storage path in the selected drive where you wish to store the records. Click

  Browse . It displays all folders which are in the drive. Select the desired folder.

Storage Settings

- **Minimum Free Space:** Specify the desired space in terms of value which is to be kept empty in the selected Local Drive. You can define the value either in Percentage (Valid Range: 1-100, Default: 5) or GB (Valid Range: 5-1024, Default: 5).

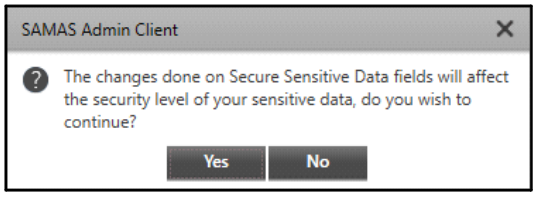
  For example, if you configure the value as 5%, **Storage Memory Low** event will be generated by the Management Server when 5% memory is empty in the drive.

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Event Images, User Images, Transaction Images. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.
- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.
- **Confirm Password**: Re-enter the password to confirm. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

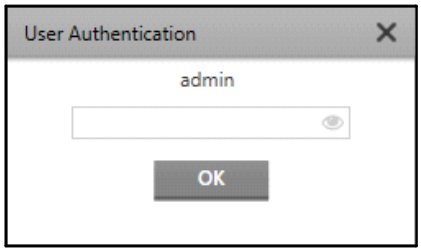
Drive Capacity

- **Total Space:** This displays total space of the Local Drive of the Management Server in GBs.
- **Used Space:** This displays the space of the Local Drive that is used in GBs.
- **Available Space:** This displays the remaining space available for storing records in the Local Drive of the Management Server in GBs.

- Click **OK** to save the Storage Drive configurations. The following pop-up will appear.



- Click **Yes** to continue. The **User Authentication** pop-up will appear.

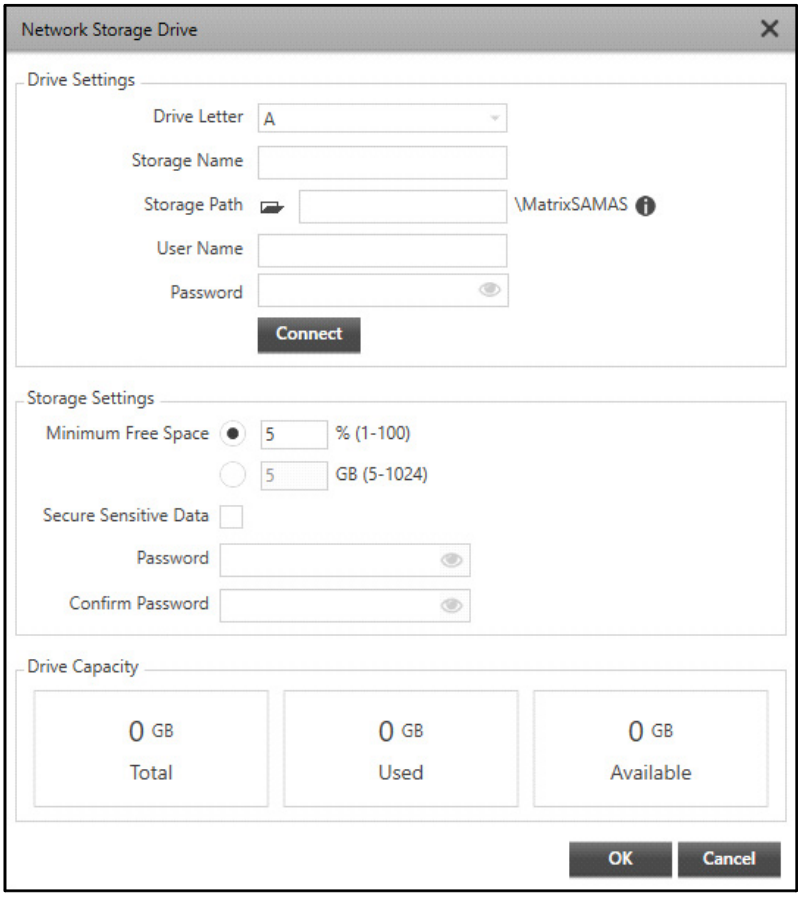


- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **OK**.

Network Drive

- Click **Add Storage Drive > Network Drive.**
- The **Network Storage Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Drive Letter:** Select a drive from the drop-down list where you wish to store the records.
- **Storage Name:** Specify a unique name. The configured Network Drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.
- **Storage Path:** Browse a storage path in the selected drive where you wish to store the records.

  Click **Browse** . It displays all drives which are in there in the network. Select the desired drive and the folder. In Storage Path, you can enter upto 255 characters. Default: Blank.

Storage Path supports both IPv4/IPv6 Address of a system or Server Name where you wish to create Network Storage Drive.

- *If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].*
- *If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.*

- **User Name**: Specify the User Name for the authentication of the Network Drive. In User Name, you can enter upto 50 characters. Default: Blank.

- **Password:** Specify the Password for the authentication of the Network Drive. In Password, you can enter upto 50 characters. Default: Blank. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **Connect** to test the connection with the specified drive. The connection will be successful if the Network Drive is accessible and the User Name and Password are valid.

Storage Settings

- **Minimum Free Space:** Specify the desired space in terms of value which is to be kept empty in the selected Network Drive. You can define the value either in Percentage (Valid Range: 1-100, Default: 5) or GB (Valid Range: 5-1024, Default: 5).

  For example, if you configure the value as 5%, **Storage Memory Low** event shall be generated by Management Server when 5% memory is empty in the drive.

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Event Images, User Images, Transaction Images. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.

- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- **Confirm Password**: Re-enter the password to confirm. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

Drive Capacity

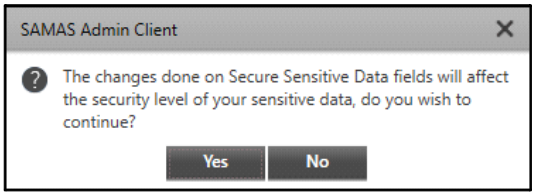
The Drive Capacity of the Network Drive will be displayed only after the connection is successful.

- **Total Space:** This displays total space of the Network Drive of the Management Server in GBs.

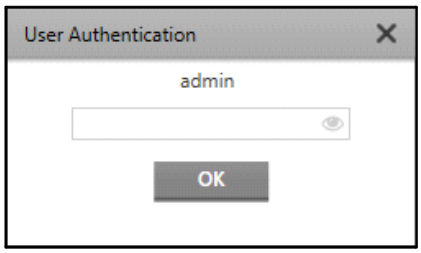
- **Used Space:** This displays the space of the Network Drive that is used in GBs.

- **Available Space:** This displays the remaining space available for storing records in the Network Drive of the Management Server in GBs.

- Click **OK** to save the Storage Drive configurations. The following pop-up will appear.



- Click **Yes** to continue. The **User Authentication** pop-up will appear.



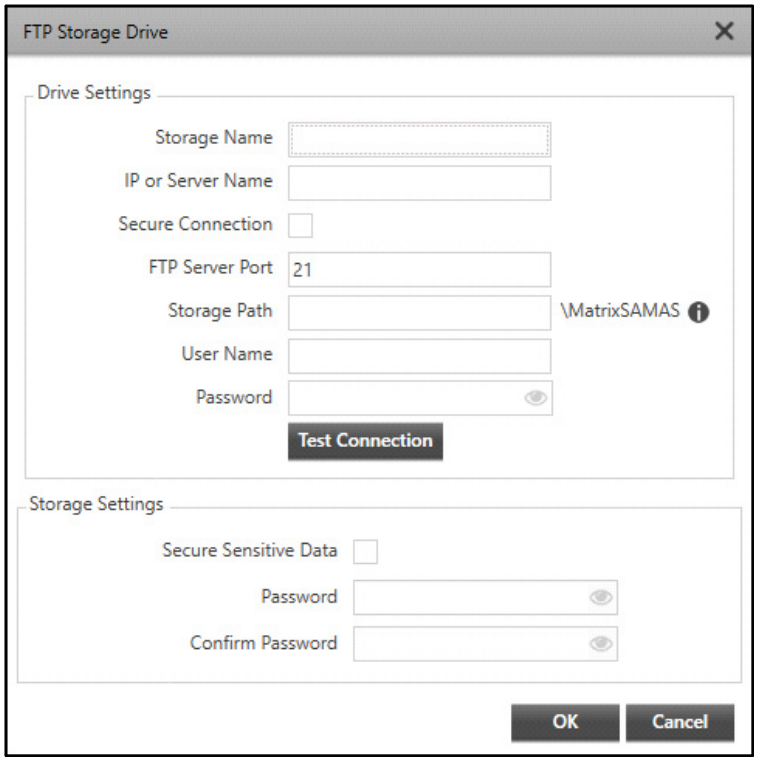
- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **OK**.

FTP Drive

- Click **Add Storage Drive > FTP Drive.**

- The **FTP Storage Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Storage Name:** Specify a unique name. The configured FTP drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.

- **IP or Server Name:** Specify the Server Name or IPv4/IPv6 Address of the FTP Server where the records are to be stored. In IP or Server Name, you can enter upto 100 characters. Default: Blank.

If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].

If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Secure Connection**: Select the check box to enable secure file transfer.
- **FTP Server Port:** Specify the FTP Listening Port number. Valid Range: 1-65535. Default: 21.
- **Storage Path:** Specify a storage path where you wish to store the records. In Storage Path, you can enter upto 300 characters. Default: Blank.

Storage Path supports both IPv4/IPv6 Address of a system or Server Name where you wish to create FTP Storage Drive.

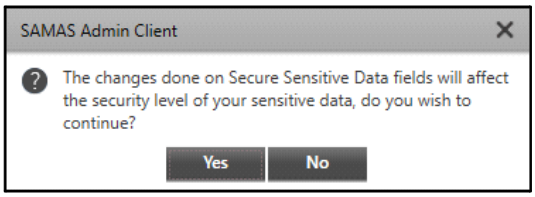
- *If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].*
- *If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.*

- **User Name**: Specify the User Name for the authentication of the FTP Drive. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password:** Specify the Password for the authentication of the FTP Drive. In Password, you can enter upto 50 characters. Default: Blank. Click **Show**  to view the password. The icon toggles to **Hide**  . Click **Hide**  to hide the password.
- Click **Test Connection** to test the connection with specified drive. The connection will be successful if the FTP Drive is accessible and the User Name and Password are valid.

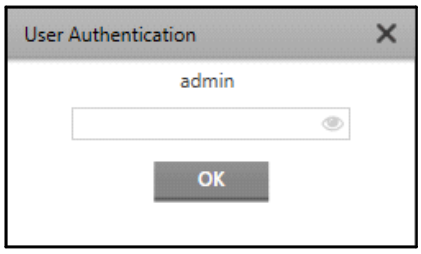
Storage Settings

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Event Images, User Images, Transaction Images. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.
- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show**  to view the password. The icon toggles to **Hide**  **.** Click **Hide**  to hide the password.
- **Confirm Password**: Re-enter the password to confirm. Click **Show**  to view the password. The icon toggles to **Hide**  **.** Click **Hide**  to hide the password.

- Click **OK** to save the Storage Drive configurations. The following pop-up will appear.



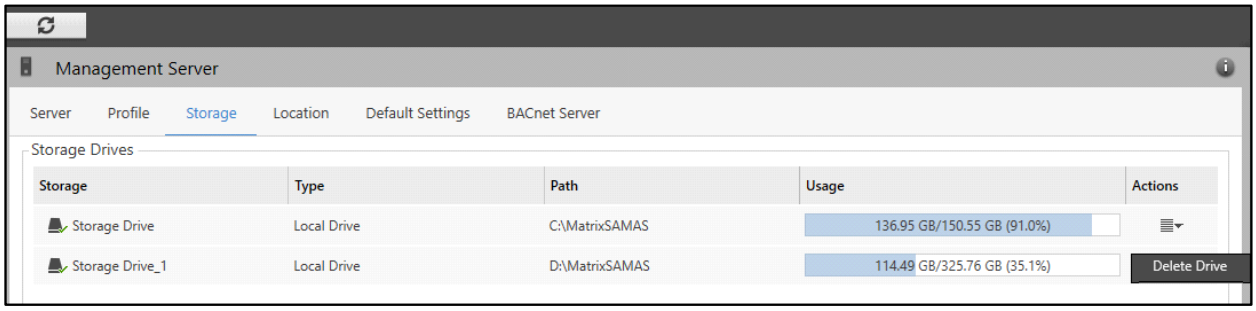
- Click **Yes** to continue. The **User Authentication** pop-up will appear.



- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **OK**.

The configured Storage Drives appear in a grid under the **Storage** tab.



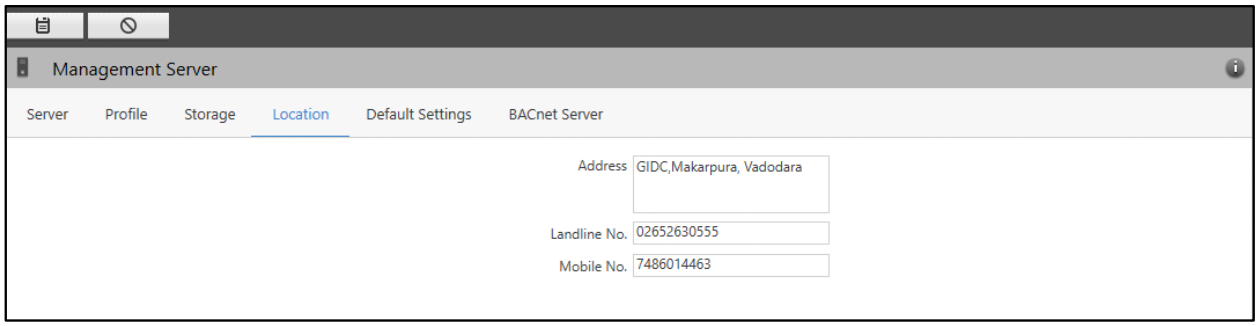
- Click **Actions** and **Delete Drive** to delete the configured Storage Drive.
- Click **Refresh** to refresh the configurations of the configured Storage Drive.

Location

This tab enables you to configure the location information of the Management Server.

To configure the location,

- Click the **Location** tab.



Configure the following parameters:

- **Address**: Specify the address where the Management Server is located. In Address, you can enter upto 150 characters. Default Blank.
- **Landline Number**: Specify the Landline Number of the place where the Management Server is located. In Landline Number, you can enter upto 15 characters. Default Blank.
- **Mobile Number**: Specify the Mobile Number of the place where the Management Server is located. In Mobile Number, you can enter upto 15 characters. Default Blank.

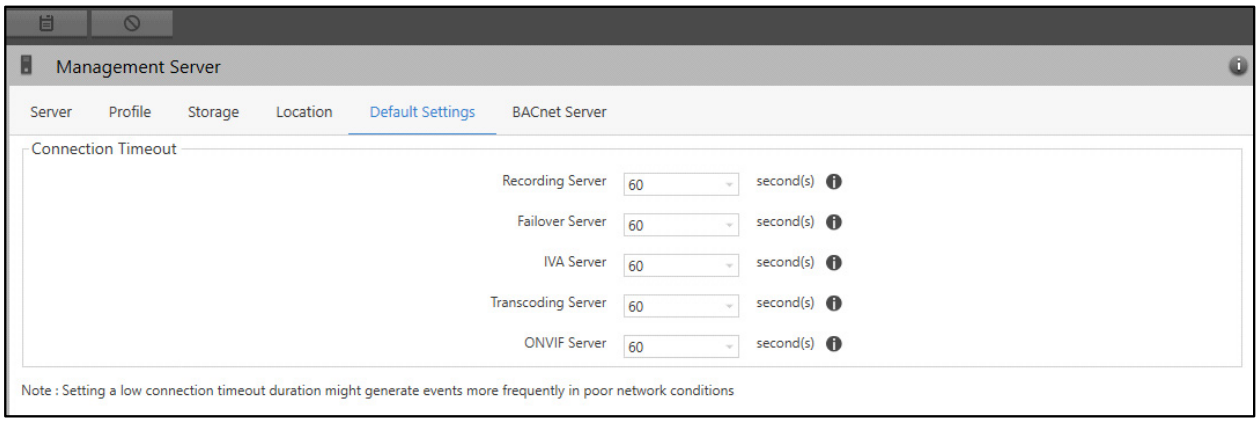
- Click **Save** to save the location details or **Cancel** to discard.

Default Settings

This tab enables you to configure the Connection Timeout for the Servers — Recording Server, Failover Server, IVA Server, Transcoding Server and ONVIF Server.

To configure the Default Settings,

- Click the **Default Settings** tab.



The default value for **Connection Timeout** is 60 seconds for all the Servers. This is the approximate time (in seconds) till which the MS will wait for reconnection with RS/FoS/IVA/TS/ONVIF Server once it is disconnected with MS. If the connection is established again within the configured time, the MS will not generate an Event, otherwise it will generate **Server Disconnected** Event.

If the additional Preferred Network 2 & Preferred Network 3 are configured during login into Admin Client, MS will wait for extra 30 seconds for each Preferred Network to establish the connection with it after the configured connection time duration is over. If the connection is established with any configured Preferred Network within 30 seconds, the MS will not generate an Event, otherwise it will generate **Server Disconnected** Event.

- Select the desired Connection Timeout for each server from the drop-down list.
- Click **Save** to save the configurations or **Cancel** to discard.

BACnet Server

*The BACnet Server tab is applicable for **Administrator** User Group only.*

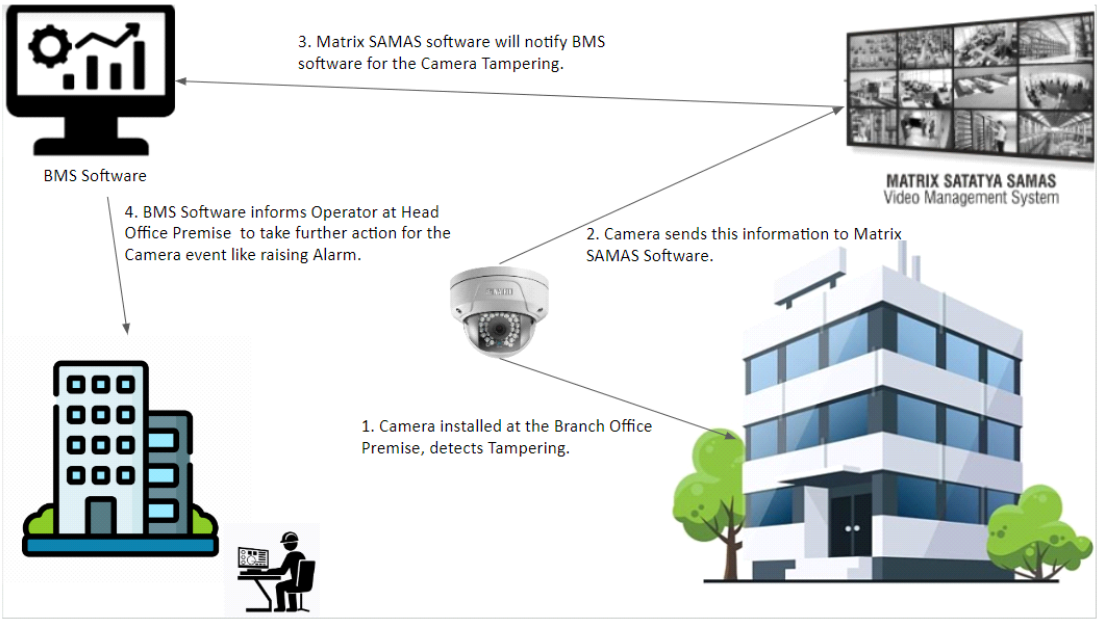
Communication over BACnet protocol is not encrypted, even if the Management Server is running in SSL mode.

BACnet (Building Automation and Control Network) is an industry-standard protocol that is specifically used in Building Automation Systems. BACnet provides a standard framework for communication, management, monitoring and control of various automation functions specific to buildings, such as Lighting, HVAC, Fire Safety, Access Control and Energy Management Systems. BACnet supports multiple communication protocols, including Ethernet, TCP/IP, and RS-485, allowing for the integration of devices from different manufacturers and technologies.

Various Building Management Systems (BMS) rely on BACnet to communicate with each other for the exchange of data and to control devices and automation systems within a building.

Integration of BACnet with SAMAS enhances its capability to integrate with 3rd party Building Management Systems. With this integration, SAMAS Severs, Devices and their Events can be used to control various automation functions.

Let us understand this with the help of an example as depicted in the diagram below.



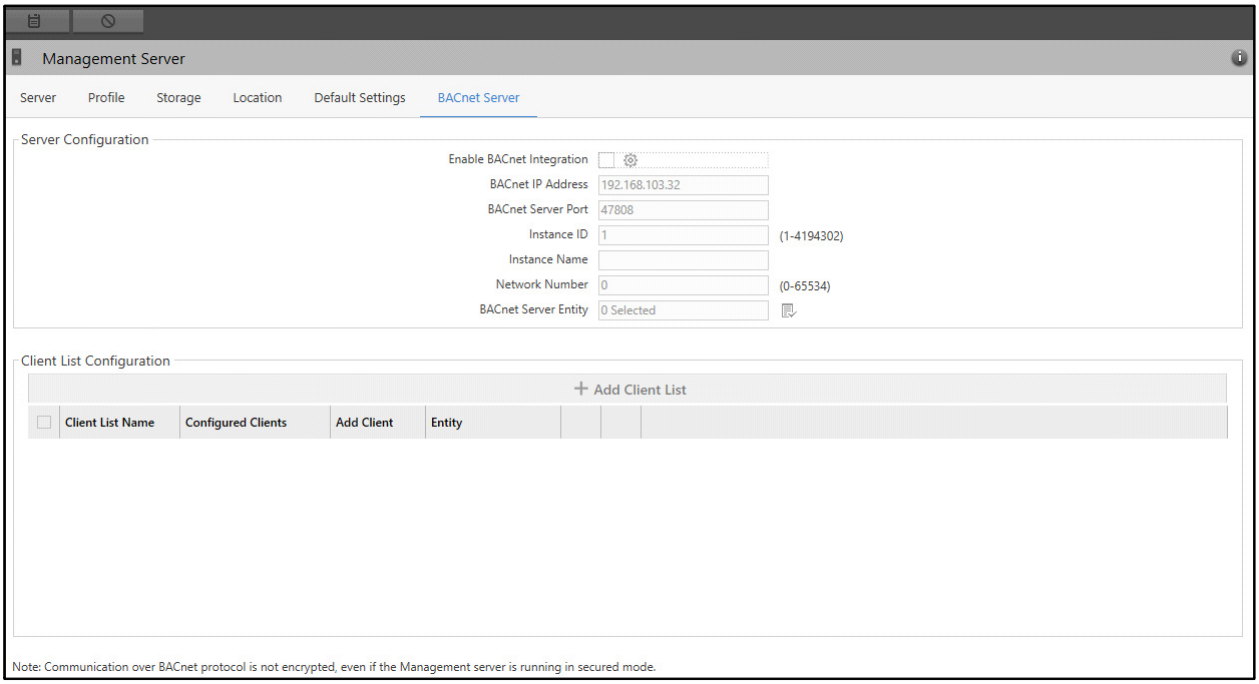
- In the above diagram there are two premises — Branch Office and Head Office. BMS is installed at Head Office.
- The BMS and SAMAS communicate using BACnet.
- When the Camera Tampering Event is generated by a camera at the Branch Office premise, the camera sends this event to SAMAS.
- SAMAS further sends this event to the BMS over BACnet.
- The BMS software controls the surveillance parameters in that premise, hence it triggers an alarm to raise awareness in the Head Office premise about the Event.
- The BMS software also notifies the Operator over BMS Portal to take action.

The SAMAS Servers and devices will be discovered by the BMS Clients over BACnet as Objects. These Objects send selected Events that are supported by SAMAS. For details, refer to “Objects supported by BACnet Server”.

BACnet supports various types of services for data exchange. There are selected services that are supported by SAMAS. For details, refer to “Services supported by BACnet Server”.

To integrate BACnet with SAMAS, you need to configure the BACnet Server and Client List.

- Click the **BACnet Server** tab.



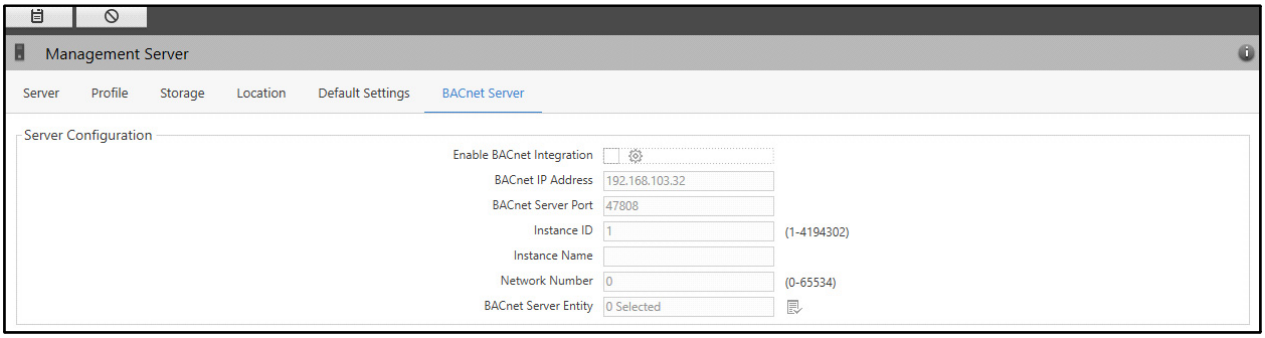
The BACnet Server tab contains these sections — “Server Configuration” and “Client List Configuration”.

Make sure the IP Addressing Protocol (IPv4/IPv6) in BACnet Server and the BACnet Clients is same to establish communication.

BACnet Server does not support Dual Stack functionality.

Server Configuration

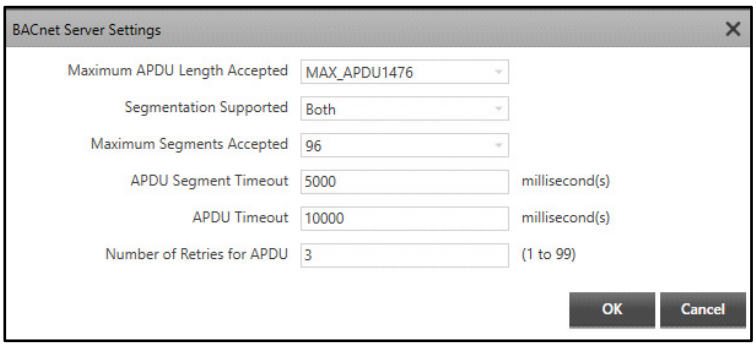
This section allows you to configure the BACnet Server parameters.



Configure the following parameters:

- **Enable BACnet Integration**: Select the check box to enable the BACnet Server Integration.

- Click **BACnet Server Settings** . The **BACnet Server Settings** pop-up appears.



Configure the following parameters:

- **Maximum APDU Length Accepted**: Select the desired option from the drop-down list as the maximum size of a single APDU that SAMAS will support. This parameter is included in the confirmed request so that the responding device may determine how to convey its response.

- **Segmentation Supported**: There may be messages that are longer than the maximum length supported by a communications network or by the sending or receiving device, hence BACnet supports Segmentation. Select the desired option from the drop-down list.

- **Maximum Segments Accepted**: Select the desired option from the drop-down list as the maximum number of segments to be transmitted in a Confirmed-Request or ComplexACK message.

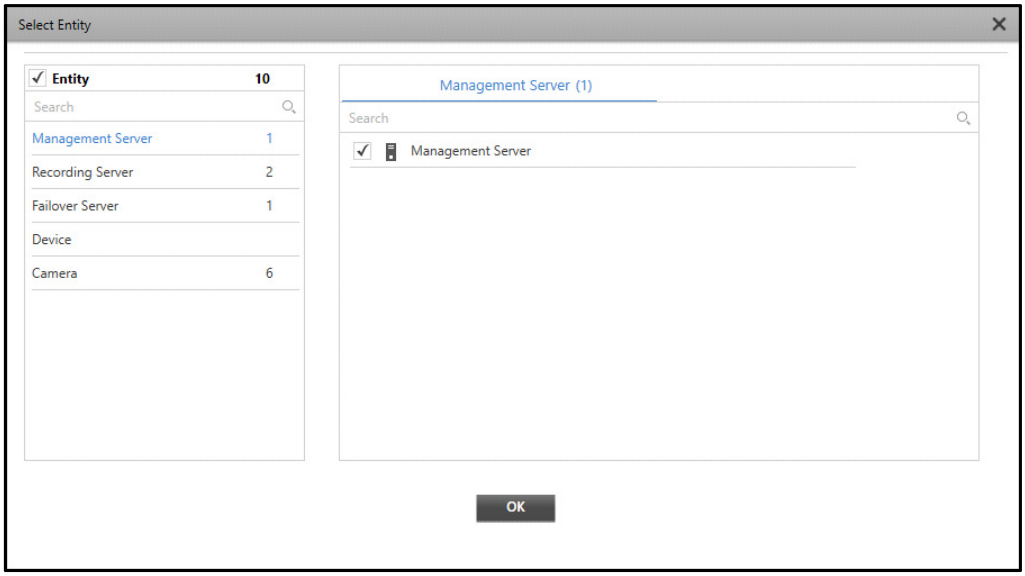
- **APDU Segment Timeout**: Specify the time duration between the transmission of two consecutive APDU segments. Valid Range: 1-4294967295 milliseconds. Default: 5000 milliseconds.

- **APDU Timeout**: This shall indicate the amount of time in milliseconds between retransmissions of an APDU requiring acknowledgment for which no acknowledgment has been received. Valid Range: 1-4294967295 milliseconds. Default: 1000 milliseconds.

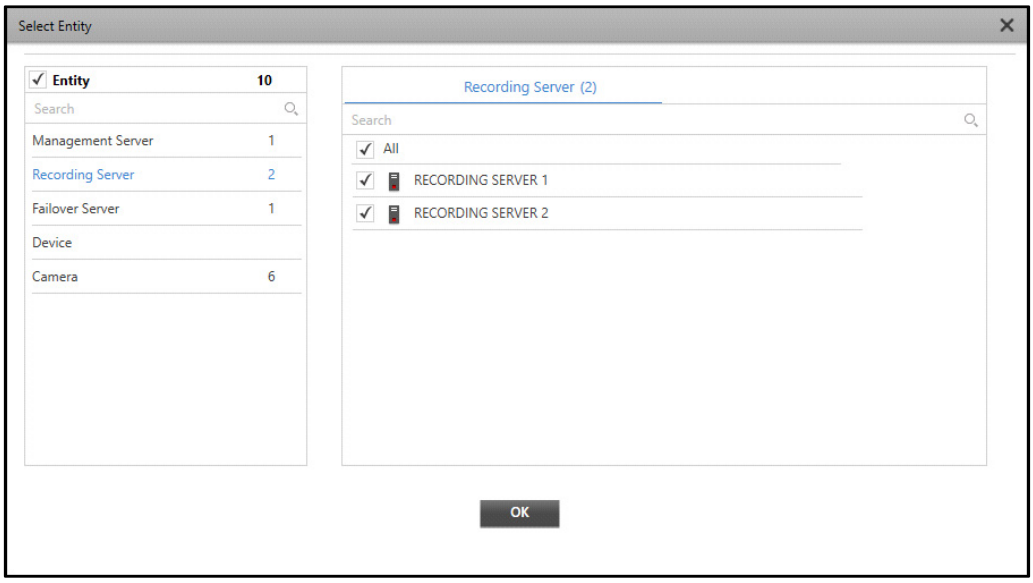
- **Number of Retries for APDU**: This shall indicate the maximum number of times that an APDU shall be retransmitted. Valid Range: 1-99. Default: 3.

- Click **OK** to save the settings. Now configure the remaining BACnet Server parameters.

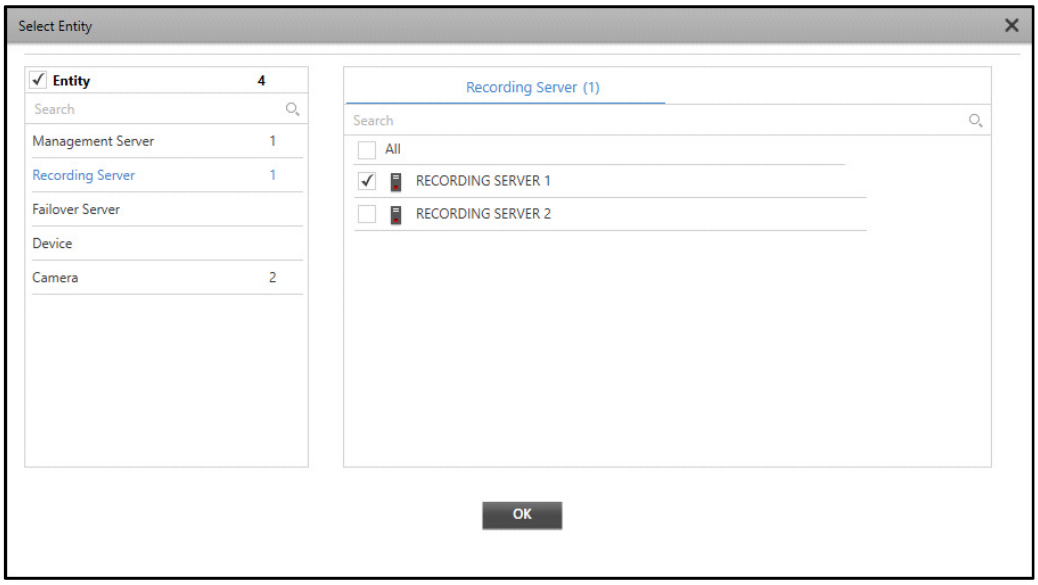
- **BACnet IP Address**: By default, this is the Management Server IPv4/IPv6 Address. In BACnet IP Address, you can enter upto 39 characters.
- **BACnet Server Port**: This is the free port of SAMAS that will be used to communicate between the BACnet Server and the BMS Client. Valid Range: 1024-65535. Default: 47808.
- **Instance ID**: Specify the Instance ID which will be used by BACnet Server to communicate with the Client. Valid Range: 1-4194302. Default: 1.
- **Instance Name**: Specify the Instance Name which will be used by BACnet Server to communicate with the Client. In Instance Name, you can enter upto 100 characters. Default: Blank.
- **Network Number**: Specify the Network Number for the BACnet Server. Valid Range: 0-65534. Default: 0.
- **BACnet Server Entity**: Click **Select Entity** picklist. The **Select Entity** pop-up appears.



- By default, all the entities are selected. Select the desired Entity whose Events you wish to send to the BMS Client via BACnet Server from the list. The list of all configured entities for the selected Entity appears in a list on the right hand side. For example, if you select Recording Server, all the configured Recording Servers appear in a list under the **Recording Server** tab on the right hand side.



- Clear the check boxes for the entities whose events you do not wish to send. The name of this tab changes as per the Entity selected from the list.

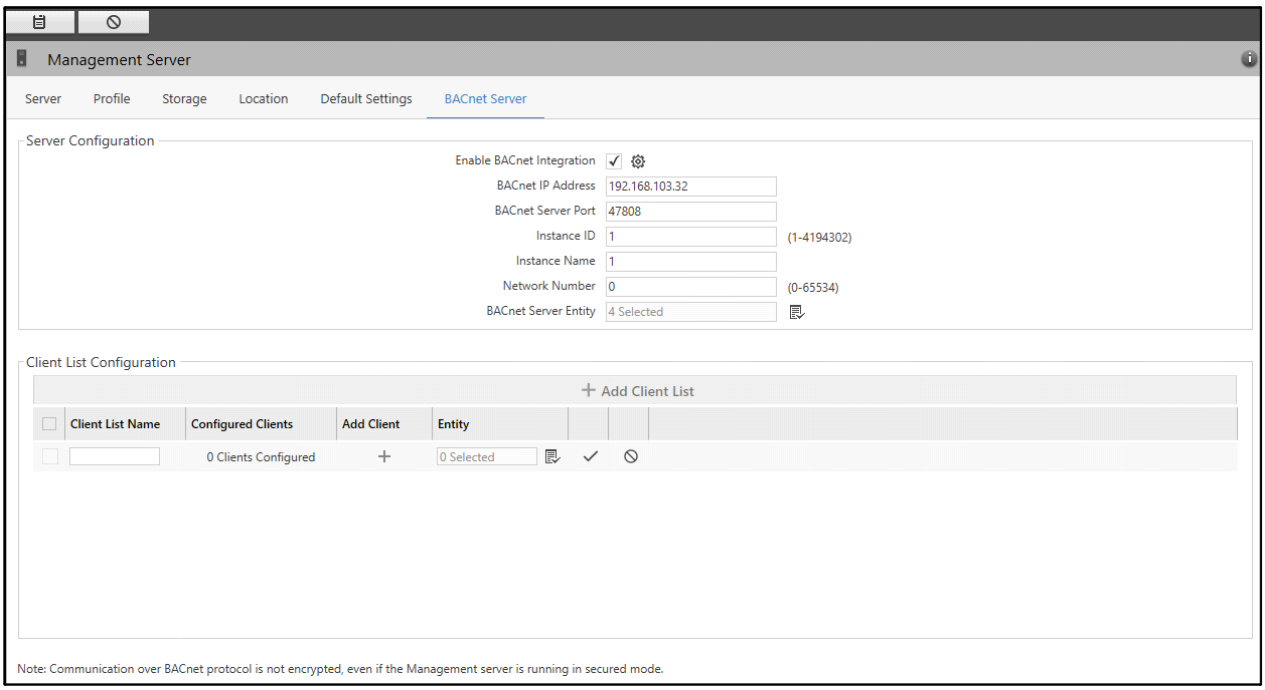


- Click **OK** to save the settings.

Client List Configuration

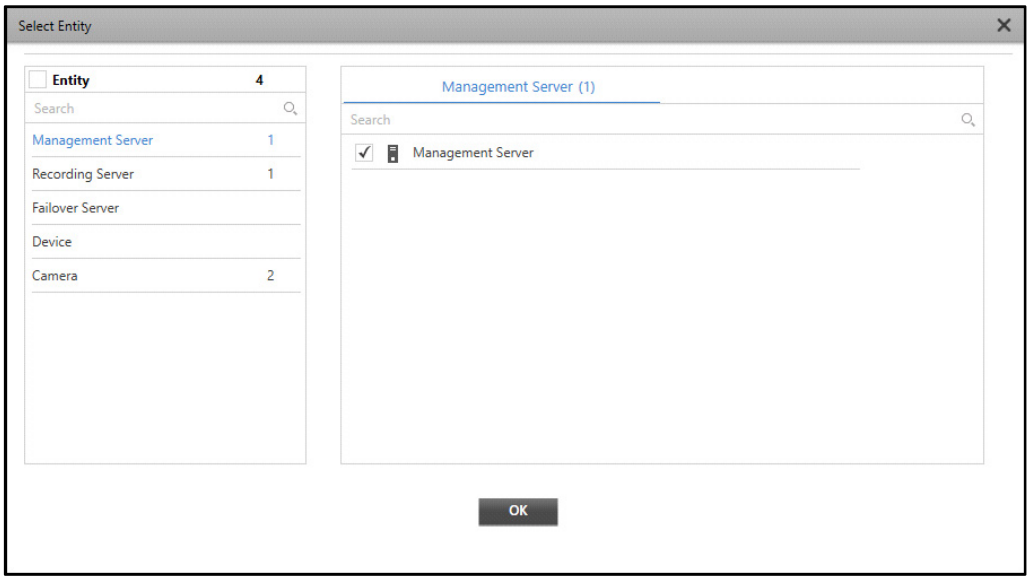
This section allows you to configure the BACnet Client List parameters.

- Click **Add Client List**. Maximum 10 Client Lists can be added.



Configure the following parameters:

- **Client List Name**: Specify a suitable name for the Client List. In Client List Name, you can enter upto 100 characters. Default: Blank.
- **Entity**: Click **Select Entity** picklist. The **Select Entity** pop-up appears.



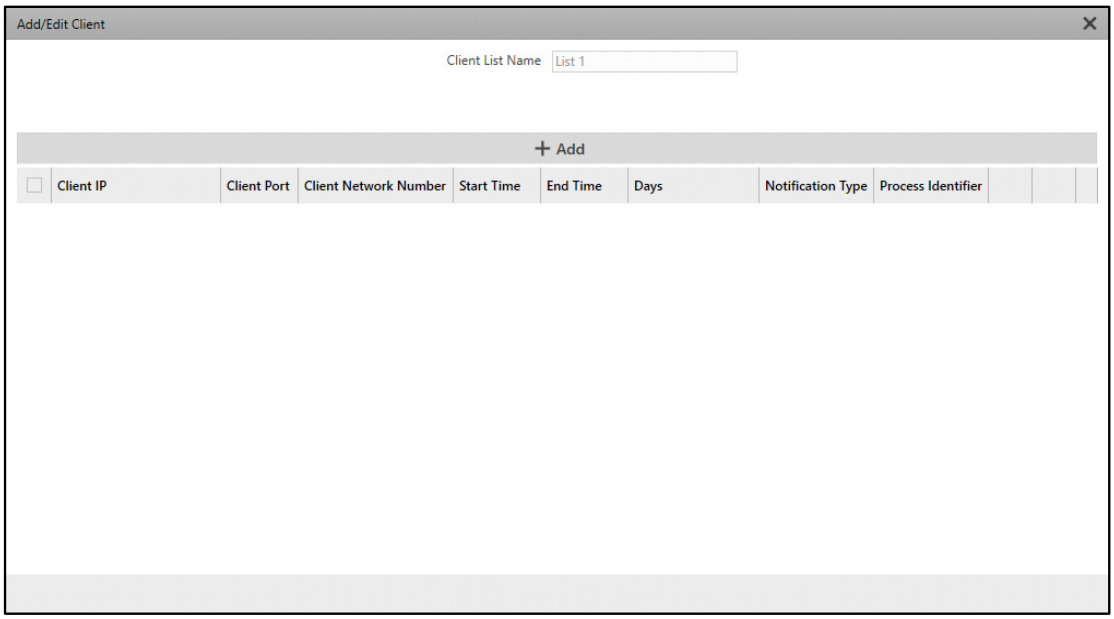
- All the entities selected in the BACnet Server Configuration appear here. If required, clear the check boxes for the entities whose events you do not wish to send.

Each Client List must have a unique list of Entities from the BACnet Server, that is, one Entity can be assigned to a single Client List.

- Click **OK** to save the settings.

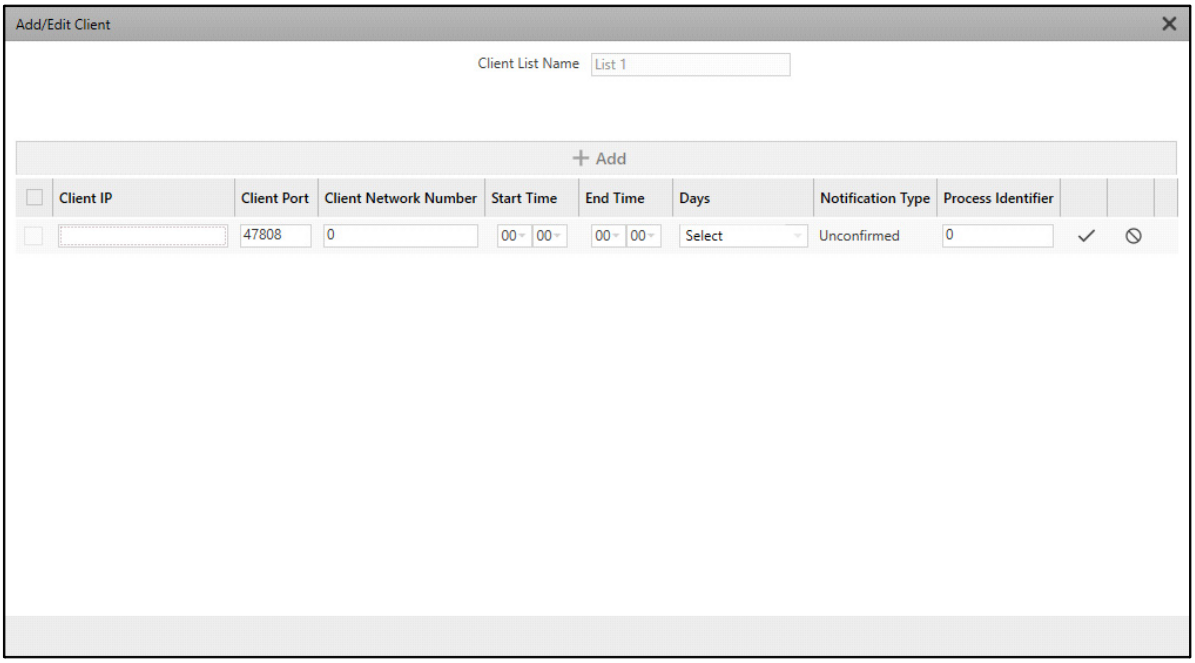
- Click **Save** to save the details. Once the entities are selected, you can add the Clients. Maximum 10 Clients can be added.

- Click **Add Client** . The **Add/Edit Client** pop-up appears.



  - The **Client List Name** displays the selected Client List.

    - Click **Add**.



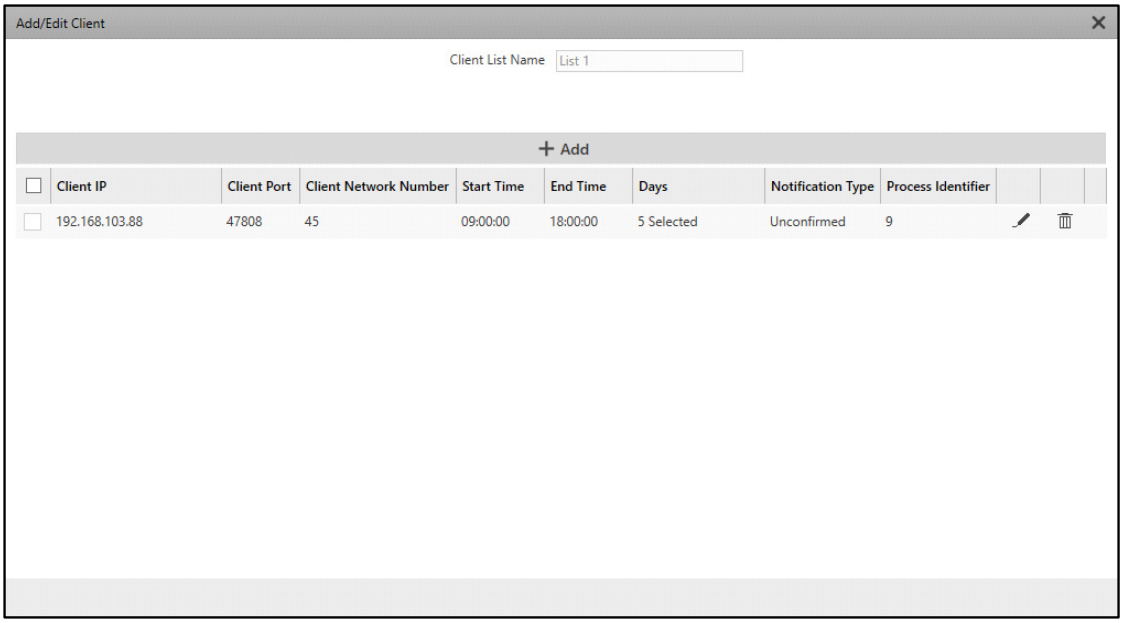
Configure the following parameters:

- **Client IP Address**: Specify the IPv4/IPv6 Address of the BACnet Client. In Client IP Address, you can enter upto 39 characters. Default: Blank.

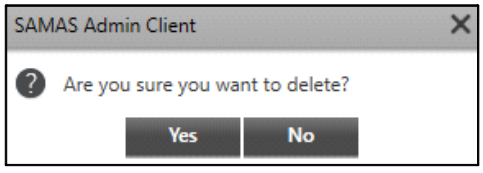
- **Client Port**: Specify the Port of the BACnet Client. Valid Range: 1-65535. Default: 47808.
- **Client Network Number**: Specify the Network Number which will be used by BACnet Server to communication with the Client. This will be provided by the Client. Valid Range: 0-65534. Default: 0.
- **Start Time**: Specify the Start Time for the schedule when data is to be sent to the BACnet Client.
- **End Time**: Specify the End Time for the schedule when data is to be sent to the BACnet Client.
- **Days**: Click to select the desired days or select **All** to select all the days, for the schedule when data is to be sent to the BACnet Client.
- **Notification Type**: Un-editable, this displays Unconfirmed Notification Type.
- **Process Identifier:** Specify the Process Identifier using which the BACnet Server will read the data. Valid Range: 0-65535. Default: Blank.

- Click **Save** to save the details.

The new Client appears in the list. You can change the configurations of the Client or delete it.



- Click **Edit** to edit the desired Client from the list.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Client. The following pop-up appears.

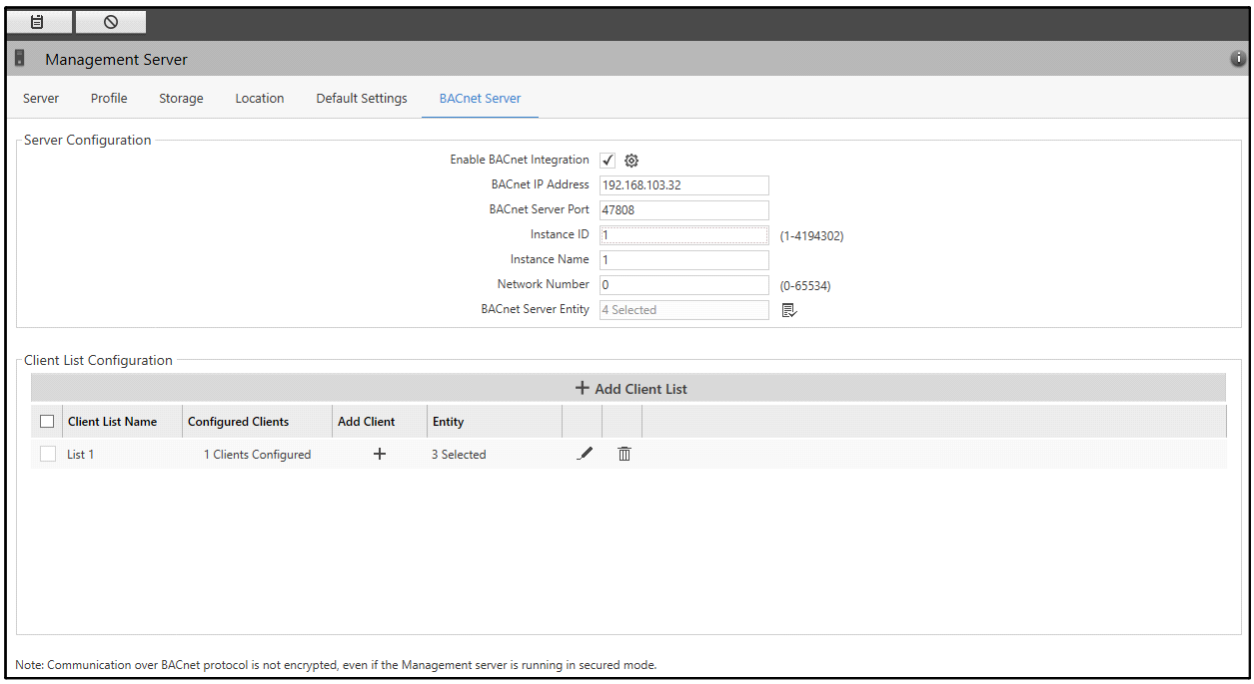


- Click **Yes** to confirm or click **No** to discard.

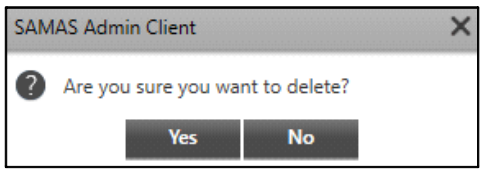
Similarly, you can add other clients.

- Close the **Add/Edit Client** pop-up. Now you can add other Client Lists if you wish to.

Once all the client lists are added, you can change the configurations of the desired Client List or delete it.



- Click **Edit** to edit the desired Client List from the list.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the desired Client List. The following pop-up appears.



- Click **Yes** to confirm or click **No** to discard.

If you wish to delete all the Client Lists, select the check box in the Header Row. Click **Delete** to delete all the Client Lists.

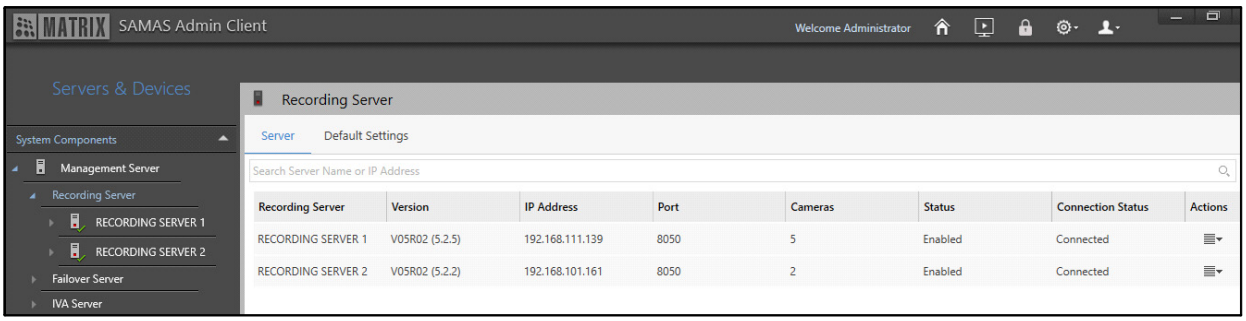
- Click **Save** to save the configurations or **Cancel** to discard.

Recording Server

The Recording Server communicates with video surveillance devices, records video streams into its Storage Drives and streams live and recorded videos to the clients — Admin Client, Smart Client, Mobile Client and Media Client. The Recording Server page displays all the activated Recording Servers. You can view and configure the Servers and Default Settings.

To configure the activated servers,

- Click **Servers & Devices > System Components > Recording Server**.



The Recording Server page contains the following tabs:

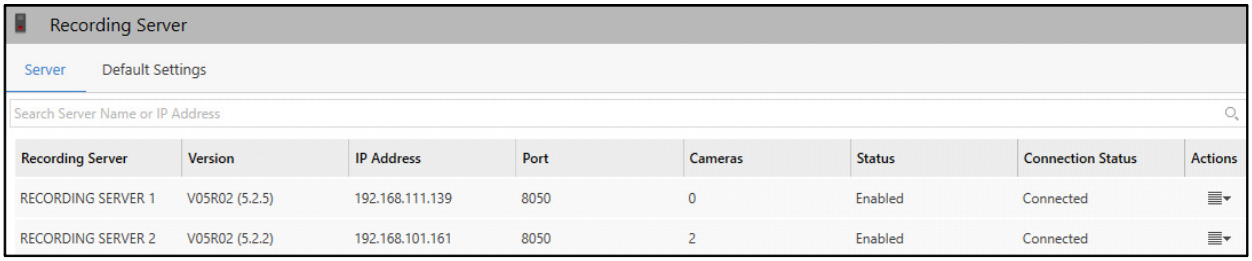
- "Server"
- "Default Settings"

Server

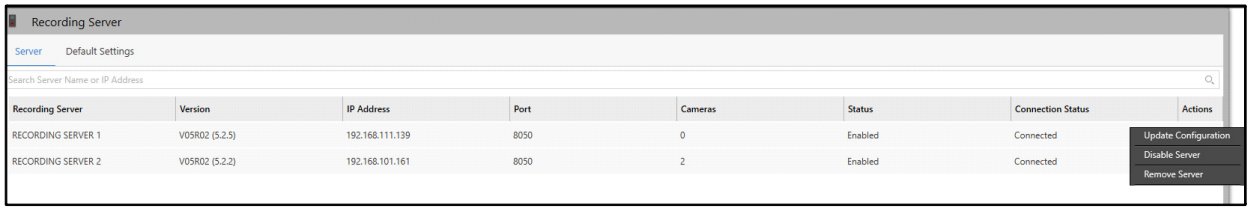
This tab enables you to edit the configurations of the activated Recording Servers.

To configure the servers,

- Click the **Server** tab. The servers assigned as Recording Server are listed in this tab.



- To make changes in the activated server's configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.



- **Update Configuration**: Selecting Update Configuration updates the configuration details of the Recording Server.
- **Disable Server**: Selecting Disable Server disables the Recording Server. For enabling it again, click **Action** and select **Enable** Option.
- **Remove Server**: Selecting Remove Server removes the Recording Server.

You can search for a particular Recording Server by specifying the Name or IPv4/IPv6 Address of the server in the **Search** bar.

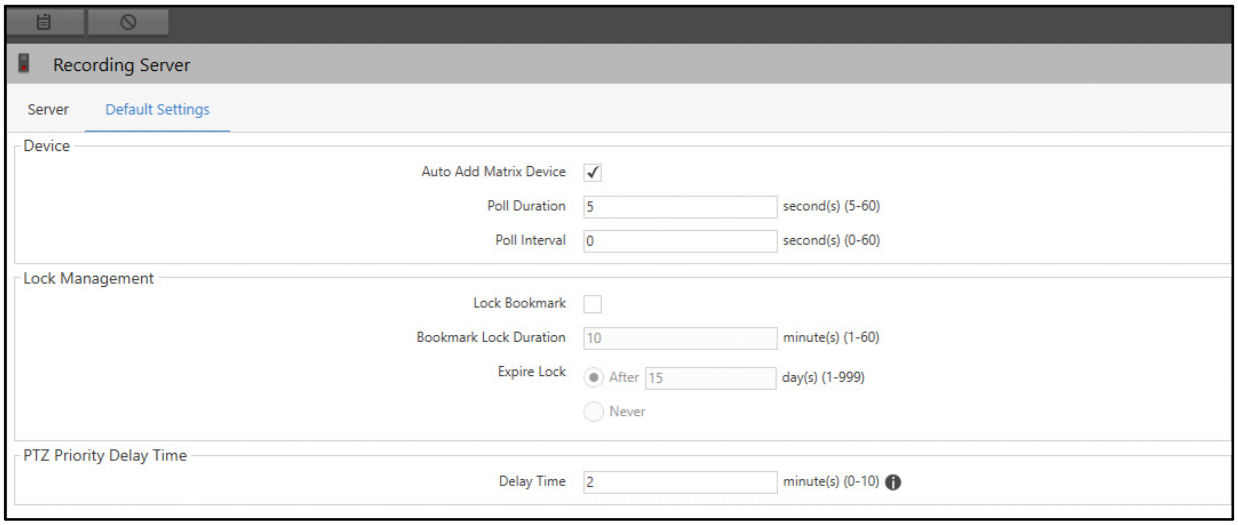
You can also click on individual Recording Server to view and configure their profiles. To know more about configuring individual Recording Server, refer to “Recording Server Configuration”.

Default Settings

This tab enables you to configure the default settings for Device and Lock Management. These settings are applicable by default for any new device (camera, HVR, DVR, NVR) added to the system.

To configure Default Settings,

- Click the **Default Settings** tab.



It is recommended to define these settings during the initial configuration.

Configure the following parameters:

Device

- **Auto Add Matrix Device**: Enable the check box to automatically add any Matrix Device detected in the network. If this option is disabled, all device requests will appear in the pending state for activation in the **New Matrix Devices** pop-up in the individual Recording Server. To view the pending requests, select the desired Recording Server, click **Add Devices** and then click **Auto Add Matrix Devices.** The requests appear in the New Matrix Devices pop-up**.**

- **Poll Duration**: Specify the time in seconds for which you want the Recording Server to wait for response from the device for communication. Valid Range: 5-60 seconds. Default: 5.

- **Poll Interval**: Specify the time interval in seconds after which the Recording Server should send the next poll. Valid Range: 0-60 seconds. Default: 0.

Lock Management

There are certain Bookmarks which are important to store even after its normal retention time. Such Bookmarks might help in investigation or can be referred to later. Thus, you can store such Bookmarks by locking them.

*The Bookmark Lock parameter can also be enabled from **General Settings > User Groups > Media Rights**. If the parameter is enabled from Media Rights, it gets disabled from Default Settings and vice versa.*

- **Lock Bookmark:** Select the check box to enable Lock Bookmark. This will lock all the Bookmarks by default as per the settings. Only Admin users can unlock the bookmark locks here.

  If Lock Bookmark is enabled from General Settings > User Groups > Media Rights, the lock duration is user-editable.

  If Lock Bookmark is enabled from Servers & Devices > Recording Server > Default Settings, the lock duration is not user-editable.

- **Bookmark Lock Duration**: Specify the duration in minutes till which the bookmark in Smart Client should be locked. Valid Range: 1-60 minutes. Default: 10.

- **Expire Lock**: Select **After** and specify number of days after which the lock will expire. Valid Range: 1-999 days. Default: 15. Select **Never** if you do not want the lock to expire.

PTZ Priority Delay Time

- **Delay Time**: Specify the time for which a lower priority user's PTZ operation should be discarded after a high priority user's PTZ operation request is received by the system. However, a high priority user's PTZ operation request will be served regardless of the delay timer value. If the time is configured as 0, the PTZ functionality will work for all users irrespective of the priority. Valid Range: 0-10 minutes. Default: 2.
- Click **Save** to save the configurations or **Cancel** to discard.

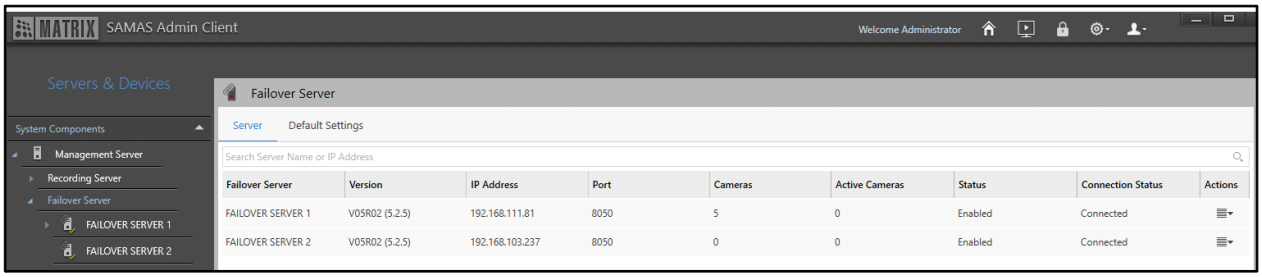
*If **PTZ Priority Delay Time** is configured, you can add a PTZ Tour but it cannot be accessed by any Smart Client user until the delay time expires or a higher priority user makes a change in the PTZ operations.*

Failover Server

Failover Server works as the replacement of the Recording Server and takes the role of Recording Server when it fails. Whenever the connection between Recording Server and device breaks, that device is assigned to the Failover Server. Failover Server does the recording and provides live view till the connection with the Recording Server resumes. The Failover Server page displays all the activated Failover Servers. You can view and configure the Servers and Default Settings.

To configure the activated servers,

- Click **Servers & Devices > System Components > Failover Server**.



The Failover Server page contains the following tabs:

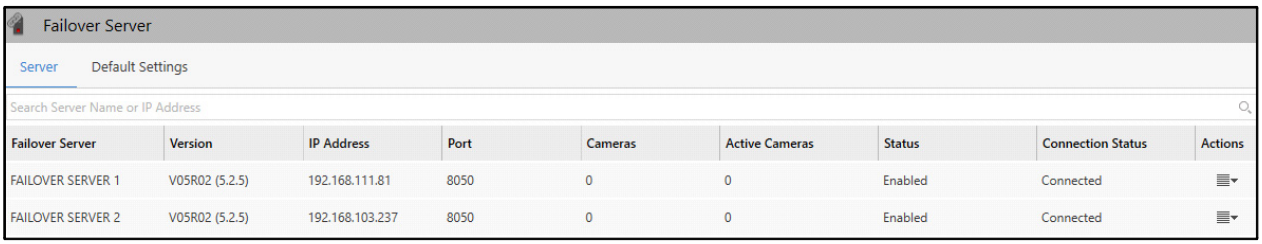
- "Server"
- "Default Settings"

Server

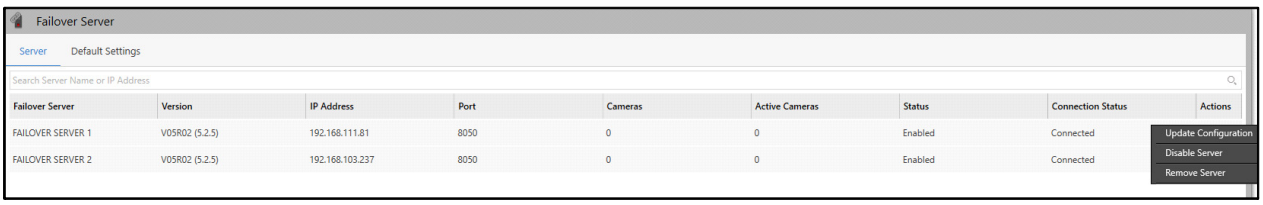
This tab enables you to edit the configurations of the activated Failover Servers.

To configure the servers,

- Click the **Server** tab. The servers assigned as Failover Servers are listed in this tab.



- To make changes in the activated server's configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.



- **Update Configuration**: Selecting Update Configuration updates the configuration details of the Failover Server.
- **Disable Server**: Selecting Disable Server disables the Failover Server. For enabling it again, click **Action** and select **Enable** Option.
- **Remove Server**: Selecting Remove Server removes the Failover Server.

You can search for a particular Failover Server by specifying the Name or IPv4/IPv6 Address of server in the **Search** bar.

The **Active Cameras** count shown in the Active Cameras column conveys the number of cameras that are currently disconnected from their respective RS and thus this particular FoS has become **Active** for those particular number of cameras.

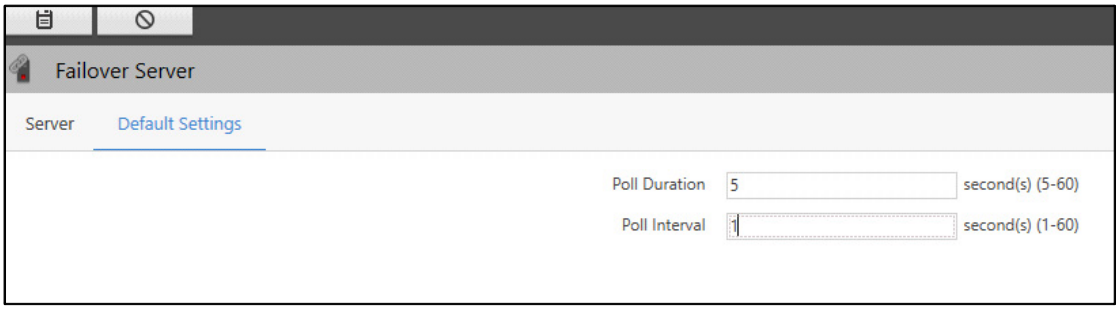
You can also click on individual Failover Server to view and configure their profiles. To know more about configuring individual Failover Server, refer to “Failover Server Configuration”.

Default Settings

This tab enables you to configure the default settings for the Failover Servers.

To configure the Default Settings,

- Click the **Default Settings** tab.



Configure the following parameters:

- **Poll Duration**: Specify the duration in seconds for which you want the Failover Server to wait for the response of poll from the Management Server. Valid Range: 5-60 seconds. Default: 5.
- **Poll Interval**: Specify the interval in seconds after which the next poll should be sent. Valid Range: 1-60 seconds. Default: 1.

- Click **Save** to save the Default Settings or **Cancel** to discard.

IVA Server

Generally, events such as Motion Detection, Camera Tampering etc. are triggered by a camera and passed on to SATATYA SAMAS. The IVA Server provides an effective alternative method for real-time event detection and analysis when the configured camera does not support these features. The IVA Server uses video content analysis to detect events such as motion and tripwire, based on live stream of a camera, irrespective of camera specifications and configuration.

*The features for Detection through IVA or Detection through Investigator will be supported as per the License purchased. For detailed license information, refer to the **SATATYA SAMAS Installation Guide**.*

The IVA Server page displays all the activated IVA Servers. You can view and configure the Servers from this page.

To configure the activated servers,

- Click **Servers & Devices > System Components > IVA Server**.



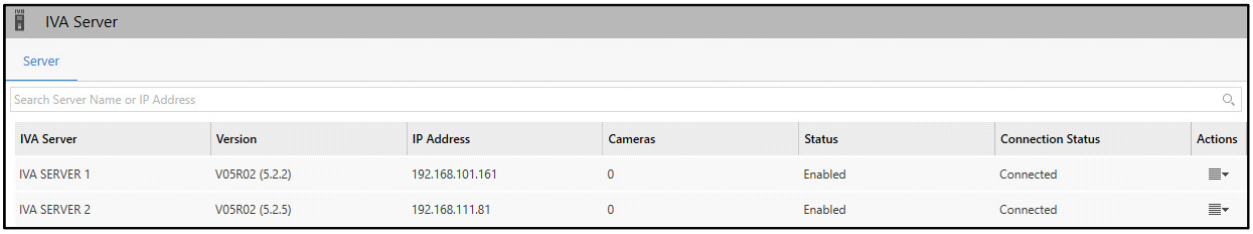
The IVA Server page contains only one tab — Server.

Server

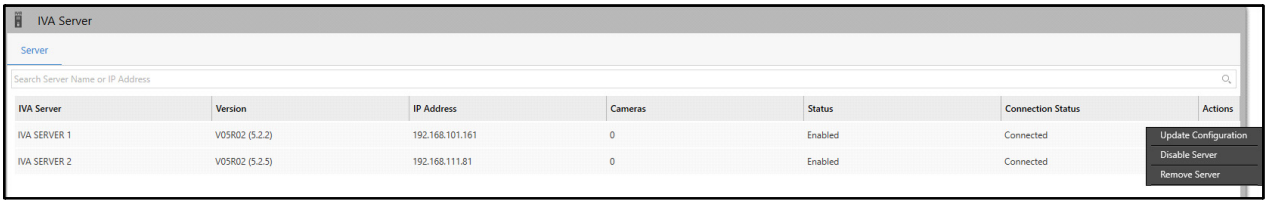
All the servers awaiting activation as IVA Servers appear in this tab along with the **IVA Server** collapsible panel on the **Management Server** page. This tab also enables you to edit the configurations of activated IVA Servers. To activate the requesting servers, refer to “Activating Server as IVA Server”.

To configure the servers,

- Click the **Server** tab. The servers assigned as IVA Servers are listed in this tab.



- To make changes in the activated server’s configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.



- **Update Configuration**: Selecting Update Configuration updates the configuration details of the IVA Server.
- **Disable Server**: Selecting Disable Server disables the IVA Server. For enabling it again, click **Action** and select **Enable** Option.
- **Remove Server**: Selecting Remove Server removes the IVA Server.

You can search for a particular IVA Server by specifying the Name or IPv4/IPv6 Address of server in the **Search** bar.

You can also click on individual IVA Server to view and configure their profiles. To know more about configuring individual IVA Server, refer to “IVA Server Configuration”.

Transcoding Server

In the current scenario we face network issues due to less bandwidth. As a result, setting up SATATYA SAMAS becomes difficult if the Recording Servers and the Failover Servers are located at different locations. In such cases during congestion, the frames might get discarded and there may be buffering issues in Live View and Playback. These issues are solved using Transcoding Server. The Transcoding Server optimizes the bandwidth for the stream usage. When there is congestion, the frames are sent to the Transcoding Server. Hence, there is uninterrupted Live View/Playback.

The Transcoding Server page displays all the activated Transcoding Servers. You can view and configure the Servers from this page.

To configure the activated servers,

- Click **Servers & Devices > System Components > Transcoding Server**.



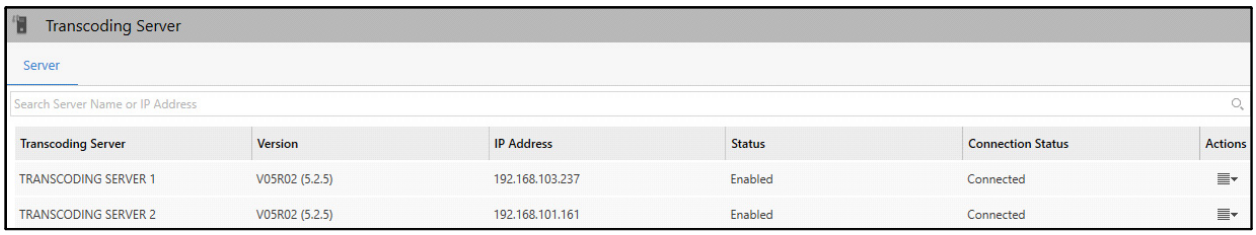
The Transcoding Server page contains only one tab — Server.

Server

All the servers awaiting activation as Transcoding Server appear in this tab along with the **Transcoding Server** collapsible panel on the **Management Server** page. This tab also enables you to edit the configurations of activated Transcoding Servers. To activate the requesting servers and configure them, refer to “Activating Server as Transcoding Server”.

To configure the servers,

- Click the **Server** tab. The servers assigned as Transcoding Servers are listed in this tab.



- To make changes in the activated server’s configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.



- **Update Configuration**: Selecting Update Configuration updates the configuration details of the Transcoding Server.
- **Disable Server**: Selecting Disable Server disables the Transcoding Server. For enabling it again, click **Action** and select **Enable** Option.
- **Remove Server**: Selecting Remove Server removes the Transcoding Server.

You can search for a particular Transcoding Server by specifying the Name or IPv4/IPv6 Address of server in the **Search** bar.

You can also click on individual Transcoding Server to view and configure their profiles. To know more about configuring individual Transcoding Server, refer to “Transcoding Server Configuration”.

ONVIF Server

The ONVIF Server acts as a bridge between SATATYA SAMAS and 3rd Party ONVIF Clients as well as RTSP Clients. This enables easy exchange of video data as well as availability of Live/Playback streams.

The ONVIF Server plays a dual role:

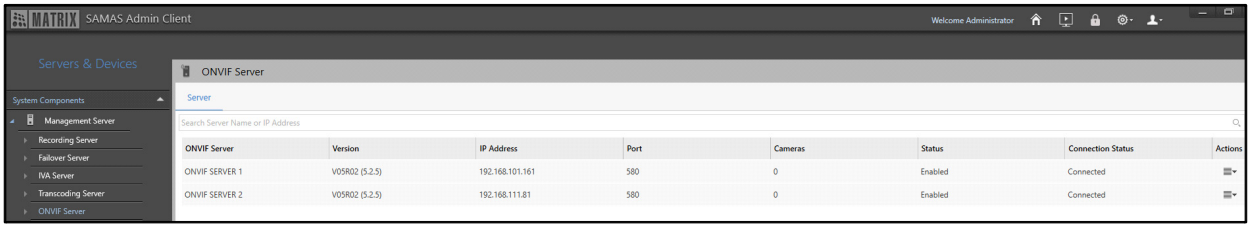
- acts as a Client for the Management Server, Recording /Failover Server.
- acts as a Server for the 3rd Party ONVIF Clients as well as RTSP Clients.

The ONVIF Server has an inbuilt RTSP Server for direct streaming to clients.You must configure the RTSP and RTP Port in the ONVIF Server Manager for the same. For details, refer to the **SATATYA SAMAS Installation Guide**.

The ONVIF Server page displays all the activated ONVIF Servers. You can view and configure the Servers from this page.

To configure the activated servers,

- Click **Servers & Devices > System Components > ONVIF Server**.



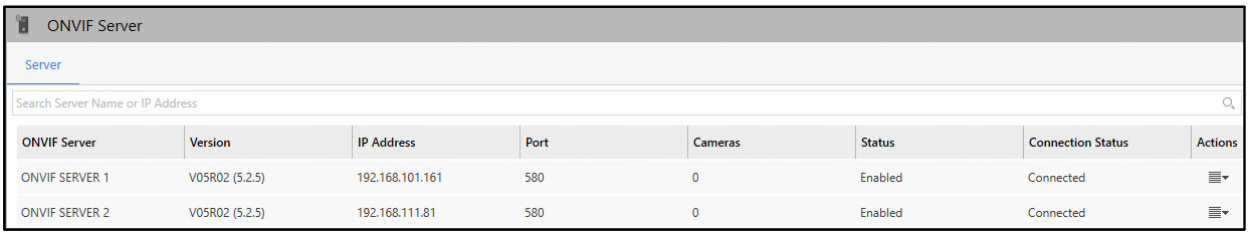
The ONVIF Server page contains only one tab — Server.

Server

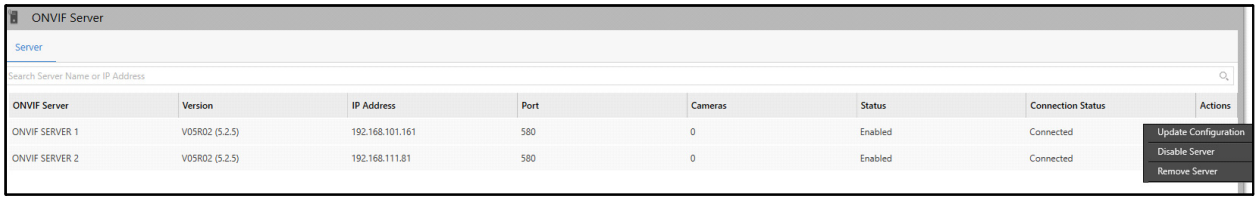
All the servers awaiting activation as ONVIF Servers appear in this tab along with the **ONVIF Server** collapsible panel on the **Management Server** page.This tab also enables you to edit the configurations of activated ONVIF Servers. To activate the requesting servers and configure them, refer to “Activating Server as ONVIF Server”.

To configure the servers,

- Click the **Server** tab. The servers assigned as ONVIF Servers are listed in this tab.



- To make changes in the activated server’s configuration, click **Actions** . You can select the desired option — Update Configuration, Disable Server or Remove Server.



- **Update Configuration**: Selecting Update Configuration updates the configuration details of the ONVIF Server.
- **Disable Server**: Selecting Disable Server disables the ONVIF Server. For enabling it again, click **Action** and select **Enable** Option.
- **Remove Server**: Selecting Remove Server removes the ONVIF Server.

You can search for a particular ONVIF Server by specifying the Name or IPv4/IPv6 Address of server in the **Search** bar.

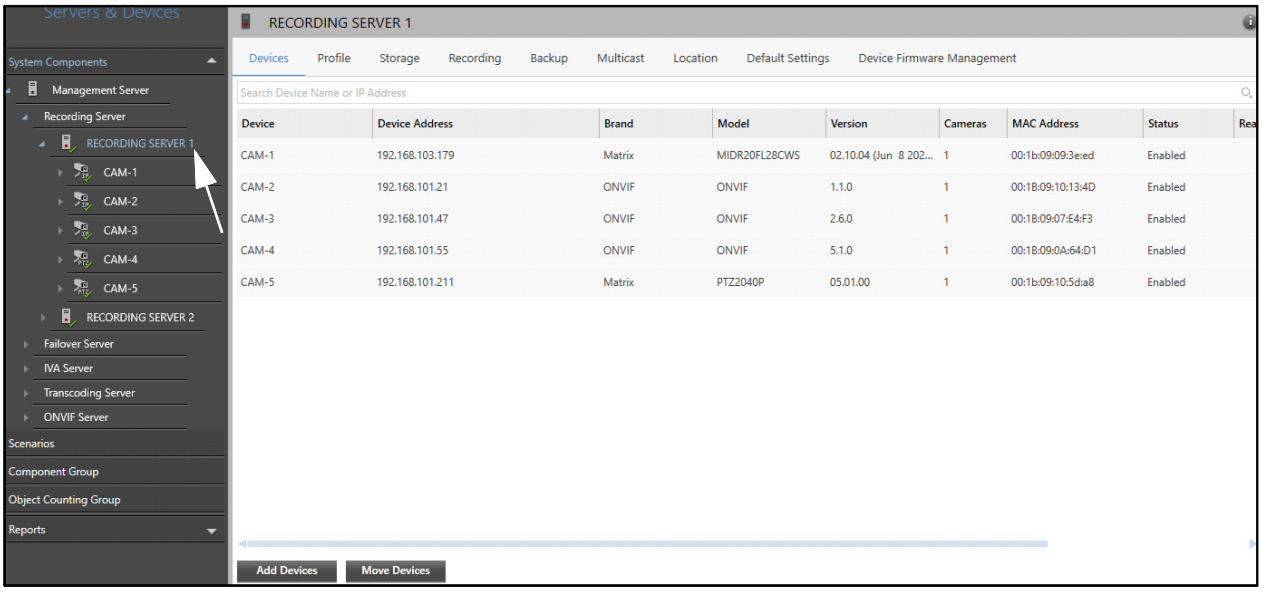
You can also click on individual ONVIF Server to view and configure their profiles. To know more about configuring individual ONVIF Server, refer to “ONVIF Server Configuration”.

Recording Server Configuration

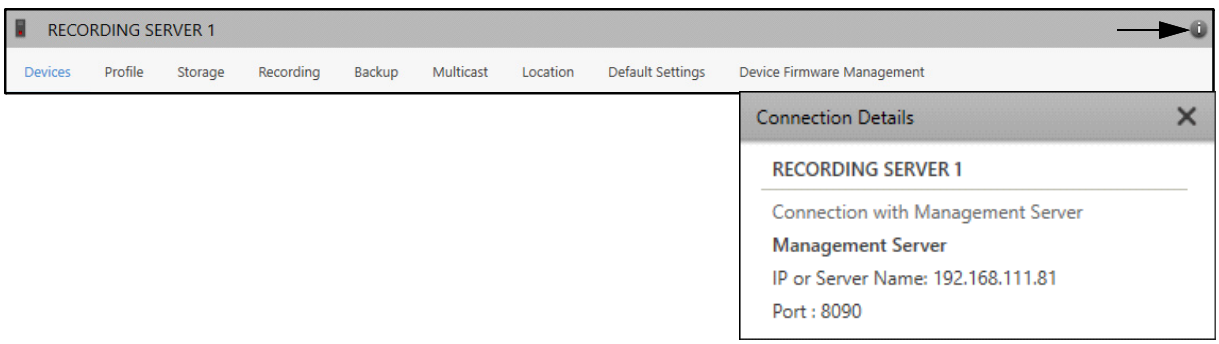
To configure a Recording Server, it must be activated first. You need to set the Server set as a Recording Server from the **Server** collapsible panel on the **Management Server** page. To activate a Recording Server, refer to “Assigning Server as Recording Server or Failover Server”.

To configure a Recording Server,

- Click **Servers & Devices > System Components > Recording Server**.
- All the Recording Servers of the system appear. The entries can be sorted. To do so, click on the desired parameter in the header row. An arrow ▲ icon appears. Click on it. Entries can be sorted in ascending or descending order.
- Select the desired Recording Server.



- To view the **Connection Details** of the Recording Server, click **Connection Details** at the top right corner of the Recording Server page. It displays the Management Server Name, IP (IPv4/IPv6) or Server Name and Port, with which Recording Server is currently connected.



Each Recording Server consists of the following tabs:

- “Devices”
- “Profile”
- “Storage”
- “Recording”
- “Backup”
- “Multicast”
- “Location”
- “Default Settings”
- “Device Firmware Management”

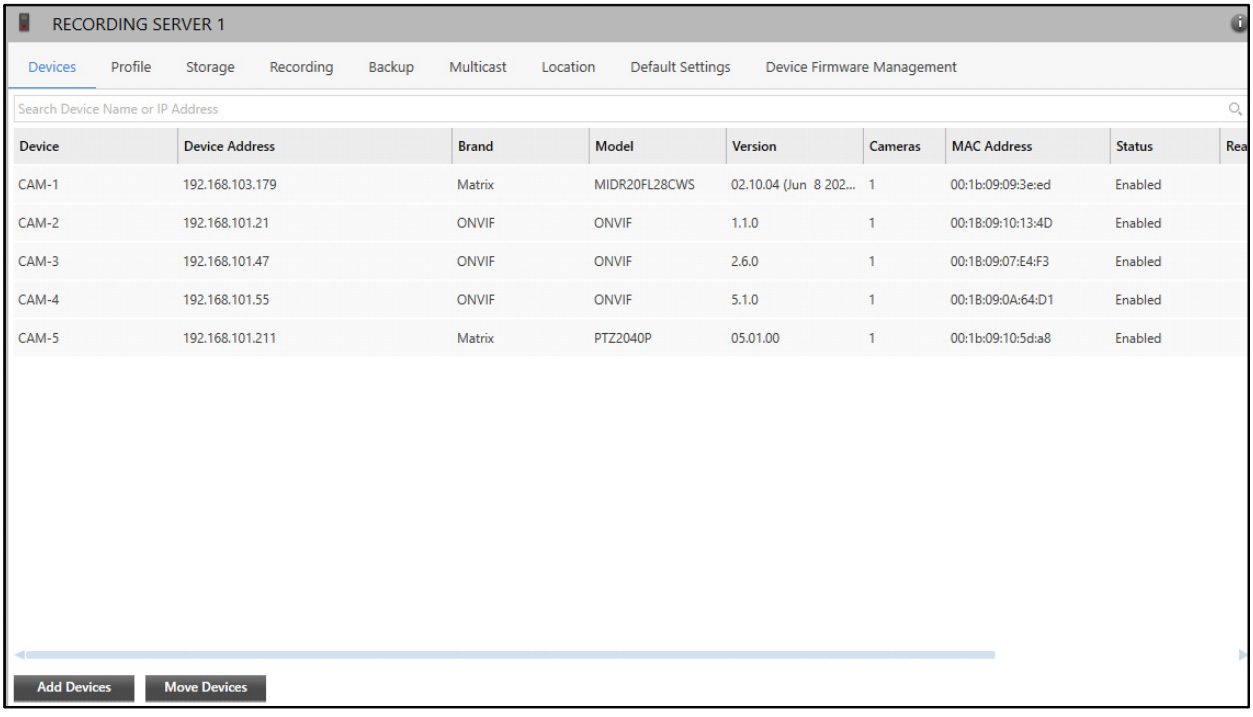
Devices

On SATATYA SAMAS, a device acts as a child entity to a Recording Server and as a parent entity for its peripherals, including its camera unit, sensors, alarm pins, audio input and output pins.

This tab enables you to view and configure the Devices added to the Recording Server. You can view, configure, add or move devices from this page.

To configure Devices,

- Select the desired Recording Server. The **Devices** tab appears by default.

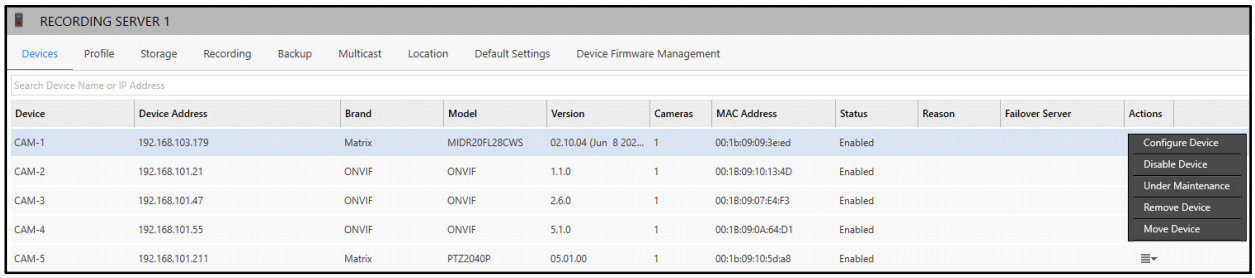


The devices added to the Recording Server when activating the server appear in this tab. You can also search for a device using the **Search Device Name or IP Address**(IPv4/IPv6) search bar.

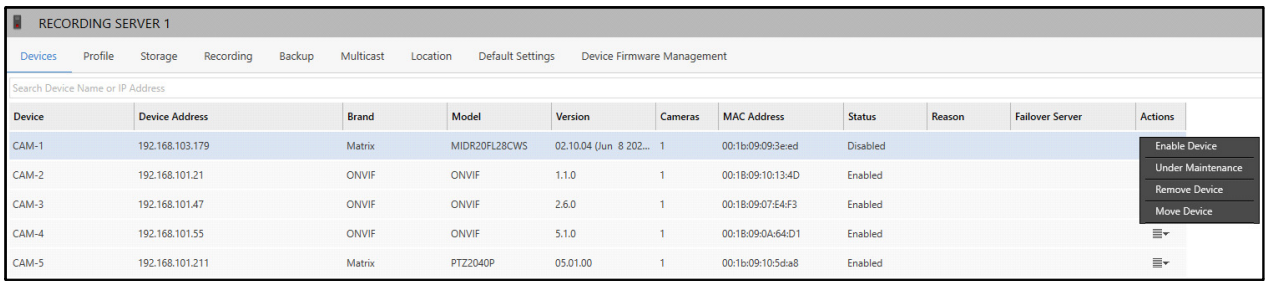
The following device details are displayed — Device, Device Address (IPv4/IPv6), Brand, Model, Version, Cameras, MAC Address, Status, Reason, Failover Server and Actions. To know more about the individual device details, refer to “Device Configuration”.

Click **Actions** . You can access the following options — Configure Device, Move Device, Disable Device, Under Maintenance and Remove Device.

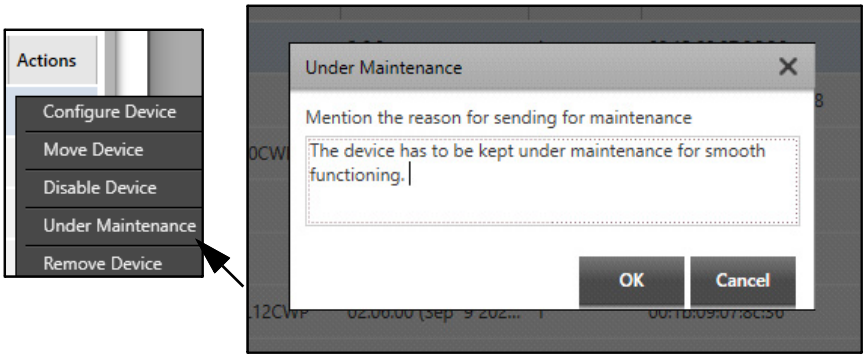
The following options are not applicable to Mobile Cameras — Configure Device, Move Device, Disable Device, Under Maintenance and Remove Device.



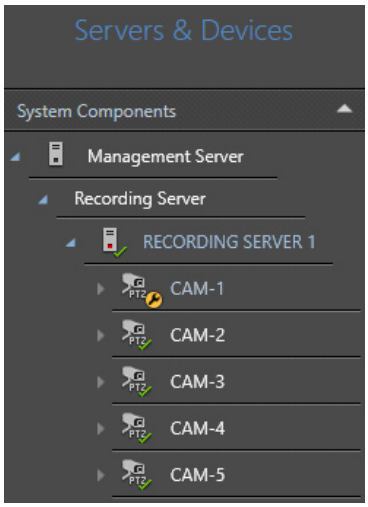
- **Configure Device**: Selecting Configure Device redirects you to the respective device configuration page, where you can view/edit the device configurations.
- **Move Device**: Selecting Move Device option allows you to move the device to the selected Recording Server. For more details, refer to “Move Device”.
- **Disable Device**: Selecting Disable Device option will disable the device. This will remove the device from the list of Recording Servers displayed on the left hand side. For enabling it again, click **Action** icon and select **Enable** Option.



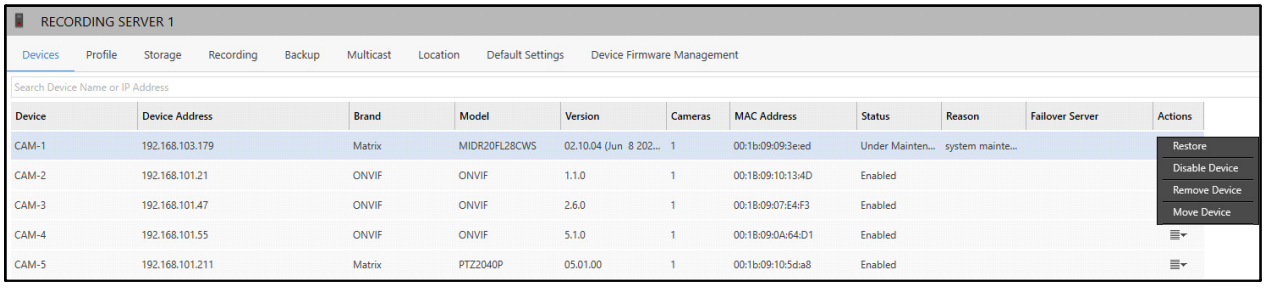
- **Under Maintenance**: Selecting Under Maintenance option allows you to indicate that the device has been kept under maintenance due to some failure, or to use the device more efficiently.
  - Click **Under Maintenance**. The **Under Maintenance** pop-up appears. Specify the reason for keeping the device under maintenance. Click **OK** to confirm or click **Cancel** to discard.



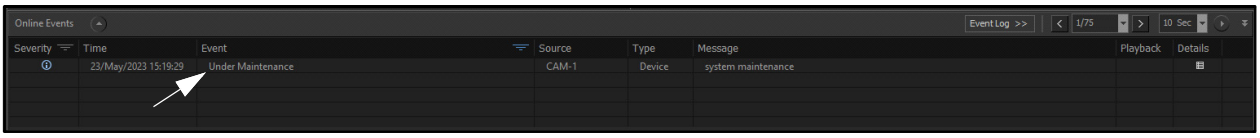
- The  icon appears, indicating that the device is under maintenance.



- Click **Action**  again to **Restore** the device from under maintenance condition.



When any device is kept under maintenance, an Event is generated in the Smart Client, indicating that the particular device has been kept under maintenance. An Event after restoring the device is also generated.



- **Remove Device**: Selecting Remove Device will remove the device from the Recording Server.

You can add devices to the Recording Server at the time of activation (refer to "Auto Adding Devices/Cameras while activating the Recording Server") or later-on. The following types of devices can be added:

- DVR
- NVR
- HVR
- IP Camera
- Mobile Camera; when **Allow Push Video** is enabled for the user. For details, refer to "Users".

For more details on supported devices, refer to "Supported Devices".

There are two ways to add IP Cameras to a Recording Server:

- Camera as a device.
- Camera connected through a Device (DVR/NVR/HVR).

Devices can be added through one of these options — "Add Manually", "Add Using Auto Discovery Tool" or "Auto Add Matrix Devices".

Mobile Camera can only be added from "Users" page.

The term **Devices** consists of both the Video Recorders and Cameras (IP Camera as well as Mobile Camera). Unless mentioned separately, the cameras are included under the term **Devices**.



A maximum of 400 cameras can be added to one Recording Server. For details, refer to "Known Points related to addition of 400 Camera".

If you upgrade to Software Version V6R3 and onwards,

- *only Matrix cameras can be added to Recording Server by selecting the Brand and Model in the respective picklist.*
- *Other brand cameras can be added by selecting ONVIF or Generic as the Brand in the Brand picklist.*
- *Other brand cameras already added by selecting Brand and Model prior the upgrade will continue to function without any change after upgrade.*

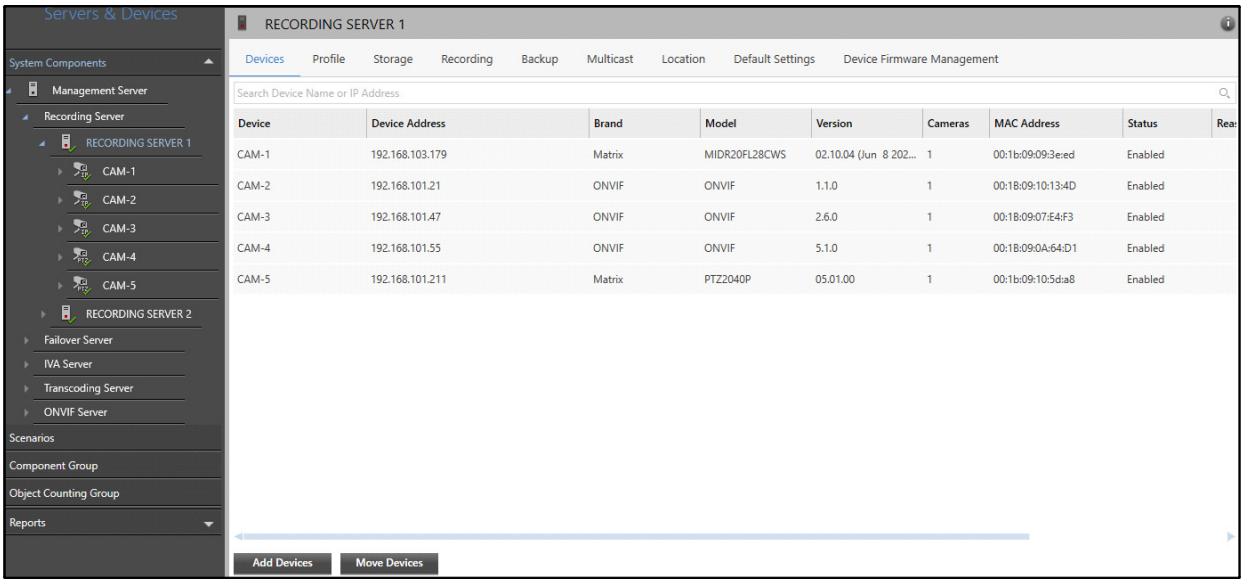
We recommend adding a camera by only one method — Brand and Model, ONVIF, Camera Initiation— in the same Recording Server, else it may hamper the functionality.

For the license details of Cameras, contact Matrix Technical Support.

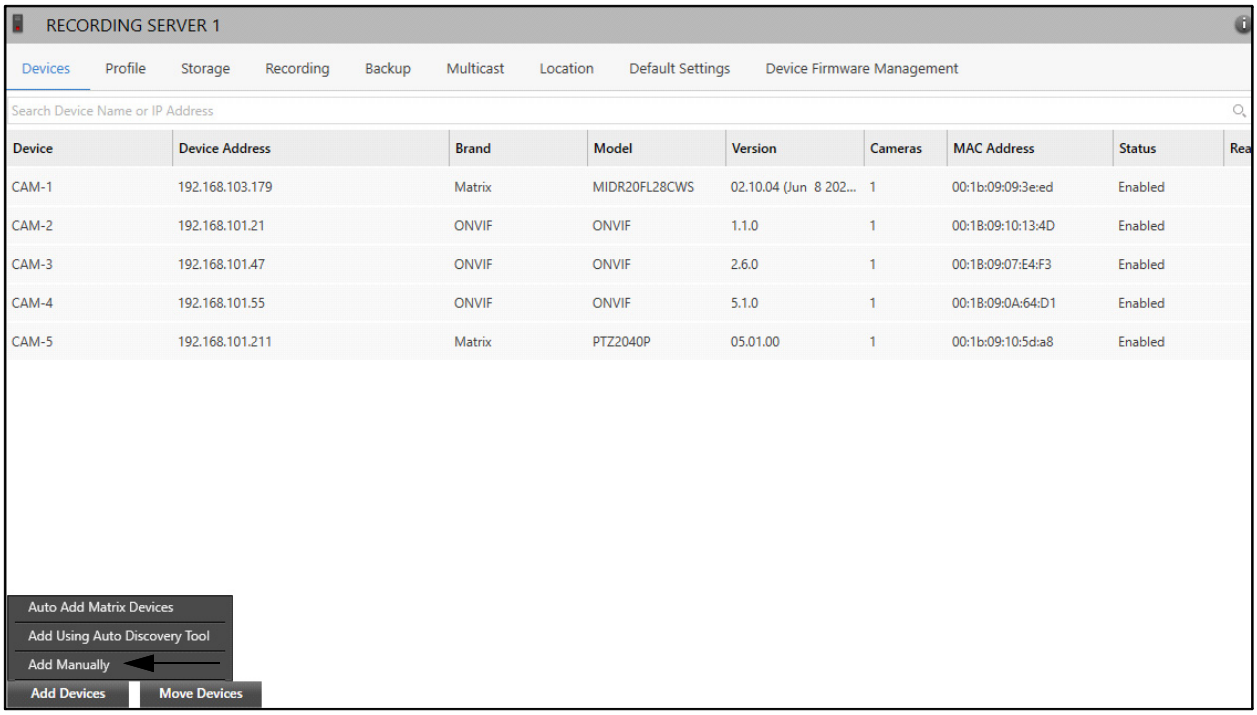
Add Manually

To add a device manually,

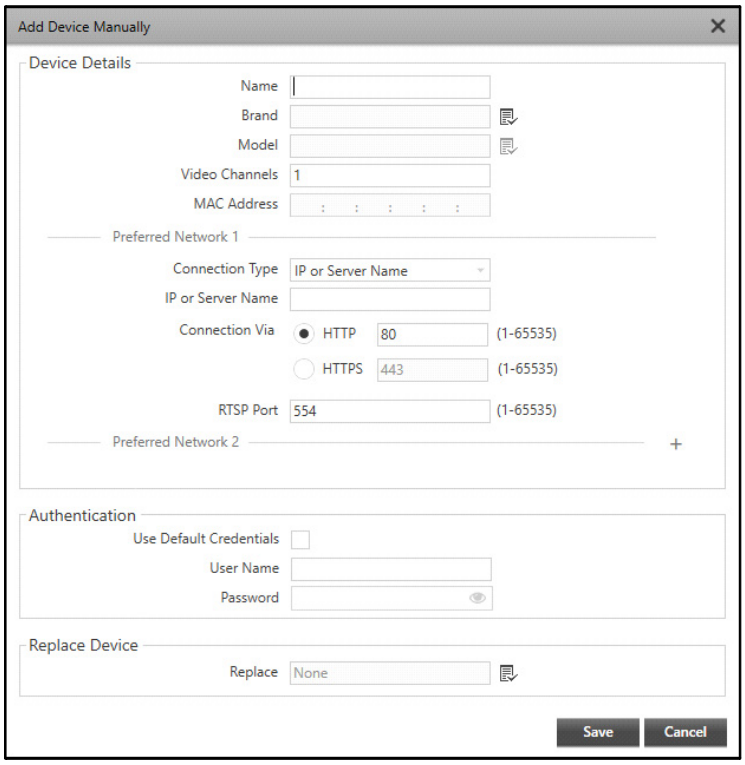
- Select the desired Recording Server. The **Devices** tab appears by default.



- Click **Add Devices**. Select **Add Manually** from the options.



- The **Add Device Manually** pop-up appears.



Configure the following parameters:

Device Details

- **Name**: Specify a suitable name for the device. In Name, you can enter upto 50 characters. Default: Blank.
- **Brand**: Select the brand of the device to be added using the **Brand** picklist.Double-click to select the desired option.
- **Model**: Select the model of the device to be added using the **Model** picklist.Double-click to select the desired option.
- **Protocol**: If you have selected **Brand** and **Model** as **ONVIF**, select the desired protocol from the drop-down list — RTSP Over TCP, RTSP Over UDP or RTSP Over HTTP/HTTPS.
- **Video Channels**: Specify the number of channels supported in the device. Valid Range: 1-99. Default: Blank.
- **Active Cameras**: If you have selected **Model** as **HVR, DVR** or **NVR,** you can select the cameras that you wish to keep active using the **Select Cameras** picklist. Select the check boxes of the desired cameras and click **OK**.
- **URL**: If you have selected **Brand** as **Generic**, specify the URL of the camera. In URL, you can enter upto 150 characters. Default: Blank.
- **MAC Address**: The MAC Address of the device is fetched automatically once the device is added successfully and is displayed in the "Devices" tab.

Preferred Network 1

- **Connection Type**: Select the connection type from the drop-down list — IP or Server Name, Matrix DNS-Host Name or Matrix DNS-MAC Address.

- **IP or Server Name**: Specify the IPv4/IPv6 Address or Server Name of the network. In IP or Server Name, you can enter upto 255 characters. Default: Blank.

If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

*If you select NVR under **Model**, you can configure IPv4/IPv6 address. However, if you select HVR/DVR under **Model**, then you can configure only IPv4 addresses.*

- **Matrix DNS- Host Name**: If you have selected the Connection Type as Matrix DNS-Host Name, specify the Host Name. In Matrix DNS-Host Name, you can enter upto 256 characters. Default: Blank.

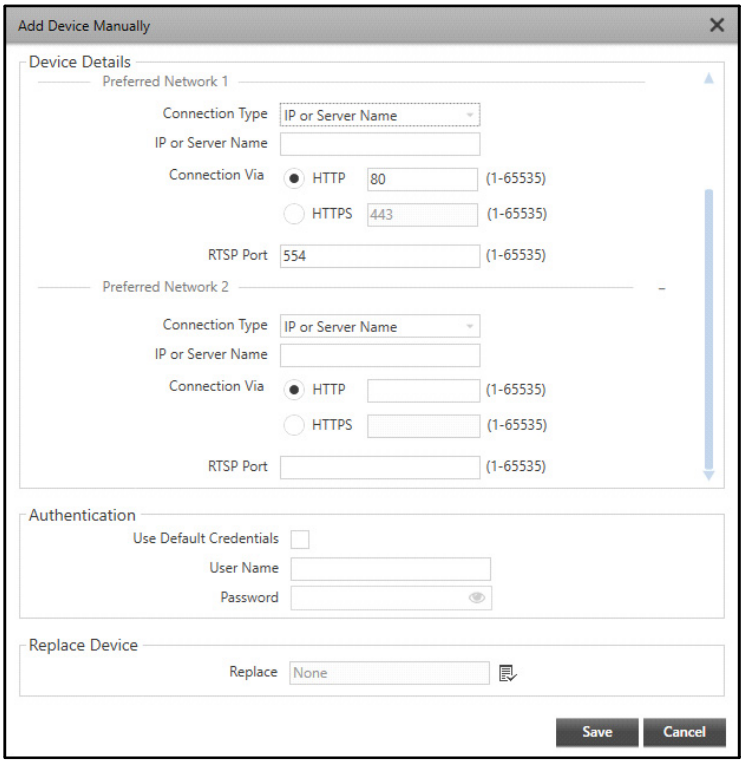
- **Matrix DNS- MAC Address**: If you have selected the Connection Type as Matrix DNS-MAC Address, specify the MAC Address. In Matrix DNS-MAC Address, you can enter upto 17 characters. Default: Blank.

- **Connection Via**: Select the Connection type from the options — HTTP or HTTPS. Specify the HTTP/ HTTPS Port. Valid Range: 1-65535. Default HTTP Port: 80, Default HTTPS Port: 443.

- **RTSP Port**: Specify the RTSP Port. Valid Range: 1-65535. Default: 554.

- **TCP Port**: If you have selected the **Model** as **HVR, DVR** or **NVR**, specify the TCP Port. Valid Range: 1-65535. Default: 8000.

- If you wish to configure an additional network, click + . The **Preferred Network 2** section appears.



- Configure the parameters for Preferred Network 2, if required.

Authentication

- **Use Default Credentials**: Select the check box to use the default user name and password to access the device.
- **User Name**: Specify the user name for the device, if you have disabled **Use Default Credentials** check box. In User Name, you can enter upto 100 characters. Default: Blank.
- **Password**: Specify the password for the device, if you have disabled **Use Default Credentials** check box.

  In Password, you can enter upto 100 characters. Default: Blank. Click **Show**  to view the password.

  The icon toggles to **Hide**  . Click **Hide**  to hide the password.

Replace Device

You can replace an existing device in the Admin Client with another device of a similar type. This can be useful when a device gets damaged, say, a camera, whose recordings need to be retained.

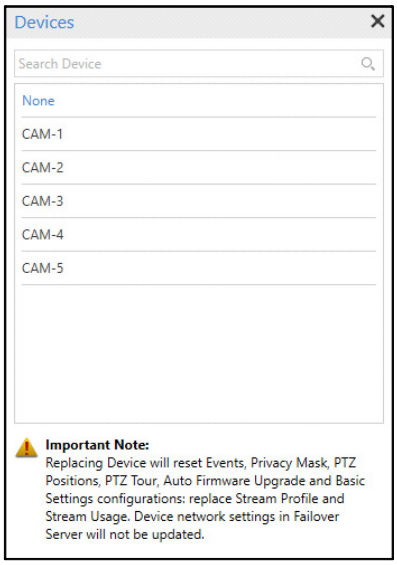
Replacing a device instead of adding a new one ensures that the new device will inherit recording configuration (Recording, Day highlights, Clip Capture, Image Capture) and backup configurations (Primary Backup, Archive 1, Archive 2) of the old device and also retain recordings of the old device, if any. Replacing a device will, however, reset all configured Events and Actions, Privacy Mask, PTZ Positions, PTZ Tour, Auto Firmware Upgrade and Basic Settings configurations. It will replace Stream Profile and Stream Usage. Also the device Network Settings in Failover Server will not be updated.

Devices can be replaced using Add Manually as well as Auto Discovery Tool. For replacing using Auto Discovery Tool, refer “Add Using Auto Discovery Tool”.

Consider the following scenario while replacing the SATATYA Devices (NVR/HVR/DVR). If a user is replacing the device (NVR/HVR/DVR) with a new device having different number of active cameras configured, the cameras which are on the same index position will be replaced while retaining the old recording and backup configuration. Remaining cameras, if any, will be added to RS with the default configuration of RS.

For example, if you are replacing device-1 having 8 (cam1 to cam8) active cameras with device-2 having 10 (cam1 to cam10) active cameras. In this case, the cameras which are on the same index number (cam1 to cam8) will be replaced while retaining the old recording and backup configuration. The remaining cameras (cam9 to cam10) will be added with the default configuration of RS. To replace the device,

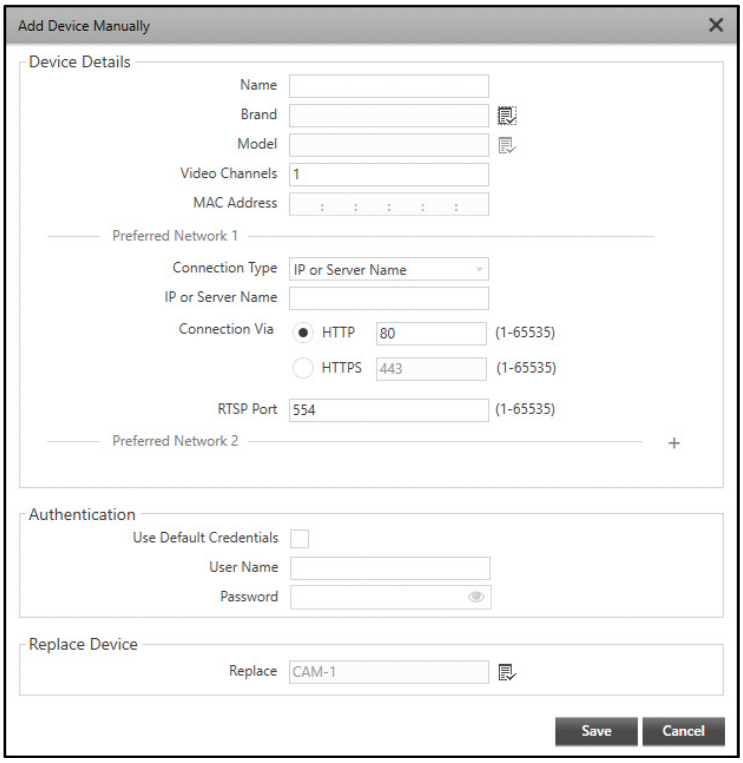
- Click **Replace Devices**  picklist. The **Devices** pop-up appears.



- Double-click the desired device you wish to replace using the **Select Device to Replace** picklist. The selected device from the picklist will be replaced with the new device you are adding.

You can only replace the same type of matrix devices with each other even if they are having a different number of channel supported. For example, NVR6408X can be replaced with NVR3204X but it cannot be replaced with HVR1624S/P or Matrix IP cameras.

If you replace any camera added via ONVIF or Brand Model with the generic camera, the MAC Address field will become blank as per the generic camera.



- Click **Save** to save or click **Cancel** to discard.

*For other ONVIF supported brands, make sure your select **ONVIF** in both **Brand** and **Model**. SATATYA SAMAS supports ONVIF Profiles S and G. On selecting ONVIF, you can also select the protocol to be used for streaming for an ONVIF supported camera.*

*For any unsupported camera brands (not mentioned in **Supported Devices** list), camera must be added using the option Add Manually. Make sure you select **Generic** option in **Brand**. Depending on the Model selected, specify the HTTP/RTSP camera URL to receive streams from the camera.*

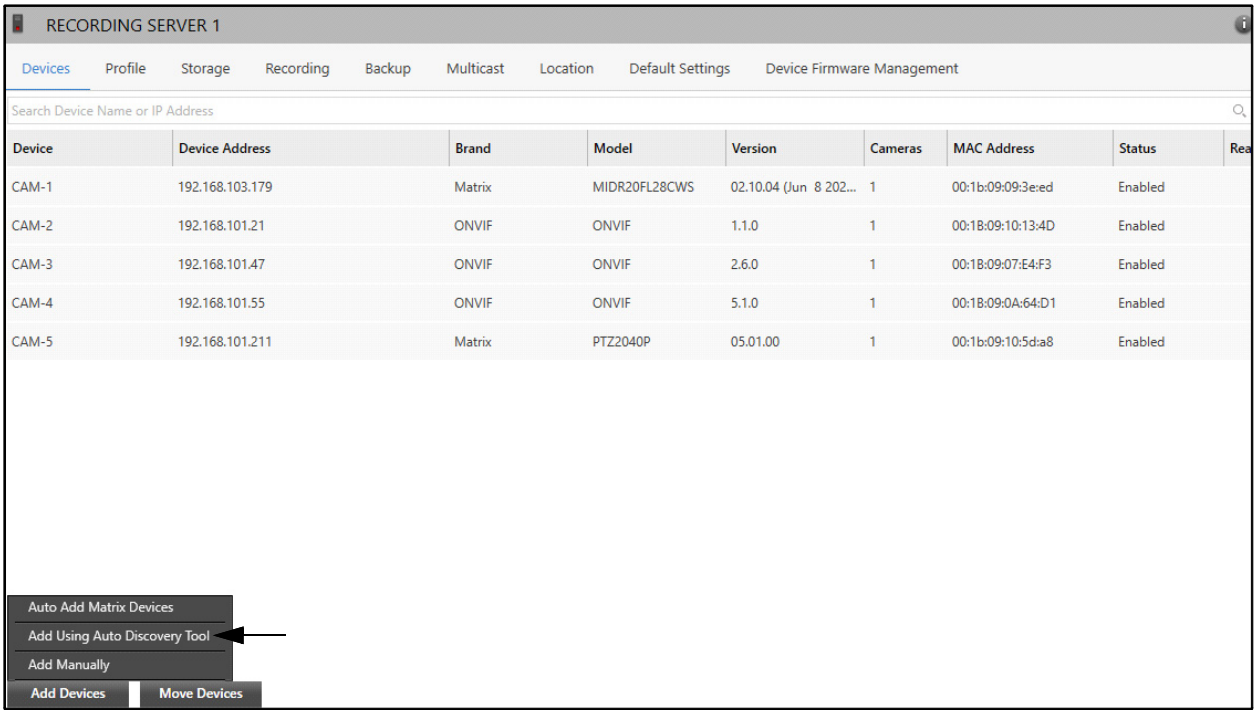
Add Using Auto Discovery Tool

Auto Discovery of network cameras is possible using the **Auto Discovery Tool**. The tool enables you to search through the network of Recording Server and identify all the discoverable IP cameras and add them one at a time or all together.

The cameras in the network will be fetched based on the IP Addressing mode (IPv4/IPv6) of the Recording Server. For example, if IPv4 Addressing mode is enabled for the Recording Server, then only IPv4 cameras in the network will be fetched.

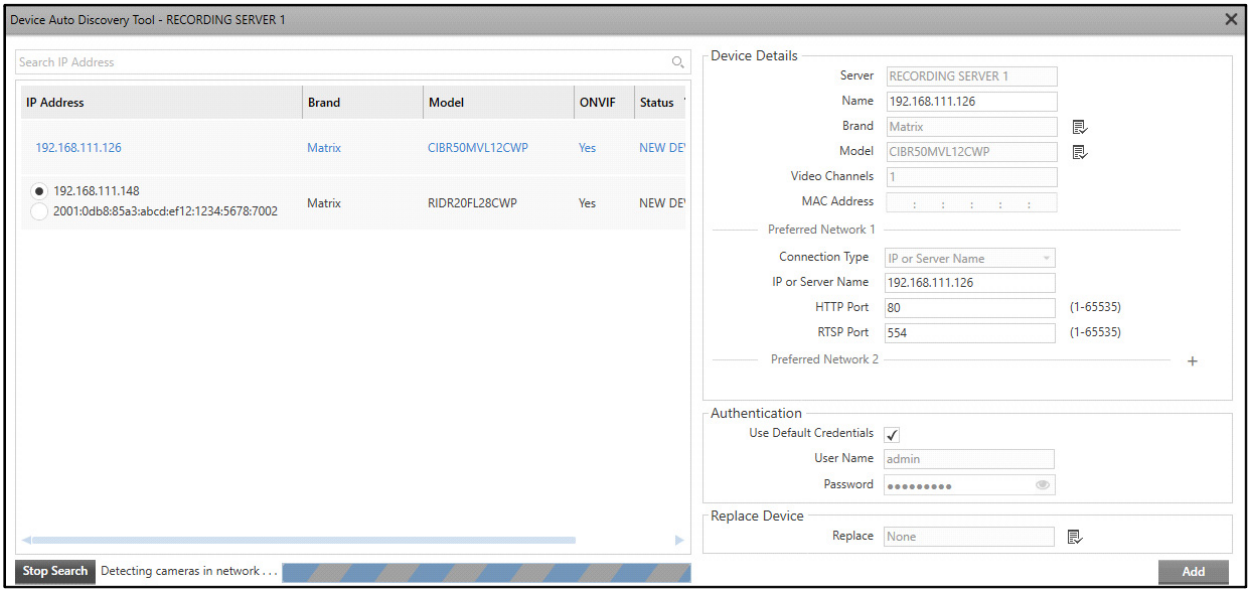
To add cameras using the Auto Discovery Tool,

- Select the desired Recording Server.
- Click **Add Devices**. Select **Add Using Auto Discovery Tool** from the options.

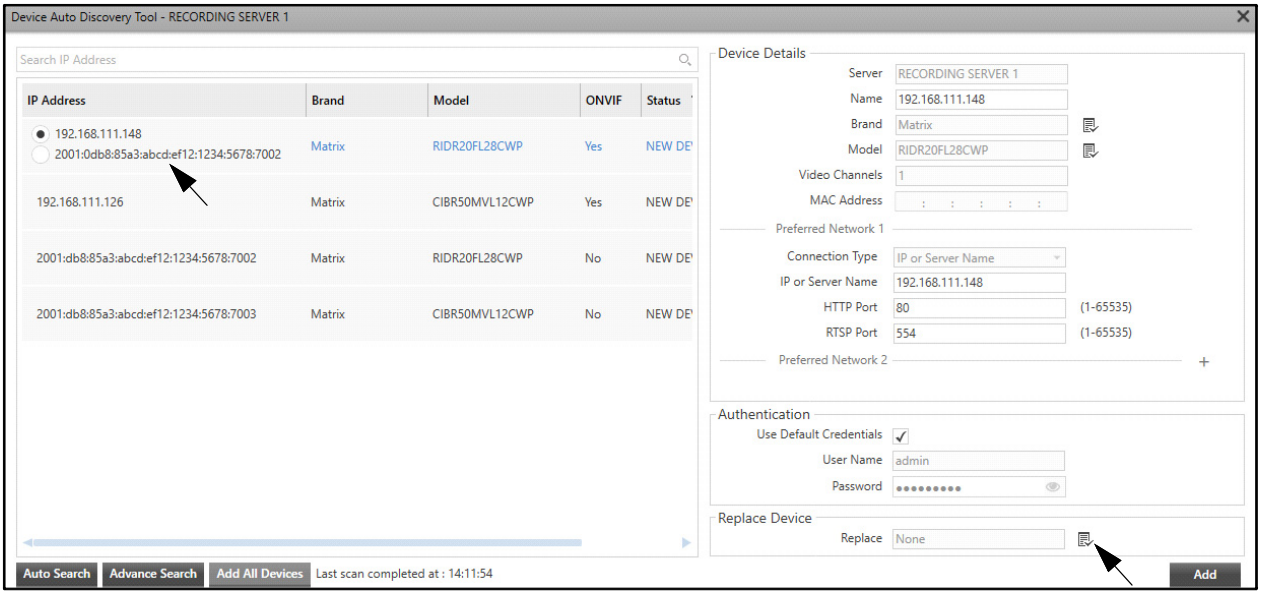


- The **Device Auto Discovery Tool** pop-up appears. The tool will search the local network for the available cameras and retrieve a list of the same.

If both IPv4/IPv6 Address of cameras are available in the network, then the search result will display both the IP Addresses of the cameras. You can add the camera using both the IPv4/IPv6 Addresses. If you add the camera with IPv4 Address using Auto Discovery, then the same camera can be added manually using its IPv6 Address and vice versa.

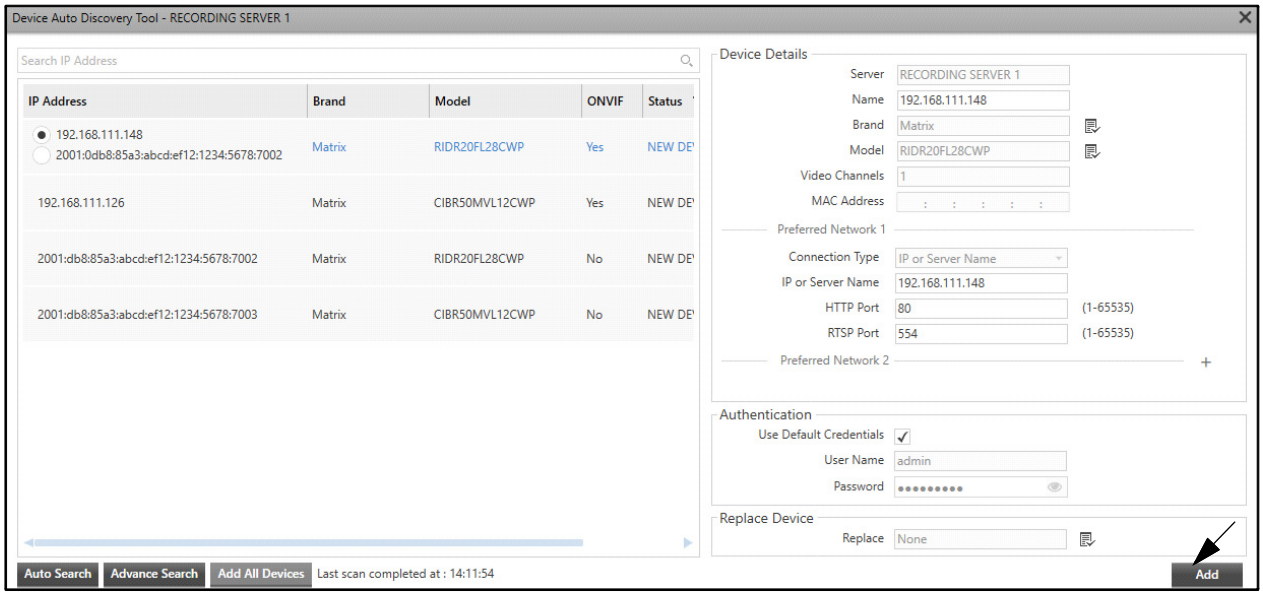


- Select the IPv4/IPv6 address of the desired camera from the retrieved list with which you wish to add it. Edit the desired configuration and authentication details. To configure the details and network, refer to “Add Manually”.

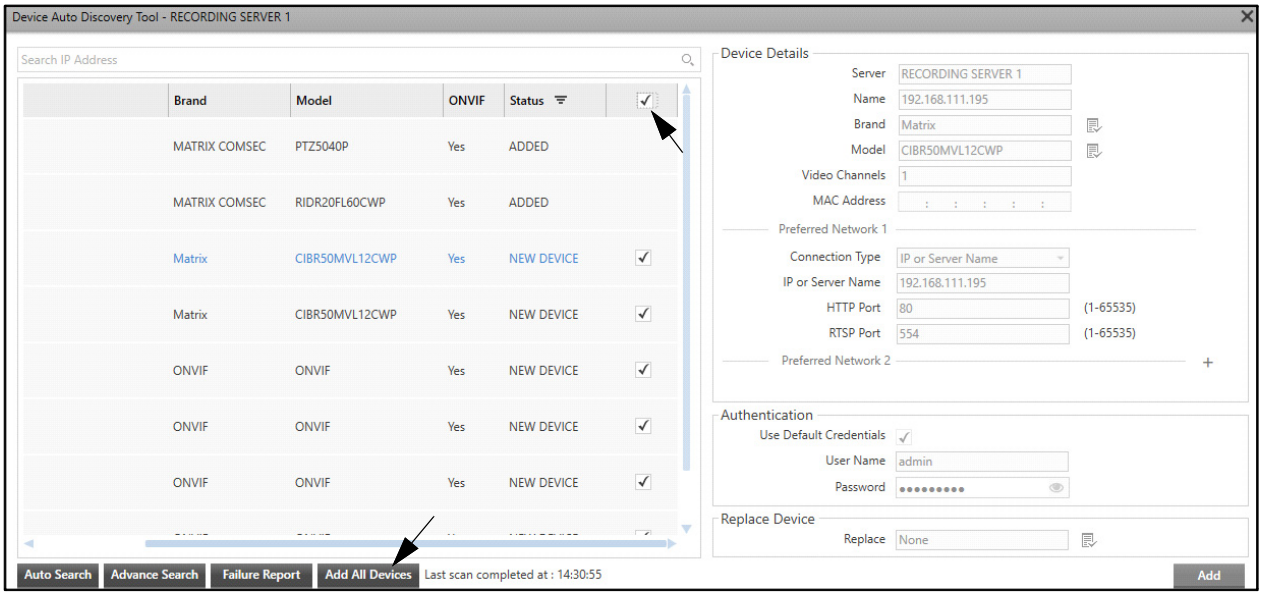


- To replace an existing camera, select the camera using the **Select Device to Replace** picklist. For more details, refer to “Replace Device”.

- Click **Add** to add the camera to the Recording Server.

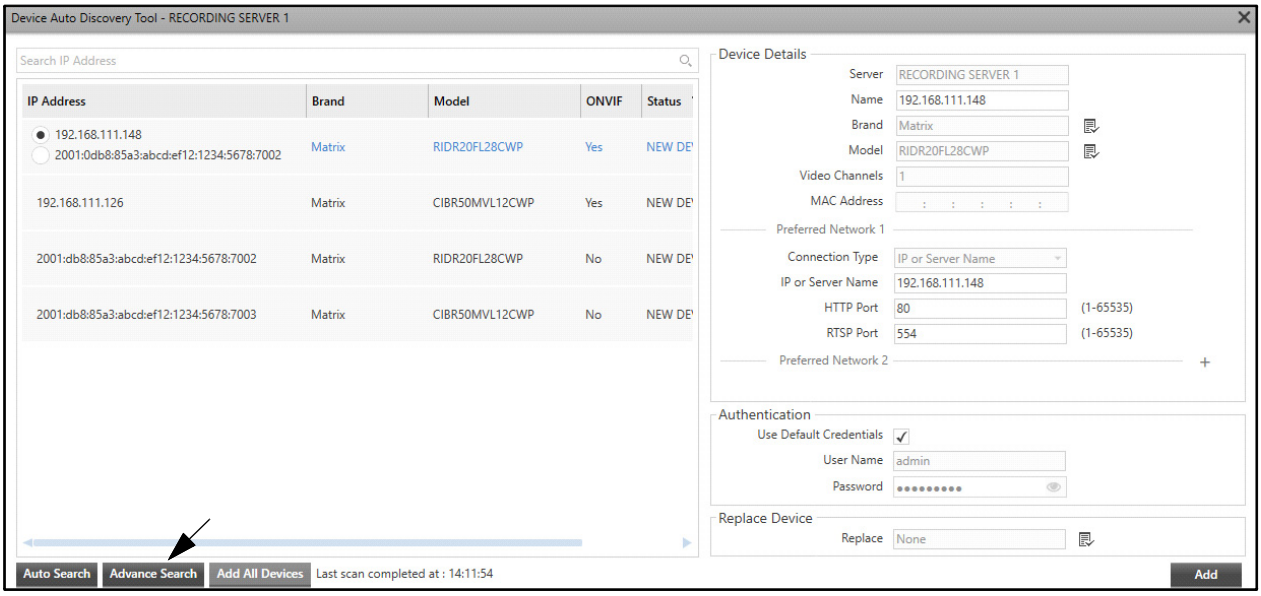


- To add all identified cameras at once, select all the cameras with the **Status** as NEW DEVICE. The **Add All Devices** option is enabled. The camera and network configurations are disabled. Click **Add All Devices** to add all the selected cameras.The **Auto Add and Configure IP Device** pop-up appears. For details, refer to “Auto Add and Configure IP Device”.

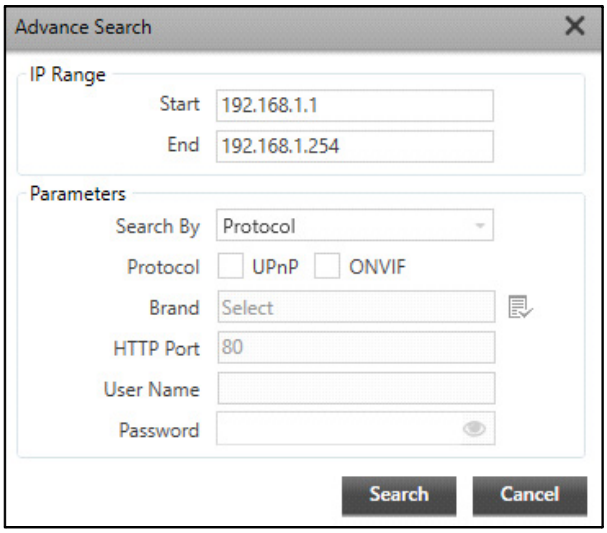


- If you wish to add cameras from another network, click **Advance Search**.

*The Auto Discovery option searches for the cameras from the local network only. Use the **Advance Search** option in the **Device Auto Discovery Tool** window to discover cameras from a different network for a user-defined IP range (can be of different subnet). The search can be based either on device brand or protocol.*



- The **Advance Search** pop-up appears.



Configure the following parameters:

IP Range

- **Start**: Specify the starting IPv4/IPv6 Address of the required IP Range. In Start IP Range, you can enter upto 39 characters. Default: 192.168.1.1.

- **End**: Specify the ending IPv4/IPv6 Address of the required IP Range. In End IP Range, you can enter upto 39 characters. Default: 192.168.1.254.

Parameters

- **Search By**: Select the search mode from the Search By drop-down list — Protocol or Brand.

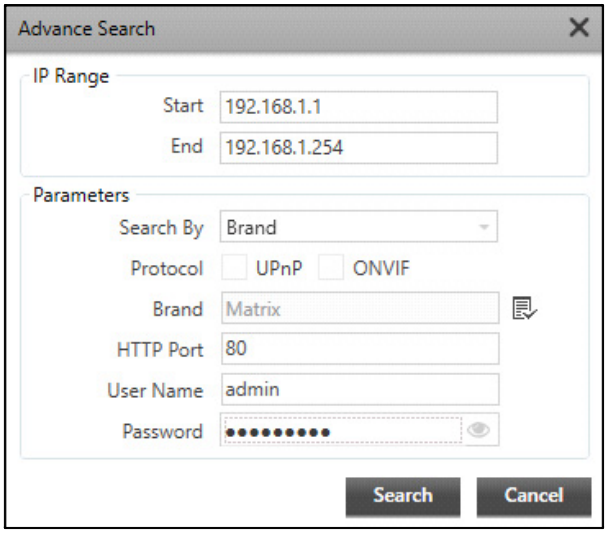
  If you select **Protocol**, select the desired protocol check box — **UPnP** , **ONVIF** or you can also select both the check boxes.

Only Matrix Cameras will be fetched by UPnP Protocol.

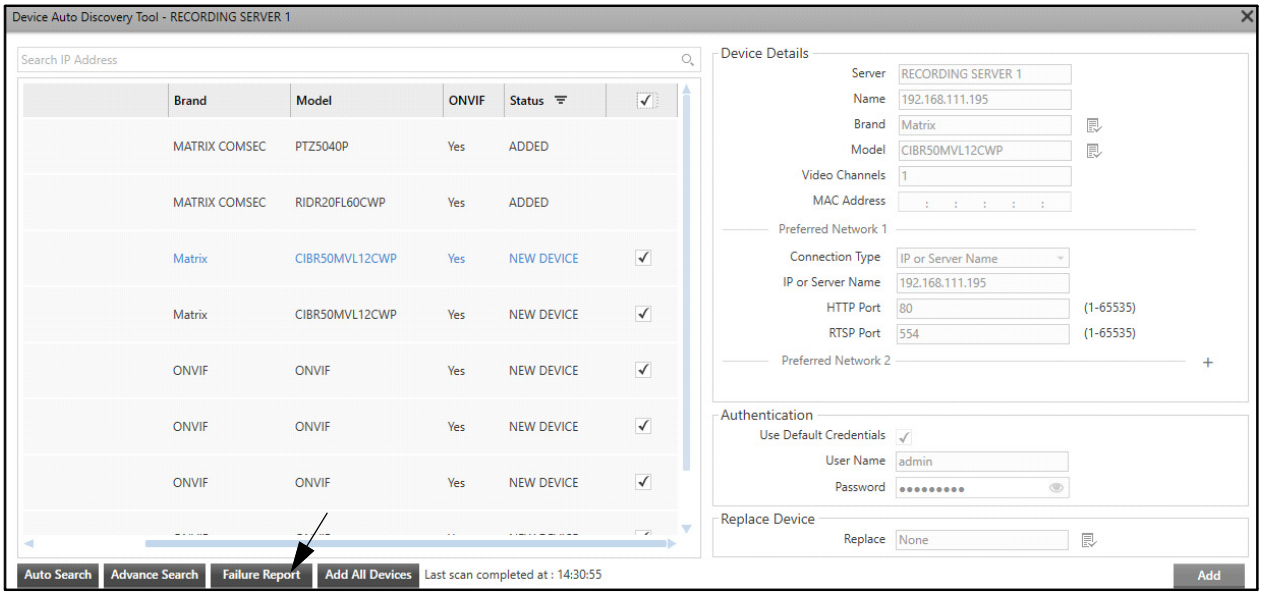
If you select **Brand**, select the device brand from the **Brand** picklist. Double-click to select the desired option.

- **HTTP Port**: Specify the HTTP Port. Valid Range: 1-65535. Default: 80.
- **User Name**: Specify the User Name. In User Name, you can enter upto 100 characters. Default: Blank.
- **Password**: Specify the Password. In Password, you can enter upto 100 characters. Default: Blank.Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

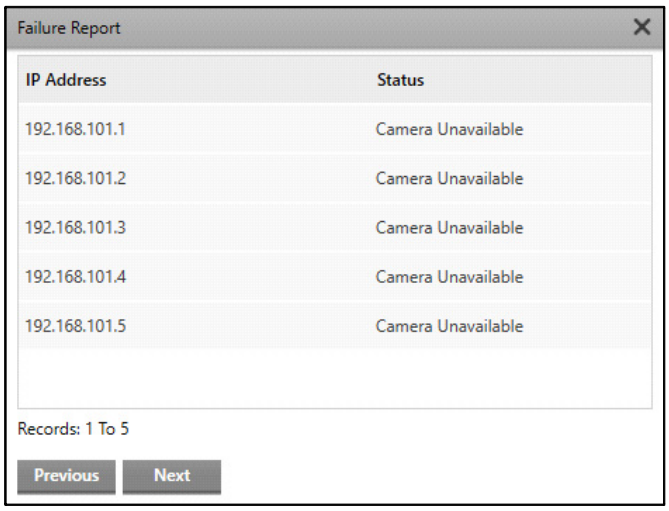
- Click **Search** to search using the defined parameters or click **Cancel** to discard.



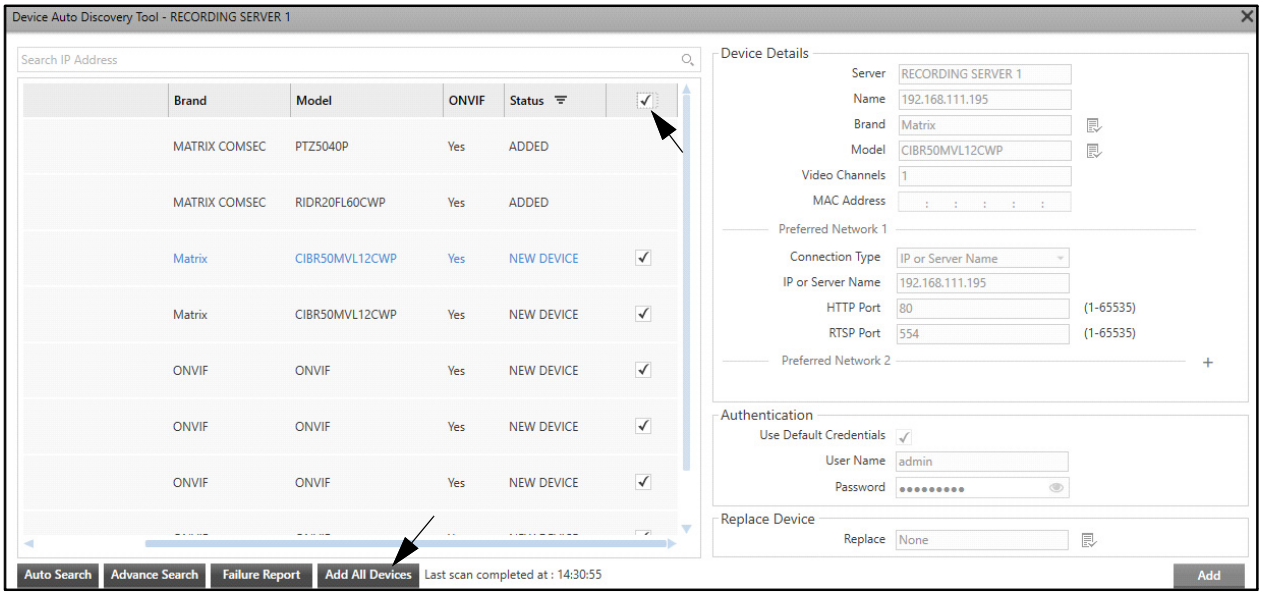
- The tool will search the network for the available cameras and retrieve a list of the same.



- If the search result is not successful for any cameras, then to view the details, click **Failure Report**.

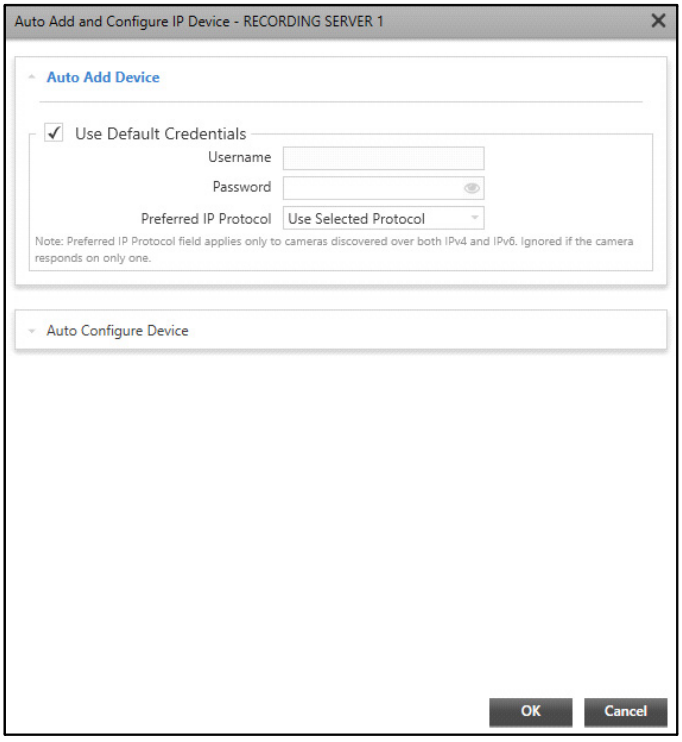


- To add all identified cameras at once, select all the cameras with the **Status** as NEW DEVICE. The **Add All Devices** option is enabled. The camera and network configurations are disabled. Click **Add All Devices** to add all the selected cameras.



Auto Add and Configure IP Device

- The **Auto Add and Configure IP Device** pop-up appears. You can edit the camera configurations here.



Auto Add Device

- **Use Default Credentials:** Select this check box to add the cameras using default credentials for authentication.

  If you wish to specify user-defined credentials in User Name and Password field for authentication, make sure you clear the **Use Default Credentials** check box.

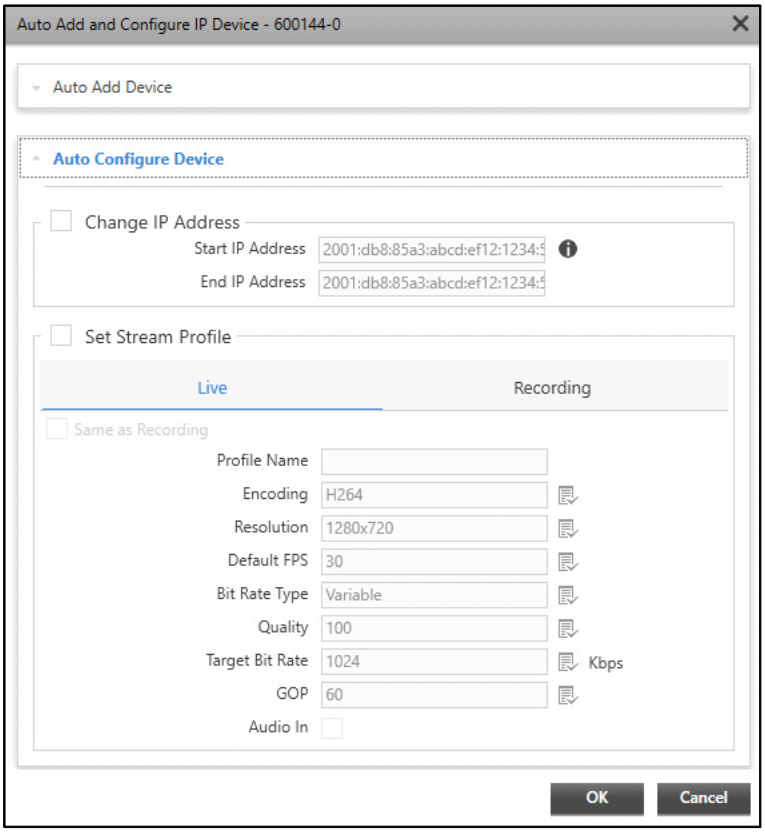
- **User Name**: Specify the User Name to search the cameras using user-defined credentials. In User Name, you can enter upto 100 characters. Default: Blank.
- **Password**: Specify the Password for authentication. In Password, you can enter upto 100 characters. Default: Blank. Click **Show** to view the password. The icon toggles to **Hide**. Click **Hide** to hide the password.
- **Preferred IP Protocol**: Select the desired option with which you wish to add the searched cameras from the drop-down list — Use Selected Protocol, IPv4, IPv6.

Preferred IP Protocol will be applicable only when two IP addresses — IPv4,IPv6 — are fetched for a camera.

If you select **Use Selected Protocol**, all the cameras will be added with the selected IP Address for each camera in the Auto Discovery Tool search list. For details, refer to "Add Using Auto Discovery Tool".

If you select **IPv4/IPv6**, all the cameras will be added with the IPv4/IPv6 Address for each camera irrespective of the IP Address selected for each camera in the Auto Discovery Tool search list. For details, refer to "Add Using Auto Discovery Tool".

Auto Configure Device



- **Change IP Address**: Select the check box to enable changing the IP Addresses of all the discovered cameras. This may be useful especially in instances when all the added cameras are of a particular

brand and have the same IP Address. In such cases, system will identify only a single IP Address and only one camera will be added, unless different IP Addresses are assigned to all the cameras.

Make sure the cameras support IPv4/IPv6 Addressing Mode before changing the IP Address.

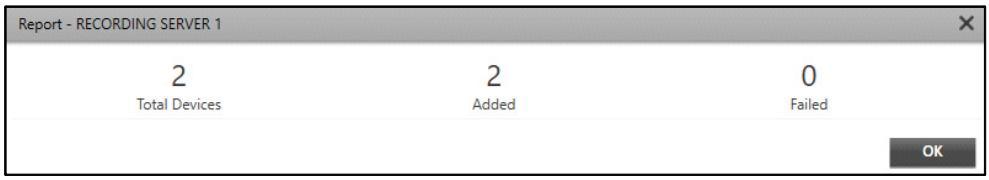
- **Start IP Address**: Specify the Start IPv4/IPv6 Address for the IP range. In Start IP Address, you can enter upto 39 characters. Default: Depends on the subnet of the PC where Recording Server is installed.
- **End IP Address**: Specify the End IPv4/IPv6 Address for the IP range. In End IP Address, you can enter upto 39 characters. Default: Depends on the subnet of the PC where Recording Server is installed.
- **Set Stream Profile**: Select the check box to set user-defined stream profile settings. To set the Stream Profile, refer to "Camera Configuration".

*If **Set Stream Profile** is disabled, Live stream and Recording stream will be set as per default stream profile settings.*

- You can define Stream Settings separately under the **Live** and **Recording** tabs. You can also replicate settings of **Live** tab to **Recording** tab and vice-versa. Select **Same as Recording** check box under **Live** tab or **Same as Live** under **Recording** tab**.**

- Click **OK** to add all cameras with the above configuration. Click **Cancel** to discard.

Once the cameras are added in the Recording Server, a Report for the same appears.



- Click **OK**.

Auto Add Matrix Devices

*For the Auto Addition feature to work, you must ensure that SATATYA SAMAS Integration is enabled for Matrix Devices and IP Cameras in the Device Client and camera web-page respectively. Configure the Recording Server IPv4/IPv6 Address and the **Non-Secure Mode/Secure Mode Port** as configured in the Recording Server to enable device initiation for it. For details, refer to **SATATYA SAMAS Installation Guide**.*

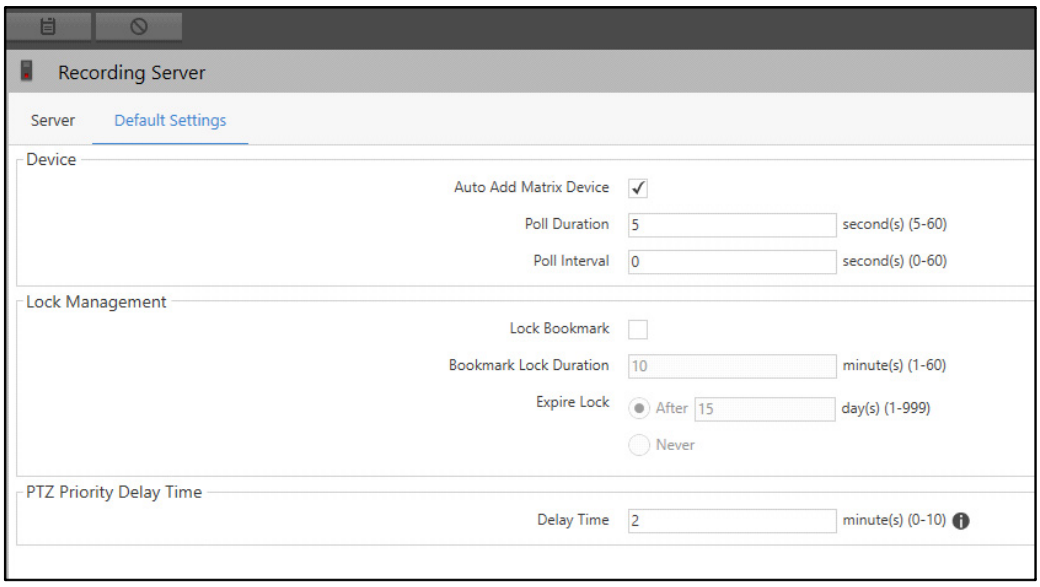
*If you wish to Auto Add **NVR**, make sure you configure IPv4/IPv6 address of the Recording Server. However, if you wish to Auto Add **HVR/DVR**, make sure you configure only IPv4 address of the Recording Server.*

This tool enables you to detect the requesting Matrix Devices (NVRs, HVRs, DVRs) and Matrix IP cameras present in the same or different network as that of the Admin Client and add them automatically to a Recording Server.

To enable the Auto Addition feature for Matrix Devices,

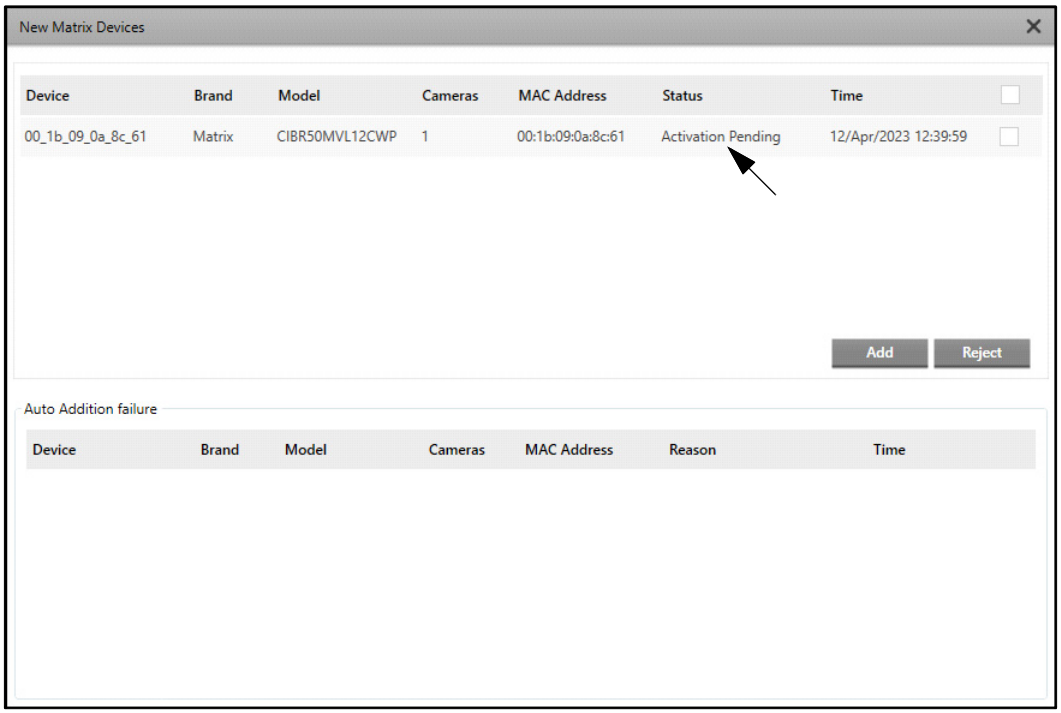
- Click **Servers & Devices > Recording Server > Default Settings**.

- Select the **Auto Add Matrix Device** check box.

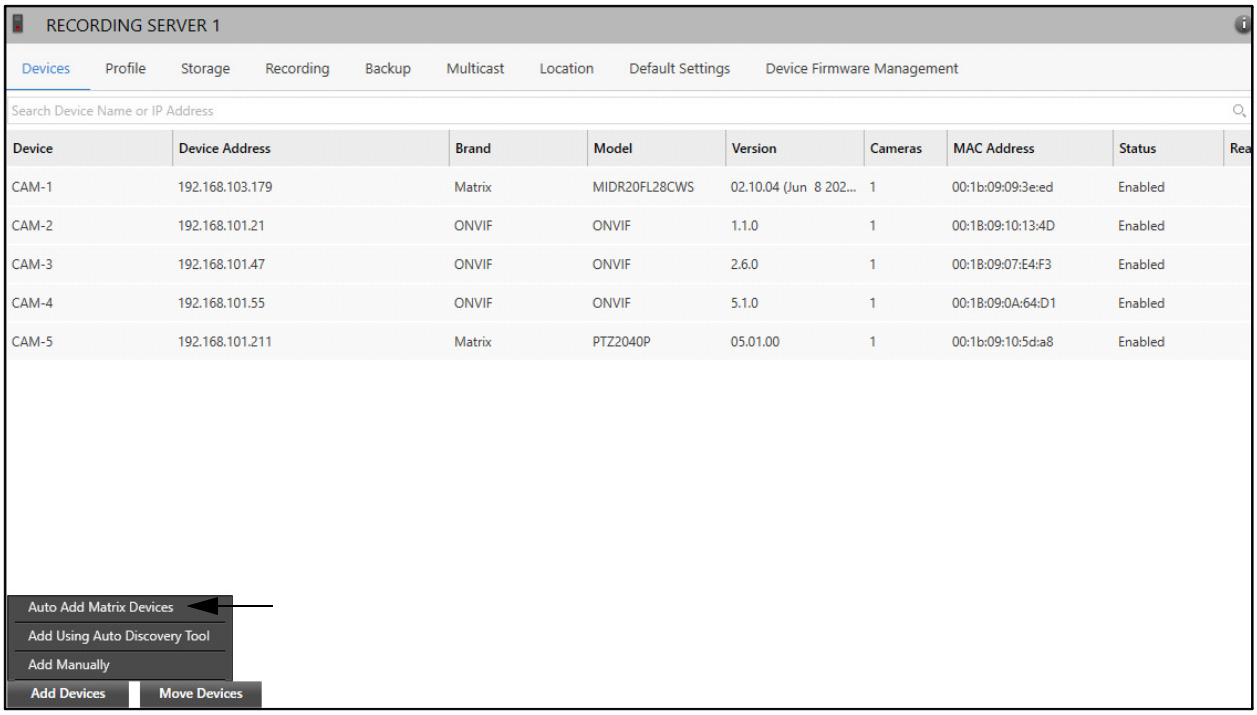


- Click **Save** .

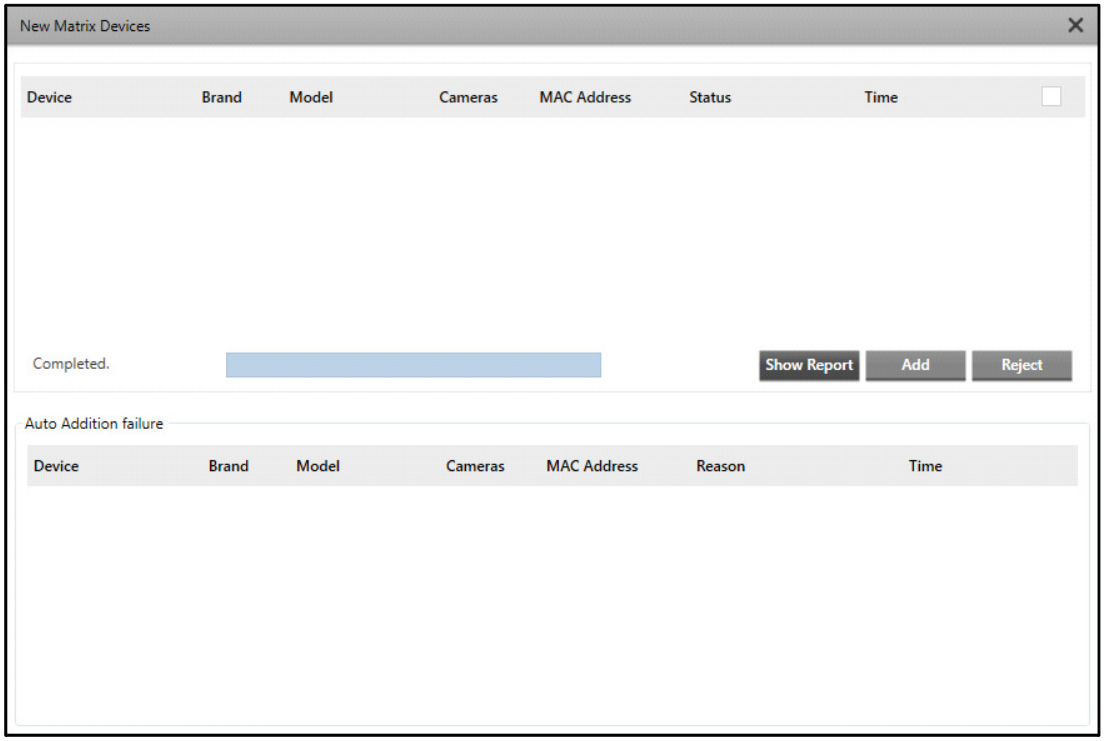
- On enabling Auto Addition, Matrix Devices detected with a new MAC Address, will be automatically added in the configured Recording Server. However, if this feature is disabled, all new device addition requests will appear in the pending state for activation in the **New Matrix Device** pop-up.



- To Auto Add Matrix Devices, click **Add Devices**. Select the **Auto Add Matrix Devices** options.



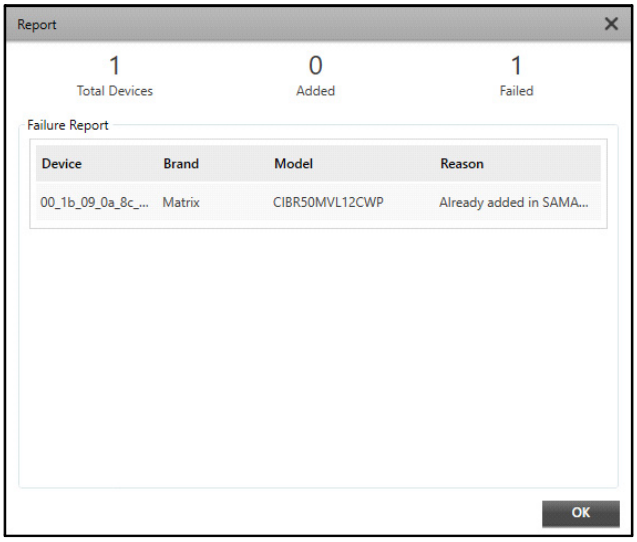
- The **New Matrix Devices** pop-up appears. Select the check box of the desired Matrix device from the list. Click **Add** to add the device or click **Reject** to reject the device request.



The status of device addition appears once you add or reject the device.

If for any reason the devices are not added automatically, then click **Show Report**.

The **Report** pop-up appears with the details.

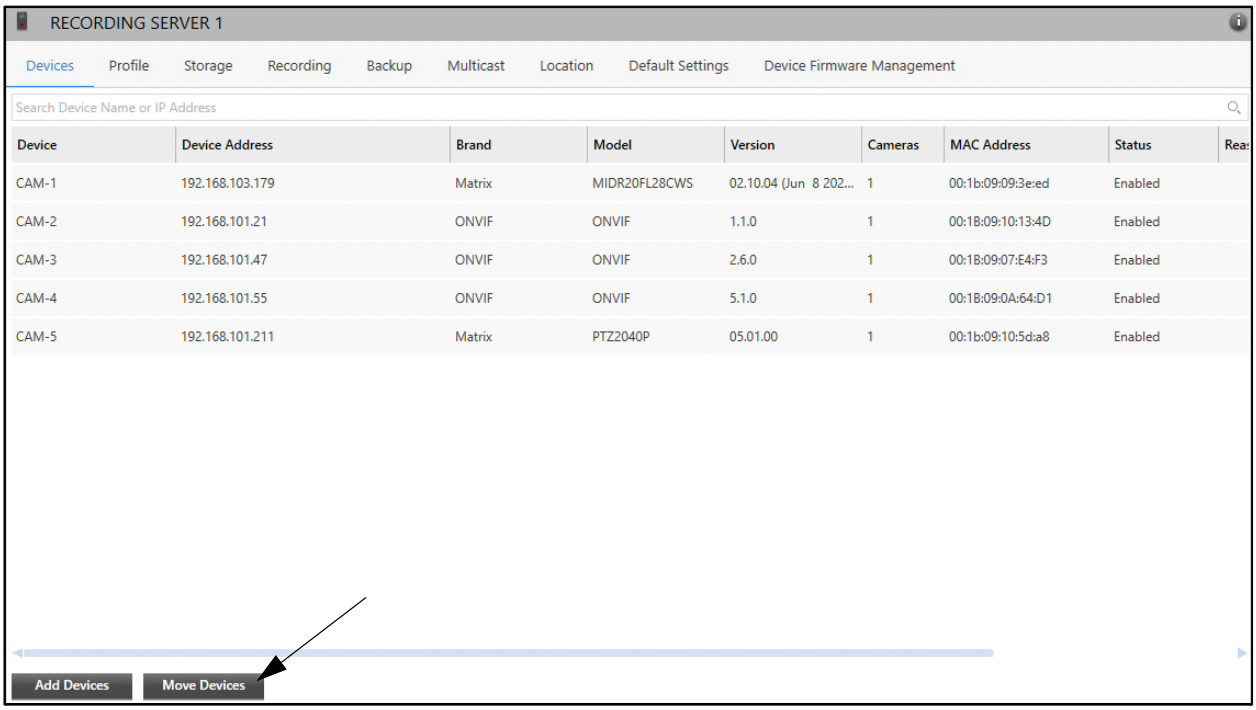


Move Device

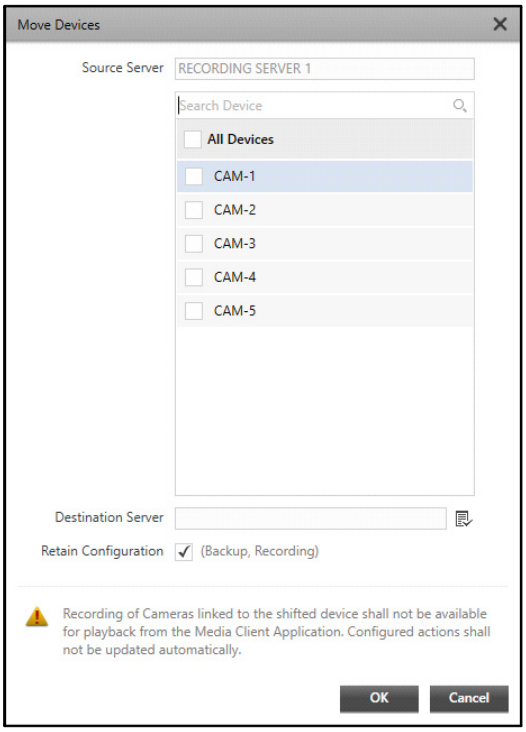
This option enables you to move a device from one Recording Server to another.

To move a device,

- Select the Recording Server from where you wish to move a device. Click **Move Device**.



- The **Move Devices** pop-up appears.



- The **Source Server** displays the Recording Server from where you wish to move a device. Select the check boxes against the desired devices you wish to move. You can also search for the devices using the **Search Device** option.
- Select the **Destination Server** from the **Recording Server** picklist. Double-click to select the desired option.
- Select the **Retain Configuration** check box if you wish to retain the recording (Recording, Day highlights, Clip Capture, Image Capture) and backup (Primary Backup, Archive 1, Archive 2) configuration of the devices of the source RS to the destination RS, by keeping the default storage configuration of the destination RS.

If the default recording storage of destination RS is not available, the recording for the moved devices will be turned off without assigning the recording storage.

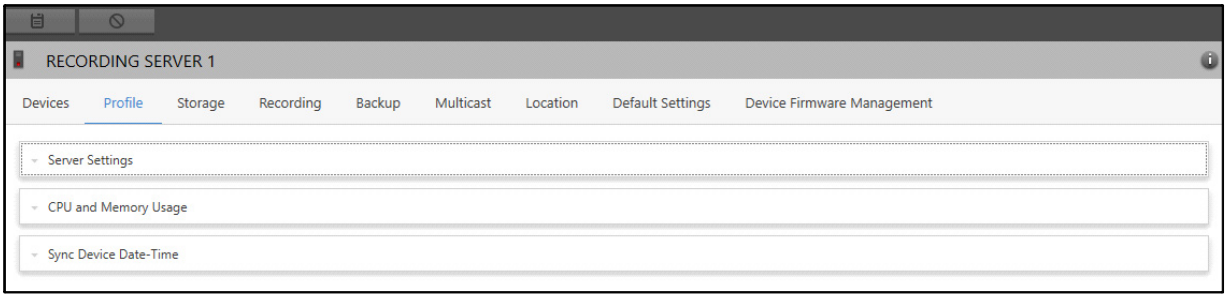
- Click **OK** to move the devices or click **Cancel** to discard.

Profile

This tab enables you to view and configure Server Settings, CPU and Memory Usage and Sync Device Date-Time.

To configure the Profile settings,

- Click the **Profile** tab.



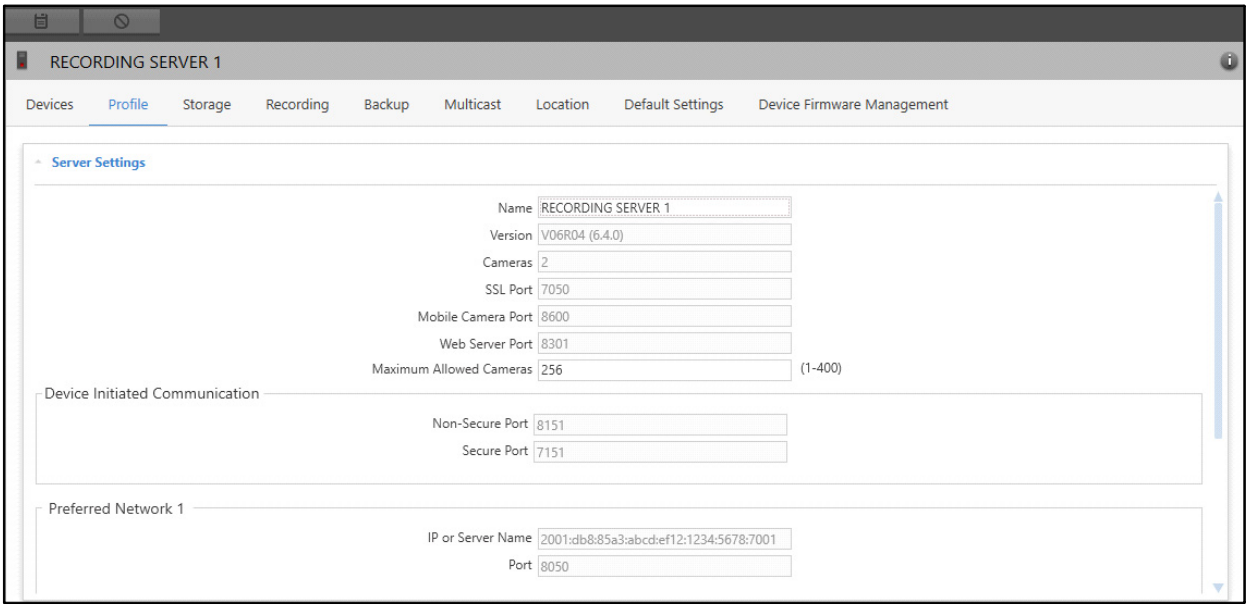
The Profile tab contains three collapsible panels — “Server Settings”, “CPU and Memory Usage” and “Sync Device Date-Time”.

Server Settings

This panel displays the Server Settings of the Recording Server. You can edit and configure the Recording Server Name from this collapsible panel.

To configure the Server Settings,

- Click the **Server Settings** collapsible panel.



This collapsible panel displays the Server Settings and configured Preferred Networks. The parameters of the Server Settings of the Recording Server displayed are — Name, Version, Cameras, SSL Port, Mobile Camera Port, Web Server Port and Maximum Allowed Cameras.

The Device Initiated Communication displays the Non-Secure and Secure Port via which the cameras and NVR can communicate in non-secure and secure mode respectively with the Recording Server when added via Auto Add Matrix Device.

The Preferred Networks display the IPv4/IPv6 Address or Server Name and Port of the Recording Server via which the Client (Admin Client, Smart Client, IVA Server) can be connected with the Recording Server.

You can configure the following parameters:

- **Name**: Specify a name for the Recording Server. In Name, you can enter upto 50 characters. Default: Name of the system where Recording Server is installed.

- **Maximum Allowed Cameras**: Specify the number of cameras allowed to be configured with the Recording Server. Valid Range: 1-400[6]. Default: 256.

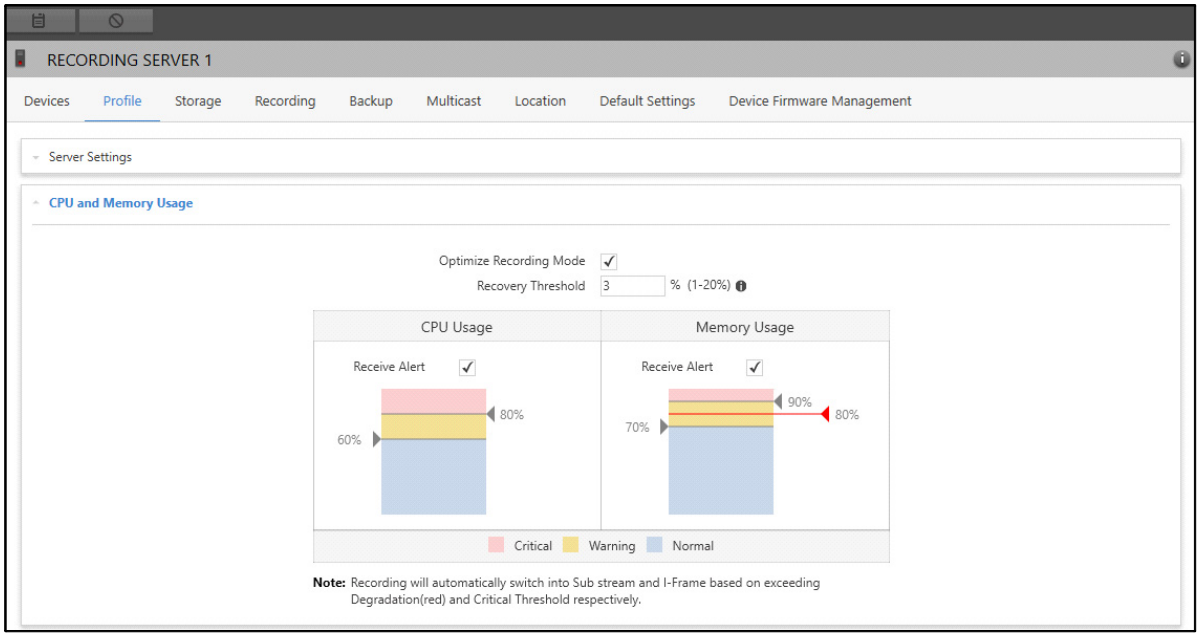
- Click **Save** to save the settings or click **Cancel** to discard.

CPU and Memory Usage

This panel allows you to configure the threshold value of CPU and Memory Usage and receive alerts when the Recording Server crosses these set values.

To configure the CPU and Memory Usage settings,

- Click the **CPU and Memory Usage** collapsible panel.



- **Optimize Recording Mode**: This check box is selected by default, that is the recording of cameras will be optimized according to the Memory Usage. The **Degradation Threshold** (a red line) appears on the Memory Usage.

*It is recommended not to clear the **Optimize Recording Mode** check box when Degradation is in-progress. If done, you will have to restart the Recording Server to recover all the cameras.*

*Make sure you have fulfilled the pre-requisites if you are adding 400 cameras in the RS and if you wish to use **Optimize Recording Mode**. For details, refer to SATATYA SAMAS Installation Guide.*

- **Recovery Threshold**: Specify the Recovery Threshold in percentage. Valid Range: 0-20%. Default: 3%. The memory threshold at which the degraded cameras — those whose recording streams have been switched to Sub Stream or iframe — are restored to either the Main Stream or the Sub Stream. For details, refer to “Functionality of Recording Server with respect to High Memory Usage”.

6. *If you configure the value as 400, make sure the RS pre-requisites are fulfilled. For details, refer to **SATATYA SAMAS Installation Guide**.*

- **Receive Alert**: This check box is selected by default, to receive alerts when the Recording Server crosses the set threshold value under **CPU Usage** and **Memory Usage**. We recommend you not to clear this check box.

- **Critical, Warning and Normal Threshold Values:** The Critical, Warning and Normal Threshold Values for CPU and Memory Usage can be configured by dragging the pointer or tapping on the empty area. Valid Range: 0-100%.

  For example, the CPU Usage and Memory Usage thresholds are configured as 60% for Warning and 80% for Critical respectively. Hence, you will receive an alert when the CPU Usage or the Memory Usage goes beyond 60% and 80%, that is when it crosses the Warning and Critical limit as well as when it comes back to its Normal limit again.

- **Degradation Threshold**: For Memory Usage, drag the red line between the configured Warning and Critical Threshold to configure the Degradation Threshold. When the memory usage goes beyond the Degradation Threshold, the recording stream of the cameras is switched to Sub Stream or iframe from Main Stream. For details, refer to “Functionality of Recording Server with respect to High Memory Usage”.

Default Threshold Values	CPU Usage	Memory Usage
Warning	60%	70%
Degradation	-	80%
Critical	80%	90%

- Click **Save**  to save the settings or click **Cancel**  to discard.

Functionality of Recording Server with respect to High Memory Usage

When the Memory Usage of Recording Server spikes and crosses to high usage, the Recording Server might misbehave, affecting the camera recording. To prevent this, SAMAS intelligently switches the recording stream of cameras according to the rise in Memory Usage. Once the Memory Usage comes back to normal, the recording stream of the cameras is restored accordingly.

In this manner, by “Graceful Degradation” and “Graceful Recovery”, SAMAS prevents recording loss while handling the Memory Usage spikes.

For the details of the events generated, refer to “Event Generation as per Thresholds”.

Graceful Degradation

When the Memory Usage crosses from Warning to Degradation and Degradation to Critical Thresholds, the following will occur.

Threshold	Recording Stream
Warning to Degradation	Cameras remain in Main Stream
Above Degradation	Cameras are switched to Sub Stream
Degradation to Critical	Cameras remain in Sub Stream

Threshold	Recording Stream
Above Critical	Cameras are switched to iframe and "Edge Recording" will stop automatically, even if enabled.

This will ensure the camera recording is preserved even when Recording Server is experiencing increased memory consumption. Now, when the Memory Usage comes down, the recording stream of cameras is again restored in a phase-wise manner. This is called as "Graceful Recovery".

Graceful Recovery

When the Memory Usage comes down from Critical to Degradation and Degradation to Warning Thresholds, the following will occur.

Threshold	Recording Stream
Above Critical	Cameras remain in iframe and "Edge Recording" will stop automatically, even if enabled.
Critical to Degradation	In batches, 50 cameras at a time out of the total Cameras in RS are restored from iframe to Sub Stream. "Edge Recording" will resume automatically, if enabled.
Degradation to Warning	In batches, 50 cameras at a time out of the total Cameras in RS are restored from Sub Stream to Main Stream
Warning to Normal	In batches, 50 cameras at a time out of the total Cameras (either in iframe or Sub Stream) in RS are restored to Main Stream

When memory usage drops, the Recording Server does not restore all cameras at once. Instead, it recovers camera streams in batches of upto 50 cameras at a time out of the total cameras, ensuring smooth and stable system performance.

During each recovery cycle, there is a possibility that some cameras might fail in switching the recording stream, due to reasons such as, camera offline, Main Stream not available or maximum stream usage reached. SAMAS then stores the list of cameras that fail. Once all the batches for switching the cameras have been completed, SAMAS generates the **Degradation Stopped** event automatically along with the list of failed cameras in the Smart Client.

Event Generation as per Thresholds

When the configured thresholds — Warning, Degradation, Critical — are crossed, respective events will be generated:

Description	Event Generated
Above Critical Threshold	Memory Usage Critical

Description	Event Generated
Above Degradation Threshold	Degradation Started
Above Warning Threshold	Memory Usage Exceeded
Below Warning Threshold	Memory Usage Normal
When all batches of the cameras have been recovered	Degradation Stopped

You can configure scenarios as well as actions to be taken for the events generated. For details, refer to "Basic Scenario".

In the Smart Client,

- the CPU Usage/Memory Usage Exceeded pop-ups appear with a yellow boundary.
- the CPU Usage/Memory Usage Critical pop-ups appear with a red boundary.
- the CPU Usage/Memory Usage Critical event is highlighted in red color under Online Events.
- the Degradation Started pop-ups appear with a yellow boundary.
- the Degradation Stopped pop-ups appear with a blue boundary.

Let us understand this functionality with the help of an example:

The following configurations have been set for Memory Usage of Recording Server 1:

- No. of cameras added in Recording Server 1= 100
- Optimize Recording Mode= Selected
- Recovery Threshold= 5%
- Warning Threshold= 70%
- Degradation Threshold= 80%
- Critical Threshold= 90%

Now, as per the Recovery Threshold, Degradation and Critical Threshold, SAMAS will automatically calculate the Degradation Recovery, for example 75% and Critical Recovery, for example 85%.

When Memory Usage of Recording Server crosses from Warning to Degradation and Degradation to Critical Thresholds, the recording stream of cameras will switch as per "Graceful Degradation". And, when the Memory Usage comes down from Critical to Degradation and Degradation to Warning Thresholds, the recording stream of the cameras will recover as follows:

Threshold	Recording Stream
Above Critical (90%)	100 Cameras remain in iframe
Drops below Critical Recovery (upto 85%)	In batches, 50 Cameras out of the 100 are restored from iframe to Sub Stream
Drops below Degradation Recovery (upto 75%)	In batches, 50 Cameras out of the 100 are restored from Sub Stream to Main Stream
Drops below Warning (drops below 75%)	In batches, 50 Cameras out of the 100 are restored from iframe/Sub Stream to Main Stream

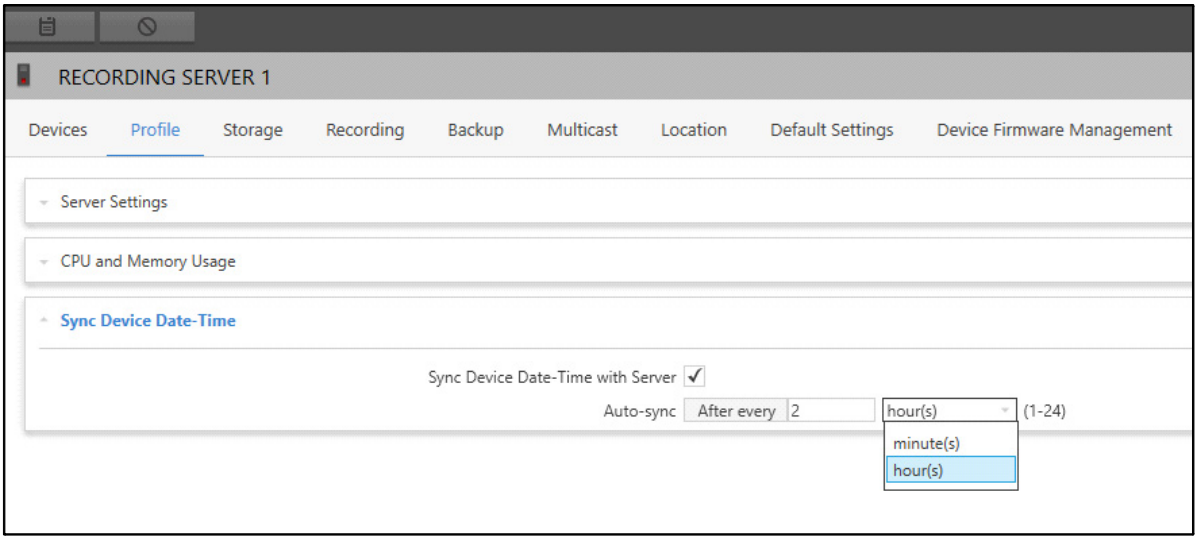
In this manner, the recording stream of the cameras is recovered in a phased manner to stabilize the Memory Usage of Recording Server.

Sync Device Date-Time

This panel allows you to synchronize the Date and Time between cameras and devices and the Recording Server. The Recording Server will set its current Date and Time on the connected devices if the **Sync Device Date-Time with Server** check box is selected.

To configure Sync Device Date-Time settings,

- Click the **Sync Device Date-Time** collapsible panel.



- **Sync Device Date-Time with Server**: Select the Sync Device Date-Time with Server check box.
- **Auto-sync**: Select the Auto-sync time from the drop-down list — **hour(s)** and **minute(s)**. Specify the Auto-sync time. The Recording Server will Sync the Date and Time repeatedly as per the set configured time period. Valid Range: 1-1440 minutes or 1-24 hours. Default: 30 minutes or 2 hours.

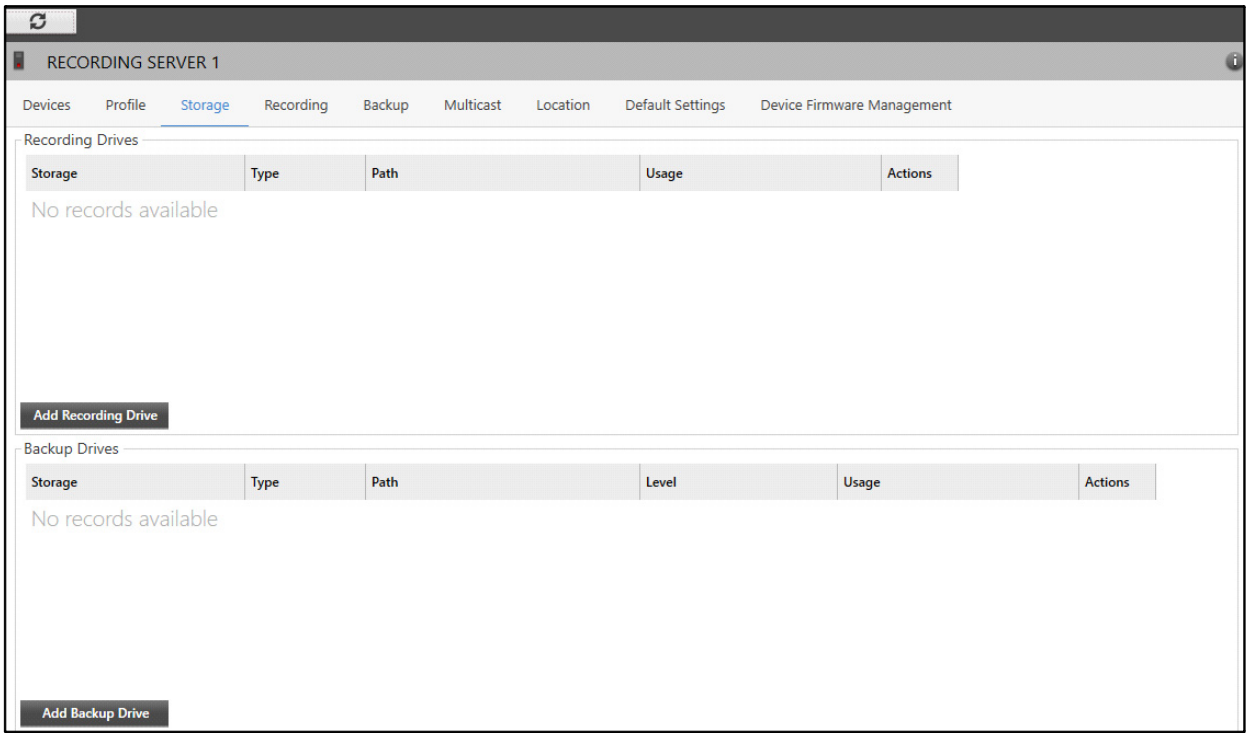
  For example, if you set the **Auto-sync** time as **After Every** 2 hours, the Recording Server will synchronize the Date and Time with the device/camera after every 2 hours.
- Click **Save** to save the settings or click **Cancel** to discard.

Storage

This tab enables you to add Recording and Backup Drives and define storage settings for them.

To configure Storage settings,

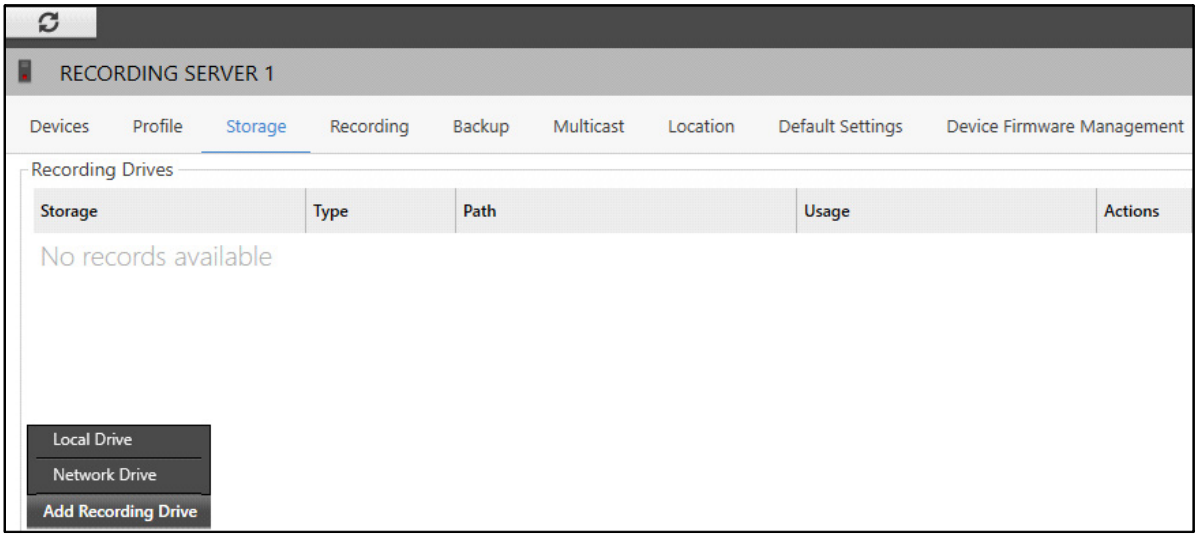
- Click the **Storage** tab.



The Storage tab consists of two sections — “Recording Drive” and “Backup Drive”.

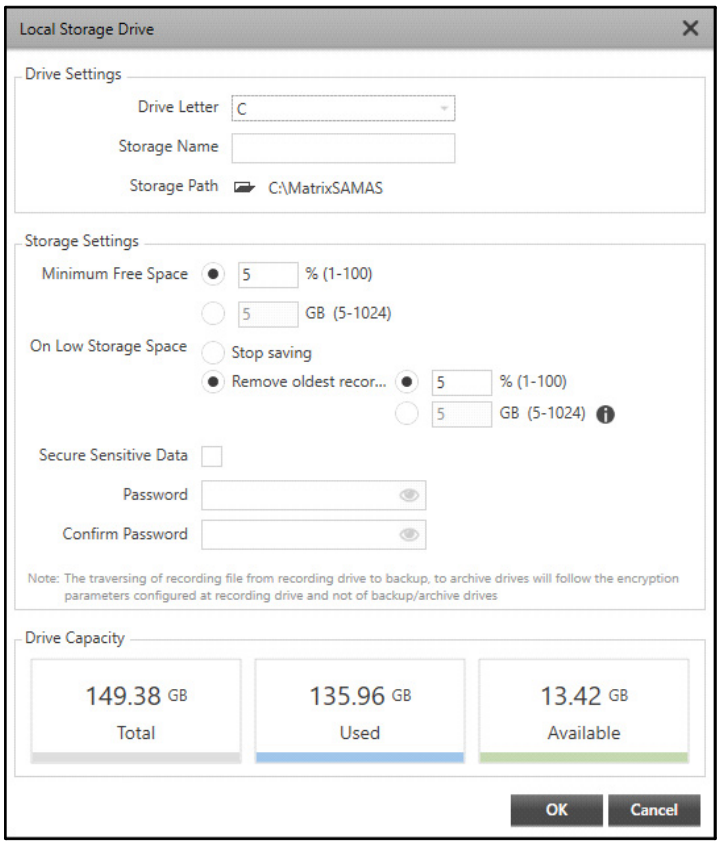
Recording Drive

- Click **Add Recording Drive**. You can add two types of Recording Drives — “Local Drive” and “Network Drive”.



Local Drive

- Select **Local Drive** as the **Add Recording Drive** option. The **Local Storage Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Drive Letter:** Select a drive from the drop-down list where you wish to store the records.
- **Storage Name:** Specify a unique storage name. The configured Local Drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.
- **Storage Path:** Browse a storage path in the selected drive where you wish to store the records. Click **Browse** . It displays all the folders which are in the drive. Select the desired folder.

Storage Settings

- **Minimum Free Space:** Specify the space in terms of value which is to be kept empty in the selected Local Drive. You can define the value either in Percentage (Valid Range: 1-100, Default: 5) or GB (Valid Range: 5-1024, Default: 5).

  For example, if you configure the value as 5%, **Storage Memory Low** event shall be generated by Recording Server when 5% memory of the drive is remaining to be filled.

- **On Low Storage Space**: Select the action to be taken when the available memory on the drive is low — Stop Saving or Remove Old Records.
  If you select **Stop Saving**, the records will not be saved when the drive is low on storage space.

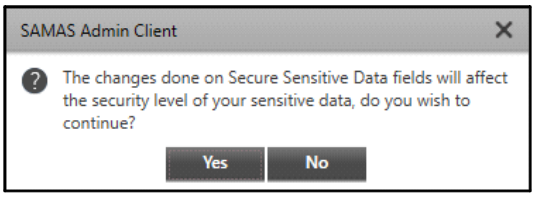
If you select **Remove Old Records**, the old records will be removed. You can define the value either in Percentage (Valid Range: 1-100, Default: 5) or GB (Valid Range: 5-1024, Default: 5).

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Recordings (All types of recording), Backup and Archives Recording, Snapshots stored through CREAM Module. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.
- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.
- **Confirm Password**: Re-enter the password to confirm. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

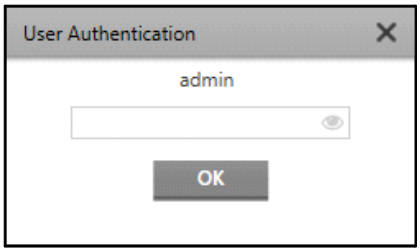
Drive Capacity

- **Total Space:** This displays total space of the Local Drive of the Recording Server in GBs.
- **Used Space:** This displays the space of the Local Drive that has been used in GBs.
- **Available Space:** This displays the remaining space available for storing records in the Local Drive of the Recording Server in GBs.

- Click **OK** to save the Storage Drive configurations. The following pop-up will appear.



- Click **Yes** to continue. The **User Authentication** pop-up will appear.

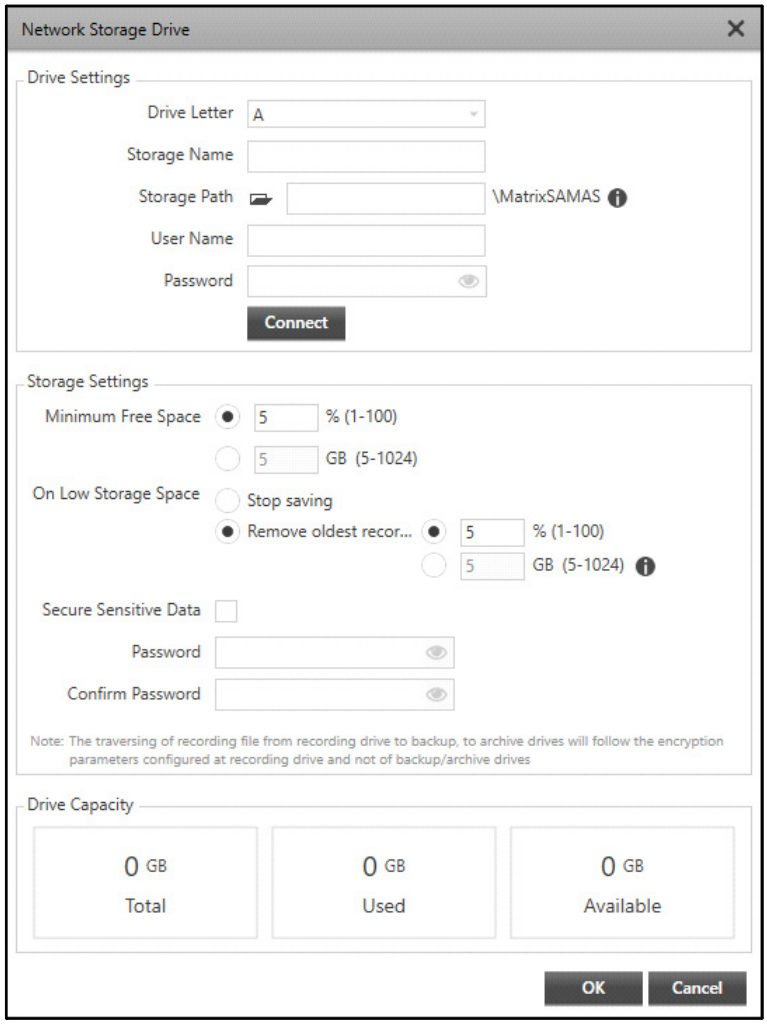


- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.
- Click **OK**.

A storage directory will always be created in accordance with the drive connected to the Recording Server. For example, when Local Drive is selected for addition, all drives that will appear for selection belong to the computer where the Recording Server is installed and not of the system from which user is accessing the Admin Client.

Network Drive

- Select **Network Drive** as the **Add Recording Drive** option. The **Network Storage Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Drive Letter:** Select a drive from the drop-down list where you wish to store the records.
- **Storage Name:** Specify a unique storage name. The configured Network Drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.
- **Storage Path:** Browse a storage path in the selected drive where you wish to store the records. Click **Browse** . It displays all drives which are in the network. Select the desired drive and the folder. In Storage Path, you can enter upto 255 characters. Default: Blank.

Storage Path supports both IPv4/IPv6 Address of a system or Server Name where you wish to create Network Storage Drive.

- *If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].*
- *If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.*

- **User Name**: Specify the User Name for the authentication of the Network Drive. In User Name, you can enter upto 50 characters. Default: Blank.

- **Password**: Specify the Password for the authentication of the Network Drive. In Password, you can enter upto 50 characters. Default: Blank Click **Show**  to view the password. The icon toggles to **Hide**  **.** Click **Hide**  to hide the password.

- Click **Connect** to test the connection with the specified drive. The connection will be successful if the Network Drive is accessible and the User Name and Password are valid.

Storage Settings

- **Minimum Free Space:** Specify the space in terms of value which is to be kept empty in the selected network drive. You can define the value either in Percentage (Valid Range: 1-100, Default: 5) or GB (Valid Range: 5-1024, Default: 5).

  For example, if you configure the value as 5%, **Storage Memory Low** event shall be generated by Recording Server when 5% memory of the drive is remaining to be filled.

- **On Low Storage Space**: Select the action to be taken when the available memory on the drive is low — Stop Saving or Remove Old Records.

  If you select **Stop Saving**, the records will not be saved when the drive is low on storage space.

  If you select **Remove Old Records**, the old records will be removed. You can define the value either in Percentage (Valid Range: 1-100, Default: 5) or GB (Valid Range: 5-1024, Default: 5).

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Recordings (All types of recording), Backup and Archives Recording, Snapshots stored through CREAM Module. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.

- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show**  to view the password. The icon toggles to **Hide**  **.** Click **Hide**  to hide the password.

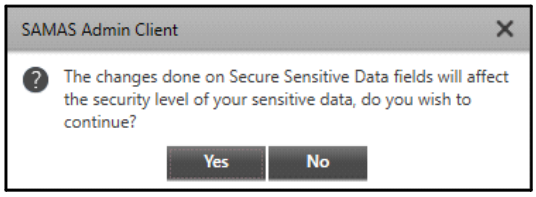
- **Confirm Password**: Re-enter the password to confirm. Click **Show**  to view the password. The icon toggles to **Hide**  **.** Click **Hide**  to hide the password.

Drive Capacity

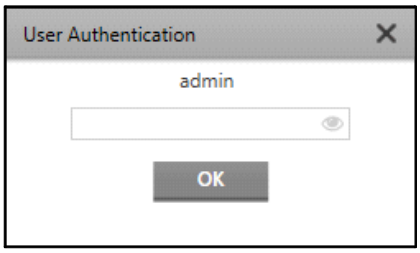
The Drive Capacity of the Network Drive will be displayed only after the connection is successful.

- **Total Space:** This displays the total space of the Network Drive of the Recording Server in GBs.
- **Used Space:** This displays the space of the Network Drive that has been used in GBs.
- **Available Space:** This displays the remaining space available for storing records in the Network Drive of the Recording Server in GBs.

- Click **OK** to save the Storage Drive configurations. The following pop-up will appear.



- Click **Yes** to continue. The **User Authentication** pop-up will appear.

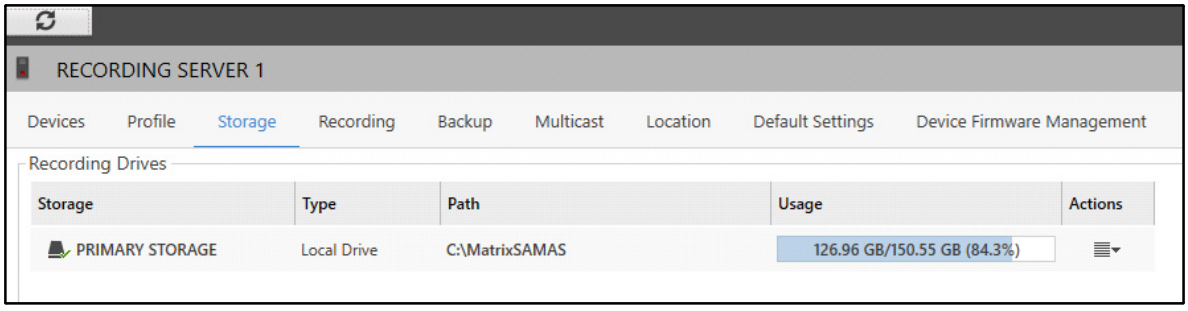


- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **OK**.

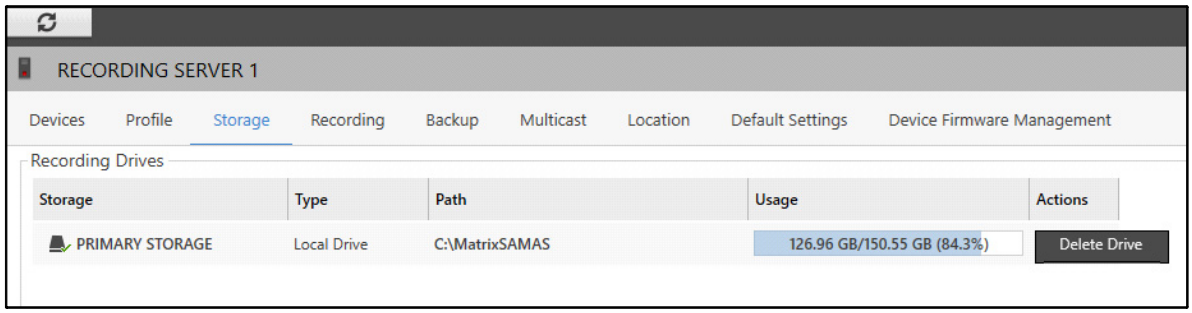
A Network Drive may require a Username and Password for allowing access. Enter the username and password in the Drive Settings and click the Connect button to establish connection with the specified drive.

The configured Recording Drives appear in the Recording Drives list.



The following details are displayed for the configured Recording Drives — Storage, Type, Path, Usage and Actions.

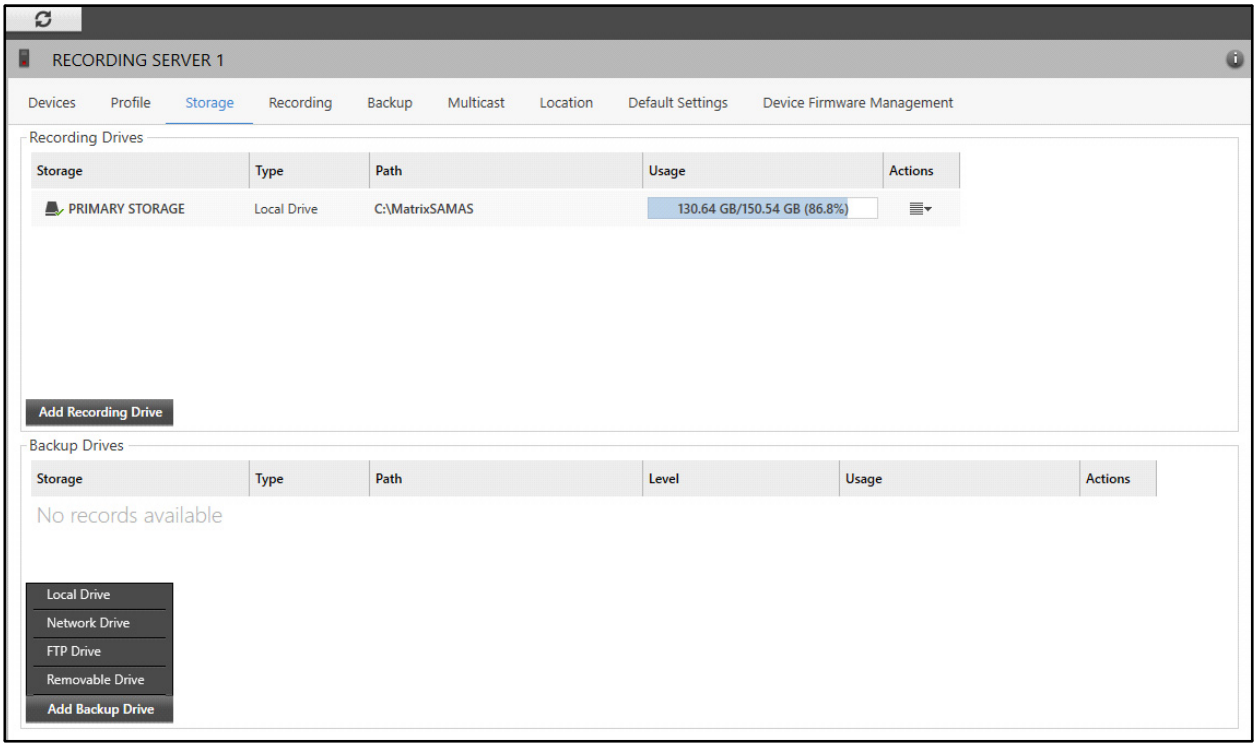
- Click **Actions** . The **Delete Drive** option appears.



- **Delete Drive**: Click Delete Drive to delete the configured Recording Drive. The drive will be removed from the Recording Drives list.

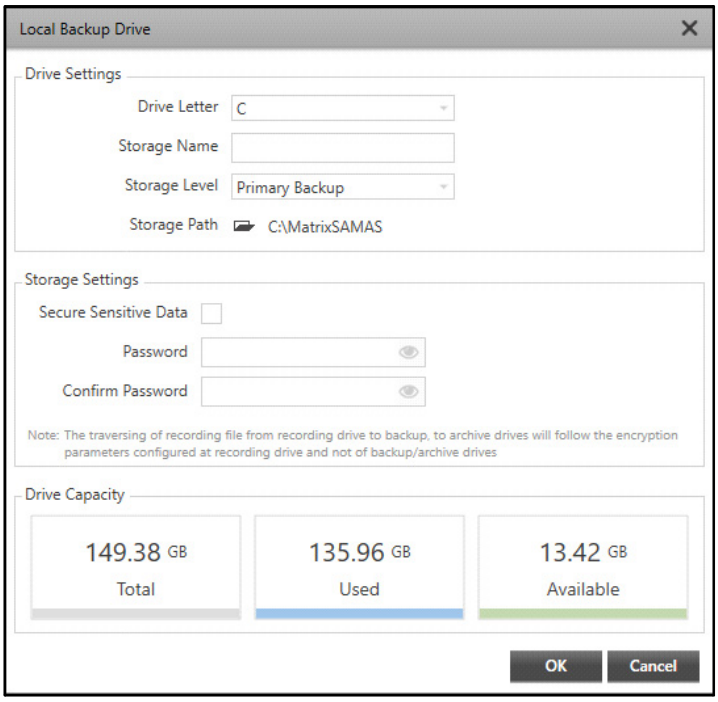
Backup Drive

- Click **Add Backup Drive**. You can add four types of Backup Drives — “Local Drive”, “Network Drive”, “FTP Drive” and “Removable Drive”.



Local Drive

- Select **Local Drive** as the **Add Backup Drive** options. The **Local Backup Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Drive Letter:** Select a drive from the drop-down list where you wish to store the records.
- **Storage Name:** Specify a unique storage name. The configured Local Drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.
- **Storage Level**: Select the Storage Level that you wish to assign to the Backup Drive from the drop-down list — Primary Backup, Archive 1 and Archive 2.
- **Storage Path:** Browse a storage path in the selected drive where you wish to store the records. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

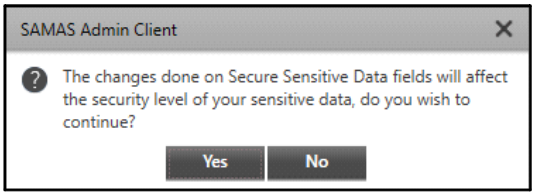
Storage Settings

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Recordings (All types of recording), Backup and Archives Recording, Snapshots stored through CREAM Module. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.
- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.
- **Confirm Password**: Re-enter the password to confirm. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

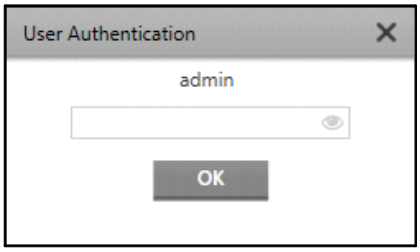
Drive Capacity

- **Total Space:** This displays total space of the Local Drive of the Recording Server in GBs.
- **Used Space:** This displays the space of the Local Drive that has been used in GBs.
- **Available Space:** This displays the remaining space available for storing records in the Local Drive of the Recording Server in GBs.

- Click **OK** to save the Backup Drive configurations. The following pop-up will appear.



- Click **Yes** to continue. The **User Authentication** pop-up will appear.

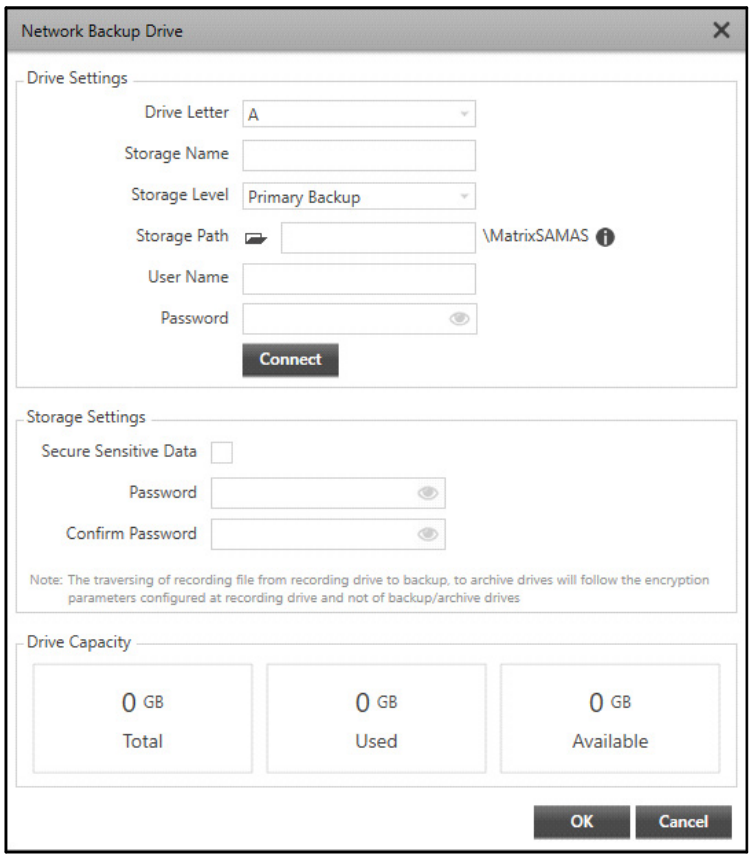


- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **OK**.

Network Drive

- Select **Network Drive** as the **Add Backup Drive** option. The **Network Backup Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Drive Letter:** Select a drive from the drop-down list where you wish to store the records.
- **Storage Name:** Specify a unique storage name. The configured Network Drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.
- **Storage Level**: Select the Storage Level that you wish to assign to the Backup Drive from the drop-down list — Primary Backup, Archive 1 and Archive 2.
- **Storage Path:** Browse a storage path in the selected drive where you wish to store the records. Click **Browse** . It displays all the drives which are in the network. Select the desired drive and the folder. In Storage Path, you can enter upto 255 characters. Default: Blank.

Storage Path supports both IPv4/IPv6 Address of a system or Server Name where you wish to create Network Backup Drive.

- *If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].*
- *If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.*

- **User Name**: Specify the User Name for the authentication of the Network Drive. In User Name, you can enter upto 50 characters. Default: Blank.

- **Password:** Specify the Password for the authentication of the Network Drive. In Password, you can enter upto 50 characters. Default: Blank. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **Connect** to test the connection with the specified drive. The connection will be successful if the Network Drive is accessible and the User Name and Password are valid.

Storage Settings

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Recordings (All types of recording), Backup and Archives Recording, Snapshots stored through CREAM Module. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.

- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show** to view the password. The icon toggles to **Hide** **.** Click **Hide** to hide the password.

- **Confirm Password**: Re-enter the password to confirm. Click **Show** to view the password. The icon toggles to **Hide** **.** Click **Hide** to hide the password.

Drive Capacity

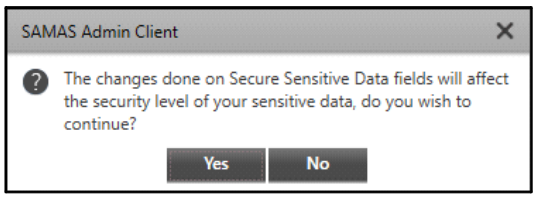
The Drive Capacity of the Network Drive will be displayed only after the connection is successful.

- **Total Space:** This displays total space of the Network Drive of the Recording Server in GBs.

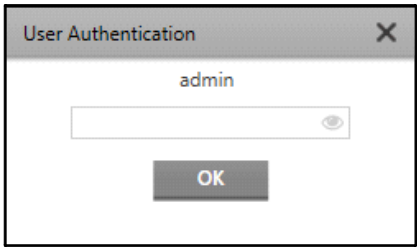
- **Used Space:** This displays the space of the Network Drive that has been used in GBs.

- **Available Space:** This displays the remaining space available for storing records in the Network Drive of the Recording Server in GBs.

- Click **OK** to save the Backup Drive configurations. The following pop-up will appear.



- Click **Yes** to continue. The **User Authentication** pop-up will appear.

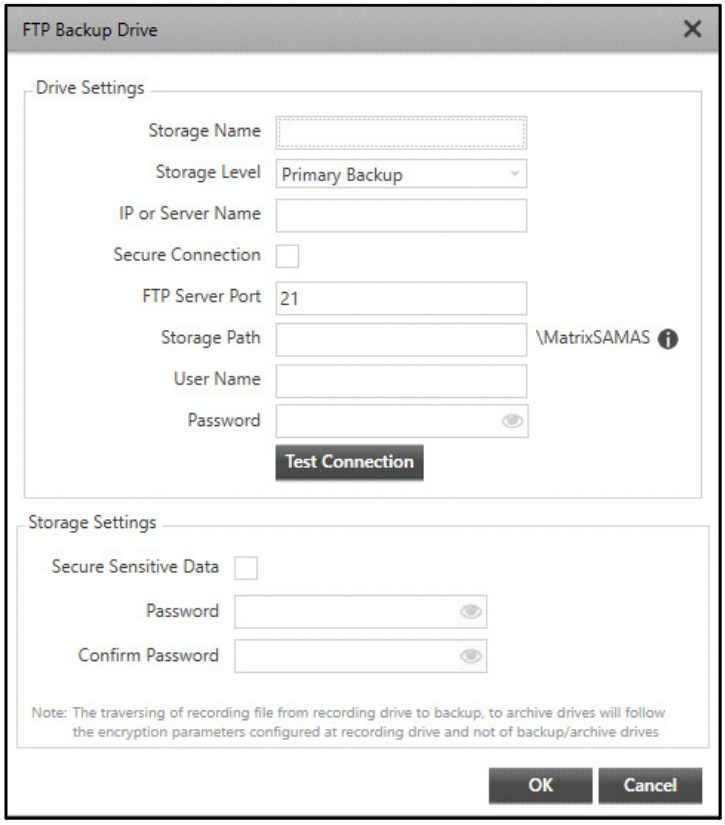


- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **OK**.

FTP Drive

- Select **FTP Drive** as the **Add Backup Drive** options. The **FTP Backup Drive** pop-up appears.



Configure the following parameters:

Drive Settings

- **Storage Name**: Specify a unique storage name. The configured FTP drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.

- **Storage Level**: Select the Storage Level that you wish to assign to the Backup Drive from the drop-down list — Primary Backup, Archive 1 and Archive 2.

- **IP or Server Name:** Specify the Host-Name or IPv4/IPv6 Address of the FTP Server where the records are to be stored. In IP or Server Name, you can enter upto 100 characters. Default: Blank.

If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].

If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Secure Connection**: Select the check box to enable secure file transfer.
- **FTP Server Port:** Specify the FTP listening Port number. Valid Range: 1-65535. Default: 21.
- **Storage Path:** Specify a storage path where you wish to store the records. In Storage Path, you can enter upto 300 characters. Default: Blank.

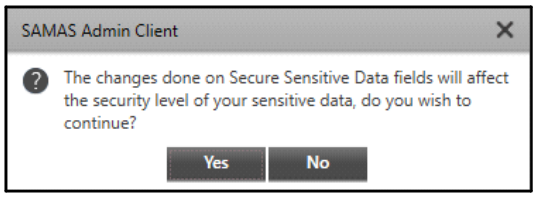
Storage Path supports both IPv4/IPv6 Address of a system or Server Name where you wish to create FTP Backup Drive.

- *If you wish to configure IPv6 Address, make sure you enclose the IPv6 Address in square brackets, for example, [2001:db8::1].*
- *If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.*

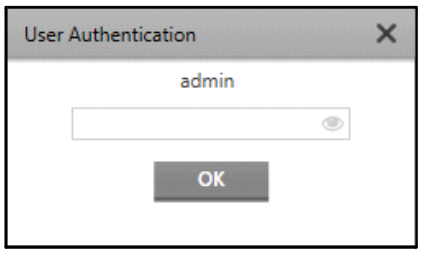
- **User Name**: Specify the User Name for the authentication of the FTP Drive. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password:** Specify the Password for the authentication of the FTP Drive. In Password, you can enter upto 50 characters. Default: Blank. Click **Show** to view the password. The icon toggles to **Hide**. Click **Hide** to hide the password.
- Click **Test Connection** to test the connection with specified drive. The connection will be successful if the FTP Drive is accessible and the User Name and Password are valid.

Storage Settings

- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Recordings (All types of recording), Backup and Archives Recording, Snapshots stored through CREAM Module. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.
- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show** to view the password. The icon toggles to **Hide**. Click **Hide** to hide the password.
- **Confirm Password**: Re-enter the password to confirm. Click **Show** to view the password. The icon toggles to **Hide**. Click **Hide** to hide the password.
- Click **OK** to save the Backup Drive configurations. The following pop-up will appear.



- Click **Yes** to continue. The **User Authentication** pop-up will appear.

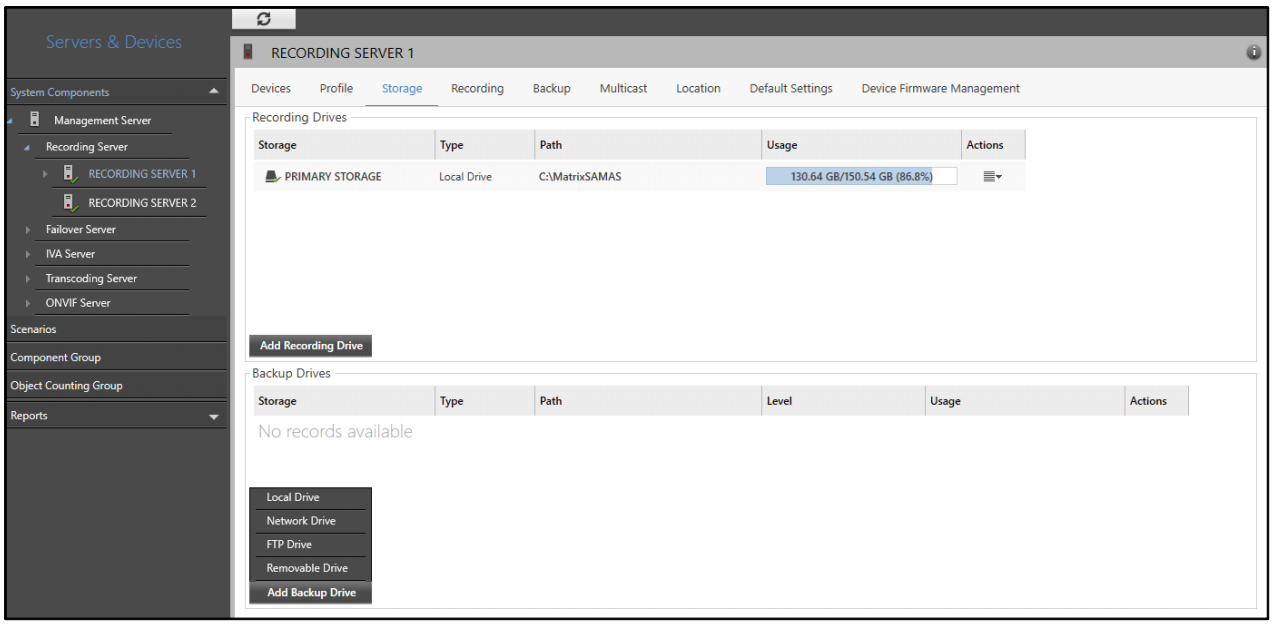


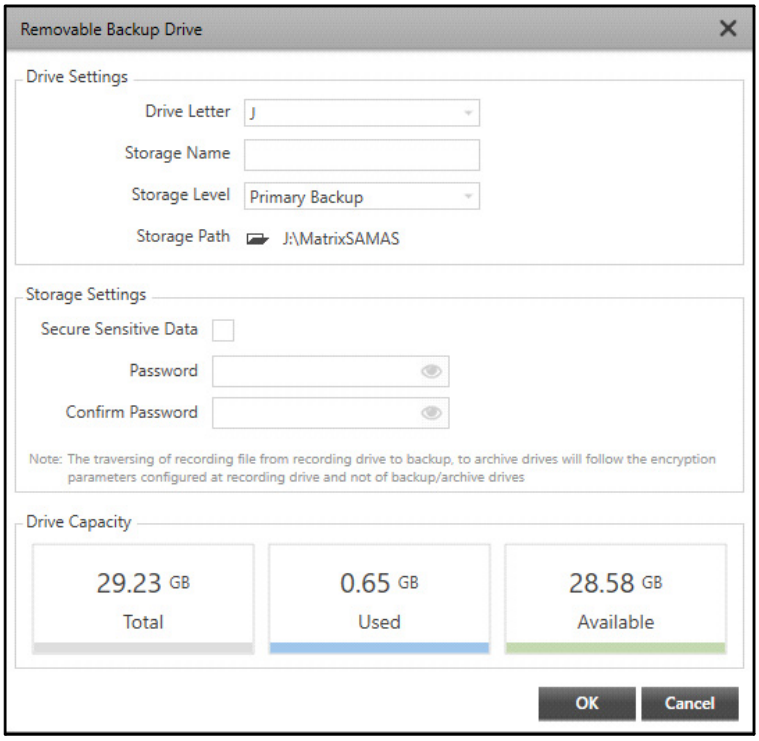
  - Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- Click **OK**.

Removable Drive

- The **Removable Drive** option is enabled when a Removable Storage Drive is configured with the PC.
- Select **Removable Drive** as the **Add Backup Drive** options. The **Drive Settings** pop-up appears.





Configure the following parameters:

Drive Settings

- **Drive Letter:** The Drive Letter is system-defined.
- **Storage Name:** Specify a unique storage name. The configured Removable Drive will be displayed by this name. In Storage Name, you can enter upto 50 characters. Default: Blank.
- **Storage Level**: Select the Storage Level that you wish to assign to the Backup Drive from the drop-down list — Primary Backup, Archive 1 and Archive 2.
- **Storage Path:** Browse a storage path in the selected drive where you wish to store the records. Click **Browse** . It displays all the folders which are in the drive. Select the desired folder.

Storage Settings

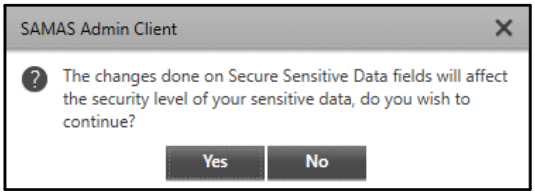
- **Secure Sensitive Data**: Select the check box to enable the encryption of sensitive data. Sensitive data includes — Recordings (All types of recording), Backup and Archives Recording, Snapshots stored through CREAM Module. It will be mandatory to decrypt the data while accessing it from SAMAS Media Player using password.
- **Password**: Specify a Password for encryption. In Password, you can enter upto 128 characters. Valid Range: 12-128. Default: Blank. Make sure you note down the created password at a secure place for future reference as the files will be decrypted in SAMAS Media Player using this password. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- **Confirm Password**: Re-enter the password to confirm. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

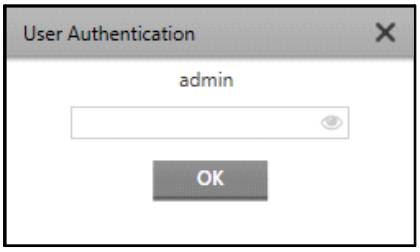
Drive Capacity

- **Total Space:** This displays total space of the Removable Drive in GBs.
- **Used Space:** This displays the space of the Removable Drive that has been used in GBs.
- **Available Space:** This displays the remaining space available for storing records in the Removable Drive in GBs.

- Click **OK** to save the Backup Drive configurations. The following pop-up will appear.



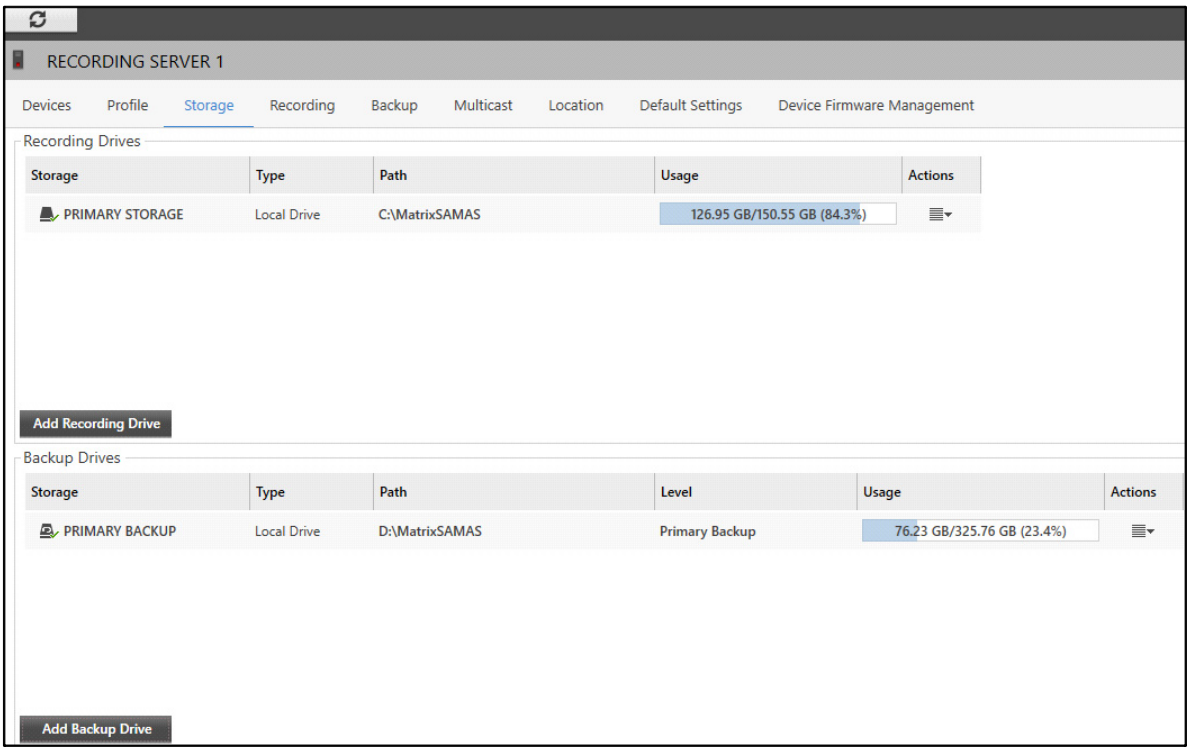
- Click **Yes** to continue. The **User Authentication** pop-up will appear.



- Specify the login password to authenticate. Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

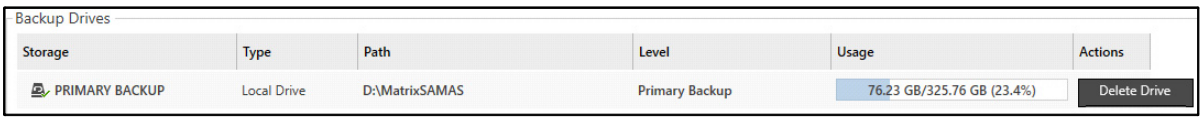
- Click **OK**.

The configured Backup Drives appear in the Backup Drives list.



The following details are displayed for the configured Recording Drives — Storage, Type, Path, Level, Usage and Actions.

- Click **Actions** . The **Delete Drive** option appears.



- **Delete Drive**: Click Delete Drive to delete the configured Backup Drive. The drive will be removed from the Backup Drives list.

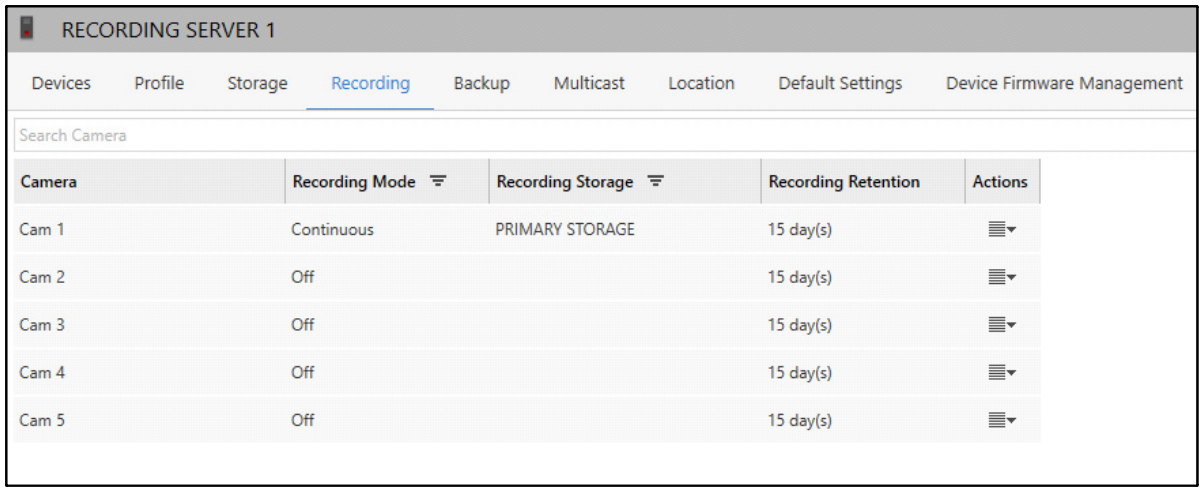
Once the storage drives are configured you can view as well as configure the recording details and backup details of a particular camera in the Recording Server from **Recording** and **Backup** tabs respectively.

Recording

This tab enables you to view and configure the Recording Settings of the added cameras. This tab displays a list of the cameras and their Recording details. You can also search for a camera using the **Search Camera** option.

To configure Recording Settings,

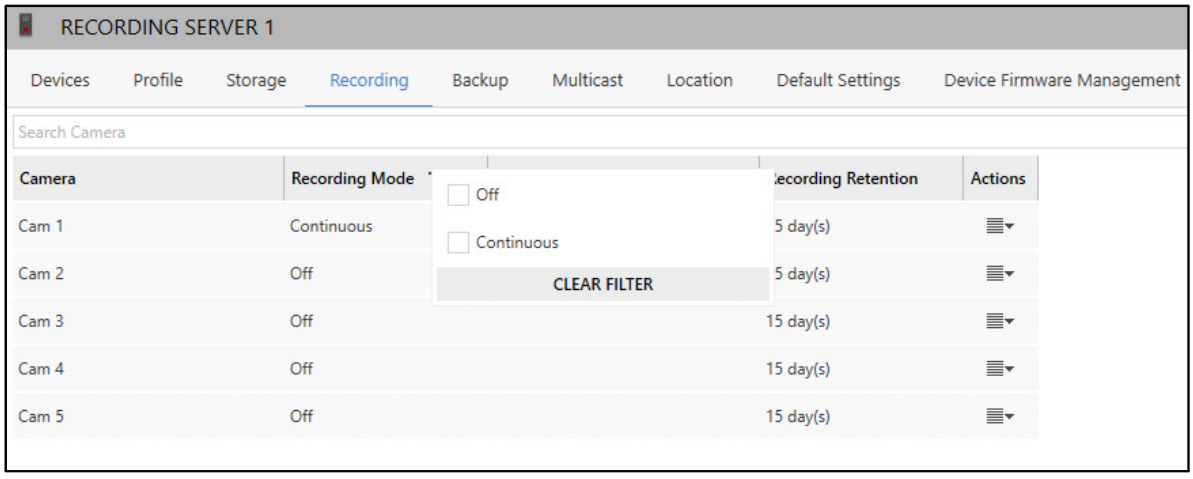
- Click the **Recording** tab.



The Recording details displayed are — Camera, Recording Mode, Recording Storage, Recording Retention and Actions.

Sort and Filter Devices

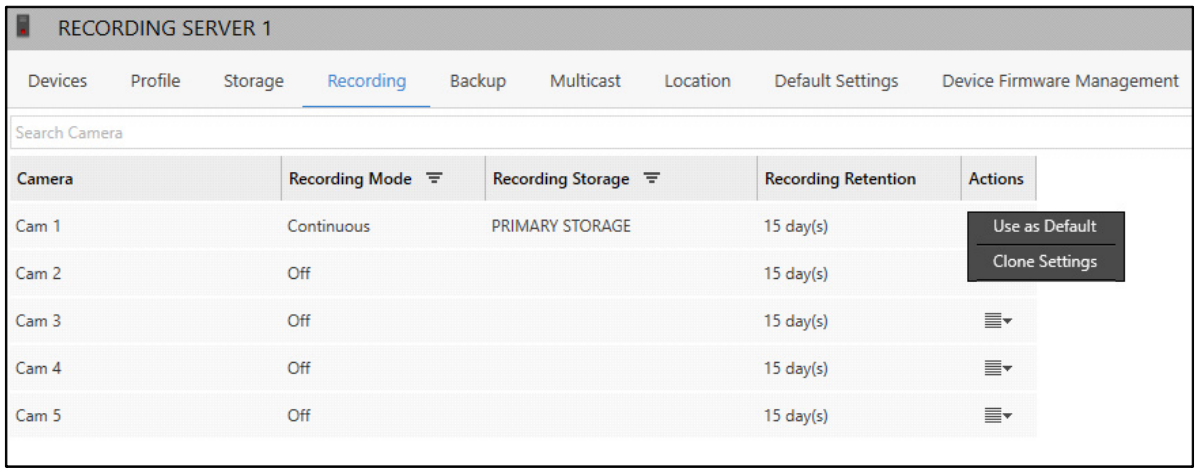
- You can **Sort** as well as **Filter** the devices.
- To Sort, click on the desired heading according to which you wish to sort the devices — Camera, Recording Mode, Recording Storage, Recording Retention.
- To Filter the devices, according to the **Recording Mode** or **Recording Storage**, click **Filter** .



- Select the desired check boxes from the **Recording Mode** and **Recording Storage** filter list. The cameras are sorted as per the set filters.
- Click **Clear Filter** to clear all the filters.

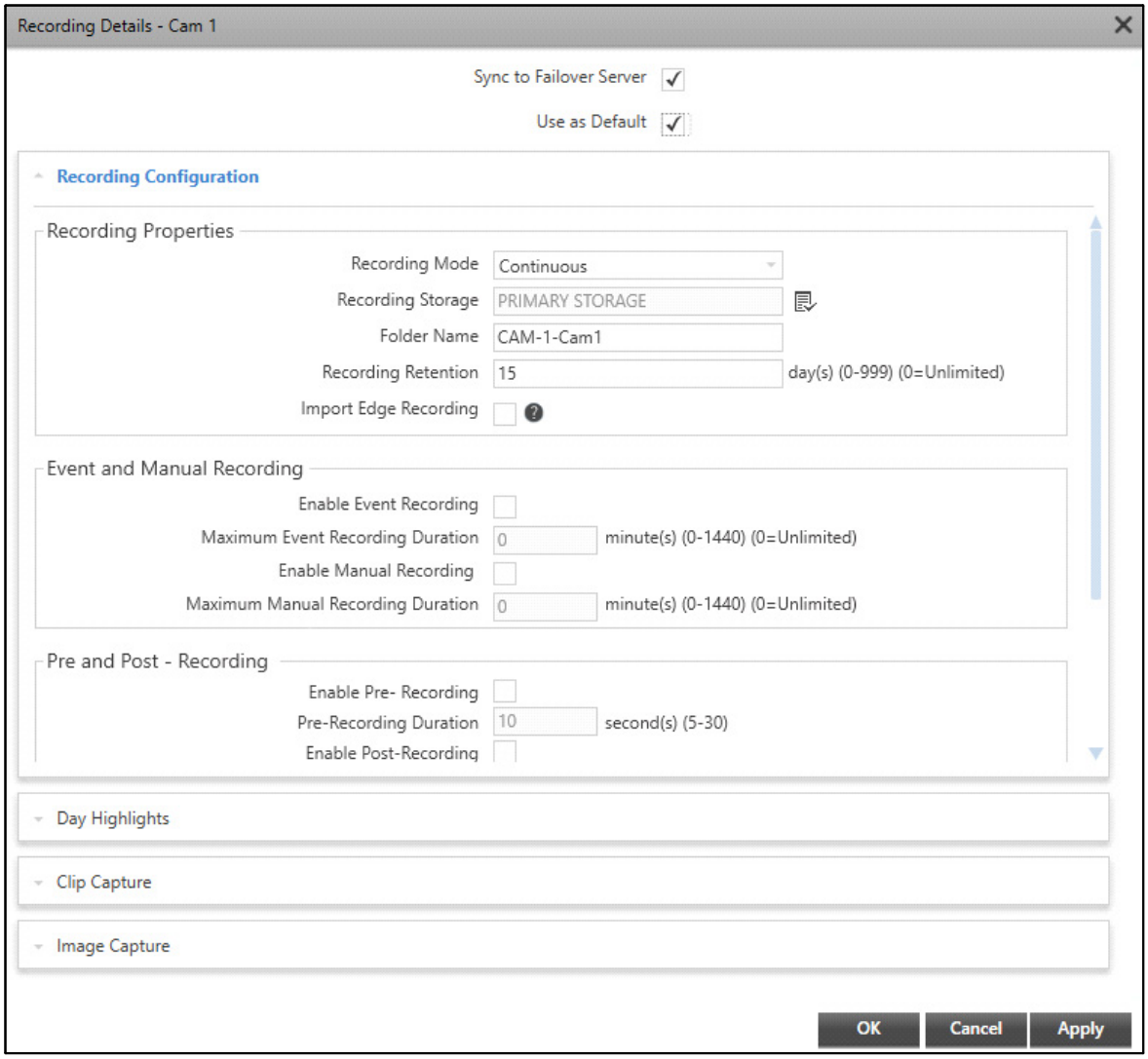
Use as Default and Clone Settings

- You can set the individual camera Recording Settings as default or clone the settings.
- Click **Actions** of the desired camera. The **Use as Default** and **Clone Settings** options appear.



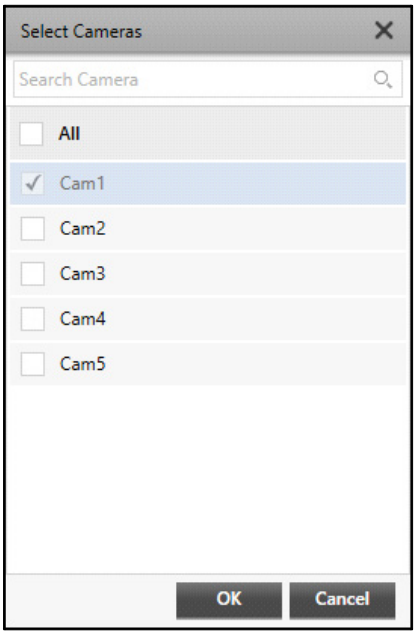
- **Use as Default**: Select Use as Default if you wish to use this camera's Recording Settings as the default. These settings will be automatically reflected in the **Recording** section of the **Default Settings** tab.

    - To disable this option, double click the camera. The **Recording Details** pop-up appears.



- Clear the **Use as Default** check box. Click **OK** to save.

- **Clone Settings**: Select Clone Settings if you wish to copy the camera's Recording Settings to other cameras. On selecting Clone Settings, the **Select Cameras** pop-up appears.



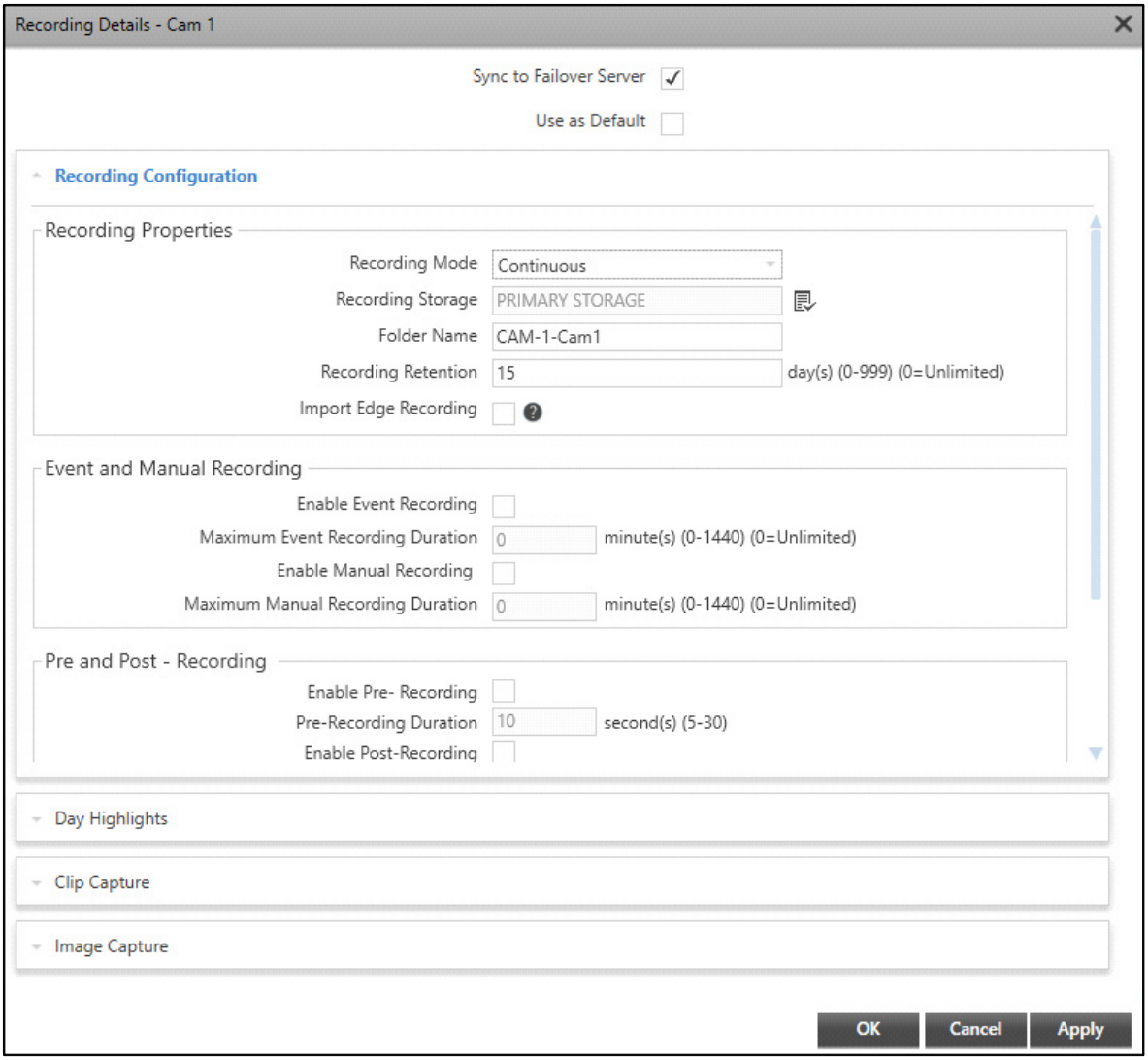
- Select the cameras to which you wish to clone the settings.

- Click **OK** to confirm or click **Cancel** to discard.

Configuring the Recording Settings for a particular camera

- You can also view and configure the Recording Settings for a particular camera.

- To do so, double click on the desired camera whose recording details are to be viewed. The **Recording Details** pop-up appears.



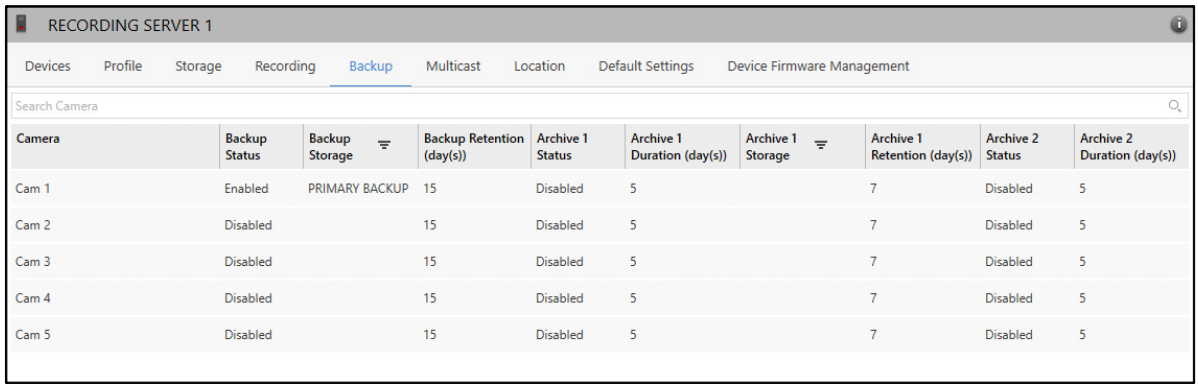
The Recording Details pop-up consists of the following collapsible panels — Recording Configuration, Day Highlights, Clip Capture and Image Capture. To view details and configure the recording for a camera, refer to “Recording”.

Backup

This tab enables you to view and configure the Backup Settings of the added devices. This tab displays a list of cameras and their Backup details. You can search for a camera using the **Search Camera** option.

To configure Backup Settings,

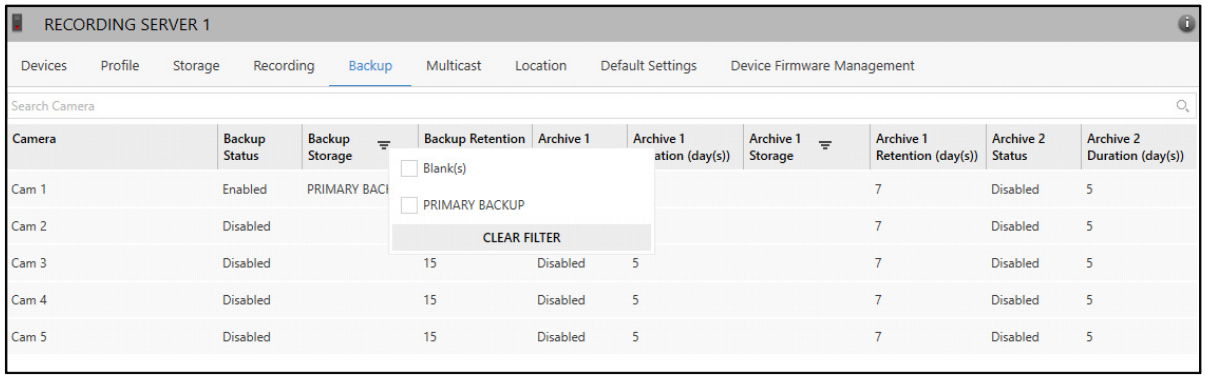
- Click the **Backup** tab.



The Backup details displayed are — Camera, Backup Status, Backup Storage, Backup Retention (day(s)), Archive 1 Status, Archive 1 Duration (day(s)), Archive 1 Storage, Archive 1 Retention (day(s)), Archive 2 Status, Archive 2 Duration (day(s)), Archive 2 Storage, Archive 2 Retention (day(s)), Evidence Lock Retention (day(s)) and Actions.

Sort and Filter Devices

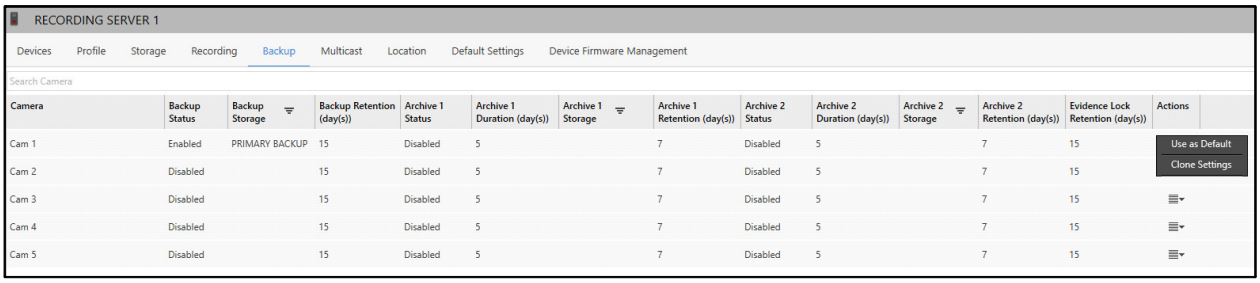
- You can **Sort** as well as **Filter** the devices.
- To Sort, click on the desired heading according to which you wish to sort the devices — Camera, Backup Status, Backup Storage, Backup Retention (day(s)), Archive 1 Status, Archive 1 Duration (day(s)), Archive 1 Storage, Archive 1 Retention (day(s)), Archive 2 Status, Archive 2 Duration (day(s)), Archive 2 Storage, Archive 2 Retention (day(s)), Evidence Lock Retention (day(s)).
- To filter the devices, according to the **Backup Storage** or **Archive 1 Storage** or **Archive 2 Storage**, click **Filter** .



- Select the desired check boxes from the **Backup Storage** or **Archive 1 Storage** or **Archive 2 Storage** filter list. The cameras are filtered as per the set filters.
- Click **Clear Filter** to clear all the filters.

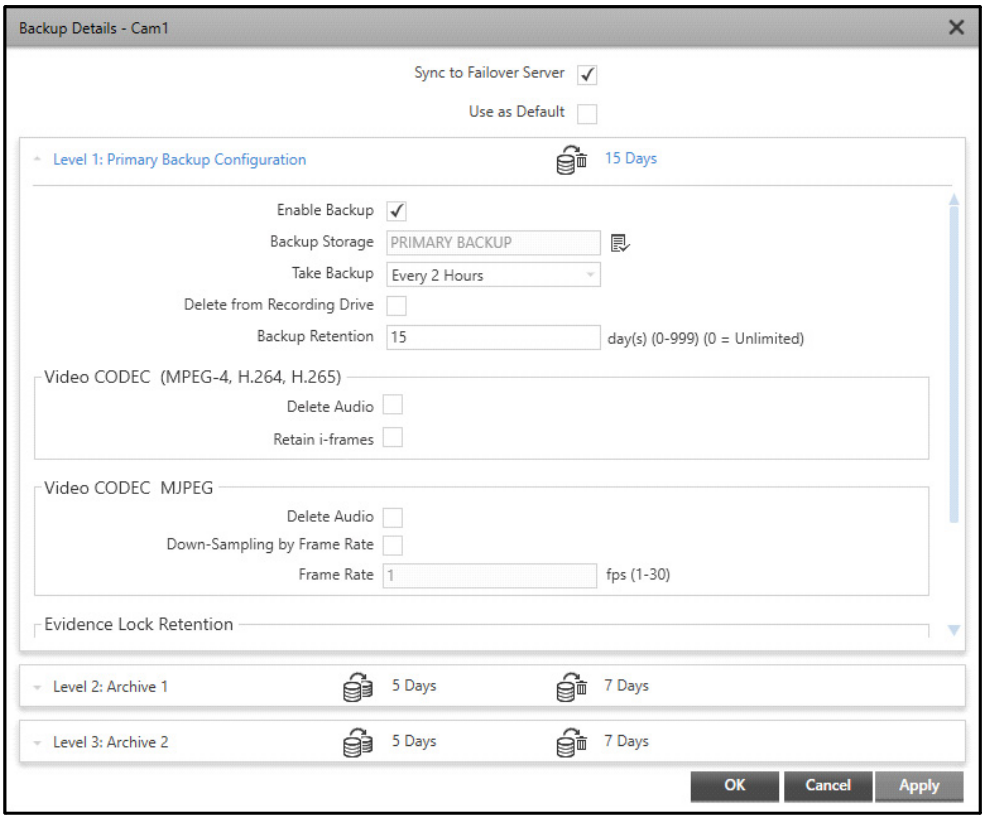
User as Default and Clone Settings

- You can set the individual camera Backup Settings as default or clone the settings.
- Click **Actions** for the desired camera. The **Use as Default** and **Clone Settings** options appear.



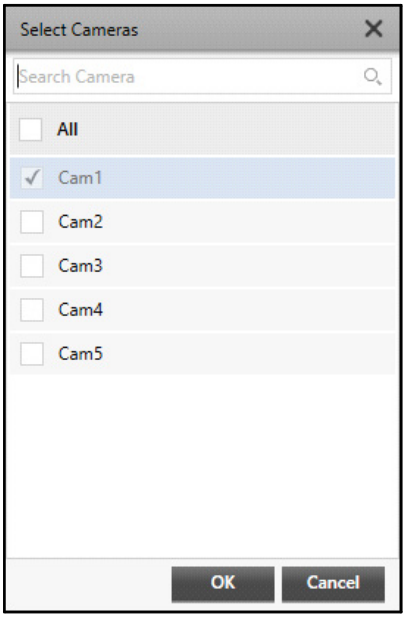
- **Use as Default**: Select Use as Default if you wish to use this camera's Backup Settings to be used as default. These settings get copied in the **Backup** section of the **Default Settings** tab.

    - To disable this option, double click the camera. The **Backup Details** pop-up appears.



    - Clear the **Use as Default** check box. Click **OK** to save.

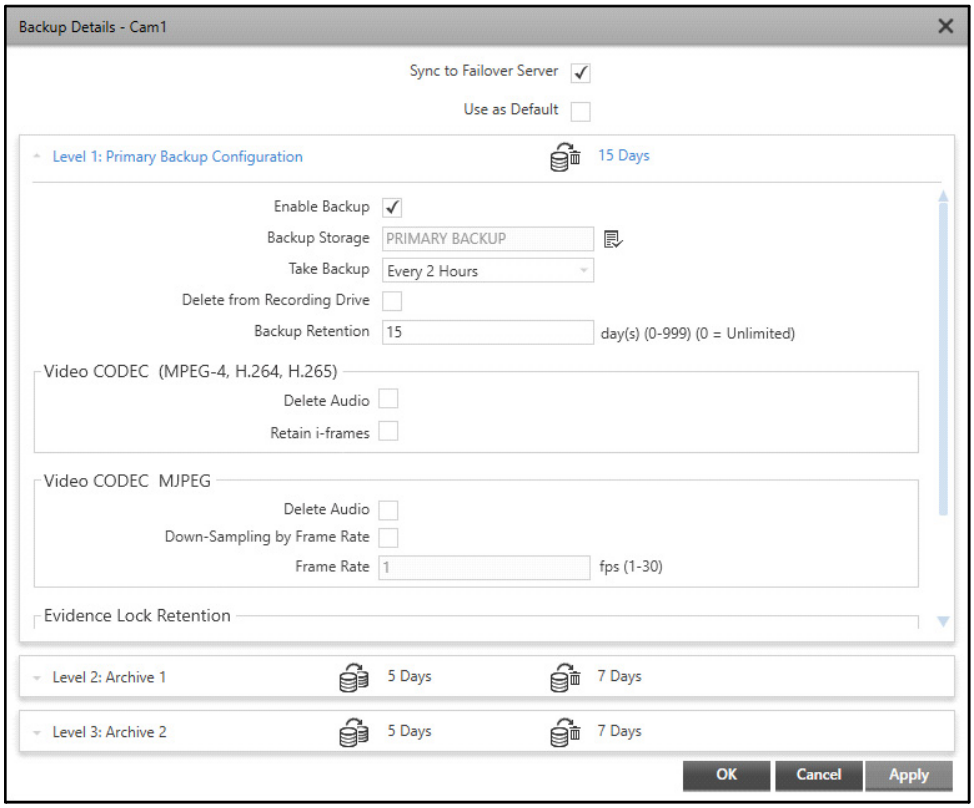
- **Clone Settings**: Select Clone Settings if you wish to copy the camera's Backup Settings to other cameras. On selecting Clone Settings, the **Select Cameras** pop-up appears.



- Select the cameras to which you wish to clone the settings.
- Click **OK** to confirm or click **Cancel** to discard.

Configuring the Backup Settings for a particular camera

- You can view as well as configure the Backup Settings for a particular camera.
- To do so, double-click on the desired camera whose recording details are to be viewed. The **Backup Details** pop-up appears.



The Backup Details pop-up consists of the following collapsible panels — Level 1: Primary Backup Configuration, Level 2: Archive 1 and Level 3: Archive 2. To view details and configure the backup for a camera, refer to “Backup”.

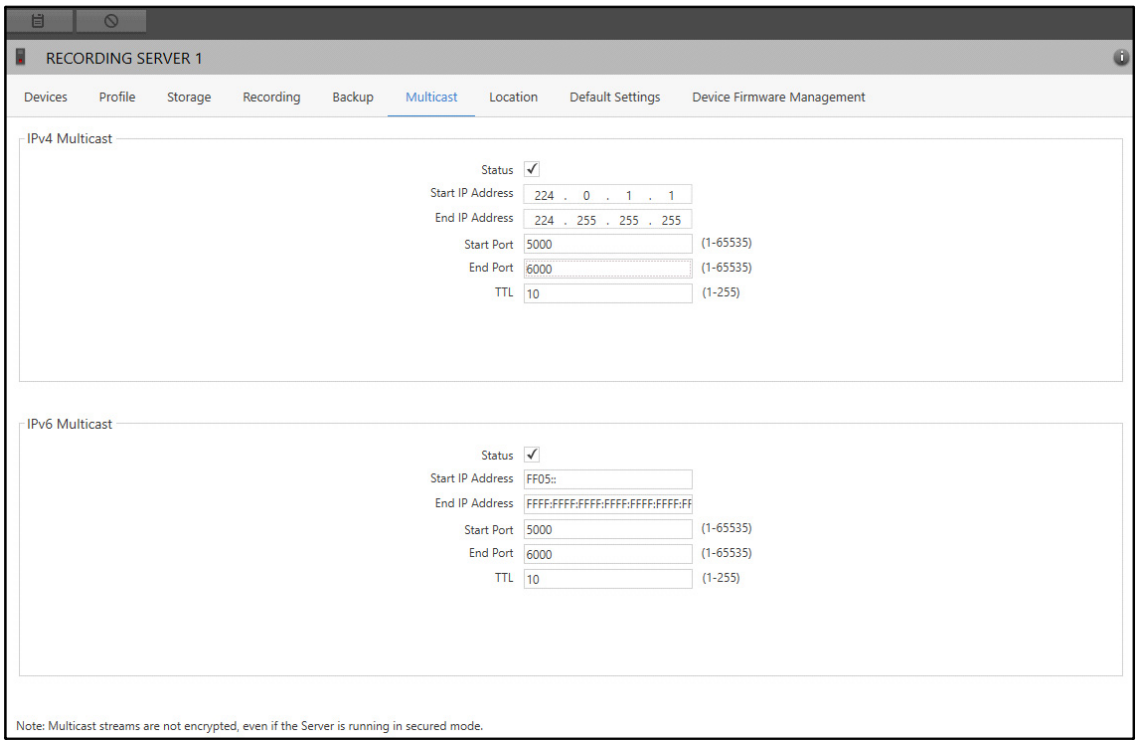
Multicast

Multicasting enables the optimization of network bandwidth consumption between the Recording Server and Smart Client/IVA Server. This tab enables you to view and configure the Multicast settings.

Multicast streams are not encrypted, even if the Recording Server is running in SSL mode.

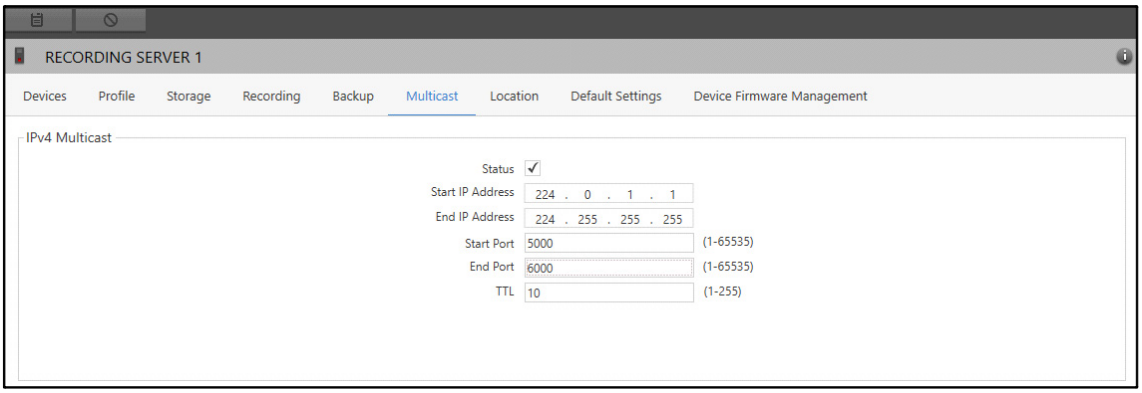
To configure Multicast settings,

- Click the **Multicast** tab.



The Multicast tab consists of two sections — “IPv4 Multicast” and “IPv6 Multicast”.

IPv4 Multicast



Configure the following parameters:

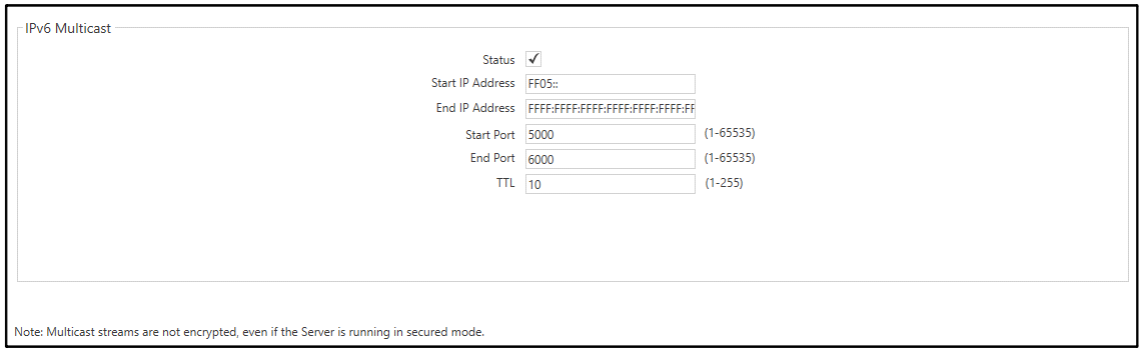
- **Status**: Select the check box to enable Multicasting. If this check box is disabled, the Recording Server will provide the stream to Smart Client/IVA Server in Unicasting.
- **Start IP Address**: Specify the Start IP Address that is to be used for Multicasting. In Start IP Address, you can enter upto 15 characters. Default: 224.0.0.1
- **End IP Address**: Specify the End IP Address that is to be used for Multicasting. The Multicasting communication will take place within this range. In End IP Address, you can enter upto 15 characters. Default: 224.255.255.255

The Start and End IP Address can be any Class D IP Addresses, ranging from 224.0.0.0 to 239.255.255.255.

IP Address Range 224.0.1.1 to 224.255.255.255 can be used for Multicasting within the same subnet. For Cross Network Multicasting, all other IP Addresses can be used.

- **Start Port**: Specify the Start Port to be used for Multicasting. Valid Range: 1-65535. Default: 5000.
- **End Port**: Specify the End Port that is to be used for Multicasting. Valid Range: 1-65535. Default: 6000.The Multicasting communication will take place between the Start and End Port range.
- **TTL**: Specify the Time-to-Live (TTL) value. This defines the number of sub-networks a packet will be allowed to cross and after this the packet will be dropped. For example: If TTL is set as 4, a packet will be allowed to cross 4 sub-networks and then the packet will be dropped. Valid Range: 1-255. Default: 10.
- Click **Save** to save the settings or **Cancel** to discard.

IPv6 Multicast



Configure the following parameters:

- **Status**: Select the check box to enable Multicasting. If this check box is disabled, the Recording Server will provide the stream to Smart Client/IVA Server in Unicasting.
- **Start IP Address**: Specify the Start IP Address that is to be used for Multicasting. In Start IP Address, you can enter upto 39 characters. Default: FF05::
- **End IP Address**: Specify the End IP Address that is to be used for Multicasting. The Multicasting communication will take place within this range. In End IP Address, you can enter upto 39 characters. Default: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

  IPv6 Address Range FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF can be used for Multicasting within same subnet. For Cross Network Multicasting all other IPv6 Addresses can be used.
- **Start Port**: Specify the Start Port to be used for Multicasting. Valid Range: 1-65535. Default: 5000.
- **End Port**: Specify the End Port that is to be used for Multicasting. Valid Range: 1-65535. Default: 6000.The Multicasting communication will take place between the Start and End Port range.

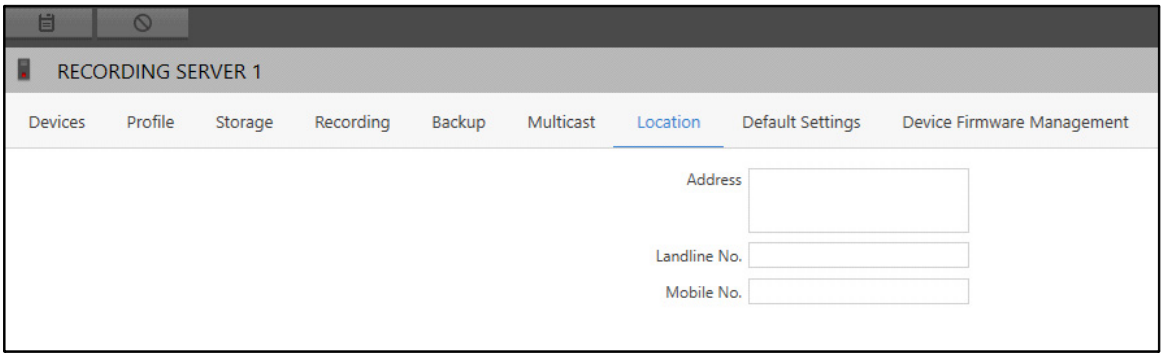
- **TTL**: Specify the Time-to-Live (TTL) value. This defines the number of sub-networks a packet will be allowed to cross and after this the packet will be dropped. For example: If TTL is set as 4, a packet will be allowed to cross 4 sub-networks and then the packet will be dropped. Valid Range: 1-255. Default: 10.
- Click **Save** to save the settings or **Cancel** to discard.

Location

This tab enables you to view and configure the location information of a Recording Server.

To configure the Location,

- Click the **Location** tab.



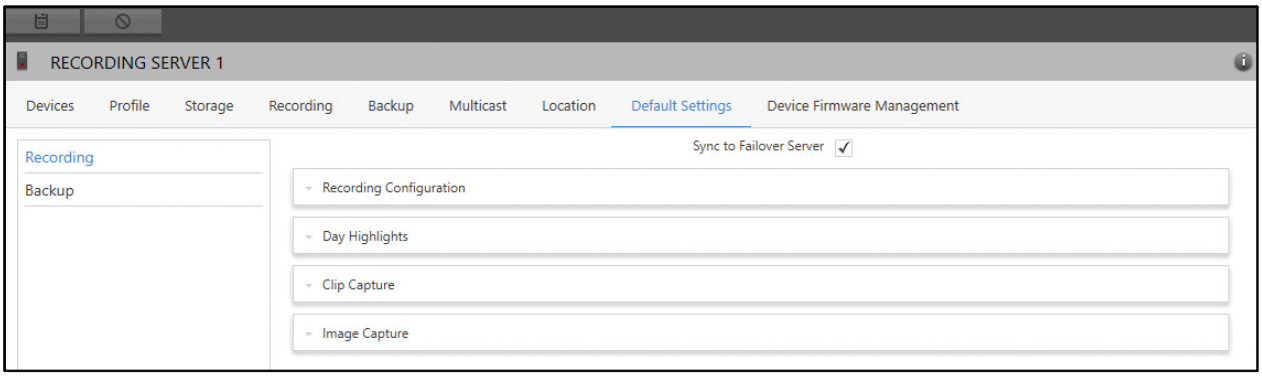
The configurations of Location Settings in Recording Server are similar to that of the Management Server. For details, refer to “Location”.

Default Settings

This tab enables you to configure the Default Recording and Backup Settings for the new cameras added to the Recording Server.

To configure Default Settings,

- Click the **Default Settings** tab.



- Select the **Sync to Failover Server** check box if you wish to sync the Recording Server’s configuration with the Failover Server.

The Default Settings tab contains two sections — **Recording** and **Backup**. The Recording section contains four collapsible panels — Recording Configuration, Day Highlights, Clip Capture and Image Capture. The Backup section contains three collapsible panels — Level 1: Primary Backup Configuration, Level 2: Archive 1 and Level 3: Archive 2.

For detailed Recording and Backup configurations, refer to "Recording" and "Backup".

Device Firmware Management

This tab enables you to upgrade the firmware of the cameras added to the Recording Server. You can upload the firmware files and can either schedule the firmware upgrade or else upgrade the firmware immediately by creating tasks as per your convenience. This cuts down the hassle of upgrading the firmware of multiple cameras individually. You can also view the status of these tasks from the "Upgrade Tasks" page.

When you upgrade the camera firmware from this tab, the configuration on the camera webpage will be overwritten with the configuration set here for the selected cameras. Hence, make sure you note down the configurations of "Auto Firmware Upgrade" tab for re-configuring the same later.

If you wish to restore the Auto Firmware Upgrade configuration of the cameras as per their original configurations, you need to re-configure the parameters in "Auto Firmware Upgrade" with the information you have already noted earlier. On saving the Auto Firmware Upgrade configuration, the same will be set on the camera webpage.



To ensure smooth functioning of this feature, make sure the Admin Client, Recording Server and Management Server are upgraded to the latest and same version.

When SAMAS is upgraded with firmware version V6R4 and later, the Recording Server will have the latest Camera Firmwares — IPCamera_S02_Firmware and IPCamera_S05_Firmware.

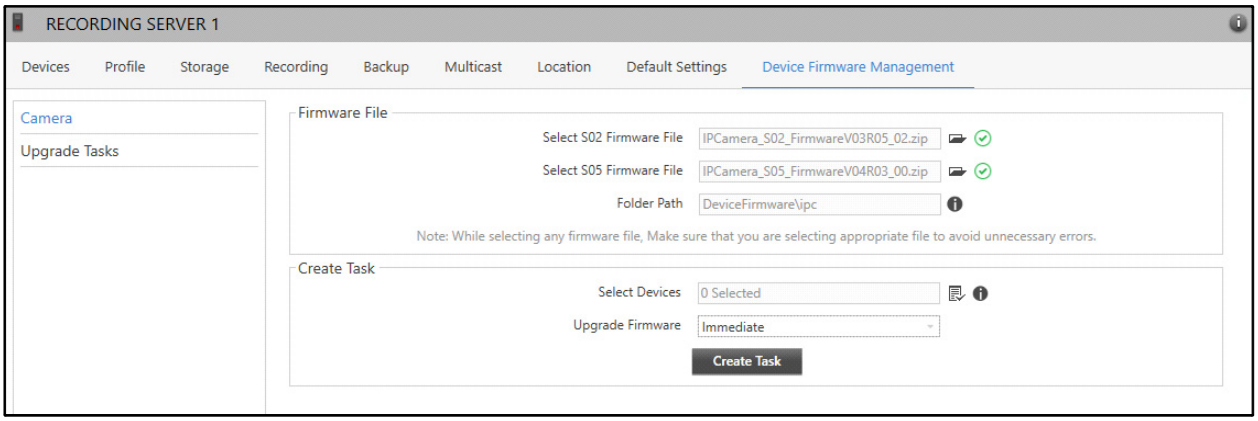
If your cameras have a version that is 2 or more versions lower than the default firmware version available with SAMAS, you need to manually upgrade the cameras. Contact Matrix Technical Support Team.

If you wish to upgrade the cameras to any other version than the default firmware version available with SAMAS, make sure you place the camera firmware files at the desired location in your PC.

If the Recording Server is running on SSL mode, then firmware upgrade process will take place in secure mode. If the Recording Server is not running on SSL Mode, then firmware upgrade process will take place in non-secure mode.

To configure Device Firmware Management,

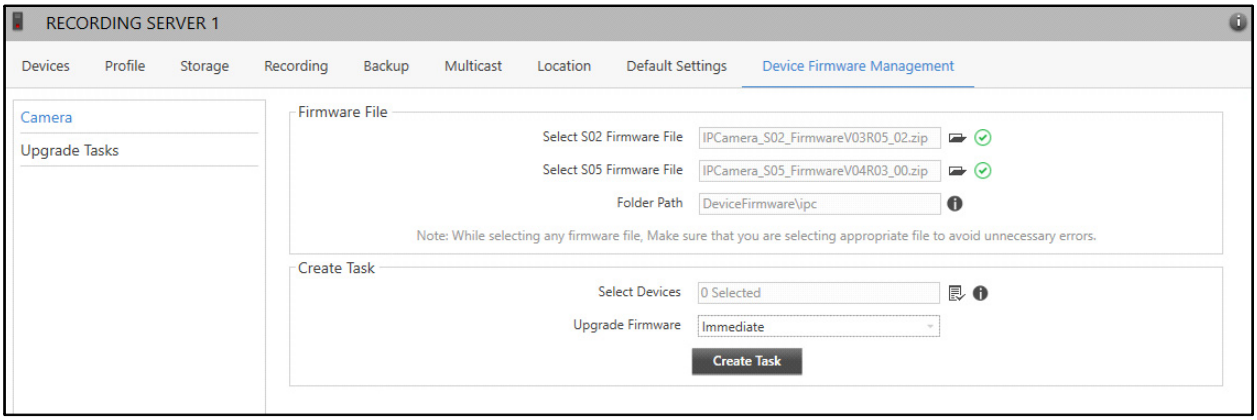
- Click the **Device Firmware Management** tab.



The Device Firmware Management tab consists of two pages — “Camera” and “Upgrade Tasks”.

Camera

The Camera page appears by default.



The Camera page consists of two sections — “Firmware File” and “Create Task”.

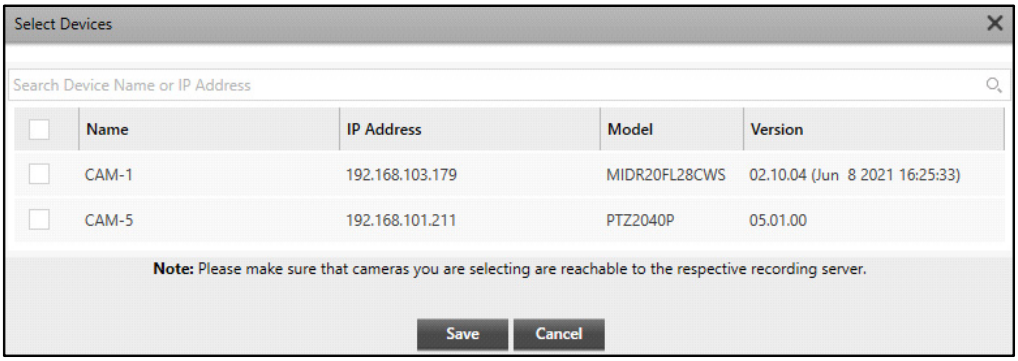
Firmware File

- **Select S02 Firmware File**: By default, the latest camera firmware file is stored in the Recording Server when you install SAMAS. Click **Browse** . It displays all folders which are in the drive. Select the desired firmware file. The file can be of upto 50 KB. Valid Format: .zip.The uploaded file will overwrite the existing firmware file at the location displayed under Folder Path.
- **Select S05 Firmware File**: By default, the latest camera firmware file is stored in the Recording Server when you install SAMAS. Click **Browse** . It displays all folders which are in the drive. Select the desired firmware file. The file can be of upto 50 KB. Valid Format: .zip.The uploaded file will overwrite the existing firmware file at the location displayed under Folder Path.
- **Folder Path**: It displays the folder path of the Recording Server where the camera firmware files are stored when you install SAMAS.

Once a firmware file is uploaded successfully, the name of the firmware file will appear against the respective firmware file along with a icon.

Create Task

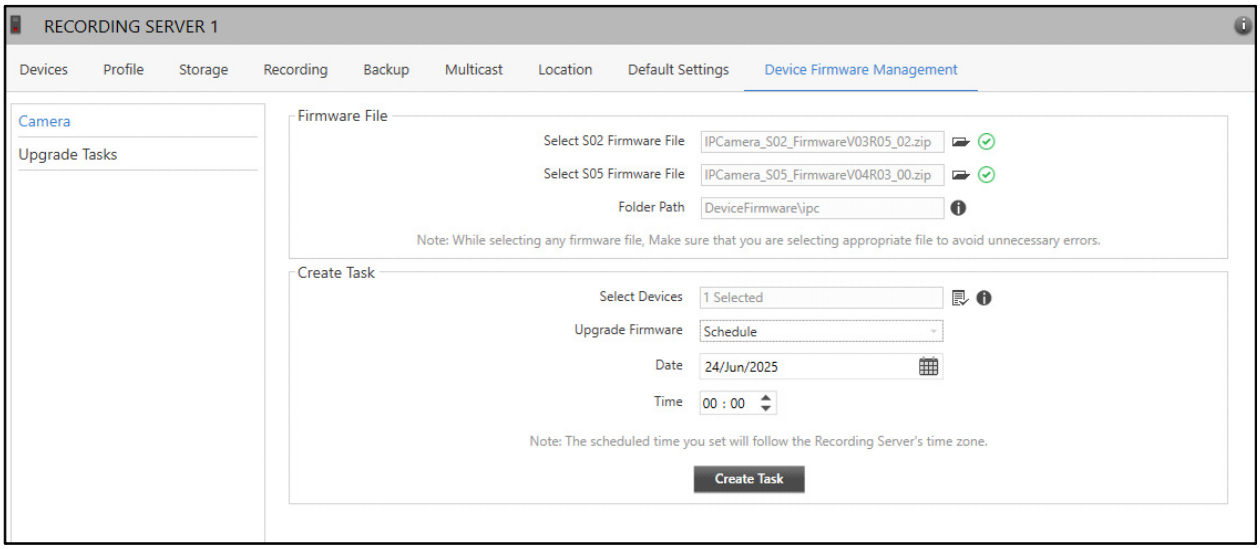
- **Select Devices**: Select the desired cameras whose firmware you wish to upgrade using the **Select Devices** picklist.
    - Click **Select Devices** picklist. The **Select Devices** pop-up appears.



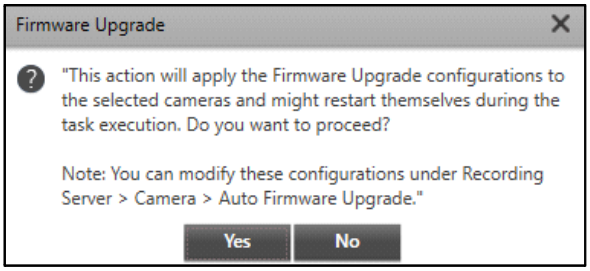
    - All the cameras added to the Recording Server via Brand and Model method appear in the list. The details displayed are — Name, IP Address (IPv4/IPv6), Model and Version. You can also search cameras using the **Search Device Name or IP Address** search bar. Select the check boxes of the cameras whose firmware you wish to upgrade.
    - Click **Save** to select the cameras. The number of selected cameras appears against **Select Devices**.
- **Upgrade Firmware**: Select the desired option for upgrading the firmware for the selected cameras from the drop-down list — Immediate, Schedule.

  If you select Upgrade Firmware as **Immediate**, then on clicking **Create Task**, the task will be created and its execution will begin immediately.

  If you select Upgrade Firmware as **Schedule**, configure the following parameters:
- **Date**: Select the date on which you wish to schedule the firmware upgrade from the calendar.
- **Time**: Specify the time at which you wish to schedule the firmware upgrade.



- Click **Create Task**. The **Firmware Upgrade** pop-up appears.

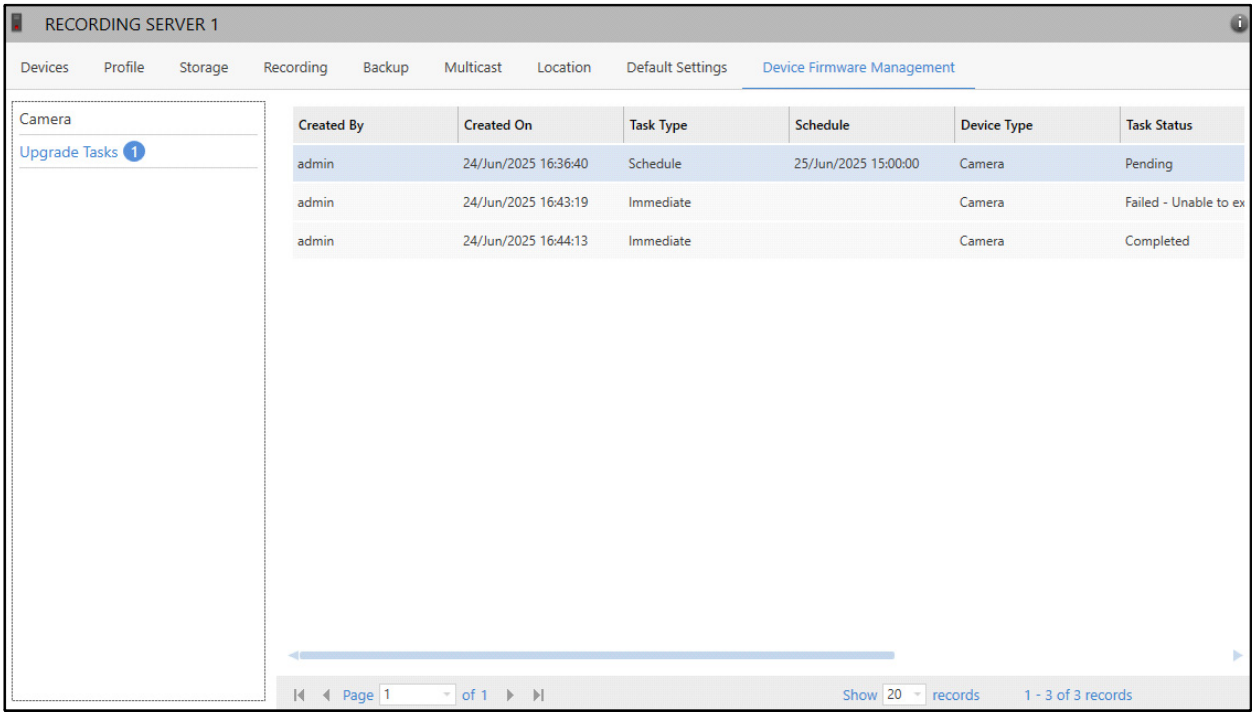


- Click **Yes** to confirm or click **No** to discard. If you click **Yes**, the firmware upgrade task will be created and will appear on "Upgrade Tasks" page. You can view the task details from "Upgrade Tasks" page.

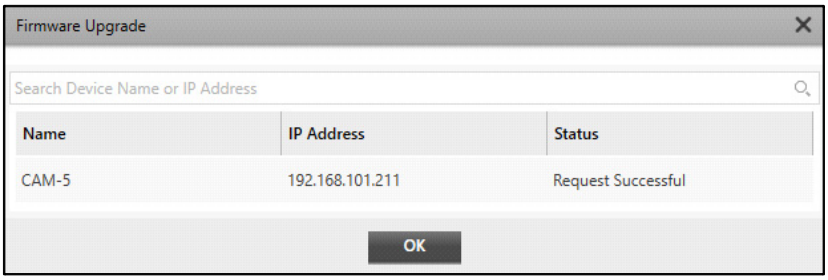
Upgrade Tasks

All the firmware upgrade tasks created from "Camera" page appear on this page. The number of tasks created is also displayed. Once the tasks are executed, the number is updated as per the Pending tasks.

- Click **Upgrade Tasks**.



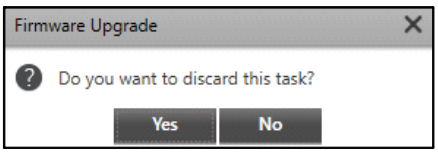
- All the tasks created from Camera page appear here. The details displayed are — Created By, Created On, Task Type, Schedule, Device Type, Task Status and Check Details. You can view the details of each task.
- Click **Check Details** corresponding to the desired task. The **Firmware Upgrade** pop-up appears.



- All the cameras selected for the firmware upgrade task appear in a list. The details displayed are — Name, IP Address (IPv4/IPv6), Status of the task.

You can also discard a task that is in Pending Status. To do so,

- Click **Discard** . The **Firmware Upgrade** pop-up appears.



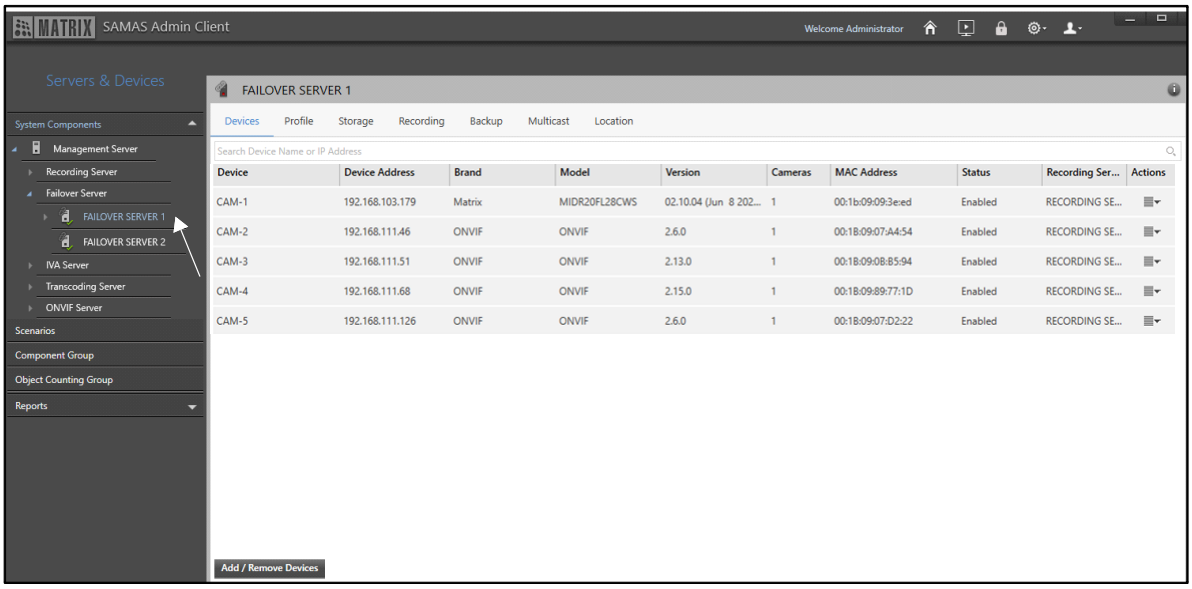
- Click **Yes** to confirm or click **No** to discard. If you click **Yes**, the task will be discarded and not executed.

Failover Server Configuration

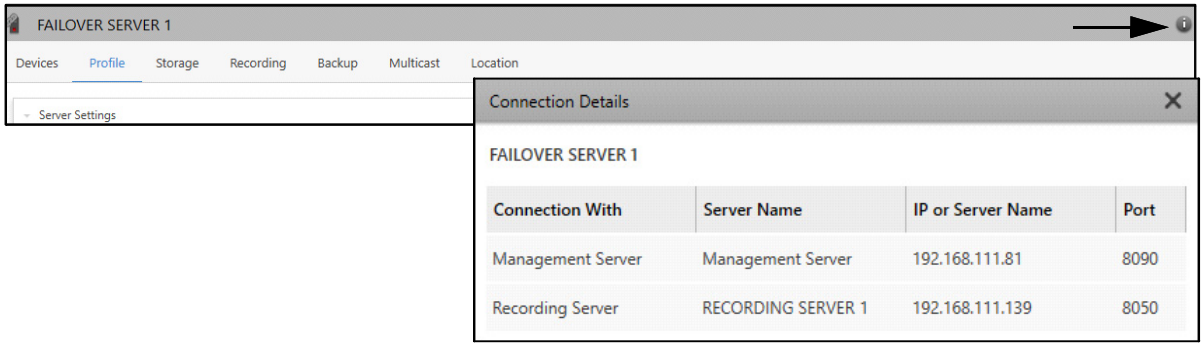
To configure a Failover Server, it must be activated first. The Server has to be set as Failover Server from the **Server** collapsible panel on the **Management Server** page. To activate a Failover Server, refer to “Assigning Server as Recording Server or Failover Server”.

To configure a Failover Server,

- Click **Servers & Devices > System Components > Failover Server**.
- All the Failover Servers of the system appear. The entries can be sorted. To do so, click on the desired parameter in the header row. An arrow ▲ icon appears. Click on it. Entries can be sorted in ascending or descending order.
- Select the desired Failover Server.



- To view the **Connection Details** of the Failover Server, click **Connection Details**  at the top right corner of the Failover Server page. It displays the connection details of the Failover Server with the Management Server and Recording Server. It displays the following details — Connection With, Server Name, IP (IPv4/IPv6) or Server Name and Port.

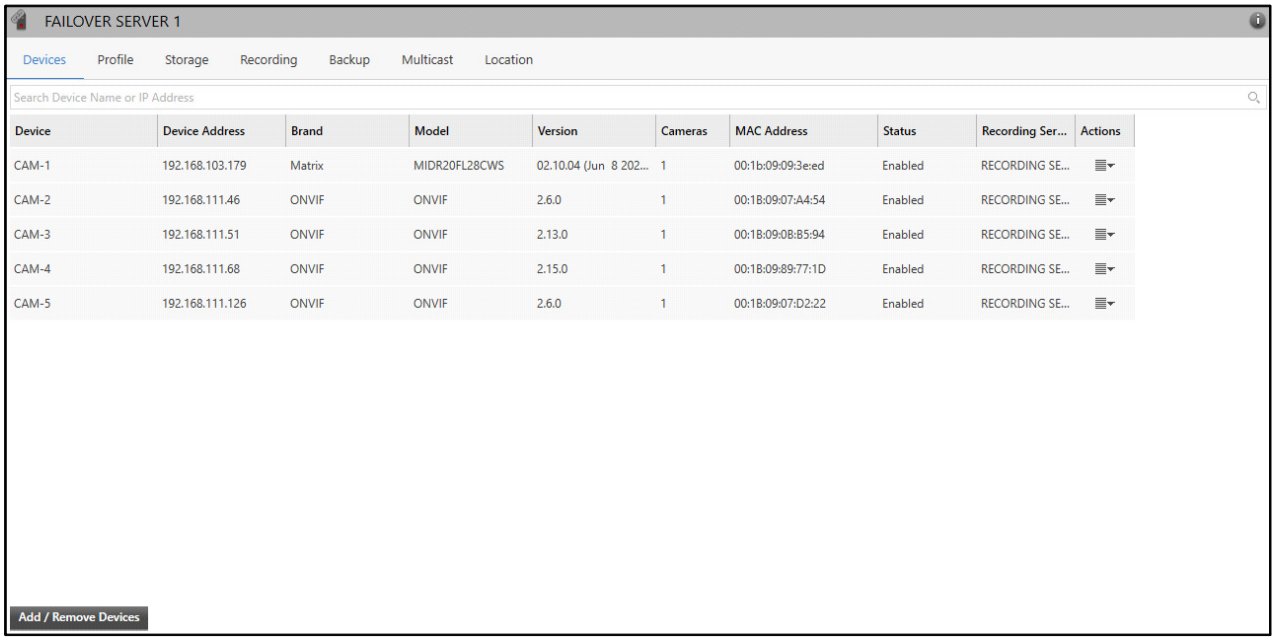


Each Failover Server consists of the following tabs:

- “Devices”
- “Profile”
- “Storage”
- “Recording”
- “Backup”
- “Multicast”
- “Location”

Devices

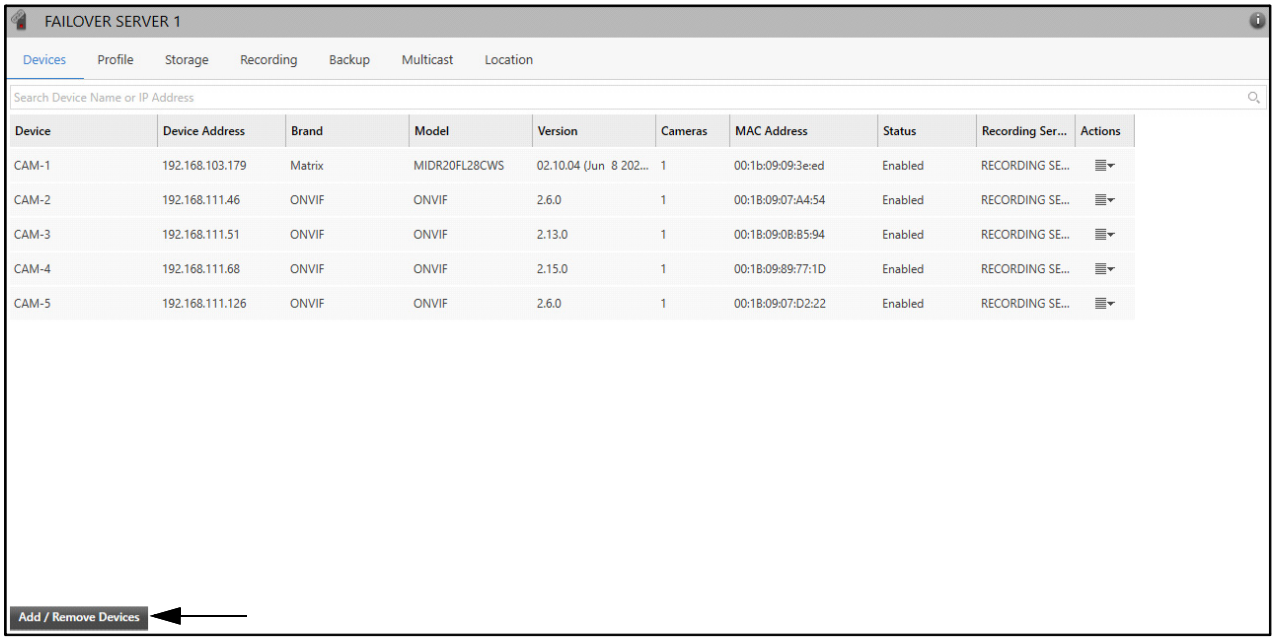
This tab enables you to view, add and remove devices from the Failover Server. The devices added to the Failover Server appear in this tab. You can also search for a device using the **Search Device Name or IP Address** (IPv4/IPv6) search bar. The following device details are displayed — Device, Device Address (IPv4/IPv6), Brand, Model, Version, Cameras, MAC Address, Status, Recording Server and Actions. To know more about the individual device details, refer to “Device Component (FoS)” and “Device Profile (FoS)”.



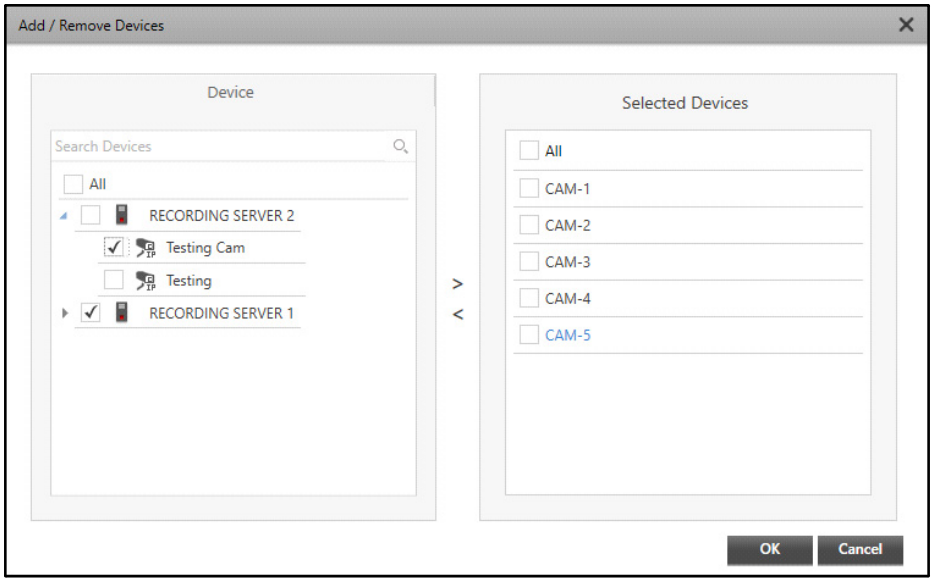
You can assign devices of the Recording Server to a Failover Server once it is activated.

To add or remove a device,

- Select the desired Failover Server. The **Devices** tab appears by default.
- Click **Add/Remove Devices**.

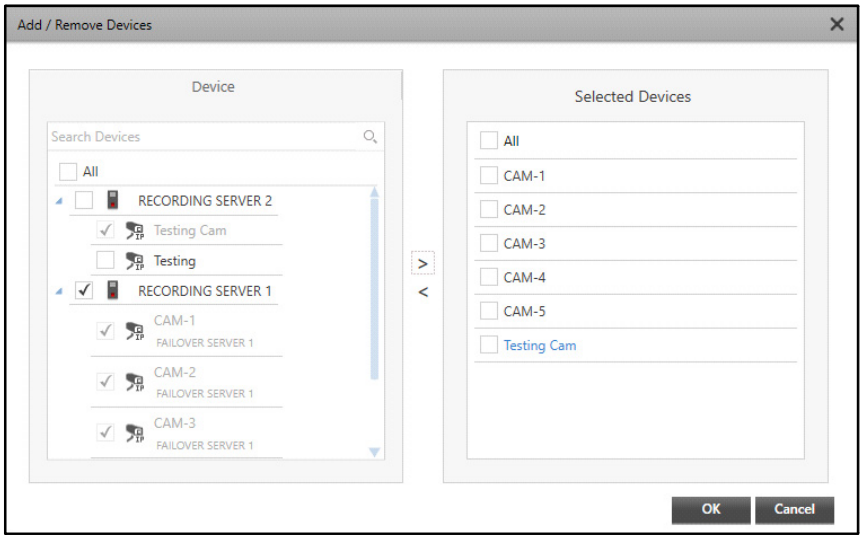


- The **Add/Remove Devices** pop-up appears.



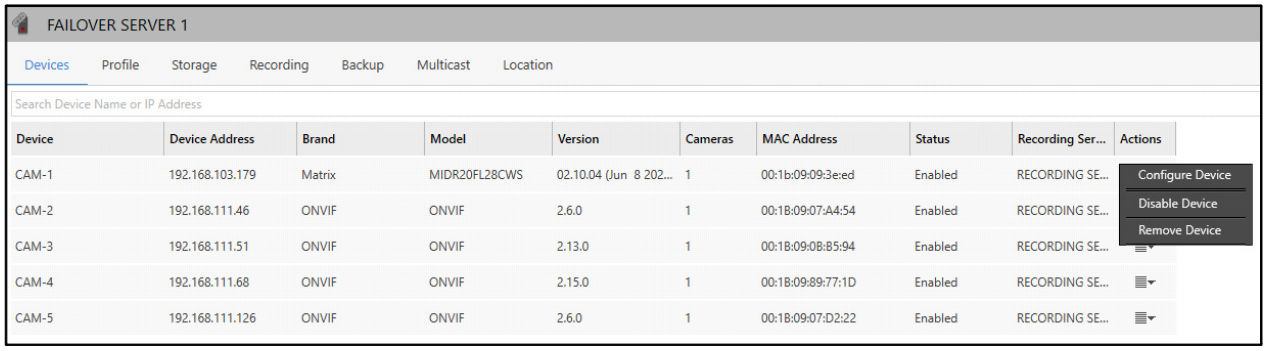
- Select the check boxes of the desired devices you wish to add from the **Device** list. Click the right arrow button to add those devices in the **Selected Devices** list. You can also search for the desired devices using the **Search Device** search bar.

  To remove devices, select the check boxes of the desired devices you wish to remove from the Selected Devices list. Click the left arrow button to remove the devices from the Selected Devices list.



- Click **OK** to confirm or click **Cancel** to discard.

The added devices appear in a list under the Devices tab. Under **Actions** you can configure the device parameters — Configure Device, Disable Device and Remove Device.



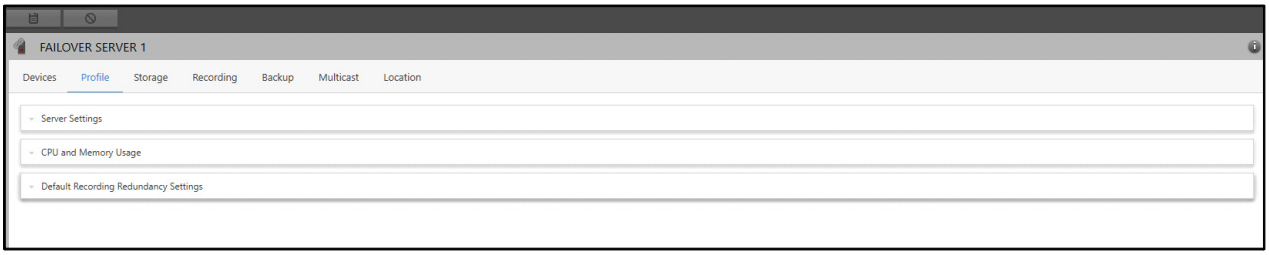
- **Configure Device**: Selecting Configure Device redirects you to the respective device configuration page, where you can view/edit the device configurations.
- **Disable Device**: Selecting Disable Device option will disable the device. This will remove the device from the list of Failover Servers displayed on the left hand side. For enabling it again, click **Action** and select **Enable** Option.
- **Remove Device**: Selecting Remove Device will remove the device from the Failover Server.

Profile

This tab enables you to view and configure Server Settings, CPU and Memory Usage and Default Recording Redundancy Settings.

To configure Profile settings,

- Click the **Profile** tab.



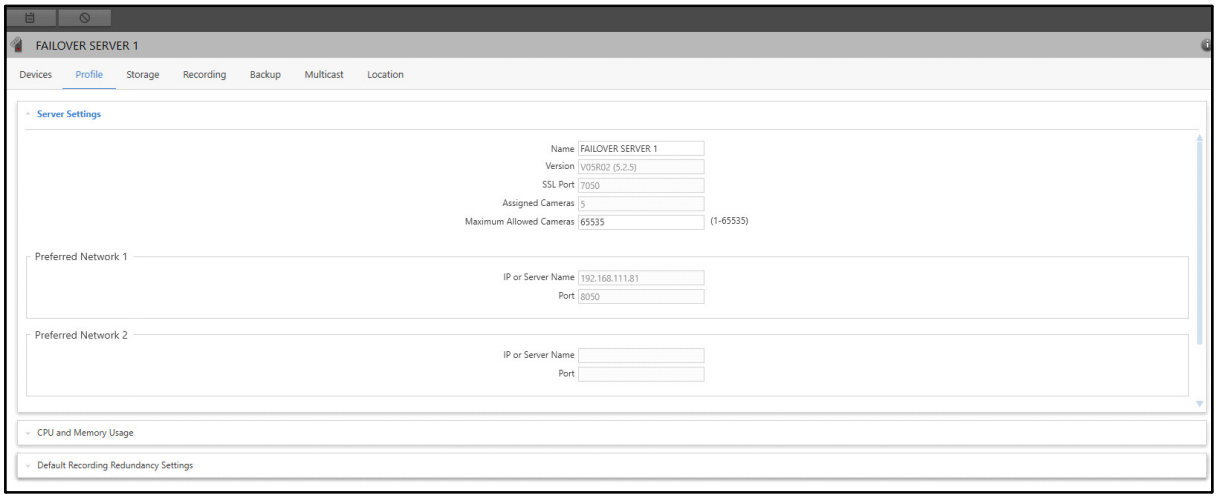
The Profile tab contains three collapsible panels — “Server Settings”, “CPU and Memory Usage” and “Default Recording Redundancy Settings”.

Server Settings

This panel displays the Server Settings of the Failover Server. This panel allows you to configure the Failover Server Name.

To configure the Server Settings,

- Click the **Server Settings** collapsible panel.



This collapsible panel displays the Server Settings and configured Preferred Networks. The parameters of the Server Settings of the Failover Server displayed are — Name, Version, Cameras, SSL Port, Assigned Cameras and Maximum Allowed Cameras.

The Preferred Networks display the IPv4/IPv6 or Server Name and Port of the Failover Server via which the Client (Admin Client, Smart Client, IVA Server) can be connected with Failover Server.

You can configure the following parameters:

- **Name**: Specify a name for the Failover Server. In Name, you can enter upto 50 characters. Default: Name of the system where Failover Server is installed.

- **Maximum Allowed Cameras**: Specify the number of cameras allowed to be configured with the Failover Server. Valid Range: 1-65535. Default: 65535.

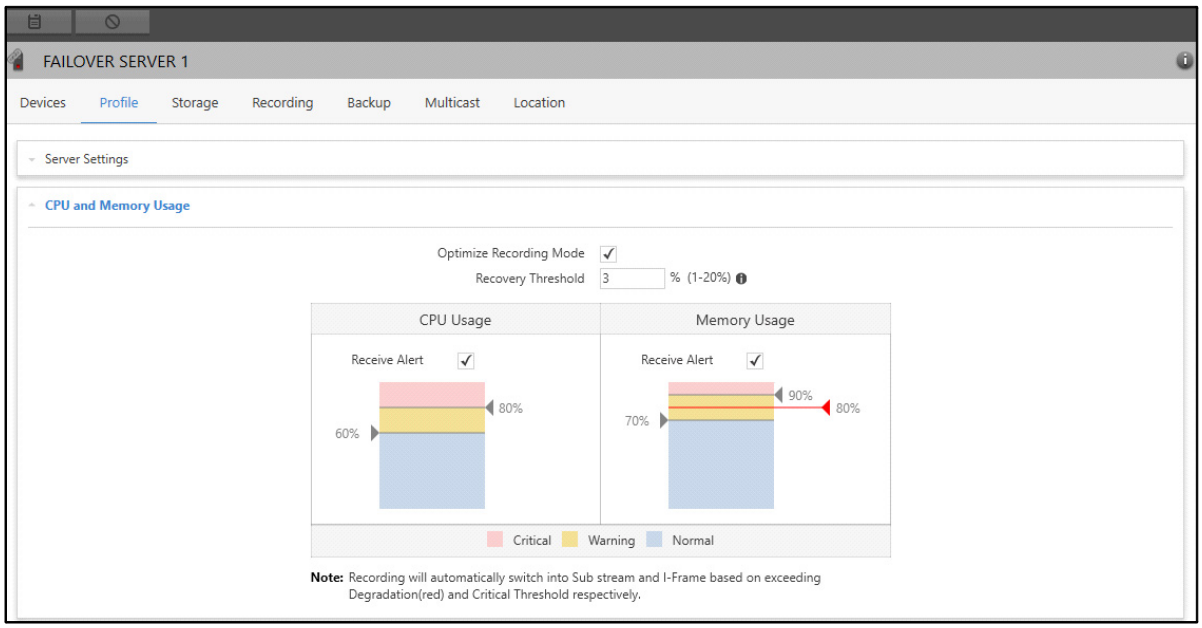
- Click **Save** to save the settings or click **Cancel** to discard.

CPU and Memory Usage

This panel allows you to configure the threshold value of CPU and Memory Usage and receive alerts when the Failover Server crosses these set values.

To configure the CPU and Memory Usage settings,

- Click the **CPU and Memory Usage** collapsible panel.



- **Optimize Recording Mode**: Select the check box if you wish that recording of cameras should be optimized according to the Memory Usage. When you select the check box, the **Degradation Threshold** (a red line) appears on the Memory Usage.

- **Recovery Threshold**: Specify the Recovery Threshold in percentage. Valid Range: 0-20%. Default: 3%. The memory threshold at which the degraded cameras — those whose recording streams have been switched to Sub Stream or iframe — are restored to either the Main Stream or the Sub Stream. For details, refer to “Functionality of Recording Server with respect to High Memory Usage”.

- **Receive Alert**: This check box is selected by default, to receive alerts when the Failover Server crosses the set threshold value under **CPU Usage** and **Memory Usage**. We recommend you not to clear this check box.

- **Critical, Warning and Normal Threshold Values:** The Critical, Warning and Normal Threshold Values for CPU and Memory Usage can be configured by dragging the pointer or tapping on the empty area. Valid Range: 0-100%. Default: Warning: 60, Critical: 80.

  In the Smart Client,
  - the CPU Usage/Memory Usage Exceeded pop-ups appear with a yellow boundary.
  - the CPU Usage/Memory Usage Critical pop-ups appear with a red boundary.
  - the CPU Usage/Memory Usage Critical event is highlighted in red color under Online Events.
  - the Degradation Started pop-ups appear with a yellow boundary.
  - the Degradation Stopped pop-ups appear with a blue boundary.

  For example, in the above screen the CPU Usage and Memory Usage thresholds are configured as 60% for Warning and 80% for Critical respectively. Hence, you will receive an alert when the CPU usage or the

memory usage goes beyond 60% and 80%, that is when it crosses the Warning and Critical limit as well as when it comes back to its Normal limit again.

- **Degradation Threshold**: For Memory Usage, drag the red line between the configured Warning and Critical Threshold to configure the Degradation Threshold. When the memory usage goes beyond the Degradation Threshold, the recording stream of the cameras is switched to Sub Stream or iframe from Main Stream. For details, refer to “Functionality of Recording Server with respect to High Memory Usage”.

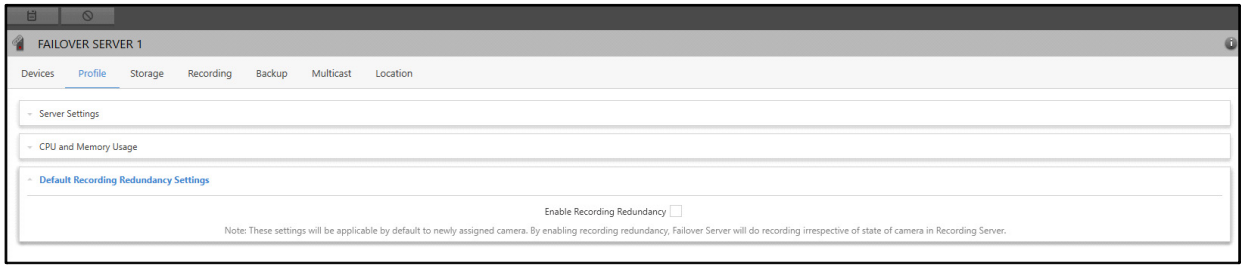
Default Threshold Values	CPU Usage	Memory Usage
Warning	60%	70%
Degradation	-	80%
Critical	80%	90%

- Click **Save** to save the settings or click **Cancel** to discard.

Default Recording Redundancy Settings

The device recordings are done in the Recording Server. You can assign a Failover Server to the devices, so that when the connectivity between the Recording Server and device is lost, the recording can be done in the Failover Server. However, switching from Recording Server to Failover Server may take some time and the recording for that duration can be lost. Hence, to ensure that no data is lost, you can select the **Enable Recording Redundancy** check box. This panel allows you to configure the Recording Redundancy Settings.
To configure the Default Redundancy Recording Settings,

- Click the **Default Recording Redundancy Settings** collapsible panel.



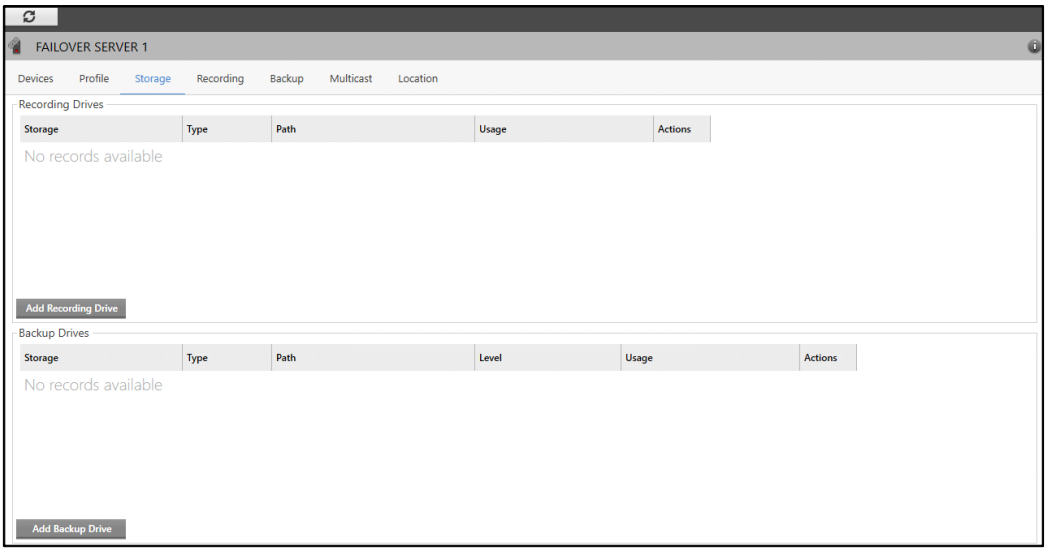
- **Enable Recording Redundancy**: Select Enable Recording Redundancy check box. If this option is enabled, the Enable Recording Redundancy check box in the Recording Settings of the Camera will be enabled by default when you add a new camera. For existing cameras, you can enable this option. For details, refer to “Recording”.
- Click **Save** to save the settings or click **Cancel** to discard.

Storage

This tab enables you to add Recording and Backup Drives and define storage settings for them.

To configure Storage settings,

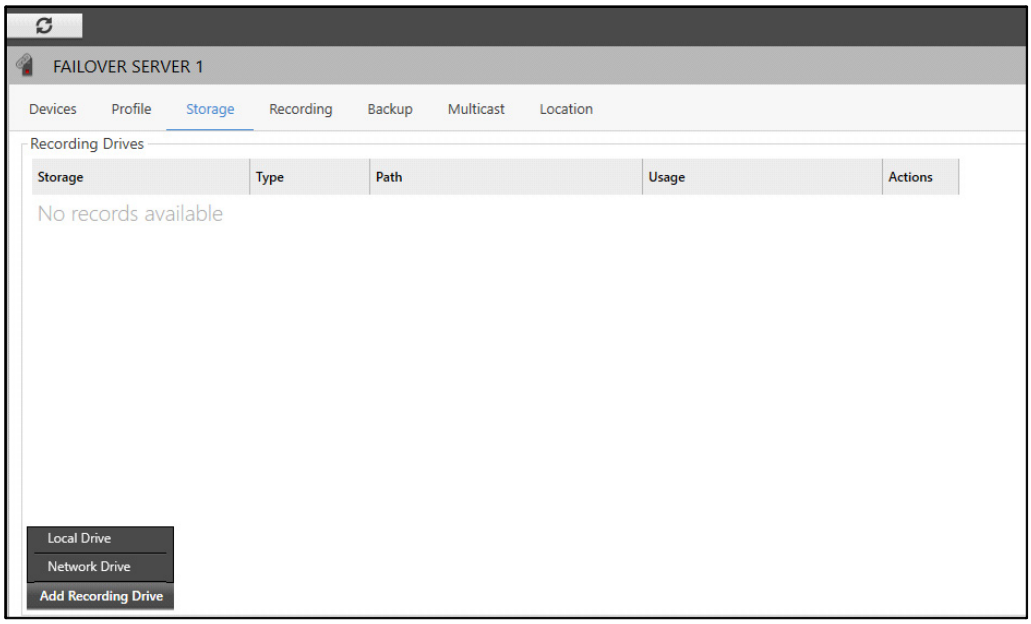
- Click the **Storage** tab.



The Storage tab consists of two sections — “Recording Drives” and “Backup Drives”.

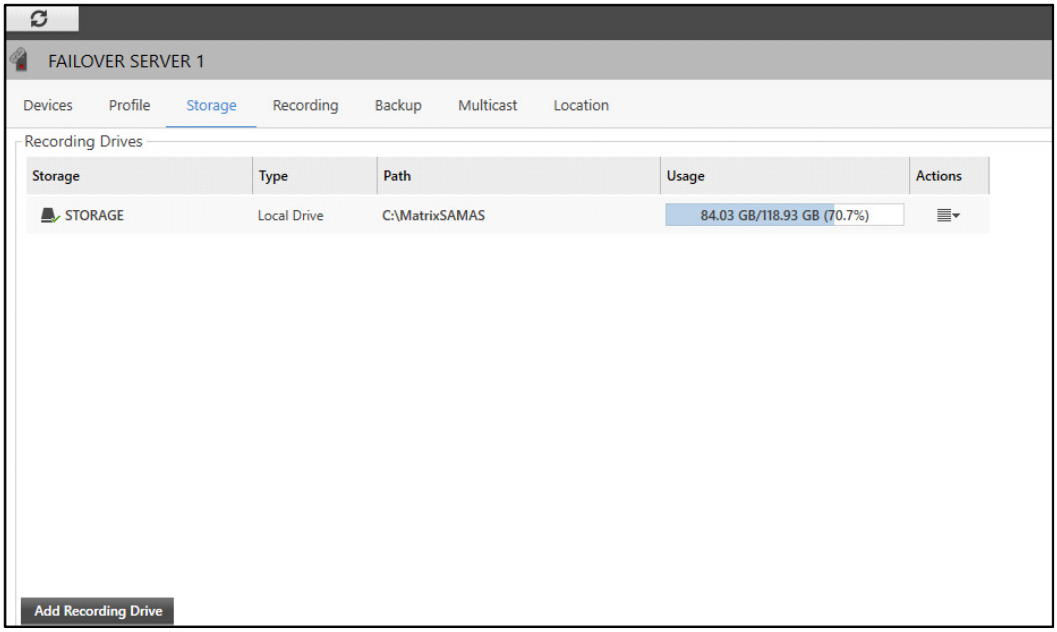
Recording Drives

- Click **Add Recording Drive**. You can add two types of Recording Drives— Local Drive and Network Drive.



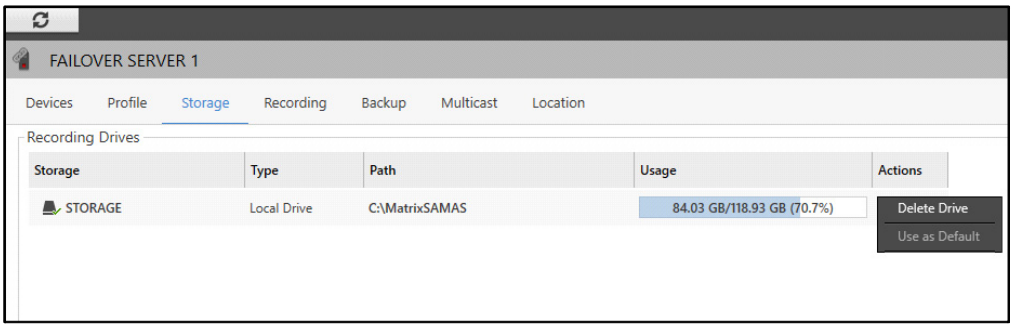
The configurations of Recording Drive Settings in Failover Server are similar to that of the Recording Server. For details, refer to “Recording Drive”.

The configured Recording Drives appear in the Recording Drives list.



The following details are displayed for the configured Recording Drives — Storage, Type, Path, Usage and Actions.

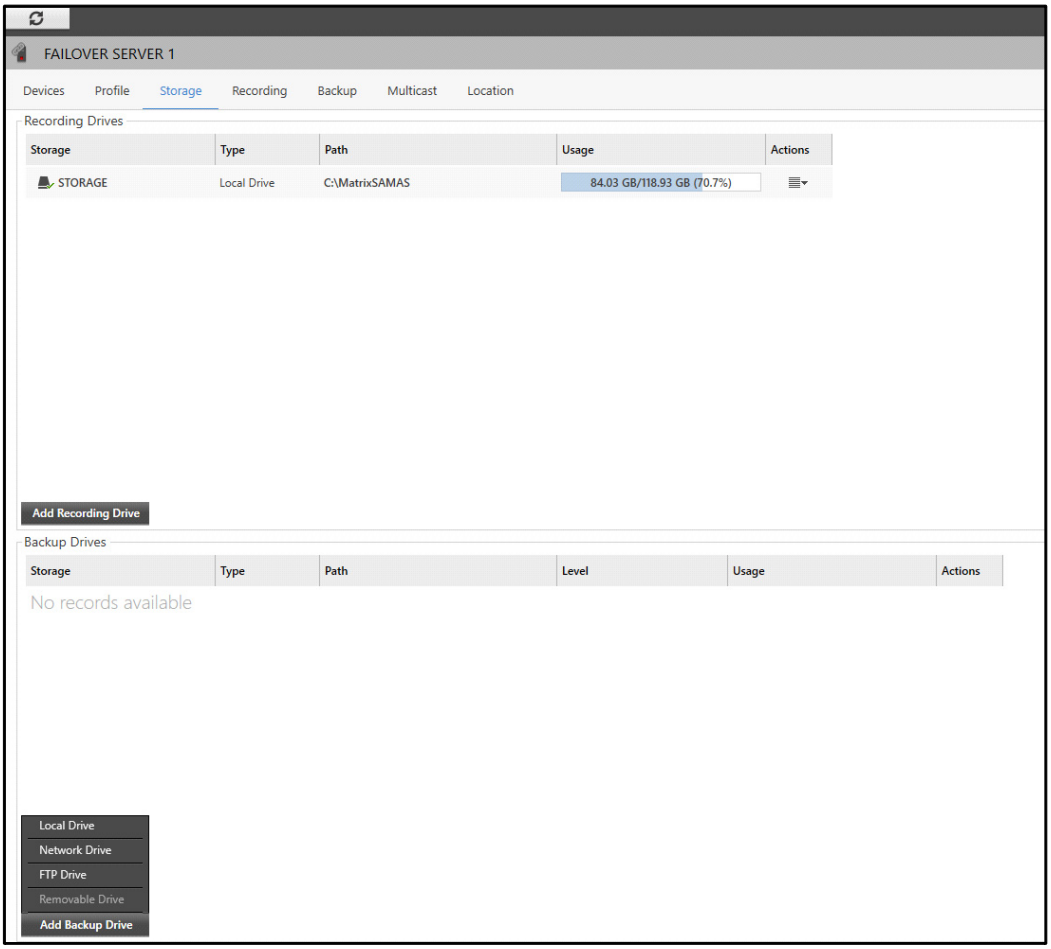
- Click **Actions** . Two options appear — **Delete Drive** and **Use as Default**.



- **Delete Drive**: Click Delete Drive to delete the configured Recording Drive. The drive will be removed from the Recording Drives list.
- **Use as Default**: Click Use as Default to set the drive as Default Storage Drive for all the newly added devices.

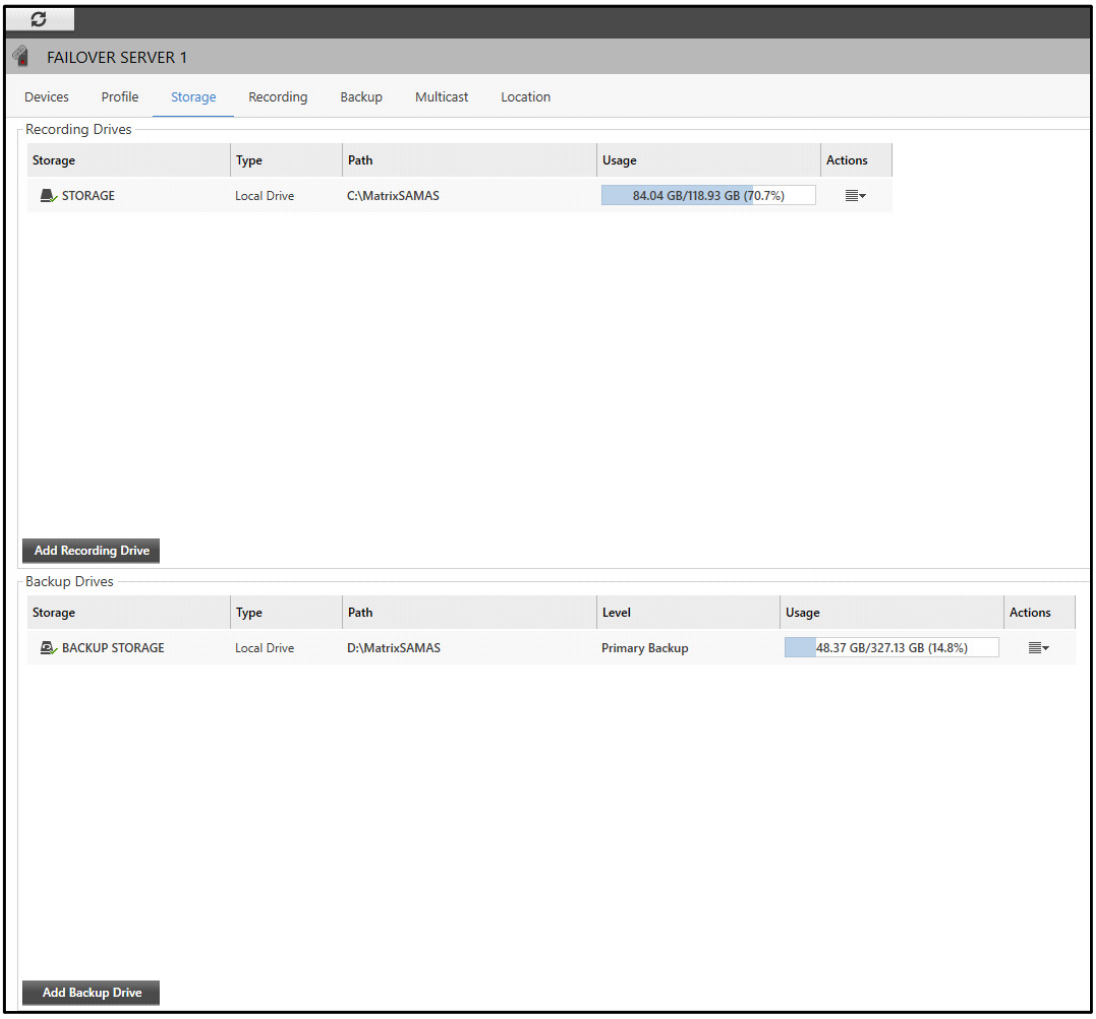
Backup Drives

- Click **Add Backup Drive**. You can add four types of Backup Drives — Local Drive, Network Drive, FTP Drive and Removable Drive.



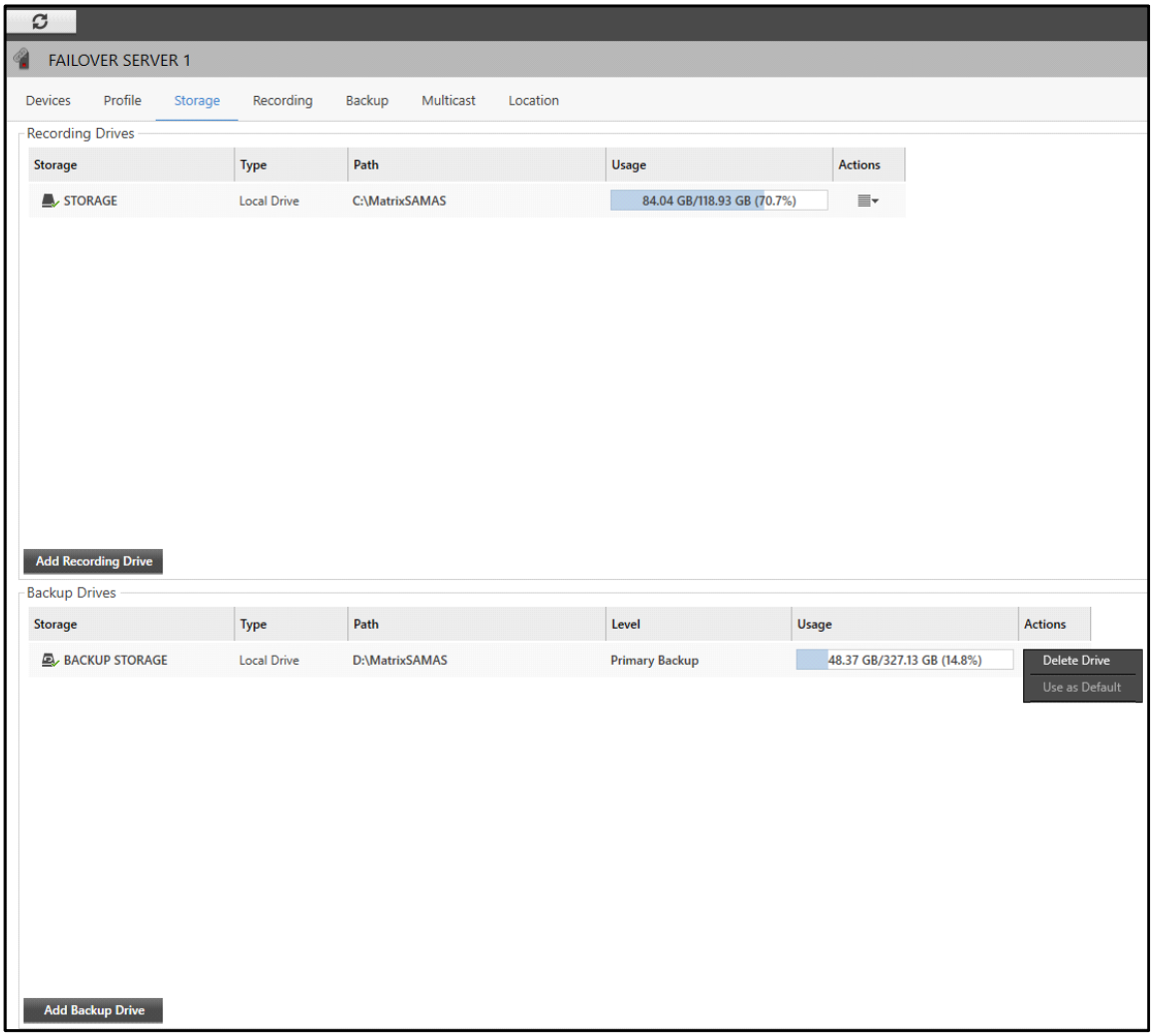
The configurations of Backup Drive Settings in Failover Server are similar to that of the Recording Server. For details, refer to “Backup Drive”.

The configured Backup Drives appear in the Backup Drives list.



The following details are displayed for the configured Backup Drives — Storage, Type, Path, Level, Usage and Actions.

- Click **Actions** . Two options appear — **Delete Drive** and **Use as Default**.



- **Delete Drive**: Click Delete Drive to delete the configured Backup Drive. The drive will be removed from the Backup Drives list.

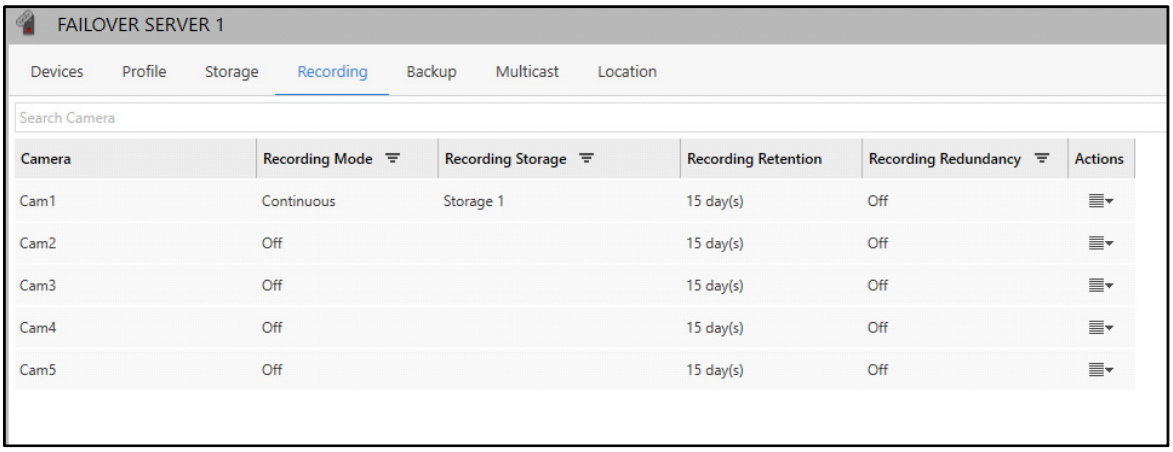
- **Use as Default**: Click Use as Default to set the drive as Default Storage Drive for all the newly added devices.

Recording

This tab enables you to view and configure the Recording Settings of the added cameras. This tab displays a list of the cameras and their Recording details. You can also search for a camera using the **Search Camera** option.

To configure Recording Settings,

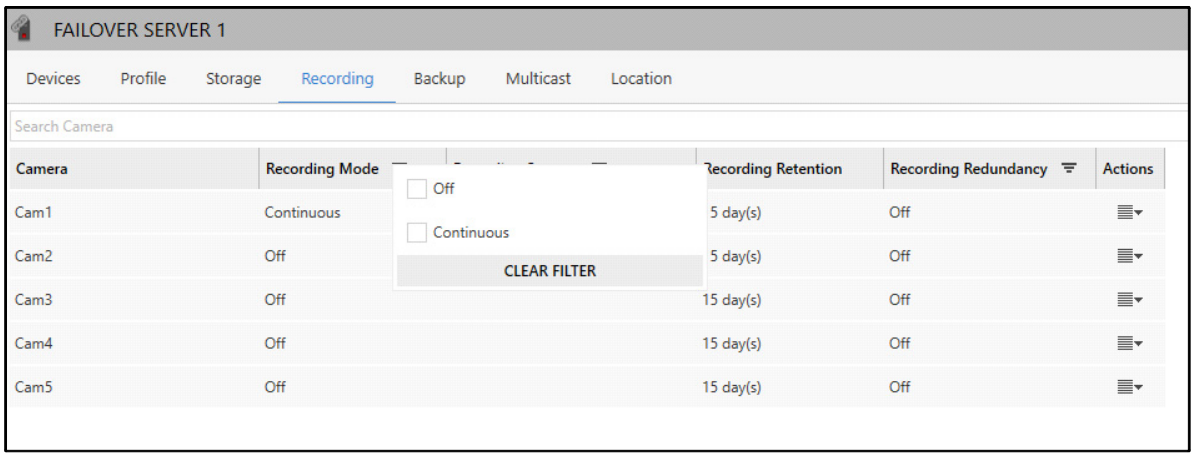
- Click the **Recording** tab.



The Recording details displayed are — Camera, Recording Mode, Recording Storage, Recording Retention, Recording Redundancy and Actions.

Sort and Filter Devices

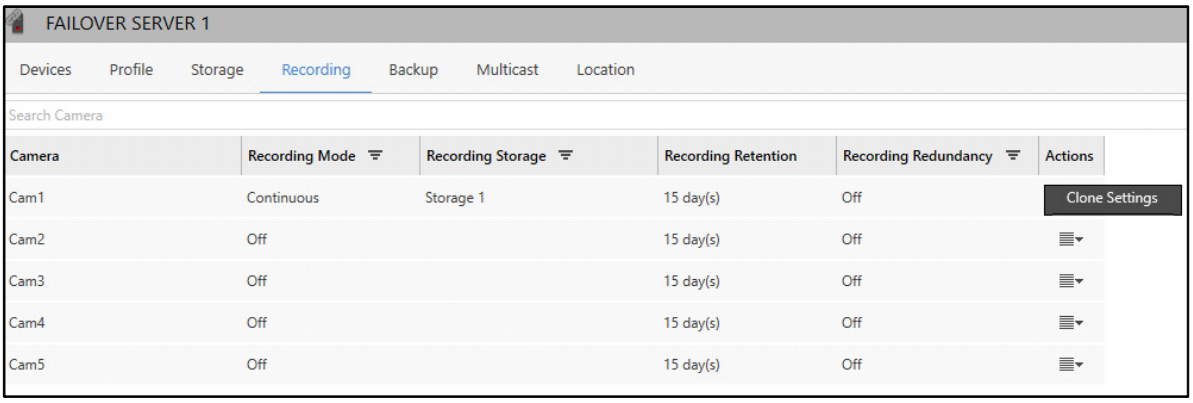
- You can **Sort** as well as **Filter** the devices.
- To Sort, click on the desired heading according to which you wish to sort the devices — Camera, Recording Mode, Recording Storage, Recording Retention, Recording Redundancy.
- To Filter the devices, according to the **Recording Mode** or **Recording Storage** or **Recording Redundancy**, click **Filter** .



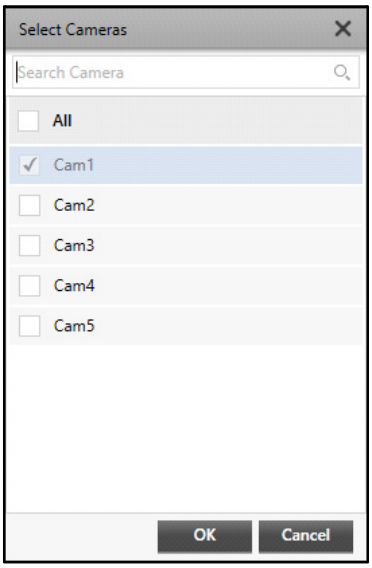
- Select the desired check boxes from the **Recording Mode**, **Recording Storage** and **Recording Redundancy** filter list. The cameras are sorted as per the set filters.
- Click **Clear Filter** to clear all the filters.

Clone Settings

- You can clone the camera Recording Settings.
- Click **Actions** for the desired camera. The **Clone Settings** option appears.



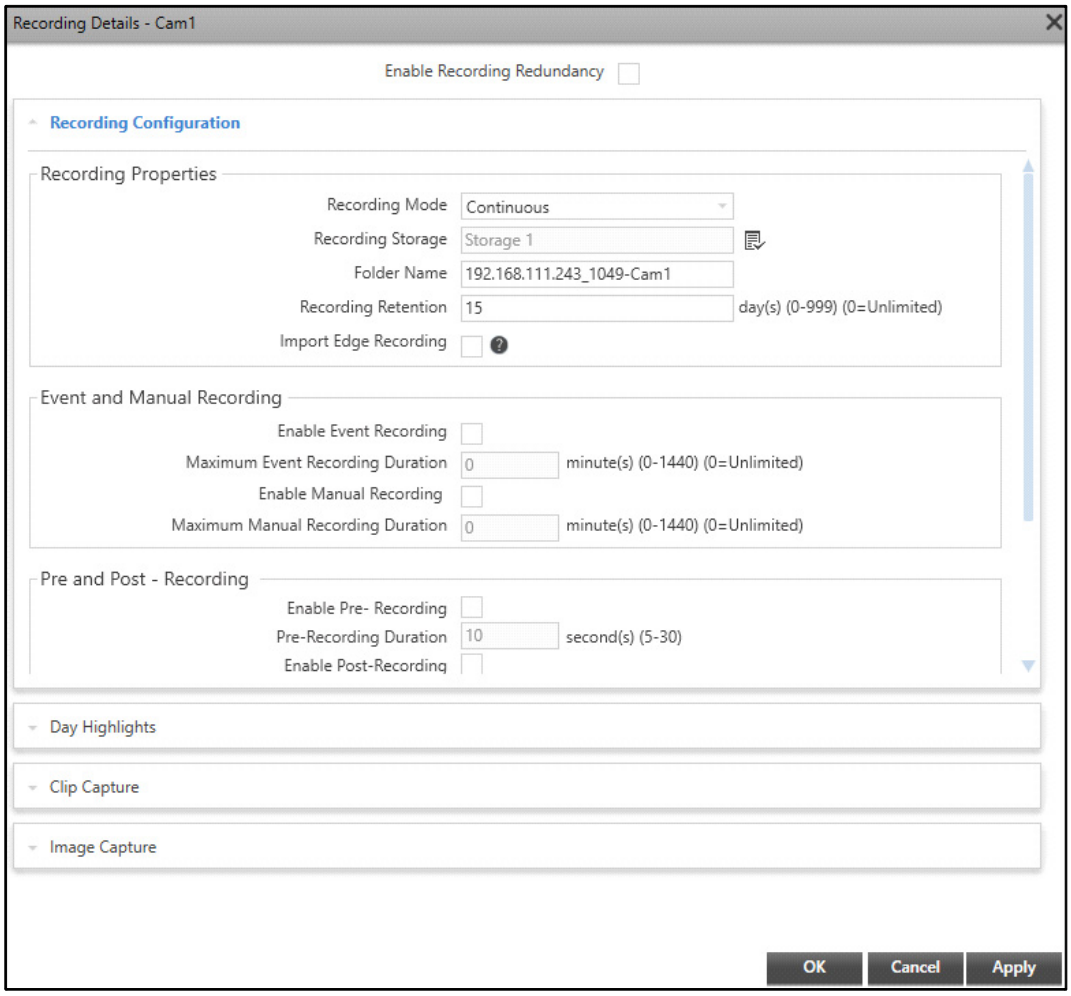
- **Clone Settings**: Click Clone Settings if you wish to copy the camera's Recording Settings to other cameras. On clicking Clone Settings, the **Select Cameras** pop-up appears.



- Select the cameras to which you wish to clone the settings.
- Click **OK** to confirm or click **Cancel** to discard.

Configuring the Recording Settings for a particular camera

- You can view as well as configure the Recording Settings for a particular camera.
- To do so, double click on the desired camera whose recording details are to be viewed. The **Recording Details** pop-up appears.



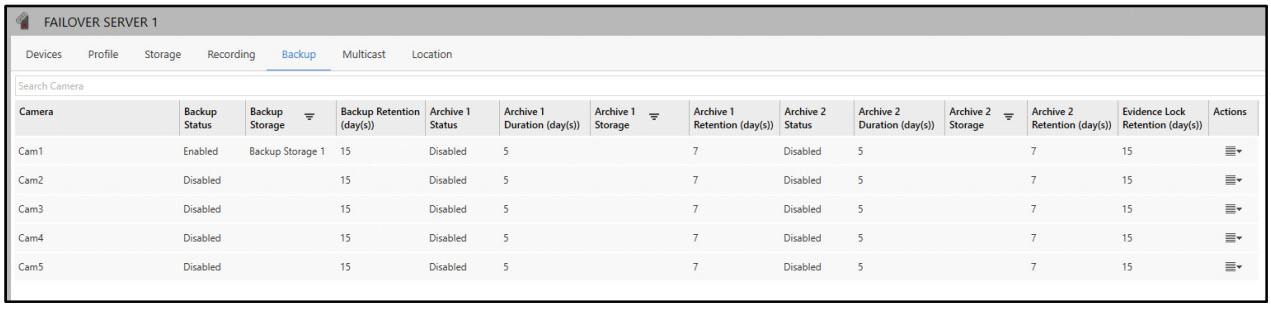
The Recording Details pop-up consists of the following collapsible panels — Recording Configuration, Day Highlights, Clip Capture and Image Capture. To view details and configure the recording for a camera, refer to “Recording”.

Backup

This tab enables you to view and configure the Backup Settings of the added devices. This tab displays a list of cameras and their Backup details. You can search for a camera using the **Search Camera** option.

To configure Backup Settings,

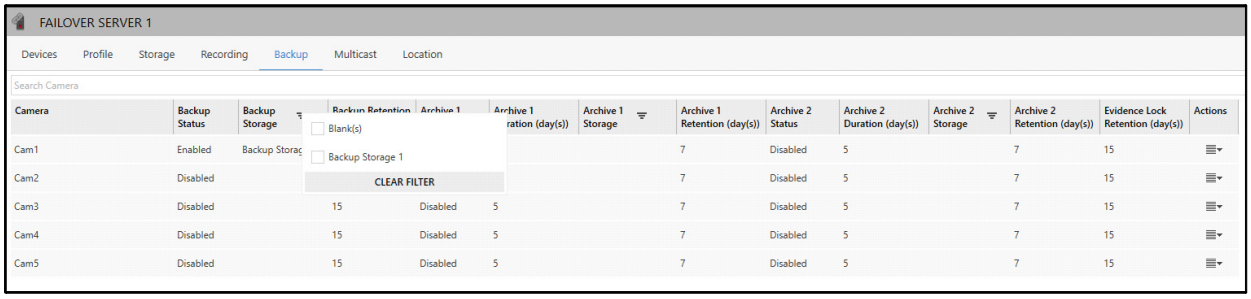
- Click the **Backup** tab.



The Backup details displayed are — Camera, Backup Status, Backup Storage, Backup Retention (day(s)), Archive 1 Status, Archive 1 Duration (day(s)), Archive 1 Storage, Archive 1 Retention (day(s)), Archive 2 Status, Archive 2 Duration (day(s)), Archive 2 Storage, Archive 2 Retention (day(s)), Evidence Lock Retention (day(s)) and Actions.

Sort and Filter Devices

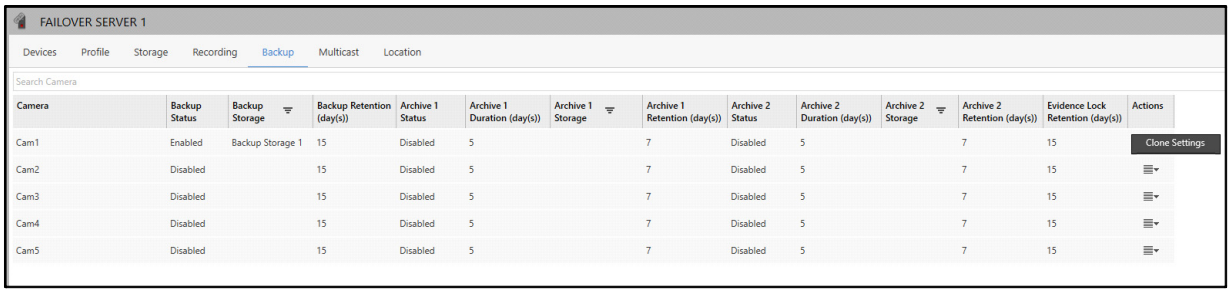
- You can **Sort** as well as **Filter** the devices.
- To Sort, click on the desired heading according to which you wish to sort the devices — Camera, Backup Status, Backup Storage, Backup Retention (day(s)), Archive 1 Status, Archive 1 Duration (day(s)), Archive 1 Storage, Archive 1 Retention (day(s)), Archive 2 Status, Archive 2 Duration (day(s)), Archive 2 Storage, Archive 2 Retention (day(s)), Evidence Lock Retention (day(s)).
- To filter the devices, according to the **Backup Storage** or **Archive 1 Storage** or **Archive 2 Storage**, click **Filter** .



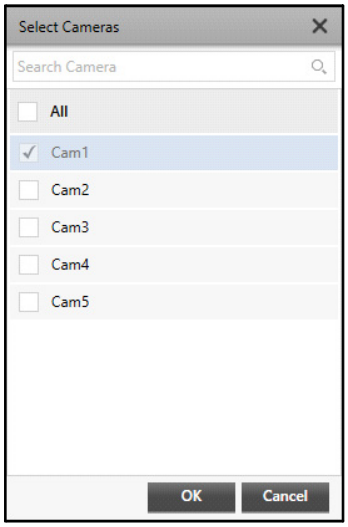
- Select the desired check boxes from the **Backup Storage** or **Archive 1 Storage** or **Archive 2 Storage** filter list. The cameras are filtered as per the set filters.
- Click **Clear Filter** to clear all the filters.

Clone Settings

- You can clone the camera Backup Settings.
- Click **Actions** for the desired camera. The **Clone Settings** option appears.



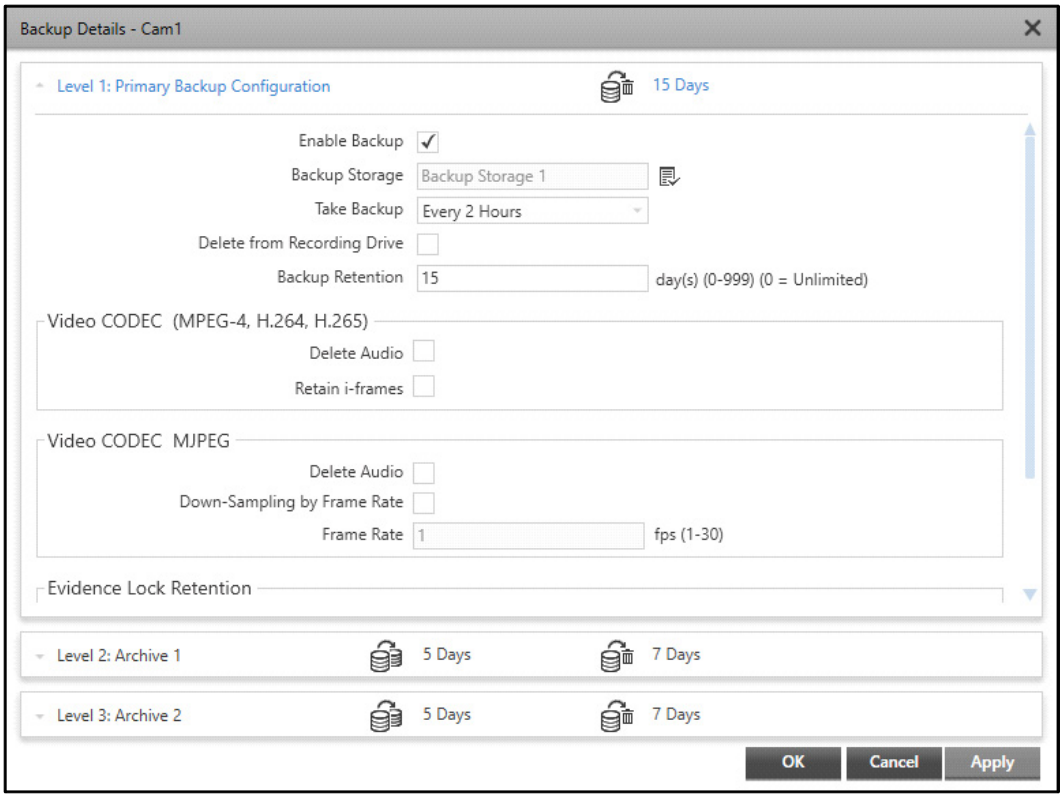
- **Clone Settings**: Click Clone Settings if you wish to copy the camera's Backup Settings to other cameras. On clicking Clone Settings, the **Select Cameras** pop-up appears.



- Select the cameras to which you wish to clone the settings.
- Click **OK** to confirm or click **Cancel** to discard.

Configuring the Backup Settings for a particular camera

- You can view as well as configure the Backup Settings for a particular camera.
- To do so, double-click on the desired camera whose recording details are to be viewed. The **Backup Details** pop-up appears.



The Backup Details pop-up consists of the following collapsible panels — Level 1: Primary Backup Configuration, Level 2: Archive 1 and Level 3: Archive 2. To view details and configure the backup for a camera, refer to“Backup”.

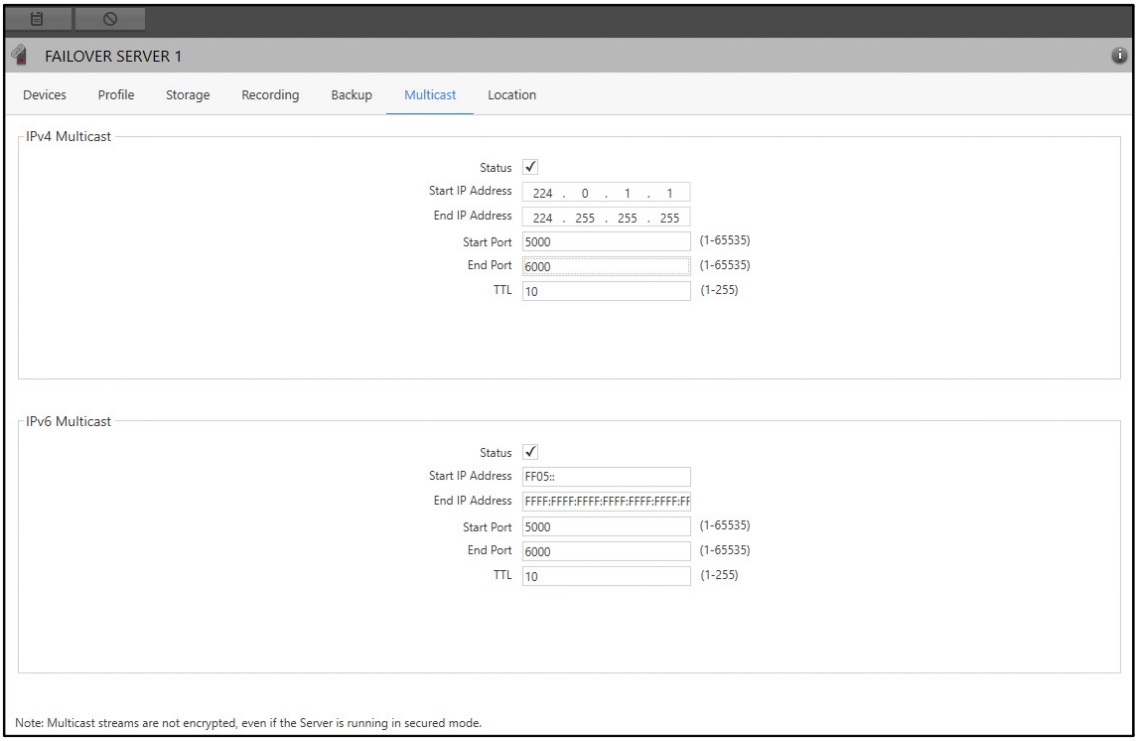
Multicast

Multicasting enables the optimization of network bandwidth consumption between the Failover Server and Smart Client/IVA Server. This tab enables you to view and configure the Multicast settings.

Multicast streams are not encrypted, even if the Failover Server is running in SSL mode.

To configure Multicast settings,

- Click the **Multicast** tab.



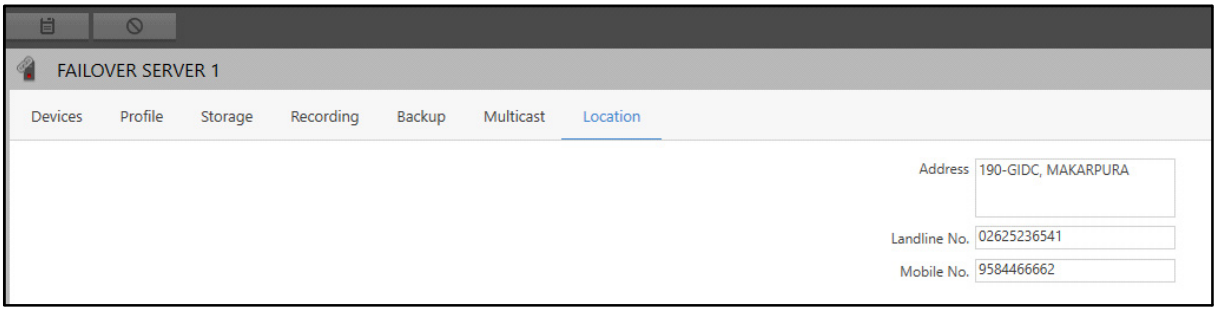
The configurations of Multicast Settings in Failover Server are similar to that of the Recording Server. For details, refer to “Multicast”.

Location

This tab enables you to view and configure the location information of a Failover Server.

To configure the Location,

- Click the **Location** tab.

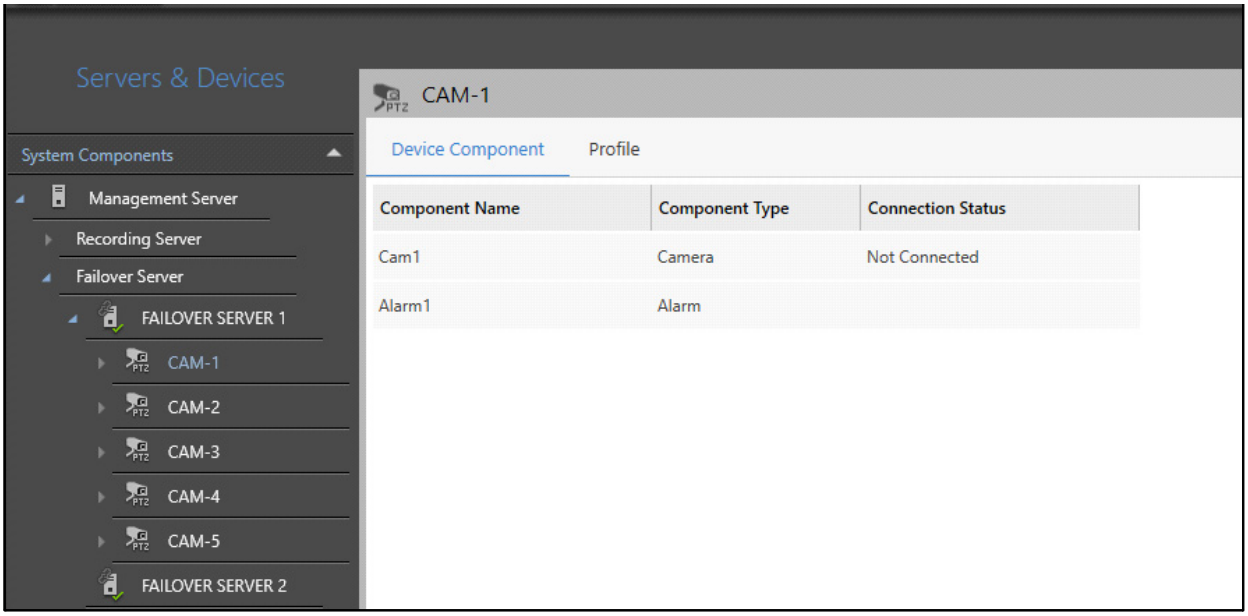


The configurations of Location Settings in Failover Server are similar to that of the Management Server. For details, refer to “Location”.

Device Component (FoS)

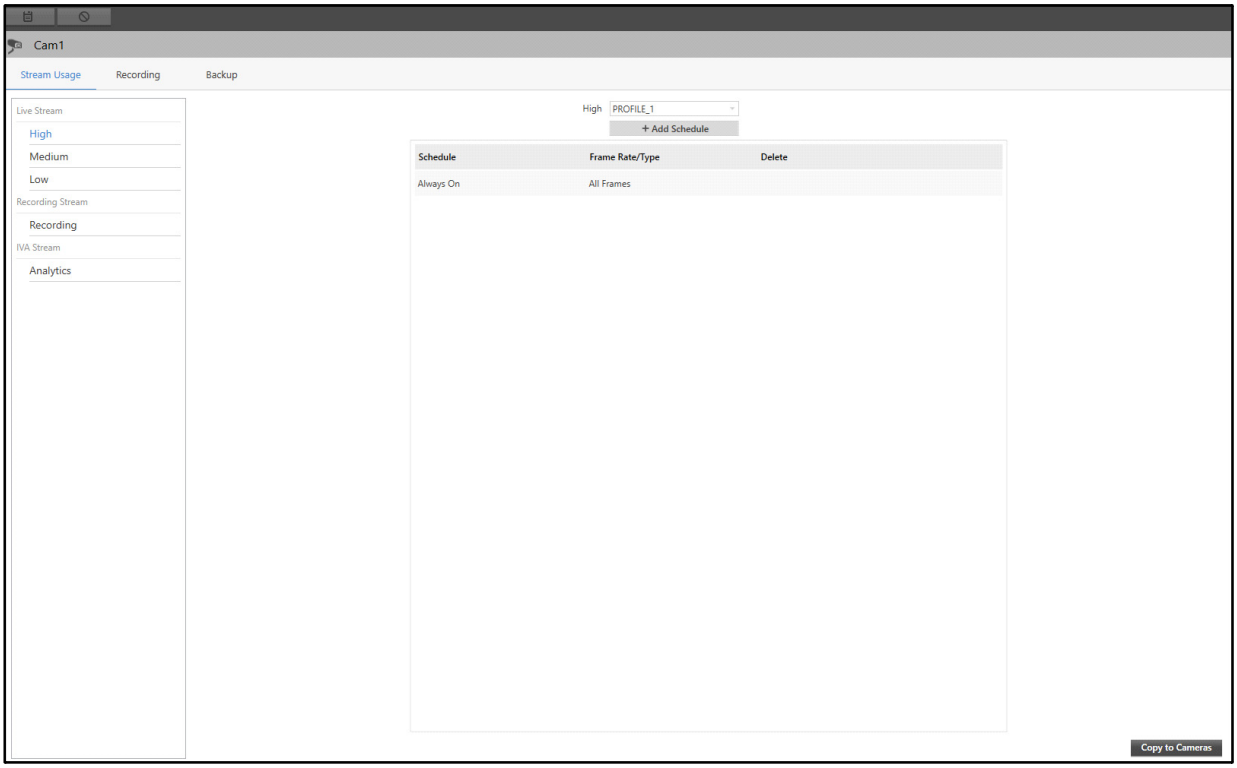
You can configure the individual devices added to the Failover Server. This tab enables you to view and configure the Device Settings for each device added to the Failover Server.
To configure the Device Settings,

- Select the desired device. The **Device Component** tab appears by default.



  This tab displays the following device parameters — Component Name, Component Type and Connection Status.

- Double-click the camera to configure its parameters. Three tabs appear — Stream Usage, Recording and Backup.



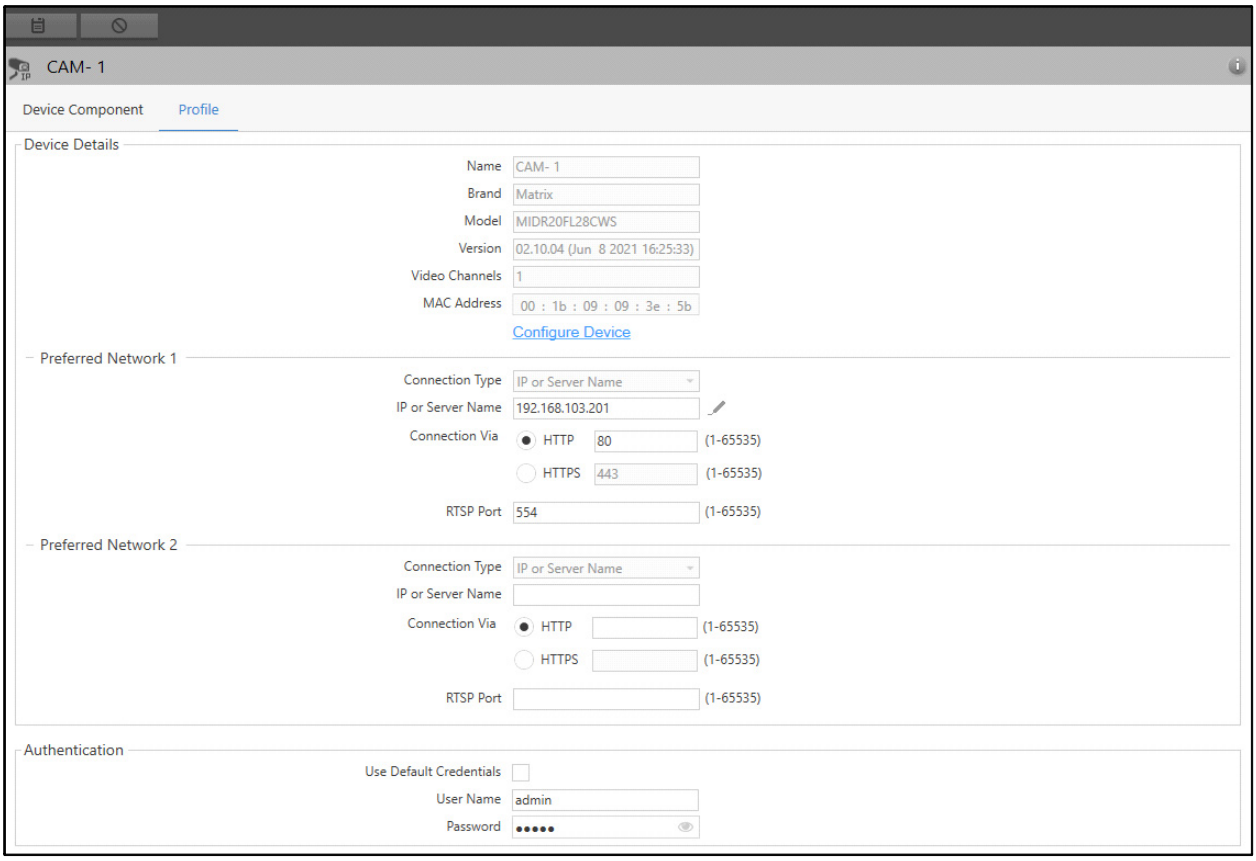
The configurations of camera parameters in Failover Server are similar to that of the Recording Server. For details, refer to “Stream Usage”, “Recording” and “Backup”.

Device Profile (FoS)

This tab enables you to view and configure the Device Profile Settings for each device added to the Failover Server.

To configure the Device Profile Settings,

- Click the **Profile** tab.



This page displays the following parameters — “Device Details”, “Preferred Networks 1/2”, “Authentication”.

Device Details

This section displays details of the device. The Device Details displayed are — Name, Brand, Model, Version, Protocol, Video Channels, MAC Address and Preferred Networks. You can configure the device by clicking on **Configure Device**.

You can configure the following parameters:

Preferred Networks 1/2

- **Connection Type**: The default Connection Type appears as **IP or Server Name**.
- **IP or Server Name**: Specify the IPv4/IPv6 Address or Server Name. In IP or Server Name, you can enter upto 255 characters. Default: IP or Server Name of the device using which it is added to Recording Server.

If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

- **Connection Via**: Select the Connection type from the options — HTTP or HTTPS. Specify the HTTP/ HTTPS Port. Valid Range: 1-65535. Default HTTP Port: 80, Default HTTPS Port: 443.
- **RTSP Port**: Specify the RTSP Port. Valid Range: 1-65535. Default: 554.

Authentication

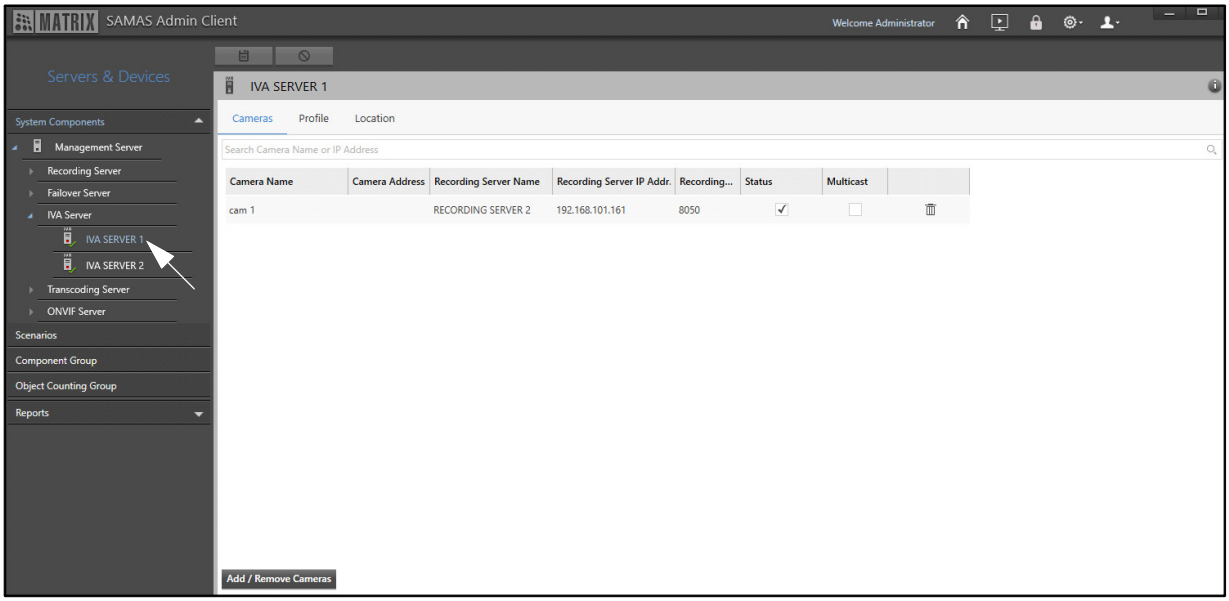
- **Use Default Credentials**: Select the check box if you wish to use the default credentials for authentication.
- **User Name**: Specify the user name for the device, if you have disabled **Use Default Credentials** check box. In User Name, you can enter upto 100 characters. Default: Blank.
- **Password**: Specify the password for the device, if you have disabled **Use Default Credentials** check box. In Password, you can enter upto 100 characters. Default: Blank. Click **Show**  to view the password. The icon toggles to **Hide**  . Click **Hide**  to hide the password.

IVA Server Configuration

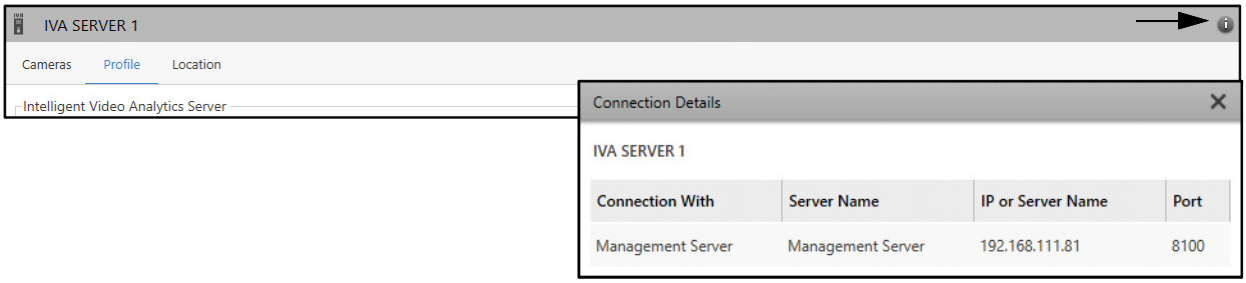
To configure a IVA Server, it must be activated first. The Server has to be activated by accepting its activation request from the **IVA Server** collapsible panel on the **Management Server** page. To activate a IVA Server, refer to “Activating Server as IVA Server”.

To configure a IVA Server,

- Click **Servers & Devices > System Components > IVA Server**.
- All the IVA Servers of the system appear. The entries can be sorted. To do so, click on the desired parameter in the header row. An arrow ▲ icon appears. Click on it. Entries can be sorted in ascending or descending order.
- Select the desired IVA Server.



- To view the **Connection Details** of the IVA Server, click **Connection Details**  at the top right corner of the IVA Server page. It displays the connection details of the IVA Server with the Management Server and Recording Server. It displays the details — Connection With, Server Name, IP (IPv4/IPv6) or Server Name and Port.



Each IVA Server consists of the following tabs:

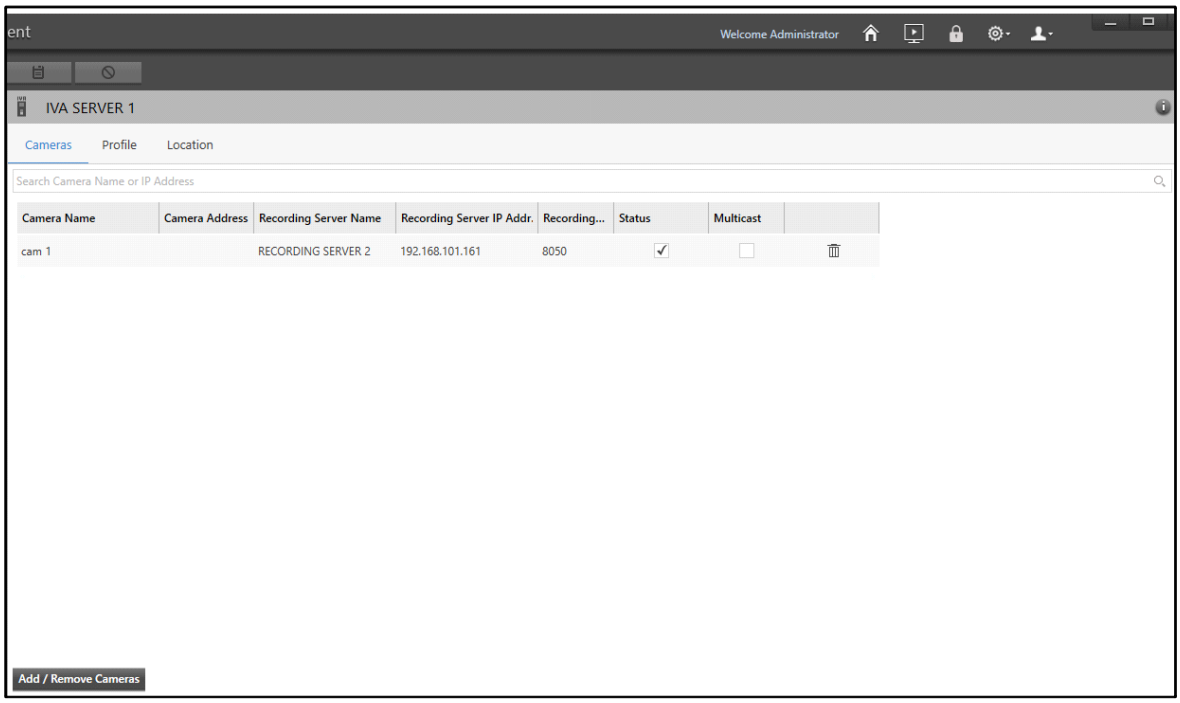
- “Cameras”
- “Profile”
- “Location”

Cameras

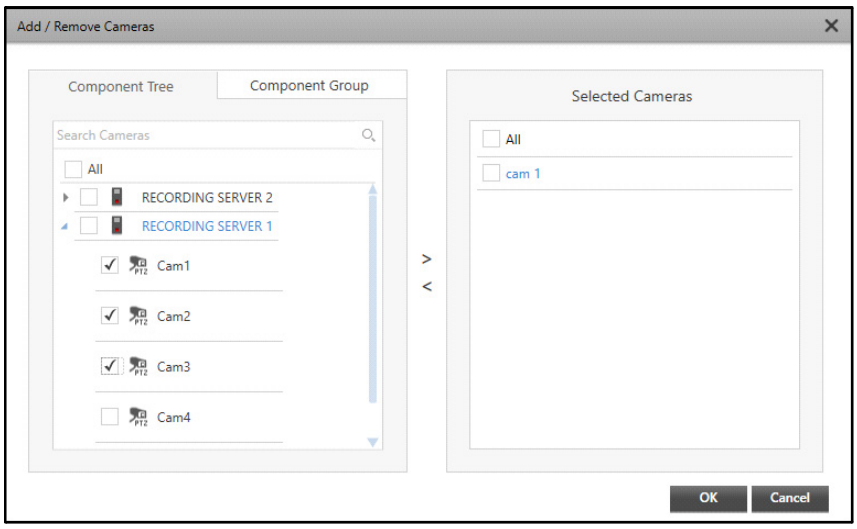
This tab enables you to add and remove cameras from the IVA Server once it is activated. The cameras added to the IVA Server appear in this tab. The following camera details are displayed — Camera Name, Camera Address (IPv4/IPv6), Recording Server Name, Recording Server IP Address, Recording Server Port, Status and Multicast.

To add or remove a camera,

- Select the desired IVA Server. The **Cameras** tab appears by default.



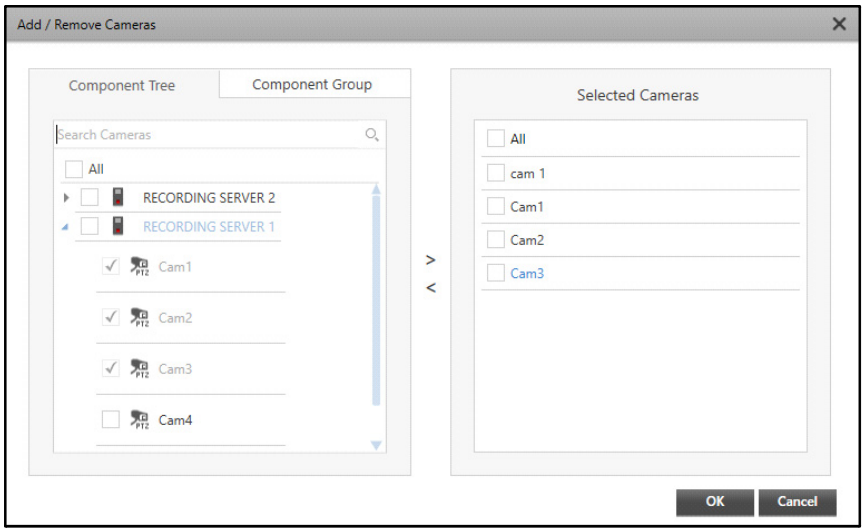
- Click **Add/ Remove Cameras**. The **Add/ Remove Cameras** pop-up appears.



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the desired cameras you wish to add from the Component Tree or Component Group tabs.

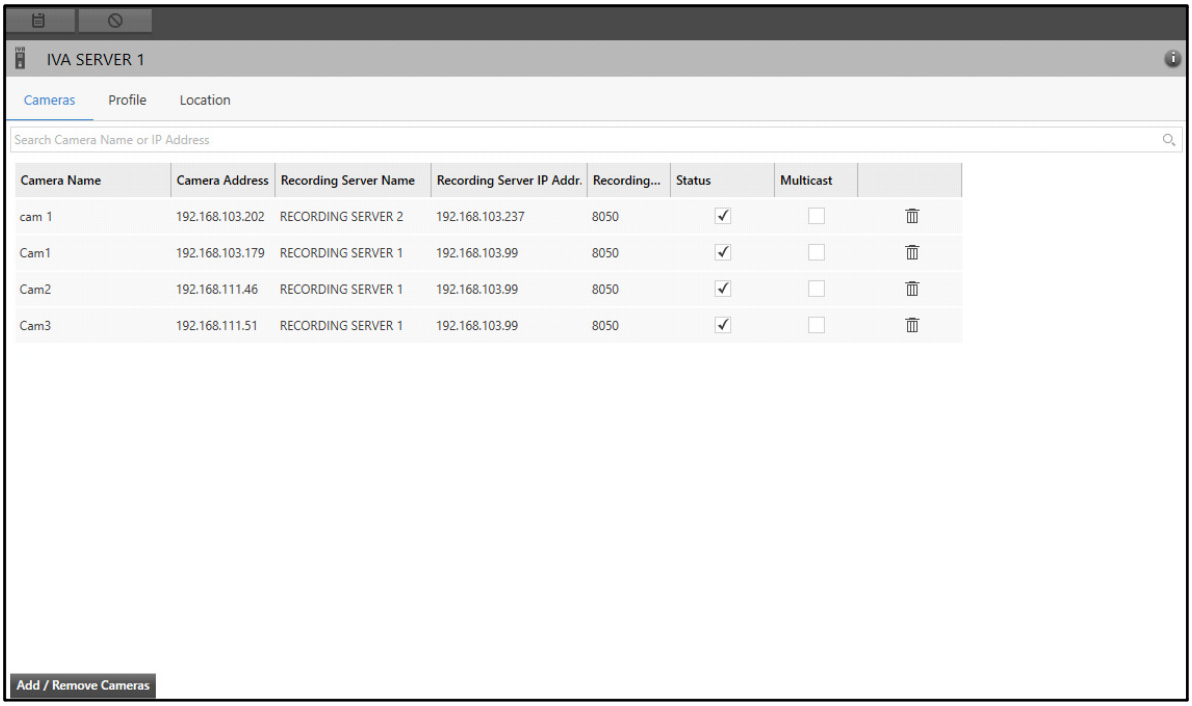
  Click the right arrow button to move these cameras to the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.



- Click **OK** to confirm or click **Cancel** to discard.

The added cameras appear in a list under the Cameras tab. You can configure the following camera parameters — Status, Multicast and Delete.



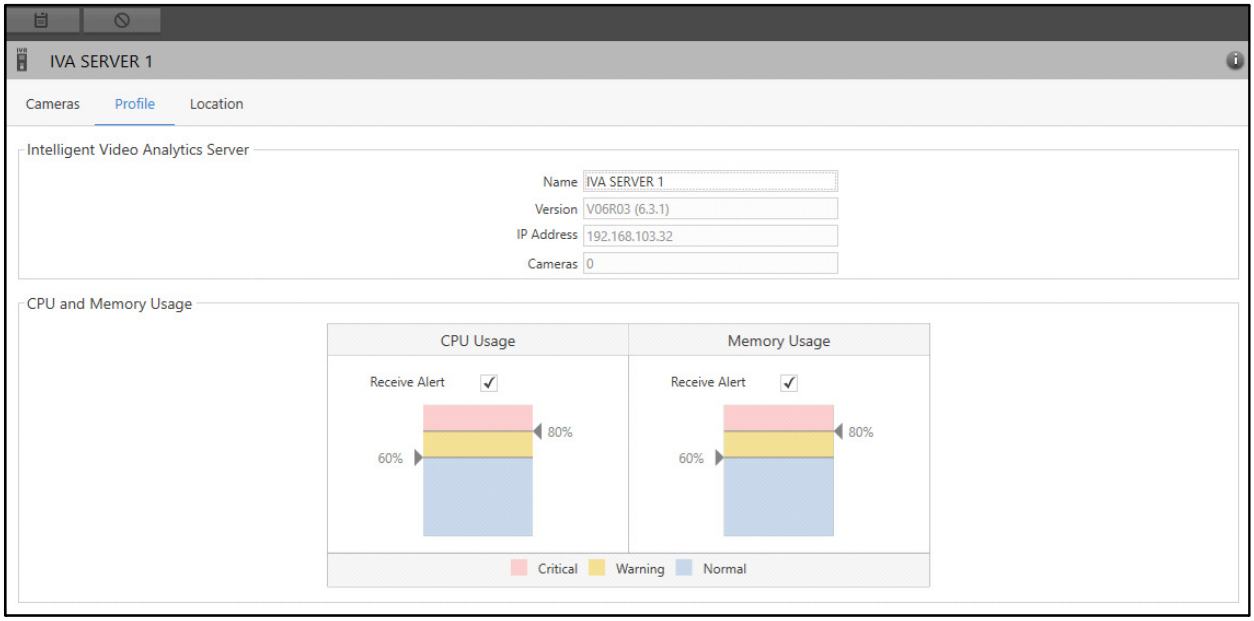
- **Status**: Select the Status check box to enable the camera. Clear the check box to disable the camera.
- **Multicast**: Select the check box to enable Multicast communication from the IVA Server. Clear the check box to disable the Multicast communication.
- **Delete**: Click **Delete** to remove the camera.

Profile

This tab enables you to view and configure Intelligent Video Analytics Server and CPU and Memory Usage.

To configure Profile settings,

- Click the **Profile** tab.



This page displays the following parameters — “Intelligent Video Analytics Server” and “CPU and Memory Usage”.

Intelligent Video Analytics Server

This section displays the details of the IVA Server like Name, Version, IPv4/IPv6 Address, and Cameras.

You can configure the following parameters:

- **Name**: Specify a name for the IVA Server. In Name, you can enter upto 50 characters. Default: Name of the system where IVA Server is installed.

- Click **Save** to save the settings or **Cancel** to discard.

CPU and Memory Usage

This section displays the CPU and Memory Usage configurations.

You can configure the following parameters:

- **Receive Alert**: This check box is selected by default, to receive alerts when the IVA Server crosses the set threshold value under **CPU Usage** and **Memory Usage**. We recommend you not to clear this check box.

- **Critical, Warning and Normal Threshold Values:** The Critical, Warning and Normal Threshold Values for CPU and Memory Usage can be configured by dragging the pointer or tapping on the empty area. Valid Range: 0-100%. Default: Warning: 60, Critical: 80.

  In the Smart Client,
  - the CPU Usage/Memory Usage Exceeded pop-ups appear with a yellow boundary.
  - the CPU Usage/Memory Usage Critical pop-ups appear with a red boundary.
  - the CPU Usage/Memory Usage Critical event is highlighted in red color under Online Events.

  For example, in the above screen the CPU Usage and Memory Usage thresholds are configured as 60% for Warning and 80% for Critical respectively. Hence, you will receive an alert when the CPU usage or the

memory usage goes beyond 60% and 80%, that is when it crosses the Warning and Critical limit as well as when it comes back to its Normal limit again.

- Click **Save** to save the settings or **Cancel** to discard.

Location

This tab enables you to view and configure the location information of a IVA Server.

To configure the Location,

- Click the **Location** tab.



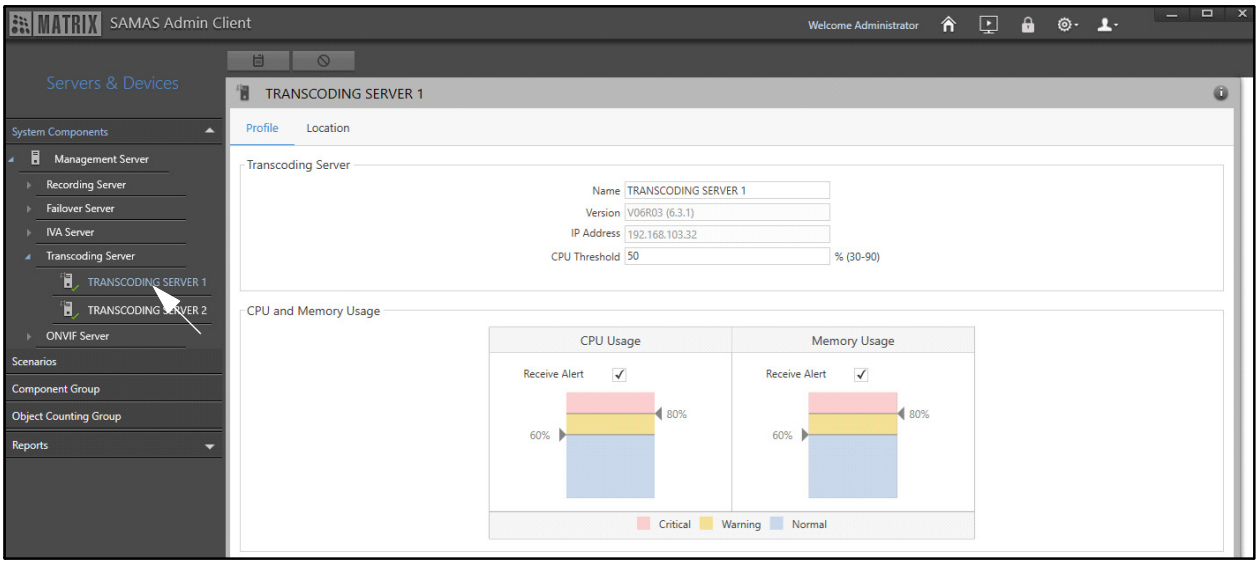
The configurations of Location Settings in IVA Server are similar to that of the Management Server. For details, refer to “Location”.

Transcoding Server Configuration

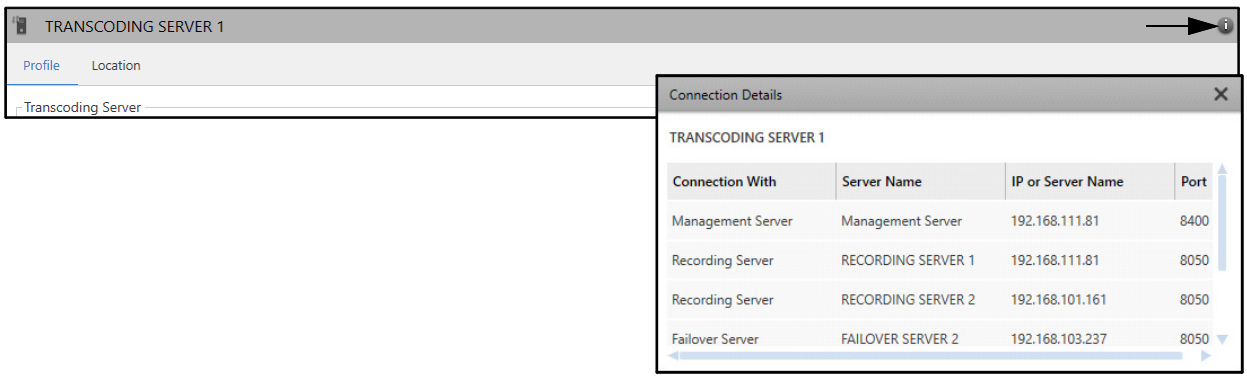
To configure a Transcoding Server, it must be activated first. The Server has to be activated by accepting its activation request from the **Transcoding Server** collapsible panel on the **Management Server** page. To activate a Transcoding Server, refer to “Activating Server as Transcoding Server”.

To configure a Transcoding Server,

- Click **Servers & Devices > System Components > Transcoding Server**.
- All the Transcoding Servers of the system appear. The entries can be sorted. To do so, click on the desired parameter in the header row. An arrow ▲ icon appears. Click on it. Entries can be sorted in ascending or descending order.
- Select the desired Transcoding Server.



- To view the **Connection Details** of the Transcoding Server, click **Connection Details**  at the top right corner of the Transcoding Server page. It displays the connection details of the Transcoding Server with the Management Server and Recording Server. It displays the following details — Connection With, Server Name, IP (IPv4/IPv6) or Server Name and Port.



Each Transcoding Server consists of the following tabs:

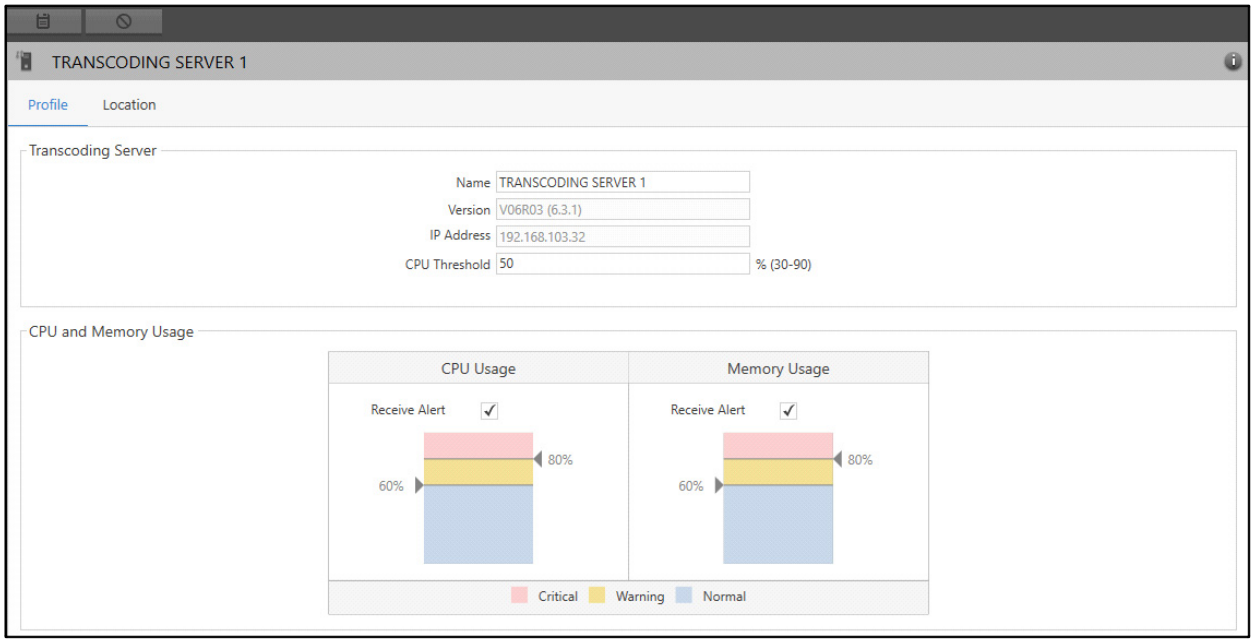
- “Profile”
- “Location”

Profile

This tab enables you to view and configure Transcoding Server and CPU and Memory Usage.

To configure Profile settings,

- Click the **Profile** tab.



This page displays the following parameters — “Transcoding Server” and “CPU and Memory Usage”.

Transcoding Server

This section displays the details of the Transcoding Server like Name, Version, IPv4/IPv6 Address, and CPU Threshold.

You can configure the following parameters:

- **Name**: Specify a name for the Transcoding Server. In Name, you can enter upto 50 characters. Default: Name of the system where Transcoding Server is installed.
- **CPU Threshold**: Specify the CPU Threshold value. This is that value of the total CPU that can be consumed by the Transcoding Server Application. Valid Range: 30-90%. Default: 50.

  If CPU Usage of Transcoding Server Application in the System where Transcoding Server is installed reaches the CPU Threshold level set by you then Transcoding will stop. Once the CPU Usage comes back

to normal then only Transcoding Server will resume accepting request for Transcoding from the Recording Server as well as Failover Server.

- Click **Save** to save the settings or **Cancel** to discard.

CPU and Memory Usage

- **Receive Alert**: This check box is selected by default, to receive alerts when the Transcoding Server crosses the set threshold value under **CPU Usage** and **Memory Usage**. We recommend you not to clear this check box.

- **Critical, Warning and Normal Threshold Values:** The Critical, Warning and Normal Threshold Values for CPU and Memory Usage can be configured by dragging the pointer or tapping on the empty area. Valid Range: 0-100%. Default: Warning: 60, Critical: 80.

  In the Smart Client,
  - the CPU Usage/Memory Usage Exceeded pop-ups appear with a yellow boundary.
  - the CPU Usage/Memory Usage Critical pop-ups appear with a red boundary.
  - the CPU Usage/Memory Usage Critical event is highlighted in red color under Online Events.

  For example, in the above screen the CPU Usage and Memory Usage thresholds are configured as 60% for Warning and 80% for Critical respectively. Hence, you will receive an alert when the CPU usage or the memory usage goes beyond 60% and 80%, that is when it crosses the Warning and Critical limit as well as when it comes back to its Normal limit again.

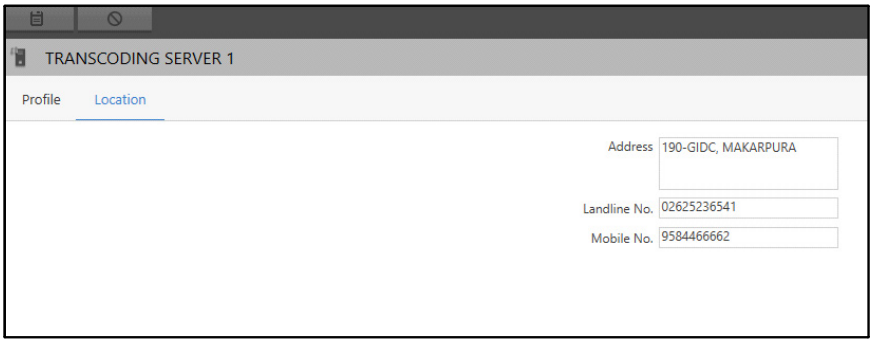
- Click **Save** to save the settings or **Cancel** to discard.

Location

This tab enables you to view and configure the location information of a Transcoding Server.

To configure the location,

- Click the **Location** tab.



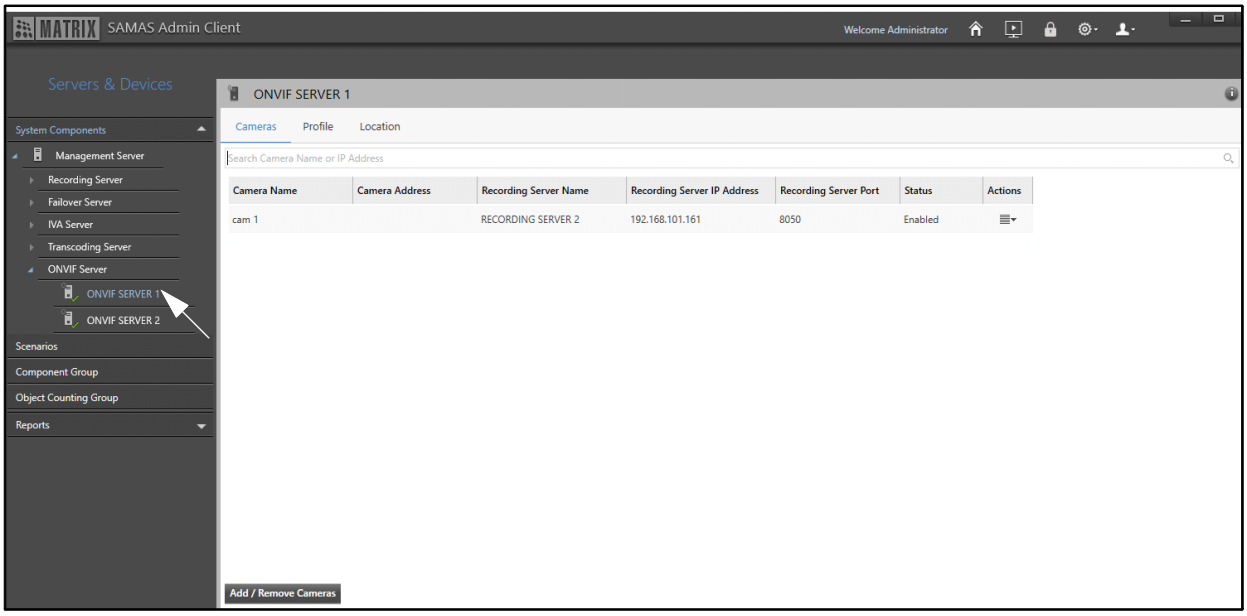
The configurations of Location Settings in Transcoding Server are similar to that of the Management Server. For details, refer to “Location”.

ONVIF Server Configuration

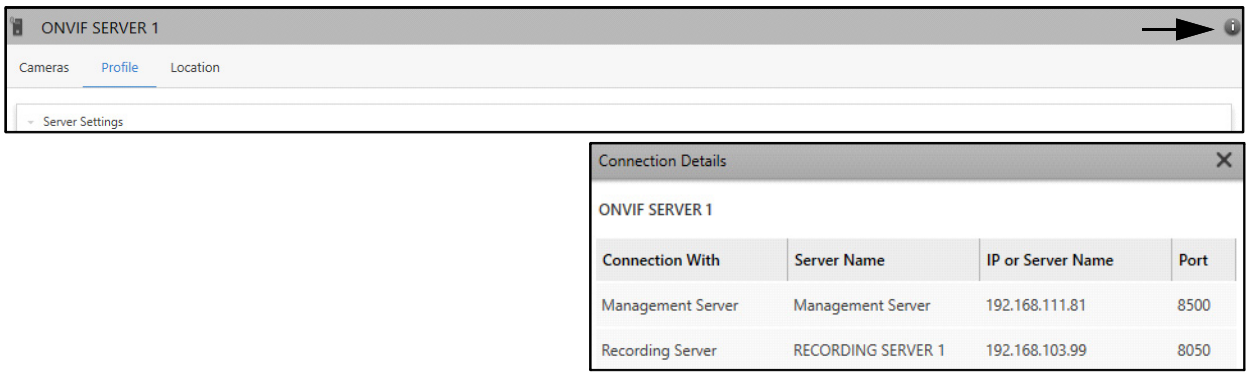
To configure a ONVIF Server, it must be activated first. The Server has to be activated by accepting its activation request from the **ONVIF Server** collapsible panel on the **Management Server** page. To activate a ONVIF Server, refer to “Activating Server as ONVIF Server”.

To configure a ONVIF Server,

- Click **Servers & Devices > System Components > ONVIF Server**.
- All the ONVIF Servers of the system appear. The entries can be sorted. To do so, click on the desired parameter in the header row. An arrow ▲ icon appears. Click on it. Entries can be sorted in ascending or descending order.
- Select the desired ONVIF Server.



- To view the **Connection Details** of the ONVIF Server, click **Connection Details**  at the top right corner of the ONVIF Server page. It displays the connection details of the ONVIF Server with the Management Server, Recording Server as well as Failover Server. It displays the following details — Connection With, Server Name, IP (IPv4/IPv6) or Server Name and Port.



Each ONVIF Server consists of the following tabs:

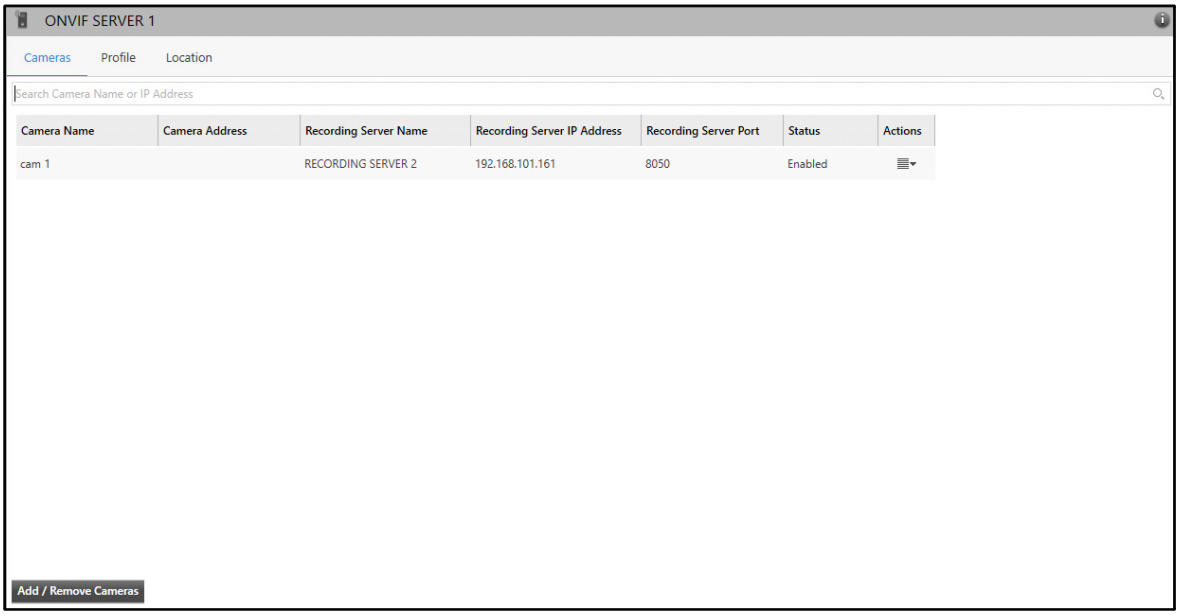
- “Cameras”
- “Profile”
- “Location”

Cameras

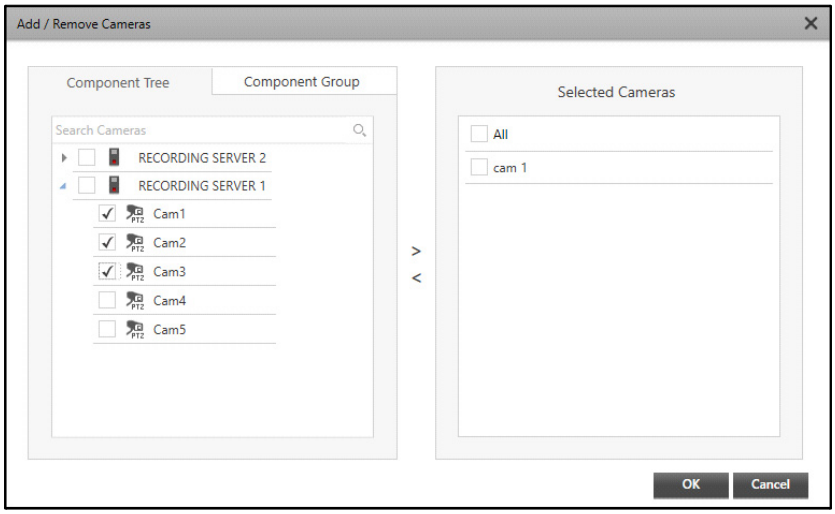
This tab enables you to add and remove cameras from the ONVIF Server. The cameras added to the ONVIF Server appear in this tab. The following camera details are displayed — Camera Name, Camera Address (IPv4/ IPv6), Recording Server Name, Recording Server IP Address, Recording Server Port, Status and Actions.

To add or remove a camera,

- Select the desired ONVIF Server. The **Cameras** tab appears by default.



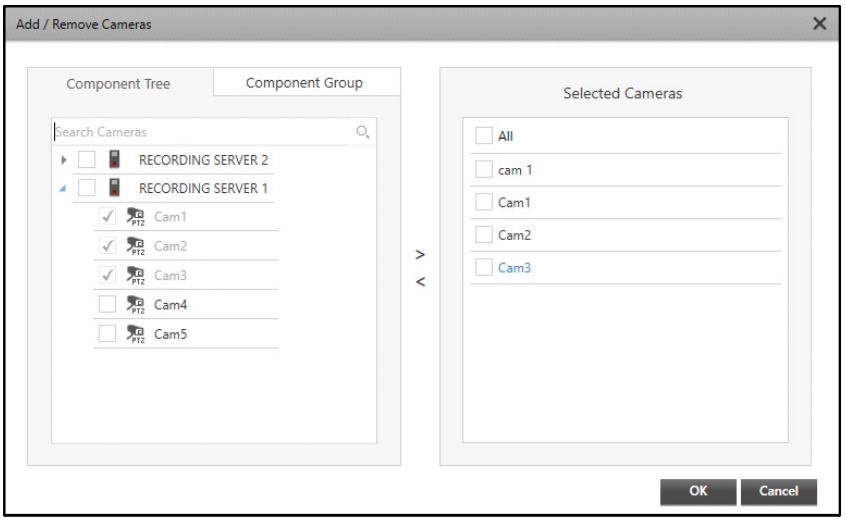
- Click **Add/ Remove Cameras**. The **Add/ Remove Cameras** pop-up appears.



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the desired cameras you wish to add from the Component Tree or Component Group tabs.

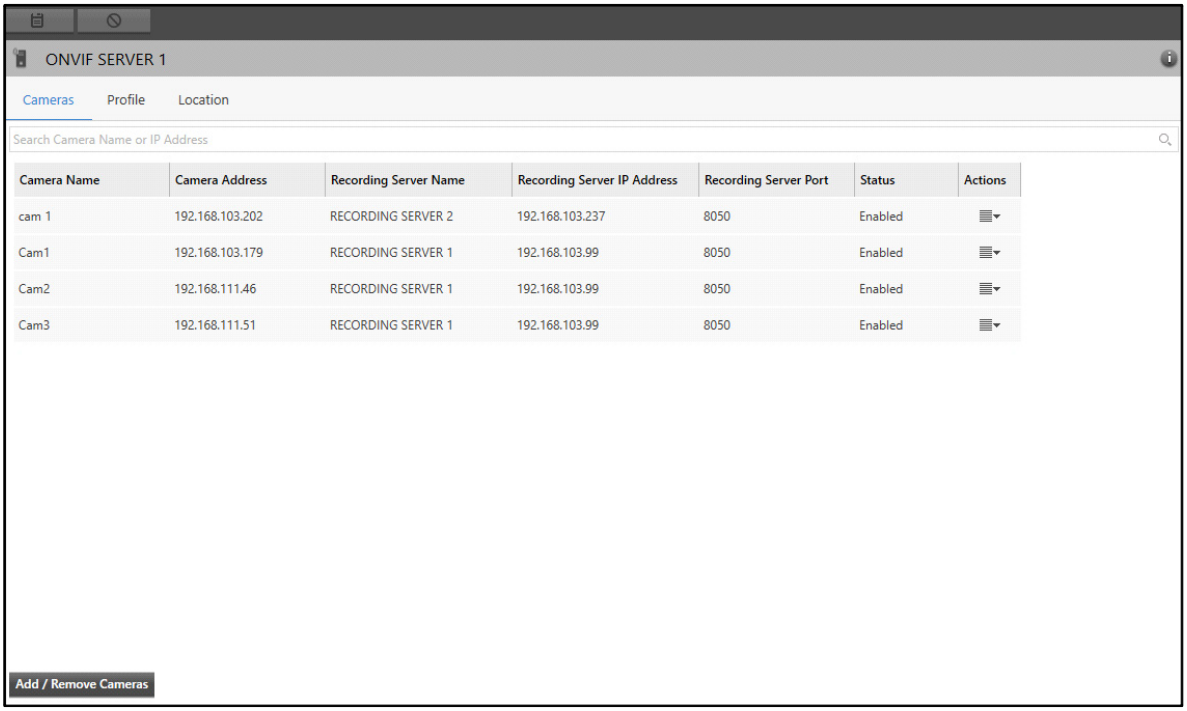
  Click the right arrow button to add these cameras to the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.

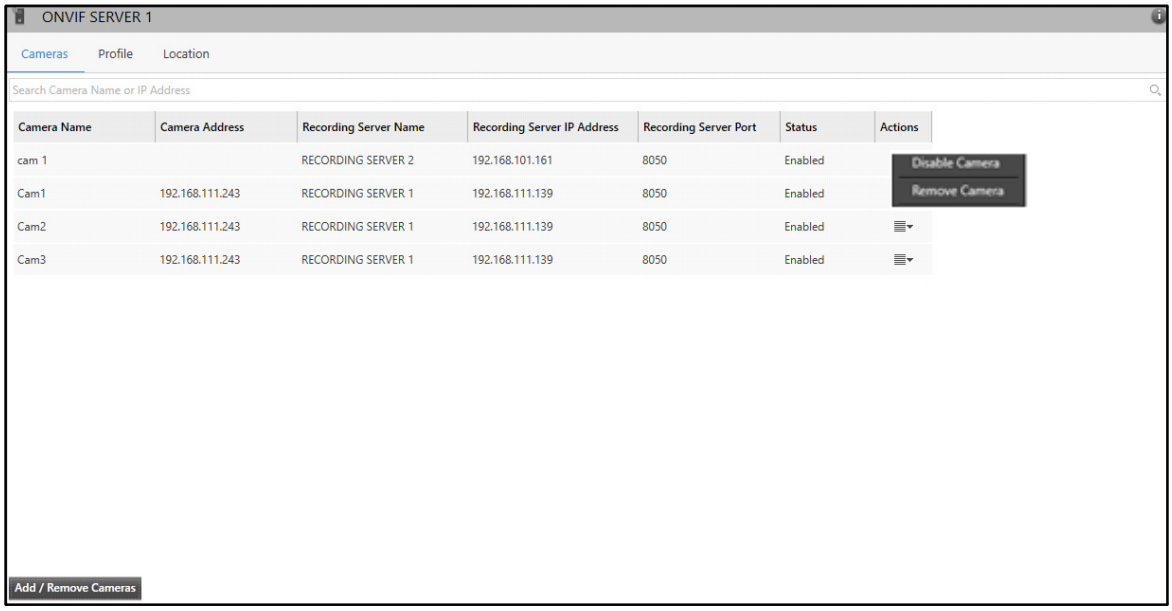


- Click **OK** to confirm or click **Cancel** to discard.

The added cameras appear in a list under the Cameras tab.



Under **Actions** , you can configure the following camera parameters — Disable Camera and Remove Camera.



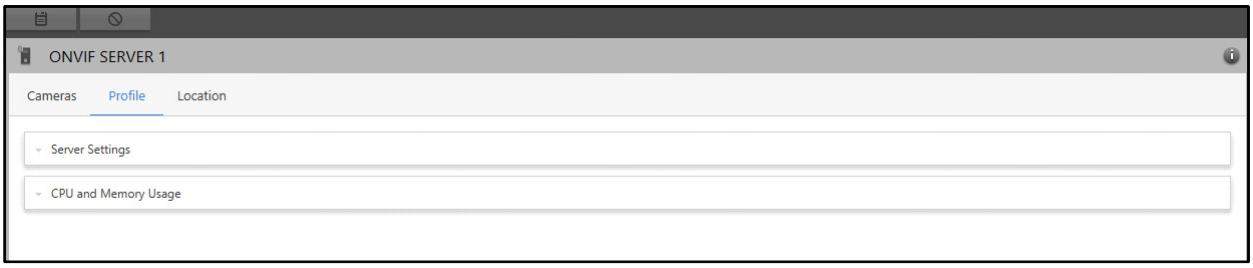
- **Disable Camera**: Selecting Disable Camera option will disable the camera. This will remove the camera from the list of ONVIF Server displayed on the left hand side. For enabling it again, click **Action** and select **Enable** Option.
- **Remove Camera**: Selecting Remove Camera will remove the camera from the ONVIF Server.

Profile

This tab enables you to view and configure Server Settings and CPU and Memory Usage.

To configure Profile settings,

- Click the **Profile** tab.



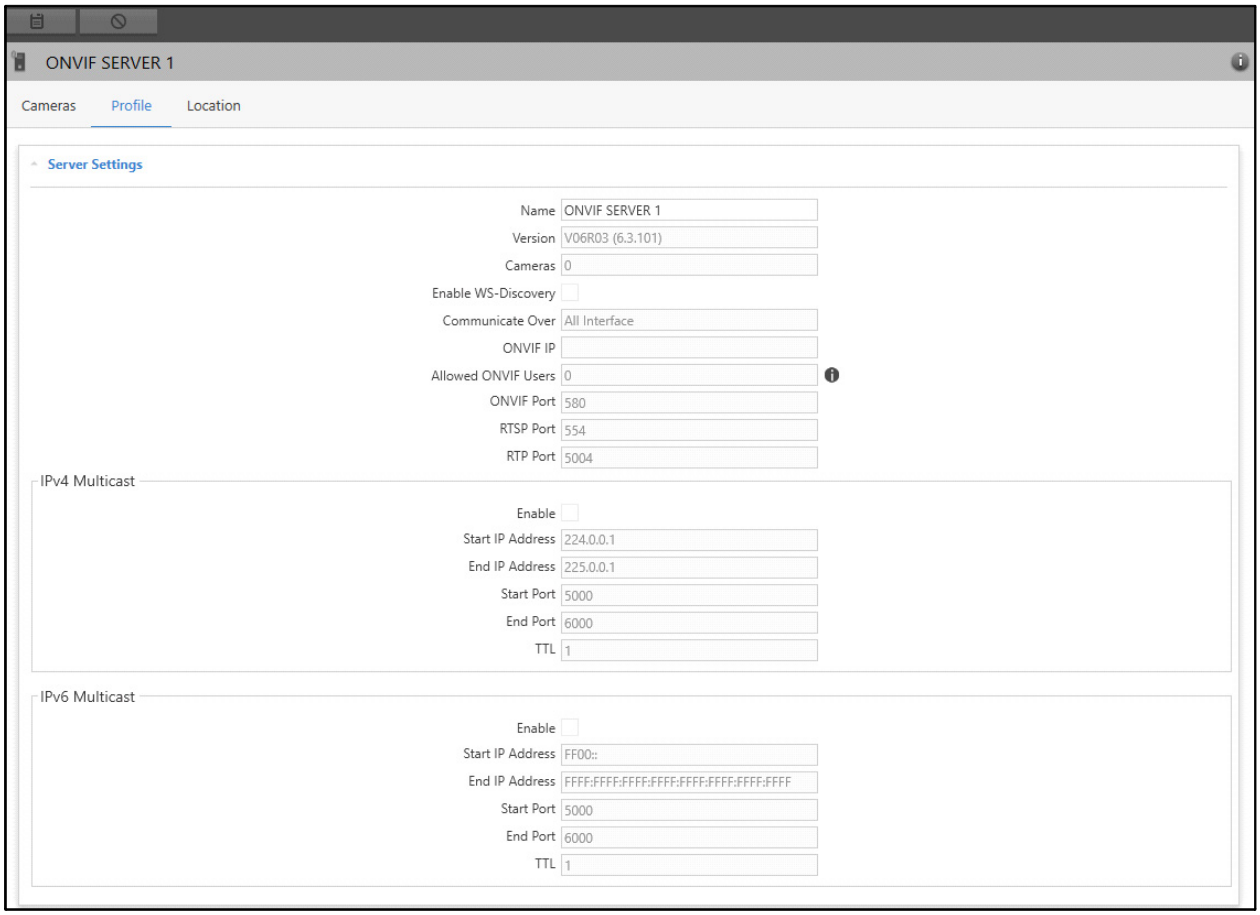
The Profile tab contains two collapsible panels — “Server Settings” and “CPU and Memory Usage”.

Server Settings

This panel displays the Server Settings of the ONVIF Server. You can edit and configure the ONVIF Server Name from this collapsible panel.

To view and edit the Server Settings,

- Click the **Server Settings** collapsible panel.



This collapsible panel displays the Server Settings and IPv4 and IPv6 Multicast Settings. The Server Settings of the ONVIF Server display — Name, Version, Cameras, Enable WS-Discovery, Communicate Over, ONVIF IP (IPv4/IPv6), Allowed ONVIF Users, ONVIF Port, RTSP Port and RTP Port.

The IPv4 and IPv6 Multicast Settings display — Start IP Address, End IP Address, Start Port, End Port and TTL.

You can configure the following parameters:

- **Name**: Specify a name for the ONVIF Server. In Name, you can enter upto 50 characters. Default: Name of the system where ONVIF Server is installed.

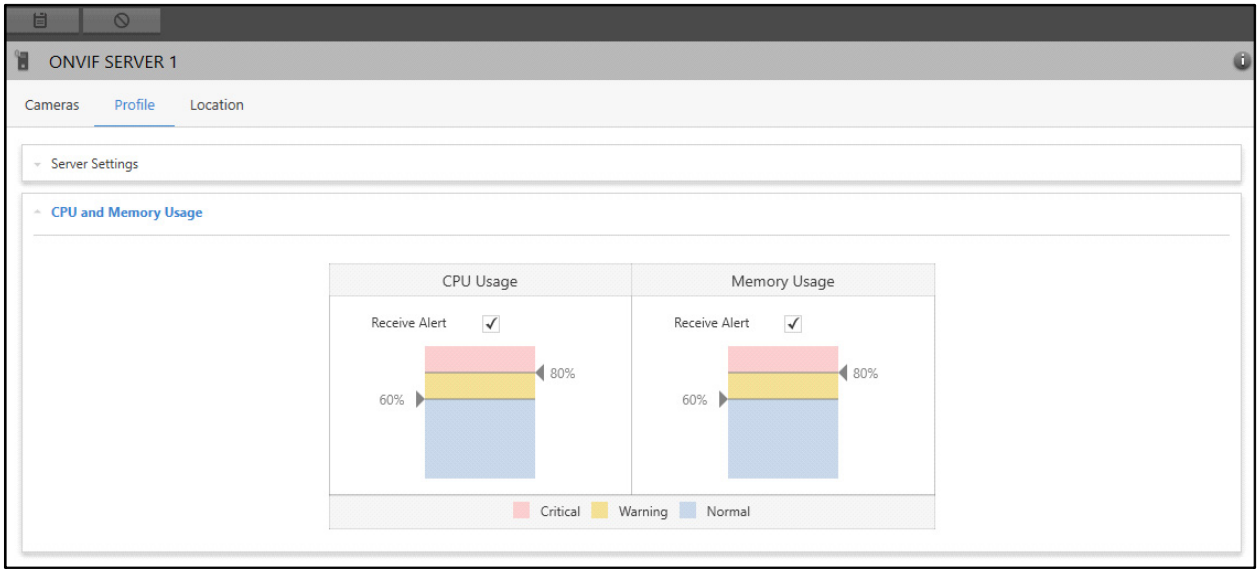
- Click **Save** to save the settings or click **Cancel** to discard.

CPU and Memory Usage

This panel allows you to configure the threshold value of CPU and Memory Usage and receive alerts when the ONVIF Server crosses these set values.

To configure the CPU and Memory Usage settings,

- Click the **CPU and Memory Usage** collapsible panel.



- **Receive Alert**: This check box is selected by default, to receive alerts when the ONVIF Server crosses the set threshold value under **CPU Usage** and **Memory Usage**. We recommend you not to clear this check box.

- **Critical, Warning and Normal Threshold Values:** The Critical, Warning and Normal Threshold Values for CPU and Memory Usage can be configured by dragging the pointer or tapping on the empty area. Valid Range: 0-100%. Default: Warning: 60, Critical: 80.

  In the Smart Client,
  - the CPU Usage/Memory Usage Exceeded pop-ups appear with a yellow boundary.
  - the CPU Usage/Memory Usage Critical pop-ups appear with a red boundary.
  - the CPU Usage/Memory Usage Critical event is highlighted in red color under Online Events.

  For example, in the above screen the CPU Usage and Memory Usage thresholds are configured as 60% for Warning and 80% for Critical respectively. Hence, you will receive an alert when the CPU usage or the memory usage goes beyond 60% and 80%, that is when it crosses the Warning and Critical limit as well as when it comes back to its Normal limit again.

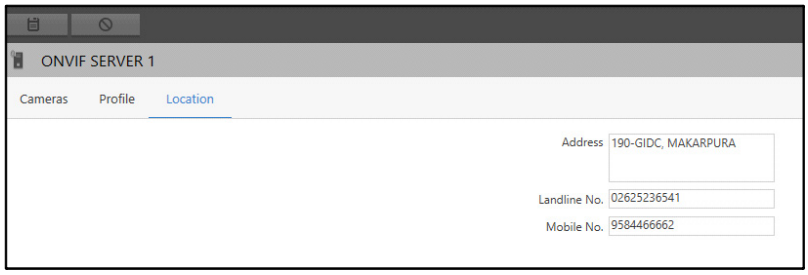
- Click **Save** to save the settings or click **Cancel** to discard.

Location

This tab enables you to view and configure the location information of a ONVIF Server.

To configure the Location,

- Click the **Location** tab.



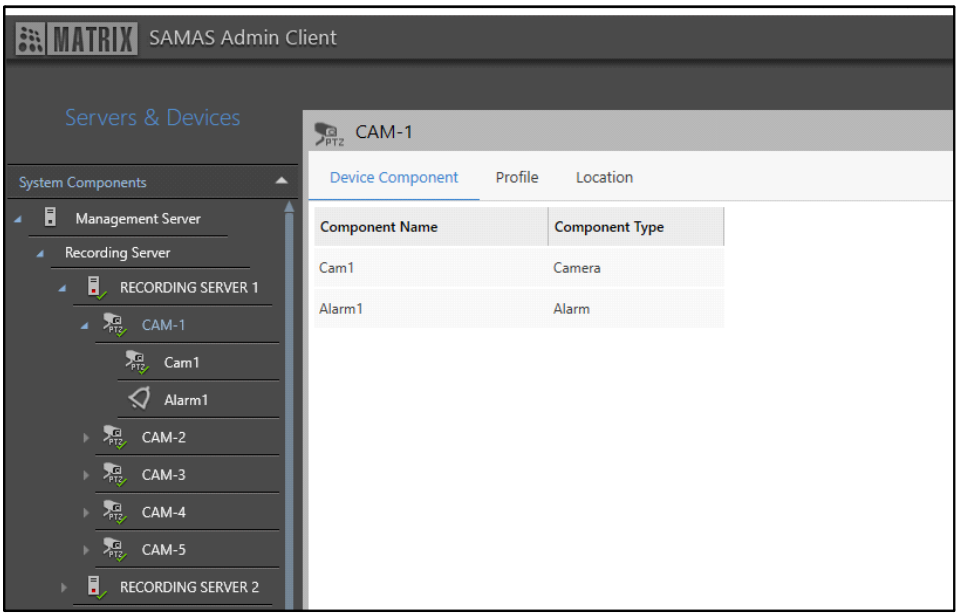
The configurations of Location Settings in ONVIF Server are similar to that of the Management Server. For details, refer to “Location”.

Device Configuration

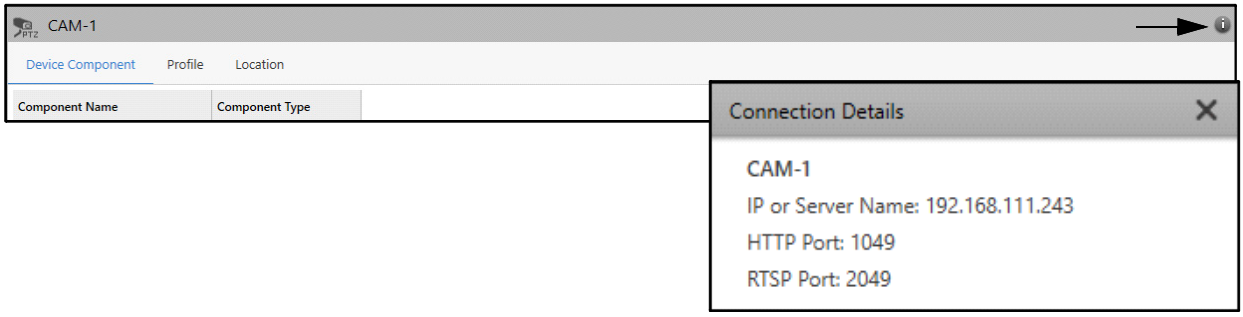
The Device page displays all the cameras assigned to the device. You can view and configure the Device Settings and specify the location of the device.

To configure Device Settings,

- Click **Servers & Devices > Recording Server > Device**
- Select the desired device.



- To view the **Connection Details** of the device, click **Connection Details** at the top right corner of the Device page. It displays the connection details of the device with the Recording Server. It displays the following details — Device Name, IP (IPv4/IPv6) or Server Name, HTTP Port and RTSP Port.



Each device consists of the following tabs.

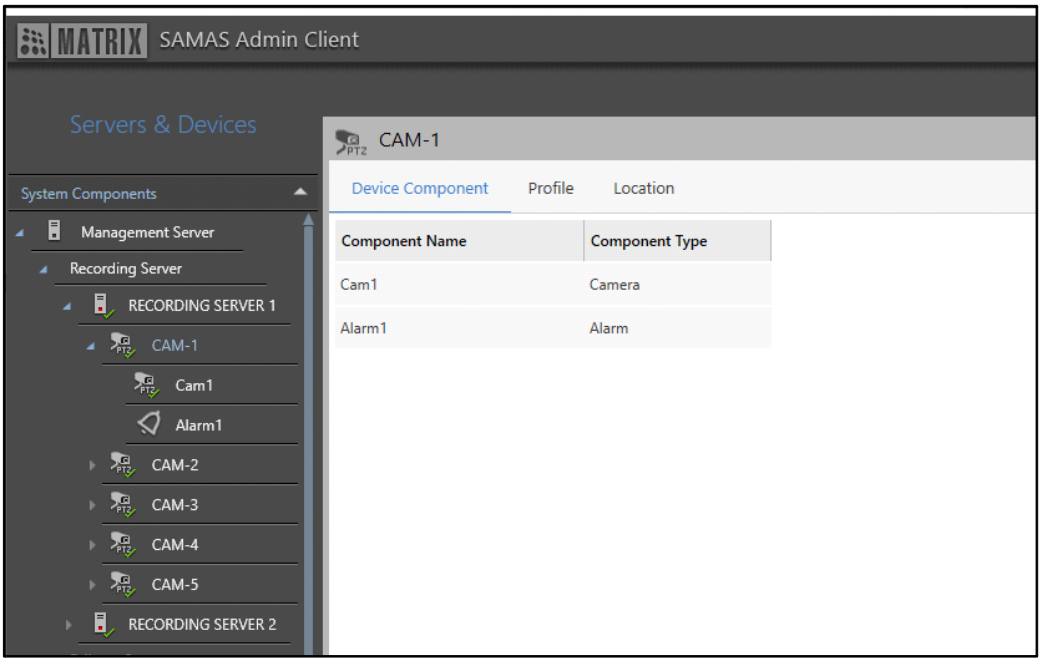
- "Device Component"
- "Profile"
- "Device Location"

Device Component

This tab enables you to view all the components of the device, including cameras, sensors and alarms.

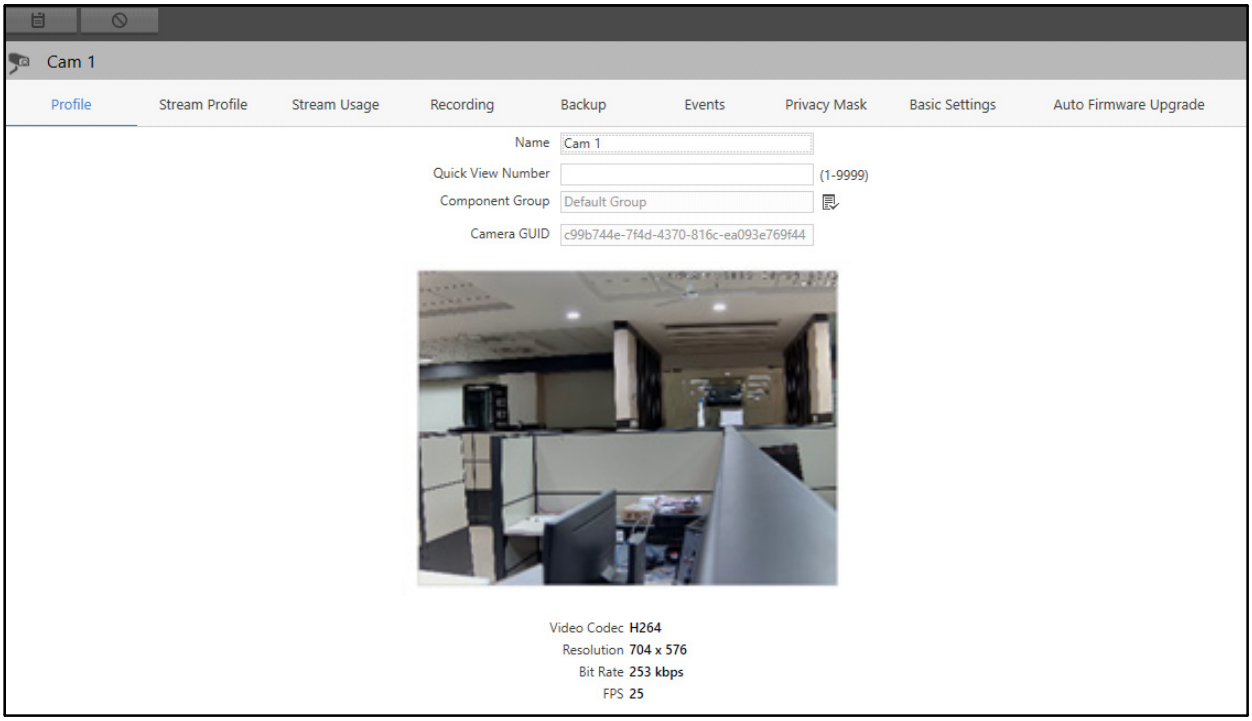
To view the components of the device,

- Select the desired device. The **Device Component** tab appears by default.



This tab displays two device parameters — Component Name and Component Type.

- Double-click the camera to configure its parameters. The following tabs appear — Profile, Stream Profile, Stream Usage, Recording, Backup, PTZ Positions, PTZ Tour, Events and Basic Settings.



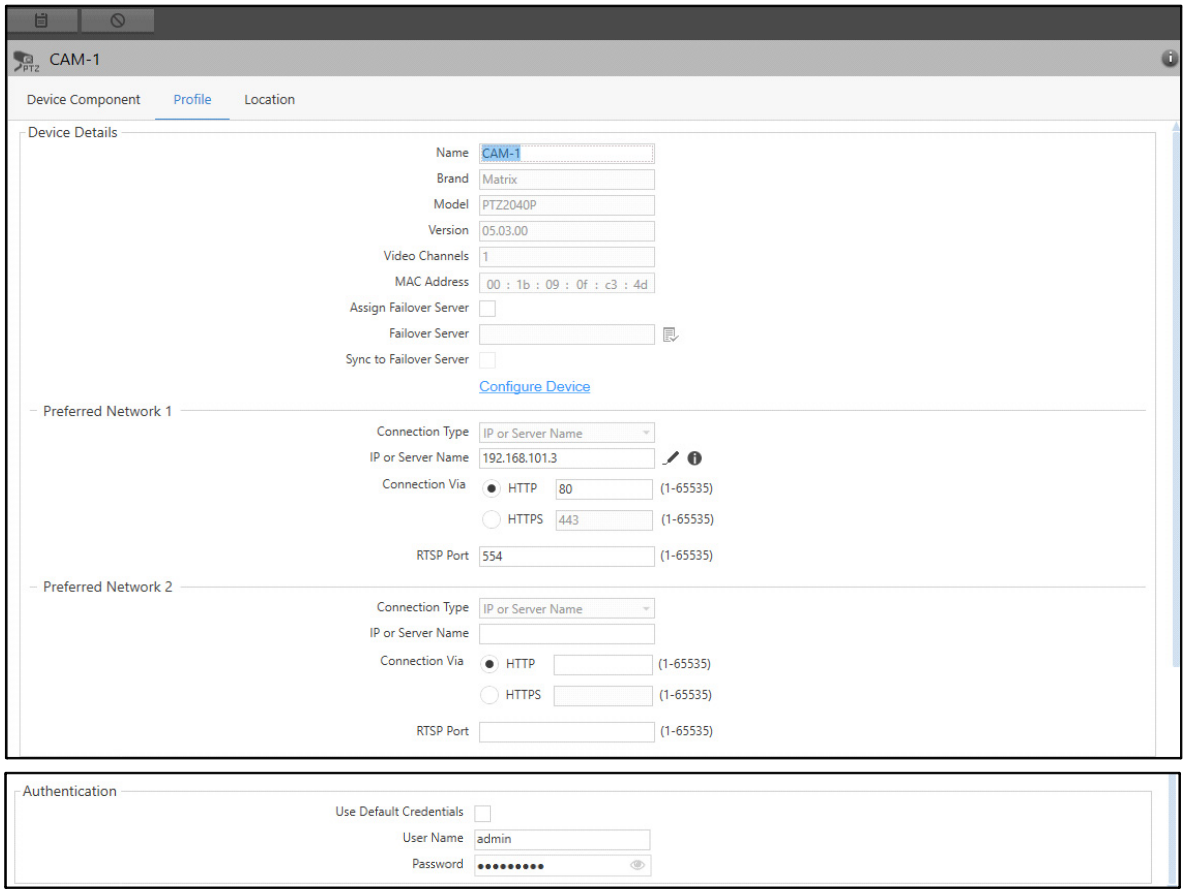
To know more about the configurations of the camera parameters, refer to “Camera Configuration”.

Profile

This tab enables you to view and configure the Device Profile for each device added to the Recording Server.

To configure the Device Profile,

- Click the **Profile** tab.



This page displays the following parameters — “Device Details”, “Preferred Networks 1/2” and “Authentication”.

For Mobile Cameras — Name, Brand, Model, Assign Failover Server and Sync to Failover Server will be applicable.

Device Details

This section displays details of the device. The Device Details displayed are — Name, Brand, Model, Version, Protocol, Video Channels, MAC Address, Failover Server details and Preferred Networks. You can configure the device by clicking on **Configure Device**.

You can configure the following parameters:

- **Name**: Specify a name for the device. In Name, you can enter upto 50 characters. Default: Blank.

- **Protocol**: If you have added the camera by selecting **ONVIF** under **Brand** and **Model** picklist, select the Protocol from the drop-down list.
- **Assign to Failover Server**: Select the check box if you wish to assign the device to a Failover Server.
- **Failover Server**: Select the desired Failover Server using the **Failover Server** picklist. Double-click to select the desired option.
- **Sync to Failover Server**: Select the check box if you wish to sync the device with the Failover Server.

Preferred Networks 1/2

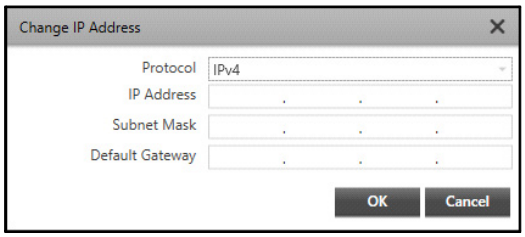
- **Connection Type**: The default Connection Type appears as **IP or Server Name**.
- **IP or Server Name**: Specify the IPv4/IPv6 Address or Server Name. In IP or Server Name, you can enter upto 255 characters. Default: IP or Server Name of the device using which it is added to Recording Server.

If Server Name is configured and the DNS Server provides both IPv4 and IPv6 IP Addresses after resolving the Domain Name, then IPv4 IP Address will be given priority.

Make sure the camera supports IPv4/IPv6 Addressing Mode before changing the IP Address.

OR

- Click **Edit** . The **Change IP Address** pop-up appears.



Configure the following parameters:

- **Protocol**: Select the Protocol from the drop-down list — IPv4,IPv6 — as per the IP Address of the camera.
- **IP Address**: Specify the new IPv4/IPv6 Address as per the selected **Protocol**. In IP Address, you can enter upto 39 characters. Default: Blank.
- **Subnet Mask/Prefix**: Specify the Subnet Mask/Prefix as per the selected **Protocol**. In Subnet Mask, you can enter upto 15 characters. In Prefix, you can enter upto 3 characters. Default: Blank.
- **Default Gateway**: Specify the Default Gateway as per the selected **Protocol**. In Default Gateway, you can enter upto 39 characters. Default: Blank.

- Click **OK** to confirm or click **Cancel** to discard.

- **Connection Via**: Select the Connection type from the options — HTTP or HTTPS. Specify the HTTP/ HTTPS Port. Valid Range: 1-65535. Default HTTP Port: 80, Default HTTPS Port: 443.
- **RTSP Port**: Specify the RTSP Port. Valid Range: 1-65535. Default: 554.

*Connection details are not displayed for devices added using the **Auto Add Matrix Devices** option.*

Authentication

- **Use Default Credentials**: Select the check box if you wish to use the default credentials for authentication.
- **User Name**: Specify the User Name for device authentication, if **Use Default Credentials** is disabled. In User Name, you can enter upto 100 characters. Default: Blank.
- **Password**: Specify the Password for device authentication, if **Use Default Credentials** is disabled. In Password, you can enter upto 100 characters. Default: Blank. Click **Show** to view the password. The icon toggles to **Hide**. Click **Hide** to hide the password.

- Click **Save** to save the settings or **Cancel** to discard.

*Use the **Configure Device** link to open the device Webpage and Camera Webpage for IP Cameras.*

On saving the changes, the device will either reboot automatically or you must reboot it manually. This depends on brand and model of the device.

The MAC address configured for the device (Online/Offline) will remain same as it was earlier if the IP Address is edited from the Device Profile page. After updating the IP Address for the offline device when the device is online again, the Admin Client will display the same MAC Address of that device while authenticating the new IP Address.

Device Location

This tab enables you to view and configure the location information of a device.

To configure the location,

- Click the **Location** tab.



The configurations of Location Settings of a device are similar to that of the Management Server. For details, refer to “Location”.



This location information will be displayed in the Event details in the Smart Client.

The configured name and location details of the device will be applicable while using the search functionality in Smart Client.

Camera Configuration

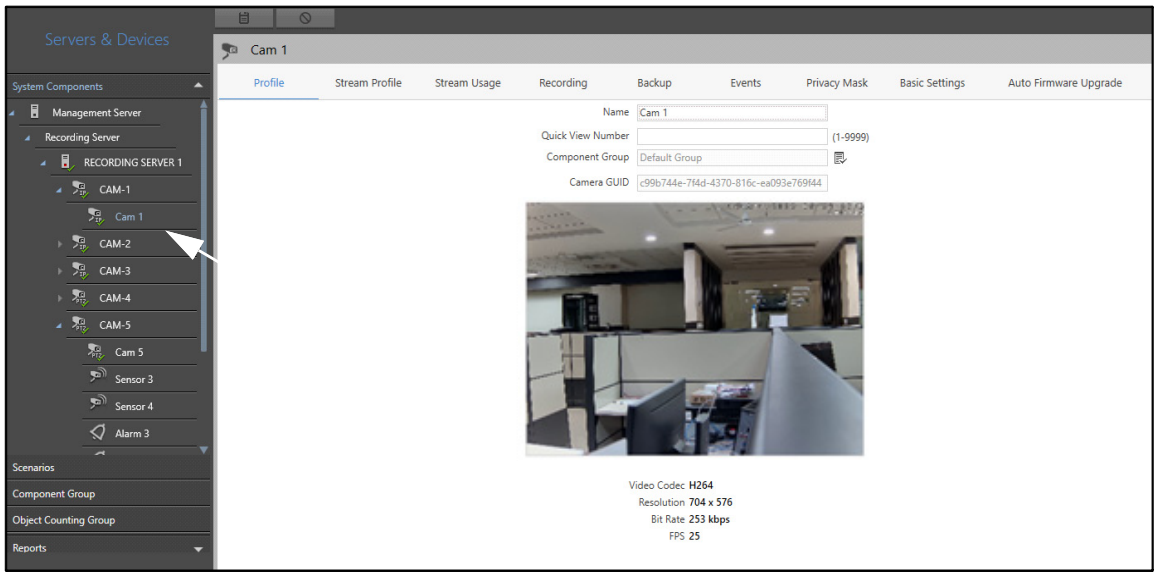
Once a device is configured and added to the Recording Server you can view all the IP cameras which are connected to the device. The Camera Configuration page displays all the camera parameters. You can view and configure the camera parameters for each camera added to the Recording Server.

Cameras added via ONVIF in Admin Client use Analytics via ONVIF for features like Motion Detection, Trip Wire, Intrusion In/Out, View Tamper and Audio Detection.

When device is connected with Recording Server/Failover Server, then the Date-Time of Recording Server/Failover Server is set for the camera.

To configure Camera parameters,

- Click **Servers & Devices > Recording Server > Device > Camera**
- Select the desired camera.



Each camera consists of the following tabs:

- “Profile”
- “Stream Profile”
- “Stream Usage”
- “Recording”
- “Backup”
- “Events”
- “PTZ Positions”
- “PTZ Tour”

- “Privacy Mask”
- “Basic Settings”
- “Location”
- “Auto Firmware Upgrade”
- “Advanced Settings”

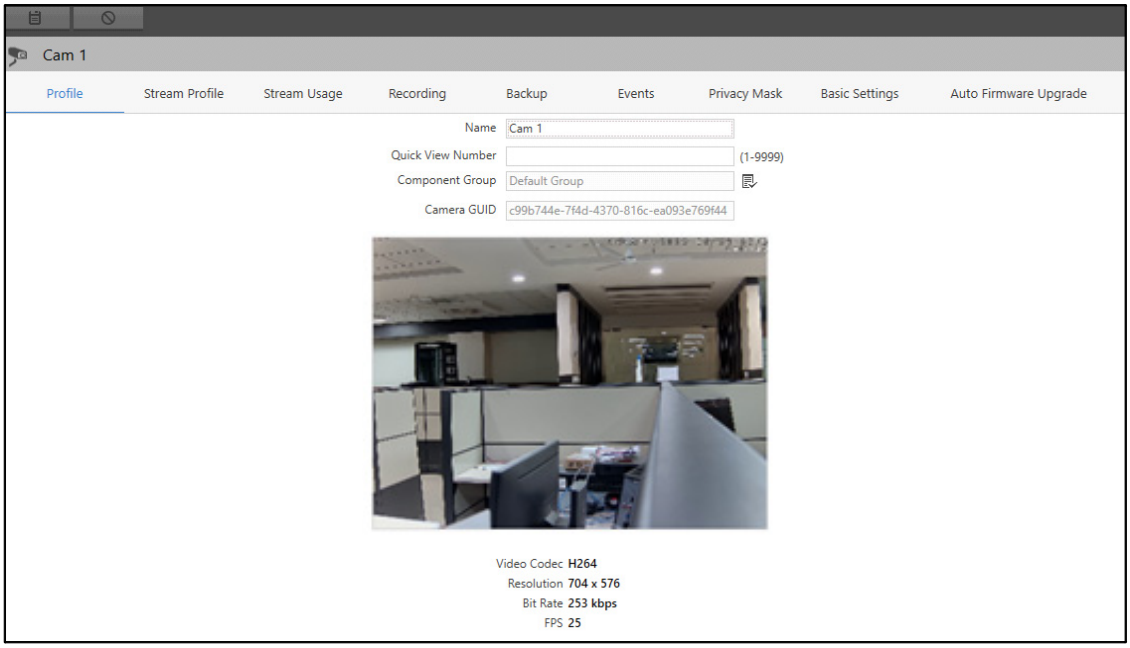
Tabs may vary according to the camera type and model. For details, refer to “Supported Devices”.

Profile

This tab enables you to view and configure the Camera Profile Settings for each camera added to the Recording Server.

To configure the Camera Profile Settings,

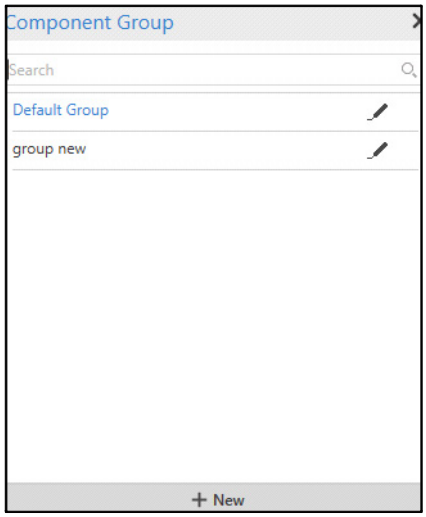
- Select the desired camera. The **Profile** tab appears by default.



Configure the following parameters:

- **Name**: Specify a name for the camera. In Name, you can enter upto 80 characters. Default: Default IP Address or Server Name of the camera using which it was added to Recording Server.
- **Quick View Number**: Assign a Quick View Number to the camera for swift selection of this camera on the Smart Client’s monitoring window in order to start its Live View. For more information on Quick View, refer the **SATATYA SAMAS Smart Client Manual**. Valid Range: 1-9999. Default: Blank.
- **Component Group**: Select the desired Component Group where you wish to assign the camera using the **Component Group** picklist.

- Click **Component Group** picklist. The **Component Group** pop-up appears.



  - Double-click to select the desired Component Group from the list. You can also edit an existing Component Group or add a new one. To know more about configuring Component Groups, refer to “Component Group”.

- **Camera GUID**: This is an unique ID assigned to the camera by the system. This is useful when the camera streams need to be sent to the third party clients through the ONVIF Server or RTSP Server.

  Live View of the camera will be displayed along with the following details — Video Codec, Resolution, Bit Rate and FPS. Live View of Mobile Camera will be visible only when the Push Video feature is being accessed from the associated Mobile Client.

- Click **Save** to save the settings or click **Cancel** to discard.

Stream Profile

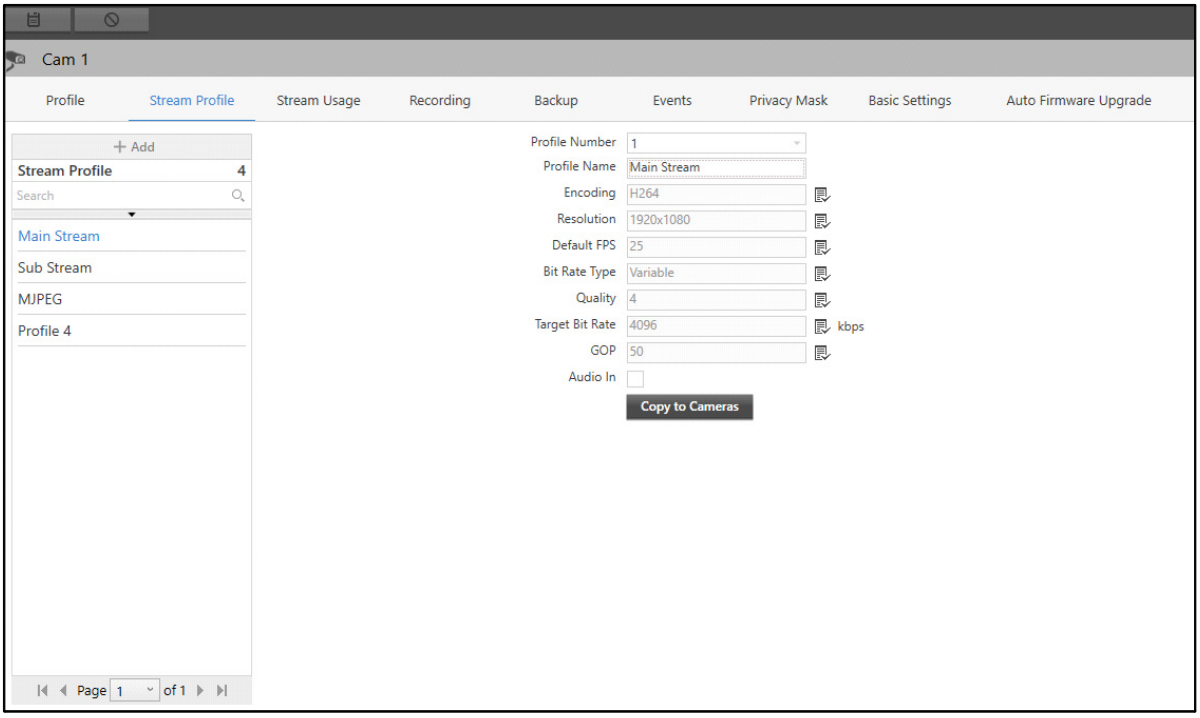
This tab enables you to set up different Stream Profiles for the camera. These profiles can be used for requesting live stream as well as for recording videos. You can also schedule the usage of these profiles depending on the video quality required and available storage.

This option is not available for Cameras connected with the NVR as well as Generic Cameras.

The quality of streamed video from a camera depends on a number of factors such as, the compression format, resolution, frame-rate, bit-rate as well as the available bandwidth for streaming. To control these factors based on the desired output quality as well as the bandwidth limitations (such as for remote viewing on a computer), you can create and configure different Stream Profiles.

To configure Stream Profiles,

- Click the **Stream Profile** tab. The Stream Profiles added already appear in a list on the left hand side.



- Click **Add**.

By default, these stream profiles are supported — Main Stream, Sub Stream, MJPEG, Profile 4 and Audio Out. The stream profiles that appear by default depend on how camera has been added, that is, via specific brand, ONVIF or Generic. The stream profiles that appear by default also differ based on the brand and model of the camera that has been added. The Stream Profile parameters and their default set values also differ based on camera brand and model.

The number of Stream Profiles that can be configured depends on the brand and model of the camera that has been added.

The Stream Profile parameters will depend on how camera has been added, that is, via specific brand, ONVIF or Generic.

The values available for selection against each parameter will depend on the camera brand and model.

*For **Mobile Cameras**, only MJPEG Stream Profile is applicable. These parameters will appear as disabled. You cannot add/delete/edit any Stream Profile.*

Configure the following parameters:

- **Profile Number**: Select the Profile Number from the drop-down list.
- **Profile Name**: Specify a Profile Name for the new Stream Profile. In Profile Name, you can enter upto 50 characters. Default: As Set on Camera webpage against the respective Profile Number.
- **Encoding**: It is the compression format for video transmission, also known as CODEC. Each Stream Profile is associated with a CODEC and its related properties. Common Video CODECs are H.264, H.265, MPEG4 and Motion JPEG (or, MJPEG). H.264 may be preferred for low bandwidth

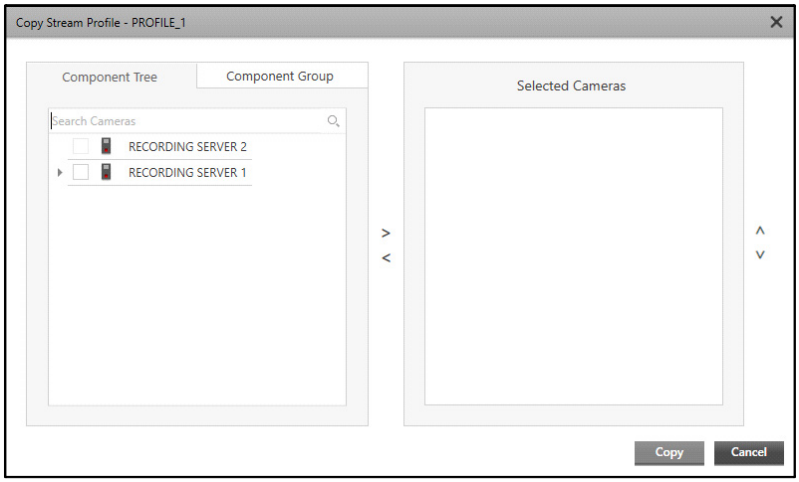
transmission as it provides higher compression in comparison to MPEG4 and MJPEG. Select the desired Encoding format using the **Encoding** picklist. Double-click on the desired option to select.

- **Resolution**: It is the size of the image on the display (normally measured in pixels). 4CIF, CIF and QCIF are some popular recording resolutions. Greater the resolution, greater would be the storage space required. Select the desired Resolution using the **Resolution** picklist. Double-click on the desired option to select.
- **Default FPS**: For a video, it is the number of frames sent per second. The higher the value of FPS, the better the speed and quality of the video. Select the desired FPS value using the **Default FPS** picklist. Double-click on the desired option to select.
- **Quality**: It determines the image quality. Select the desired value of Quality using the **Quality** picklist. Double-click on the desired option to select.
- **Target Bit Rate**: It specifies an average bit-rate that must be targeted for the video compression. Select the desired Target Bit Rate using the **Target Bit Rate** picklist. Double-click on the desired option to select.
- **GOP**: It stands for Group of Pictures. This parameter is required for specific encoding formats such as MPEG, in which coded video streams can be decoded as a sequence of successive pictures or frames (I-frames, B-frames, P-frames) carrying independent as well as predictive information. The GOP is measured as the interval or distance between two successive Intra-frames (I-frames). Higher GOP will typically result in a lower bit-rate. Select the desired value of GOP using the **GOP** picklist. Double-click on the desired option to select.
- **Audio In**: Select the check box to enable audio streaming from the camera microphone.

- Click **Save** to save the settings or **Cancel** to discard.

You can copy the Stream Profile configurations to other cameras as well.

- Click **Copy to Cameras**. The **Copy Stream Profile** pop-up appears.

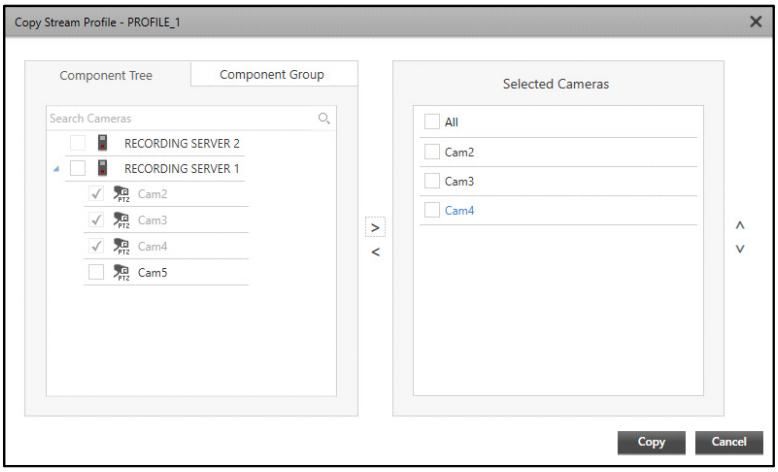


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the those cameras whose Stream Profile you wish to copy from in the Component Tree or Component Group tabs.

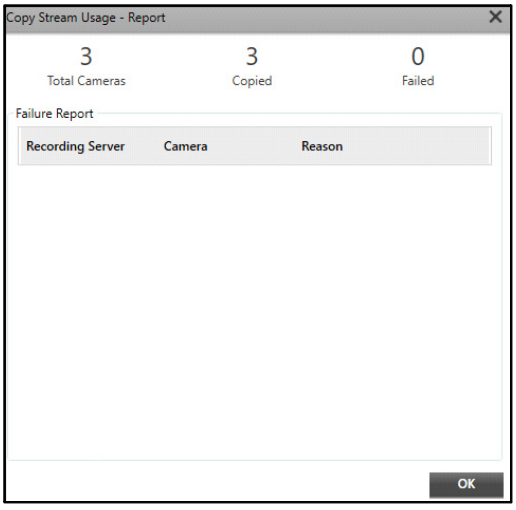
  Click the right arrow button to add these cameras to the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the desired check boxes for the cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.

  You can change the sequence of the cameras in the Selected Cameras list. To do so, select the check box of the desired cameras and click the up or down button as per your requirement.



- Click **Copy** to copy the Stream Profile to the selected cameras. The **Copy Stream Profile - Report** appears.



  The report displays the total number of cameras, the number of Stream Profiles copied successfully and the number of Stream Profiles that were not copied along with the reason of failure.

- Click **OK**.

Stream Usage

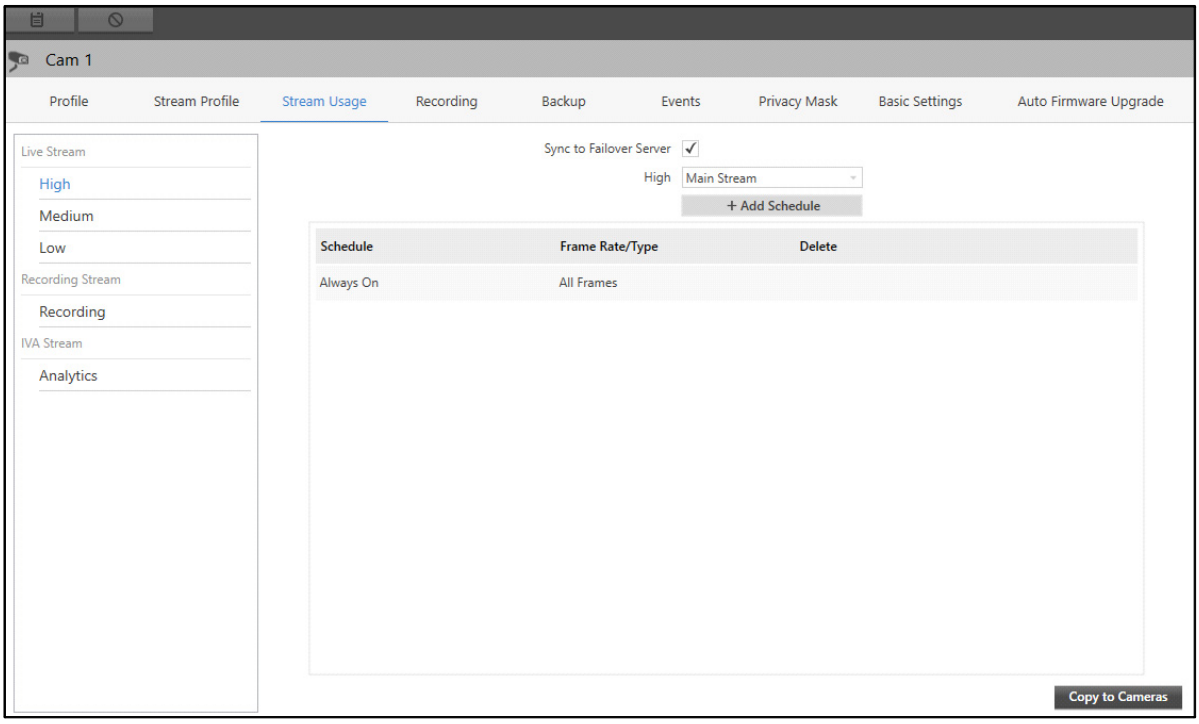
Stream Usage is not applicable to Mobile Cameras.

Once Stream Profiles are configured in the Admin Client, they can be associated with pre-defined stream types, depending on the usage. This tab enables you to map the configured Profiles against following types of stream usage:

- Live Stream — High, Medium, Low
- Recording Stream
- IVA Stream

To configure Stream Usage,

- Click the **Stream Usage** tab.



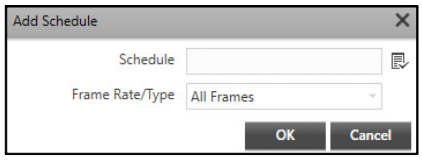
- If you select **High** from the Live Stream options.

  Configure the following parameters:

  - **Sync to Failover Server**: Select the check box to sync the configuration of the Stream Usage with the Failover Server camera Stream Usage.

  - **High**: Select the desired Stream Profile from the drop-down list.

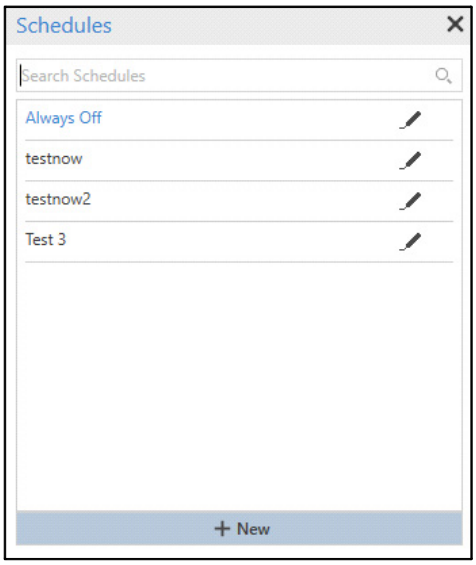
  - Click **Add Schedule**. The **Add Schedule** pop-up appears.



Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Stream Profile using the **Schedule** picklist.

  Click **Schedule** picklist. The **Schedules** pop-up appears.



  Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Frame Rate/Type**: Select the desired option for Frame Rate/Type from the drop-down list.

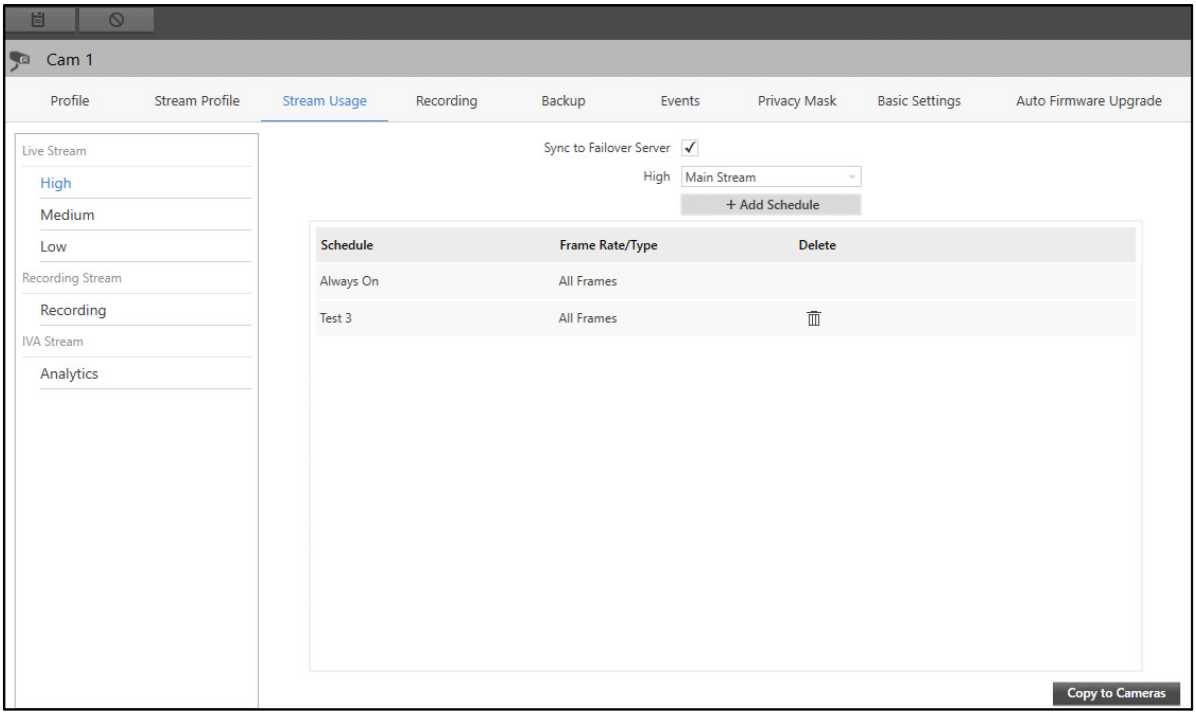
- Click **OK** to confirm or click **Cancel** to discard.

- Click **Save** to save the settings or **Cancel** to discard.

The configured schedules for the selected Stream Profile appear in the list on the left hand side.

- Click **Delete** to delete the schedule.

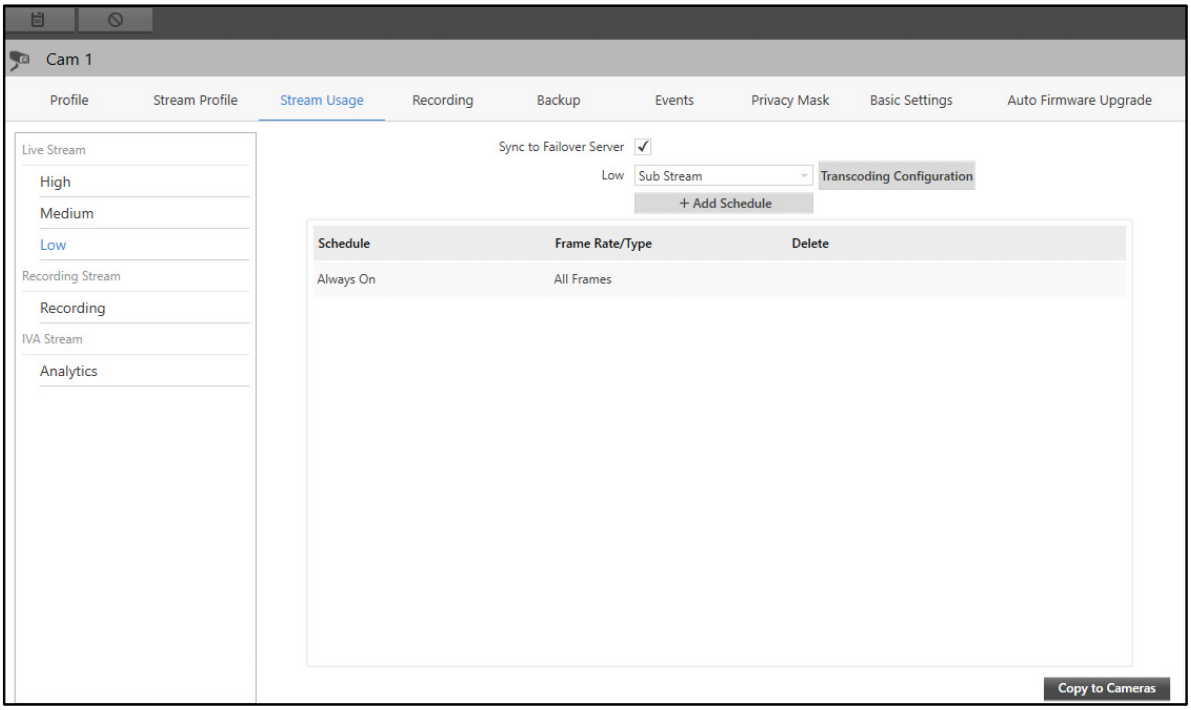
If multiple overlapping schedules are assigned to the same Stream Profile, then the highest priority would be given to the last schedule added (bottom-most schedule) and the second-highest priority would be given to the schedule added before this. However, this will be applicable only for user-defined schedules, whereas, system-defined schedules (such as “Always On”) shall always receive the lowest priority by default.



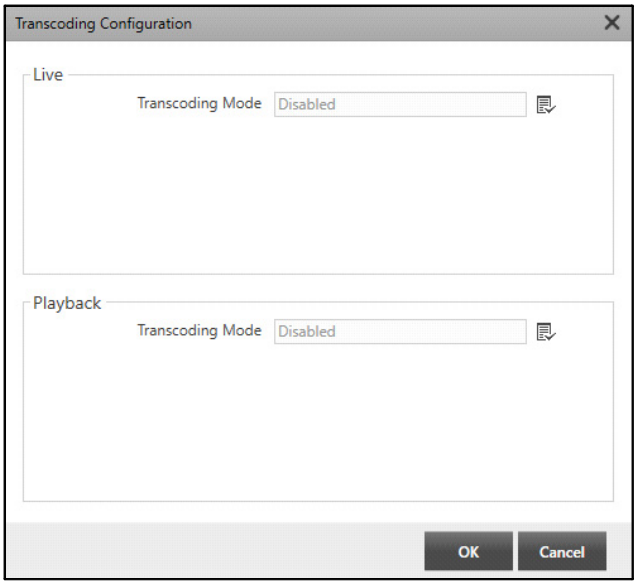
The configurations of **Medium** and **Low** Live Stream, **Recording Stream** and **IVA Stream** are similar to **High** Live Stream.

If you want to send streams to the Transcoding Server, you must select the **Low** Live Stream option and configure the desired Transcoding options.

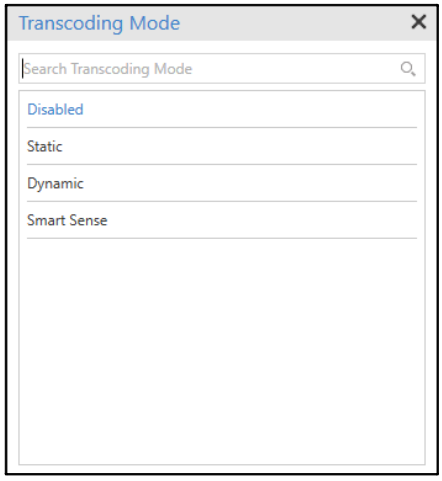
- Select **Low** from the Live Stream options. The **Transcoding Configuration** option appears.



- Click **Transcoding Configuration**. The **Transcoding Configuration** pop-up appears.



- Select the Transcoding Mode for **Live** as well as **Playback** using the **Transcoding Mode** picklist.
- Click **Transcoding Mode** picklist. The **Transcoding Mode** pop-up appears.



The following Transcoding Mode options appear — Disabled, Static, Dynamic and Smart Sense. Double-click to select the desired option.

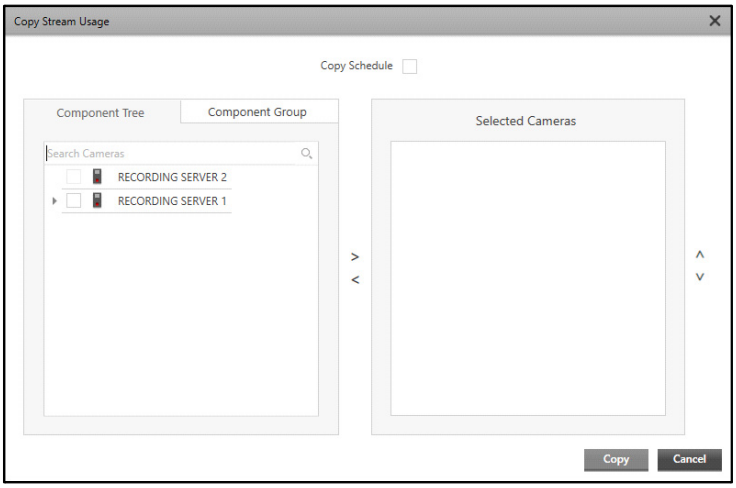
- If you select **Disable**, the streams will not be sent to the Transcoding Server and transcoding will not take place.
- If you select **Static**, the transcoding will always take place. The streams will always be sent to the Transcoding Server for optimization. The system will not check the congestion at RS/FoS end.
- If you select **Dynamic**, the transcoding will take place only when there is congestion at the Media Client end. The streams will be sent to the Transcoding Server for optimization. The stream parameters of the transcoded streams will be as per the configurations done. When there is no congestion, the RS/FoS will not send the streams to the Transcoding Server and the transcoding will stop.
- If you select **Smart Sense**, the transcoding will take place only when there is congestion at the Media Client end. The streams will be sent to the Transcoding Server for optimization. The stream parameters

of the transcoded streams will be as per the congestion at the Media Client end. When there is no congestion, the RS/FoS will not send the streams to the Transcoding Server and the transcoding will stop.

- Click **OK** to confirm or **Cancel** to discard.

Once all the Stream Usage settings are configured for the desired Stream Profiles, you can copy it to other cameras.

- Click **Copy to Cameras**. The **Copy Stream Usage** pop-up appears.



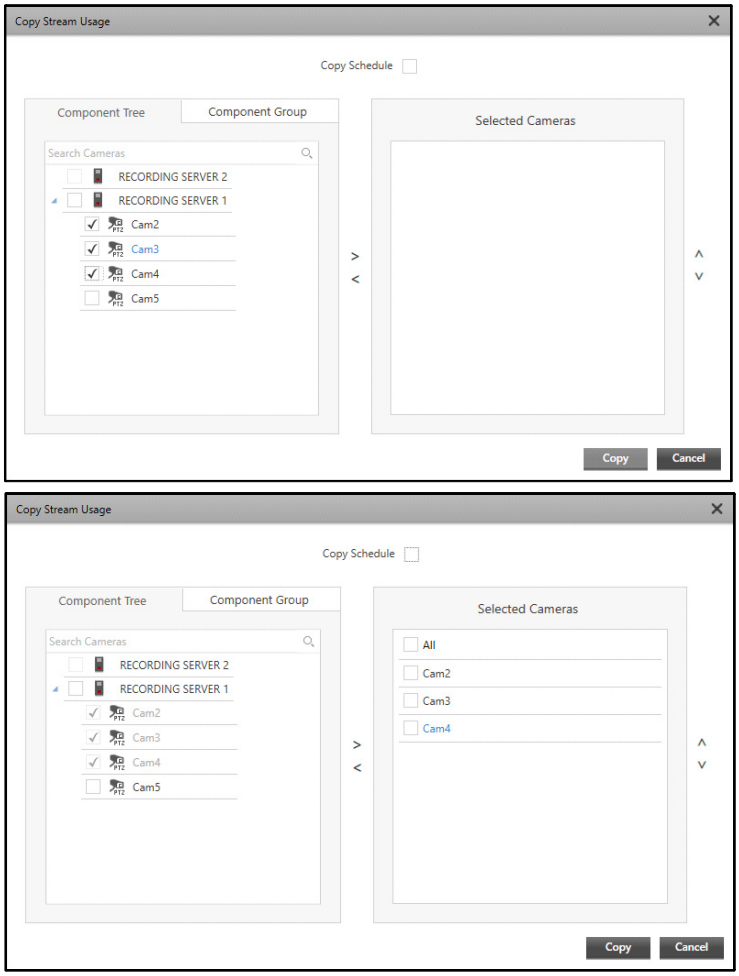
- Select the **Copy Schedule** check box if you wish to copy the configured schedules to the selected cameras.

- The list of cameras of same brand and model added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the cameras whose Stream Usage settings you wish to copy from in the Component Tree or Component Group tabs.

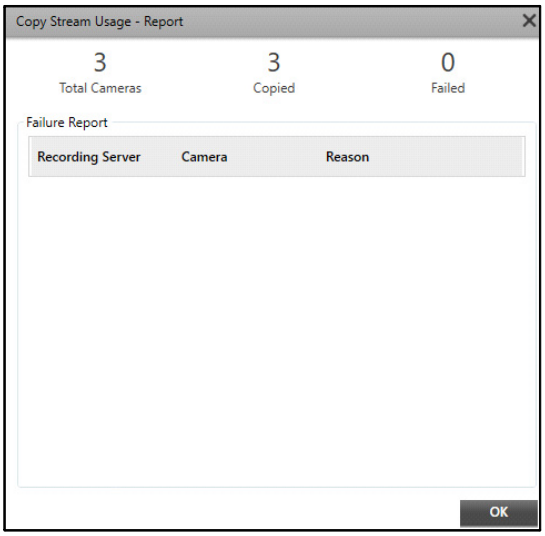
  Click the right arrow button to add these cameras to the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.

  You can change the sequence of the cameras in the Selected Cameras list. To do so, select the check box of the desired cameras and click the up or down button as per your requirement.



- Click **Copy** to copy the Stream Usage settings to the selected cameras. The **Copy Stream Usage - Report** appears.



The report displays the total number of cameras, the number of Stream Usage records copied successfully and the number of Stream Usage records that were not copied along with the reason of failure.

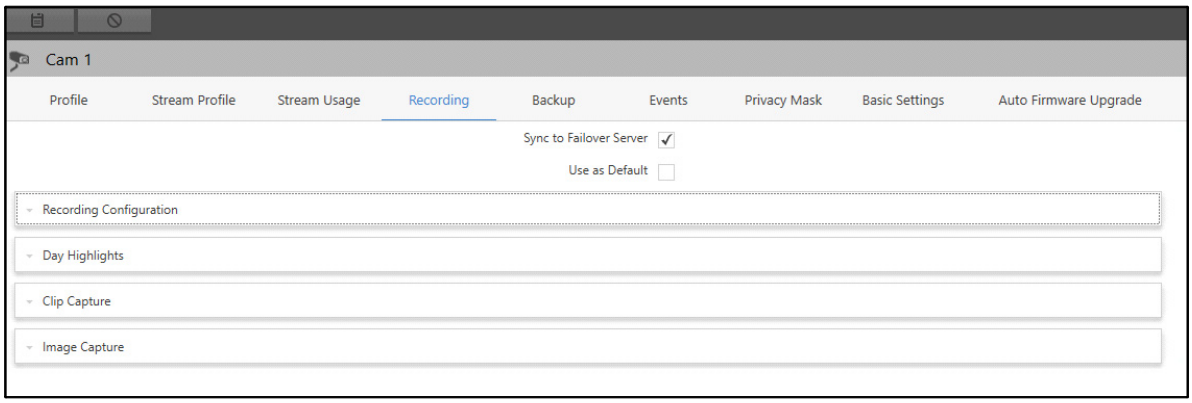
- Click **OK**.

Recording

This tab enables you to set the Recording configurations of a camera.

To configure camera Recording,

- Click the **Recording** tab.



Configure the following parameters:

The following options appear when you select a Camera's **Recording** tab from the **Recording Server**.

- **Sync to Failover Server**: Select the check box to synchronize the configuration of the Recording Server's camera Recording page with the Failover Server's camera Recording page.
- **Use as Default**: Select the check box to copy the camera's Recording configurations to the Default Recording Settings.

The above options are applicable when you select the Camera under the Recording Server.

The following option appears when you select a Camera's **Recording** tab from the **Failover Server**.

Enable Recording Redundancy: Select the check box to enable recording in the Failover Server, irrespective of the state of the Recording Server for the cameras. Hence, even if the connectivity between the device and the Recording Server is lost, the recording will always continue in the Failover Server. Also make sure, the Recording Settings of the Devices are same in both the servers — RS, FOS.

This check box is enabled by default, if you have enabled the same in **Default Recording Redundancy Settings** collapsible panel when adding a new camera. For more details, refer to "Profile".

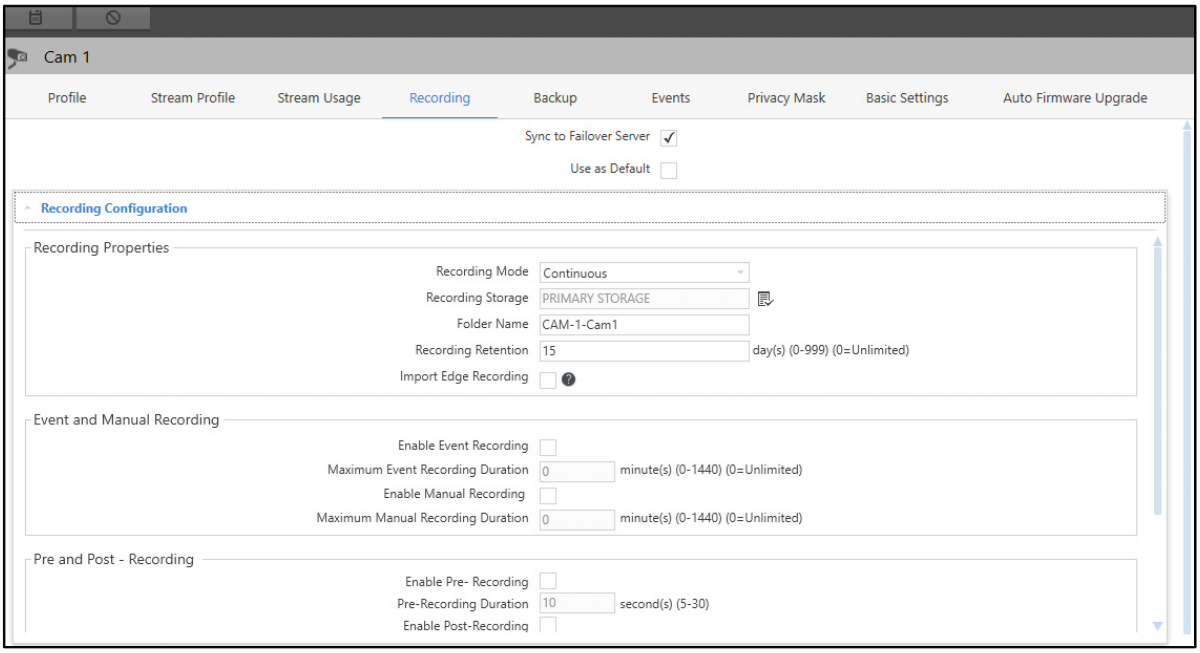
The Recording tab contains four common collapsible panels (whether accessed from the RS or FOS) — "Recording Configuration", "Day Highlights", "Clip Capture" and "Image Capture".

Recording Configuration

This panel allows you to configure the Recording properties and settings of the camera.

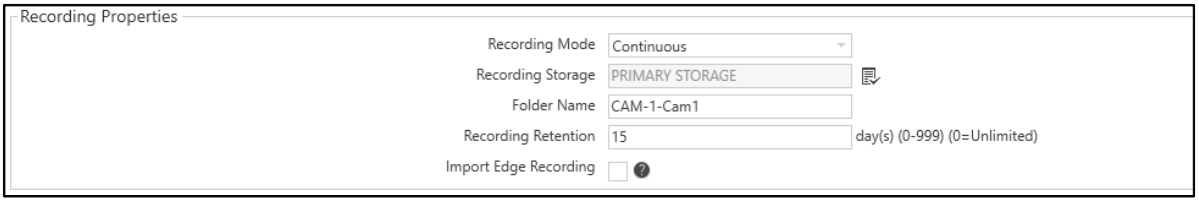
To configure the Recording parameters,

- Click the **Recording Configuration** collapsible panel.



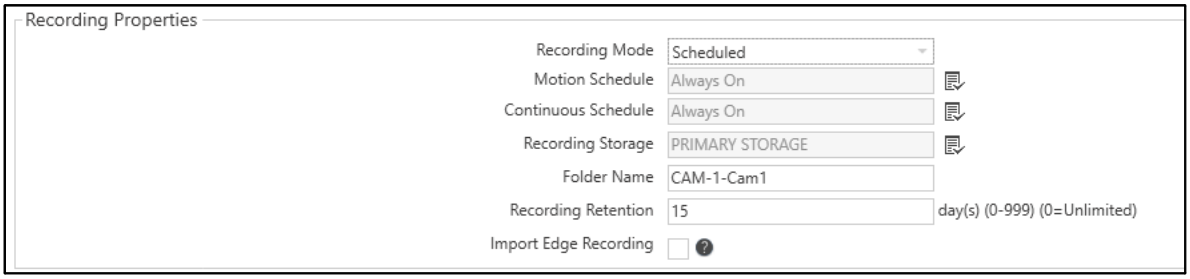
Recording Properties

This section allows you to configure the basic Recording settings of the camera.



- **Recording Mode**: Select the desired Recording Mode from the drop-down list. There are four types of Recording Modes — Off (No Recording), On Motion (Recording triggered on motion detection only), Continuous (Continuous Recording) and Scheduled (Recording triggered as per configured schedule). If you select the Recording Mode as **Scheduled**, you need to configure the **Motion Schedule** and **Continuous Schedule**.

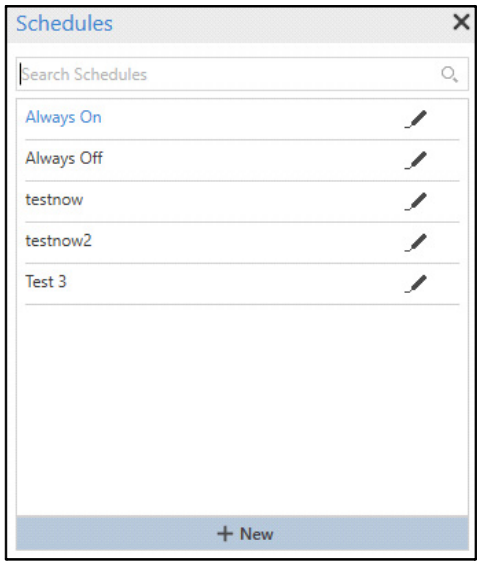
On Motion Recording Mode is not applicable to Mobile Cameras.



- **Motion Schedule**: Select the Motion Schedule using the **Motion Schedule** picklist.

Motion Schedule is not applicable to Mobile Cameras.

- Click **Motion Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".

  Similarly, select the desired schedule for the **Continuous Schedule**.

- **Recording Storage**: Select the desired Recording Storage using the **Recording Storage** picklist. All the configured Recording Drives for the Recording Server of the camera will appear in the list. Double-click to select the desired option.

- **Folder Name**: Specify the Folder Name where you wish to store the recordings in the configured Storage Drive. In Folder Name, you can enter upto 80 characters. Default: Camera name.

- **Recording Retention:** Specify the number of days after which the recording must be cleared from the configured Storage Drive. Valid Range: 0-999 days. Default: 15.

Import Edge Recording is not applicable to Mobile Cameras.

- **Import Edge Recording**: The Edge Recording feature enables Matrix Devices [DVR, HVR, NVR, Matrix Camera and Cameras added using ONVIF (that support Profile G)] to act as failover devices in the event of network or server failure. This supports continuous video recording and prevents loss of recordings over an unstable network connection.

  Select the check box to ensure that all recordings done on the device side, during the time when server was offline or device was disconnected, are automatically imported to the Recording Server once the connection is restored.

  The recordings from camera will be saved in the camera folder of the Recording Server in **mrd** file format. The edge recording details are stored in **merv** file format.

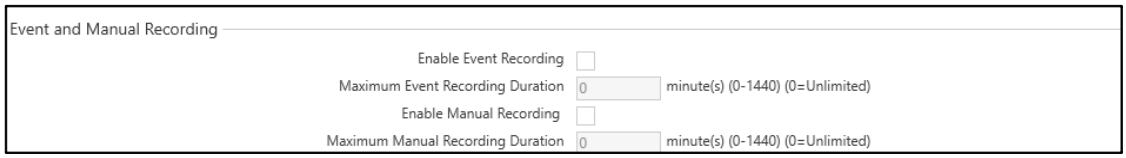
  For **Continuous** Recording Mode, all recordings will be fetched from device for the particular camera.

  For **On Motion** Recording Mode, only Alarm recordings will be fetched for the camera.

- Click **Save** to save the settings or **Cancel** to discard.

Event and Manual Recording

This section allows you to configure the Event and Manual Recording settings of the camera.



- **Enable Event Recording**: Select the check box to enable recording to be triggered by pre-defined or custom Events, such as Storage Full, Device Disconnected, etc.
- **Maximum Event Recording Duration**: Specify the maximum duration in minutes for which the recording must continue for an Event. Valid Range: 0-1440 minutes. Default: 0.

*For the same camera, if you have configured **Stop Recording after specific time and/or Stop Recording on event Activation** under "Record Event" as well as **Maximum Event Recording Duration**, then priority will be given to the configurations done for **Record Event.***

- **Enable Manual Recording**: Select the check box if you wish the Events to be recorded manually.
- **Maximum Manual Recording Duration**: Specify the maximum duration in minutes for which the Manual Recording must continue for an Event. Valid Range: 0-1440 minutes. Default: 0.

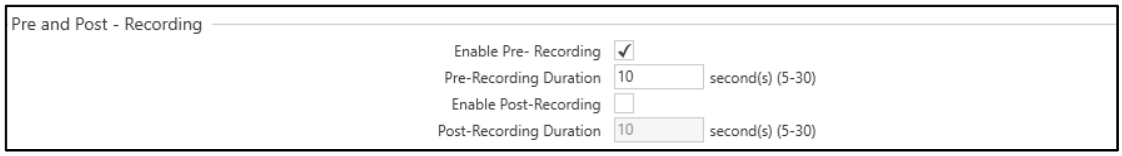
Specify the Maximum Event/Manual Recording duration as "0" to allow unlimited recording.

*To start On Motion recording, select the **Enable Event Recording** check box, and enable **Status** of **Motion Detection** in the Camera Events page.*

- Click **Save** to save the settings or **Cancel** to discard.

Pre and Post Recording

This section allows you to configure the Pre and Post Recording settings of the camera. The Pre and Post Recording feature enables a time-based buffer recording to be generated for any event-triggered recording before and after the recording duration. This is not applicable for Manual Recording.



- **Enable Pre-Recording**: Select the check box to enable Pre-Recording for any event-triggered recording.
- **Pre-recording Duration**: Specify the duration in seconds for which the Pre-Recording must continue. Valid Range: 5-30 seconds. Default: 10.
- **Enable Post-recording**: Select the check box to enable Post-Recording for any event-triggered recording.

- **Post-Recording Duration**: Specify the duration in seconds for which the Post-Recording must continue. Valid Range: 5-30 seconds. Default: 10.

- Click **Save** to save the settings or **Cancel** to discard.

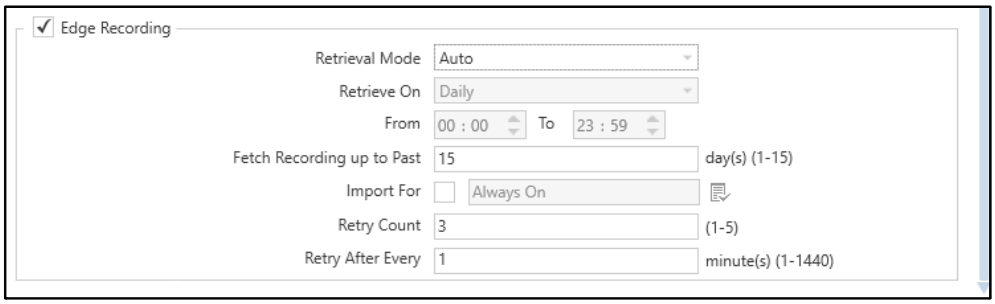
Edge Recording

Edge Recording is not applicable to Mobile Cameras.

Edge Recording will stop automatically, even if enabled when the Memory Usage of Recording Server crosses Critical Threshold. Whereas, as soon as the Memory Usage drops below Critical Threshold, the Edge Recording will resume automatically.

This section allows you to configure the **Edge Recording** settings of the camera.

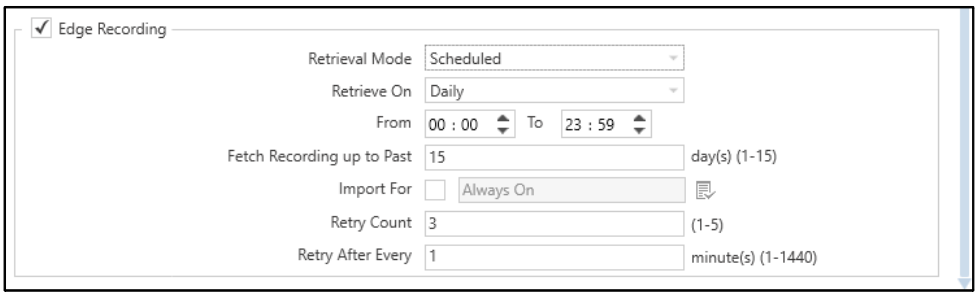
- Select the **Edge Recording** check box to download the recordings from the Matrix Devices [DVR, HVR, NVR, Matrix Camera and Cameras added using ONVIF (that support Profile G)].



- **Retrieval Mode**: Select the desired option from the drop-down list according to which Edge Recording must be imported — Scheduled, Auto.

  If you select **Auto**, the missing recordings will be fetched automatically when the device reconnects with the Recording Server.

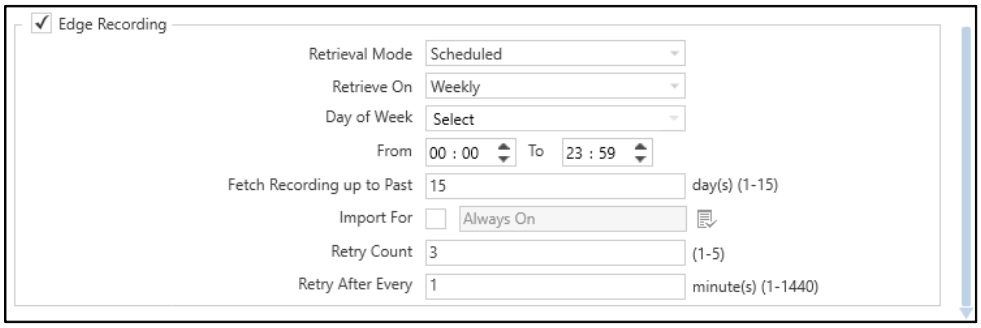
  If you select **Scheduled**, the missing recordings will be fetched as per the set schedule. Configure the following parameters:



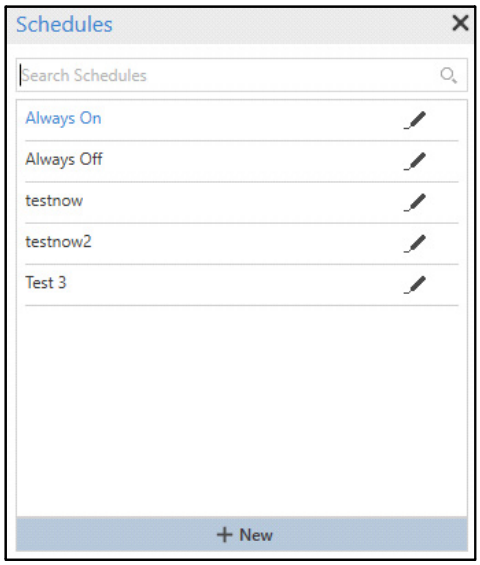
- **Retrieve On**: Select the desired option from the drop-down list according to which you wish to retrieve the missing recordings — Daily, Weekly.

  If you select **Daily**, configure the **From** and **To** time.

If you select **Weekly**, select the desired **Day of Week** from the drop-down list. Select the desired check boxes of the days of the week on which you wish to retrieve the missing recordings. Configure the **From** and **To** time.



- **Fetch Recordings upto Past**: Specify the number of days in the past from the current day till which the missing recordings should be fetched. Valid Range: 1-15 Days. Default: 15 Days. This is applicable to both Auto and Scheduled Retrieval Mode.
- **Import for:** Select the check box to configure a schedule for importing the missing recordings. Select the desired Schedule using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.
- **Retry Count**: Specify the number of times the system should retry fetching the missing recordings from the devices in the event of an unsuccessful attempt. Valid Range: 1-5. Default: 3. This is applicable to both Auto and Scheduled Retrieval Mode.
- **Retry After Every**: Specify the time till which the system should wait before attempting to fetch the missing recordings again after an unsuccessful attempt. Valid Range: 1-1440 minutes. Default: 1 minute. This is applicable to both Auto and Scheduled Retrieval Mode.

If SAMAS is installed in a network with frequent issues and the missing recordings are not fetched once the retry counts are exhausted, then SAMAS will not fetch those recordings again. Hence, make sure you configure a higher value for the Retry Count.

*Before setting the **Scheduled Retrieval Mode** parameters for Edge Recording, make sure the time of the Recording Server is synchronized with the time of the Matrix Devices (DVR, HVR, NVR).*

- Click **Save** to save the settings or **Cancel** to discard.

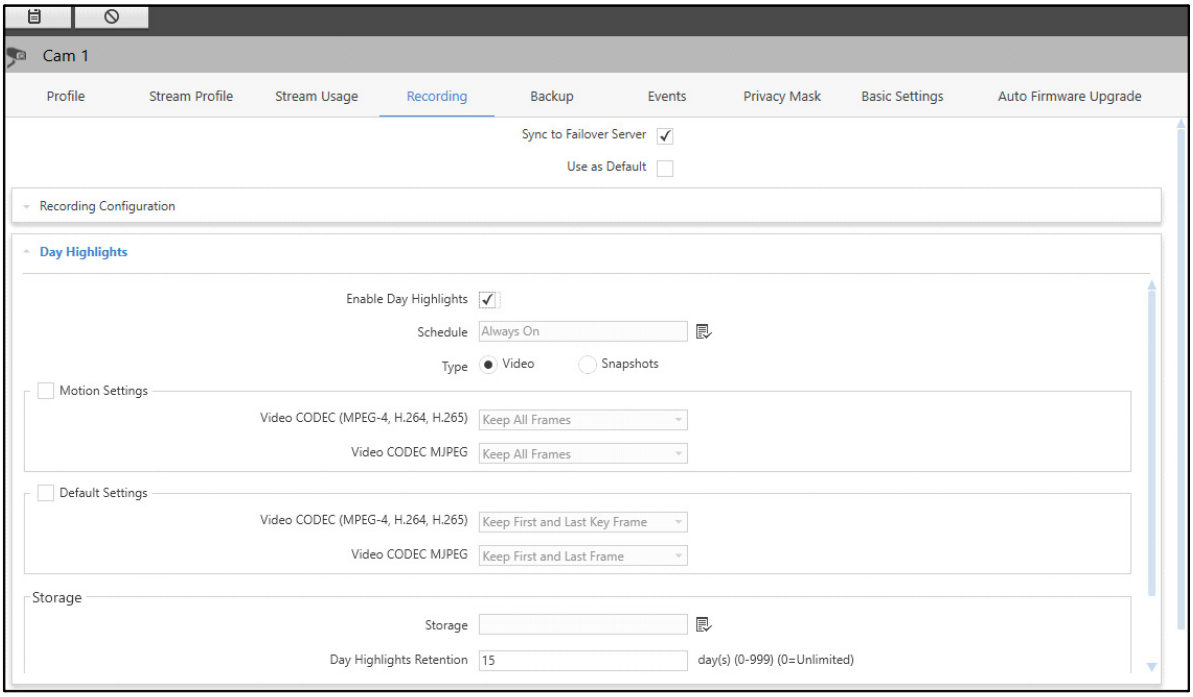
  Recording Settings can be cloned from one camera to another for the same Recording Server. For details, refer to "Recording".

Day Highlights

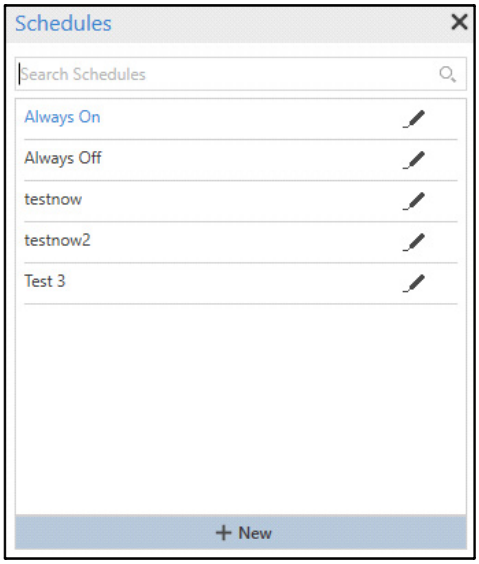
This panel allows you to have video summarizing option in which hours of recording are cut-short to few minutes clips/snapshots.

To configure the Day Highlights,

- Click the **Day Highlights** collapsible panel.



  - **Enable Day Highlights:** Select the check box to enable the Day Highlights for the selected camera.
  - **Schedule**: Select the desired Schedule of the recordings whose videos need to be summarized using the **Schedules** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Type**: Select the desired Type as **Video** or **Snapshots**.

Snapshots is not applicable to Mobile Cameras.

If you select **Video**, you need to configure the **Motion Settings** and **Default Settings**. To know more, refer to “Motion Settings” and “Default Settings”.

If you select **Snapshots**, you need to configure the **Snapshots Settings**. To know more, refer to “Snapshot Settings”.

Motion Settings and Snapshot Settings is not applicable to Mobile Cameras.

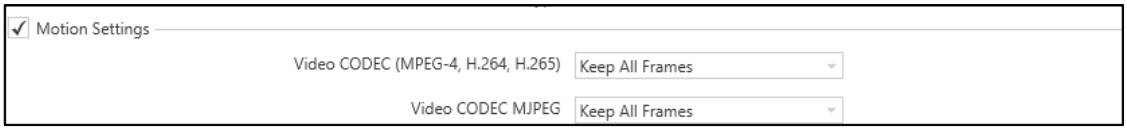
- Click **Save** to save the settings or **Cancel** to discard.

Motion Settings

Motion Settings is not applicable to Mobile Cameras.

This section allows you to configure the Motion Settings for the Day Highlights. The Motion Settings indicate how many I-frames you wish to capture when there is Motion. These frames will be a part of the summary clip.

- Select the **Motion Settings** check box.



- **Video CODEC (MPEG-4, H.264, H.265)**: Select the desired frame option to be included in the clip from the drop-down list.
- **Video CODEC MJPEG**: Select the desired frame option to be included in the clip from the drop-down list.

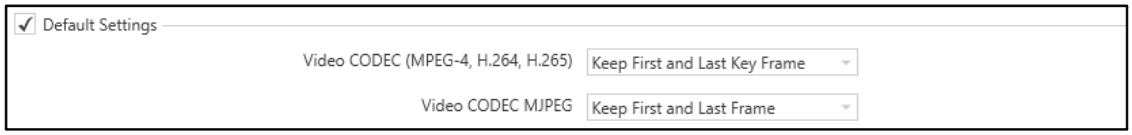
- Click **Save** to save the settings or **Cancel** to discard.

Default Settings

Video CODEC (MPEG-4, H.264, H.265) is not applicable to Mobile Cameras.

This section allows you to configure the Default Settings for Day Highlights. The Default Settings indicate how many I-frames you wish to capture when there is no Motion. These frames will be a part of the summary clip.

- Select the **Default Settings** check box.



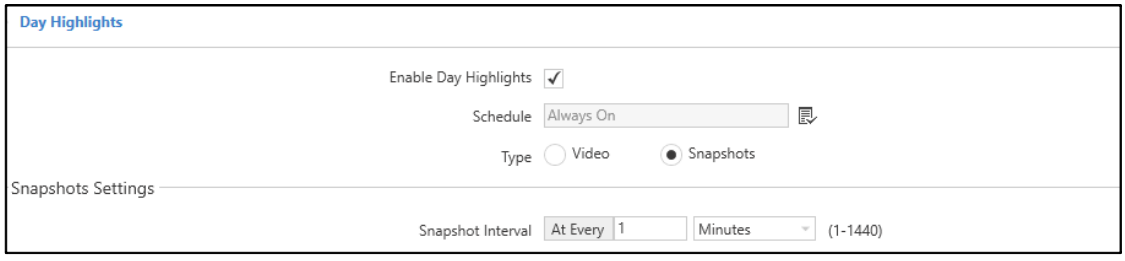
- **Video CODEC (MPEG-4, H.264, H.265)**: Select the desired frame option to be included in the clip from the drop-down list.
- **Video CODEC MJPEG**: Select the desired frame option to be included in the clip from the drop-down list.

- Click **Save** to save the settings or **Cancel** to discard.

Snapshot Settings

Snapshot Settings is not applicable to Mobile Cameras.

This section allows you to configure the Snapshots Settings for Day Highlights. By selecting **Snapshot** in Day Highlights Type, you can view multiple snapshots according to the configured snapshot interval. This feature leads to the “Time Lapse” video functionality, which enables you to view the highlights through the snapshots, one by one, like a video.



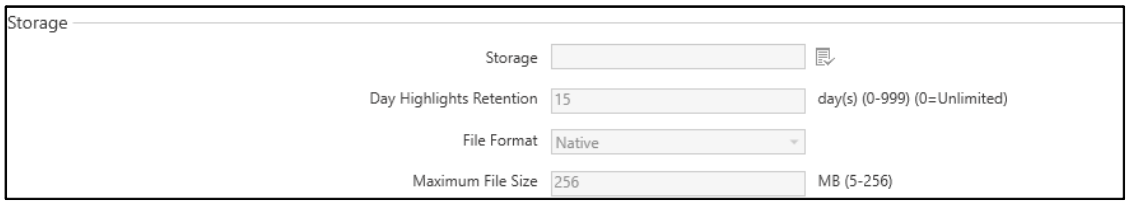
- **Snapshot Interval**: Select the desired Snapshot Interval from the drop-down list — Seconds, Minutes and Hours and enter the interval time. The Snapshots will be captured repeatedly as per the set time period.

For example, if you select the Snapshot Interval as **At every - 60 seconds**, snapshots will be captured after every 60 seconds. These snapshots will be played as video when **Day Highlights (Snapshot)** is selected in the Playback in the Smart Client.

- Click **Save** to save the settings or **Cancel** to discard.

Storage

This section allows you to configure the Storage settings for Day Highlights.



- **Storage**: Select the Backup Storage for the Day Highlights clip using the **Storage** picklist. Double-click to select the desired option. A folder named **Summary** will be created at the destination path.
- **Day Highlights Retention**: Specify the duration in days till when the Day Highlight data should be stored at the specified Storage. When the days exceed the specified retention period, the retained data will be deleted permanently. Valid Range: 0-999 days. Default: 15.

  For example, if 1 day is specified in Day Highlights Retention, the folder of the current date as well as the previous date i.e. total of 2 days is retained in the Summary folder and rest of the folders of previous records are deleted.
- **File Format**: Select the File Format in which you wish to save the files from the drop-down list.

Recordings in native format will be played in Smart Client. For AVI format, you can use other player.

- **Maximum File Size**: Specify the file size of which summarization file is to be created. Once a file of the configured size is created and its size exceeds, a new file will be created. Valid Range: 5-256 MB. Default: 256.
- **Maximum Snapshot Size**: If you have selected **Snapshots** in Day Highlights Type, specify the snapshot size to be stored in Failover Server Storage. Valid Range:1-1024 KB. Default: 100.

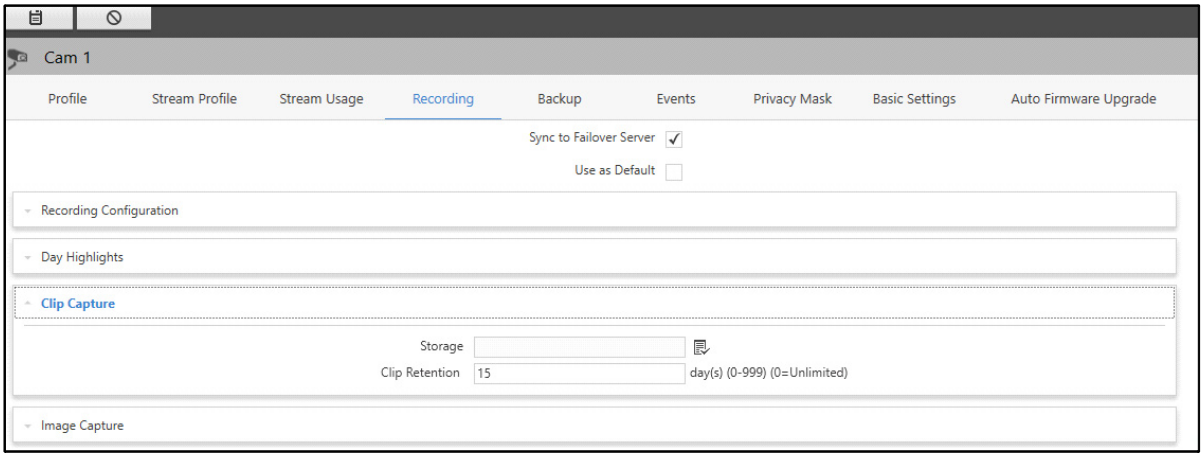
- Click **Save** to save the settings or **Cancel** to discard.

Clip Capture

This panel allows you to define a Backup Storage and Retention time for the clips.

To view and edit the Clip Capture,

- Click the **Clip Capture** collapsible panel.



- **Storage**: Select the Backup Storage for storing the captured clips using the **Storage** picklist. Double-click to select the desired option. The configurations for clip capture are available in Event and Action module. For more details, refer to “Capture Clip”.

- **Clip Retention**: Specify the duration in days till when the clip should be stored at the specified Storage. When the days exceed the specified retention period, the retained data will be deleted permanently. Valid Range: 0-999 days. Default: 15.

  For example, if the Clip Retention duration is configured as 1 day on the date 20th April 2019, the clip data of the current date (20th April, 2019) as well as the previous date (19th April 2019) i.e. total of 2 days will be retained and rest of the data of previous clips will be deleted.

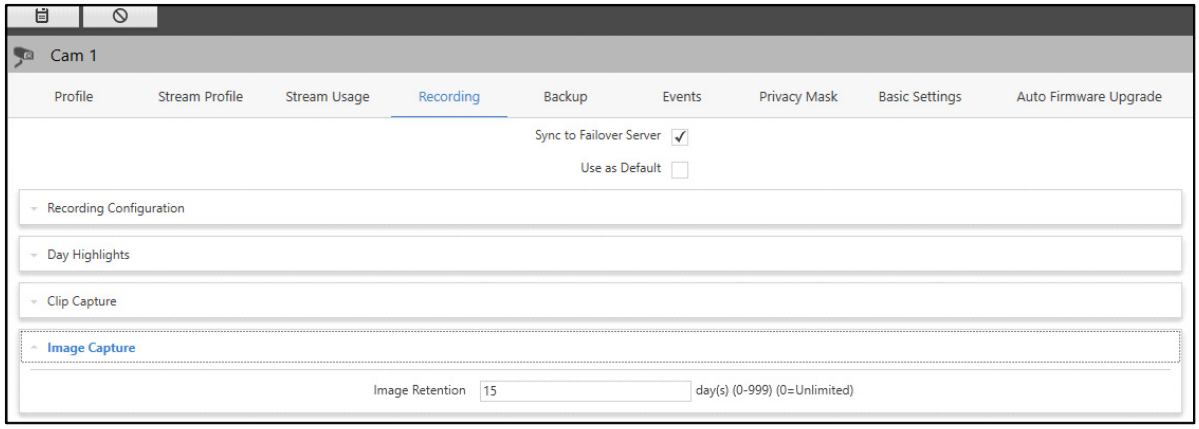
  Click **Save** to save the settings or **Cancel** to discard.

Image Capture

This panel allows you to define a Retention time for the Snapshots.

To view and edit the Image Capture,

- Click the **Image Capture** collapsible panel.



- **Image Retention:** Specify the duration in days till when the Snapshots should be stored at the specified Storage. When the days exceed the specified retention period, the retained data will be deleted permanently. Valid Range: 0-999 days. Default: 15.

For example, if the Image Retention duration is configured as 1 day on the date 20th April 2019, the Snapshots data of the current date (20th April, 2019) as well as the previous date (19th April 2019) i.e. total of 2 days will be retained and rest of the data of previous Snapshots will be deleted.

*Image Retention will work only for the Images (snapshots) which are taken by the Admin Client on the generation of an Event configured in the **CREAM Module** with the **Capture Image** action selected.*

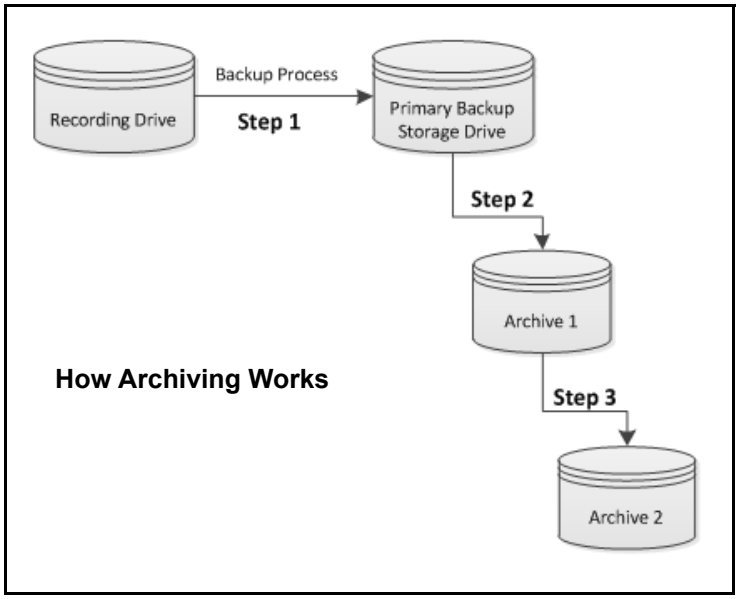
- Click **Save** to save the settings or **Cancel** to discard.

Backup

The Backup configuration for a camera is based on the concept of Video Data Grooming. SATATYA SAMAS uses the Video Data Grooming technique for taking and storing backup.

Video Data Grooming is a video-retention technique that increases storage efficiency of recorded data for prolonged storage through the creation of multi-level backup archives, especially when storage capacity is limited. This enables longer retention of recordings by degrading the record quality from time to time to optimize the available storage space.

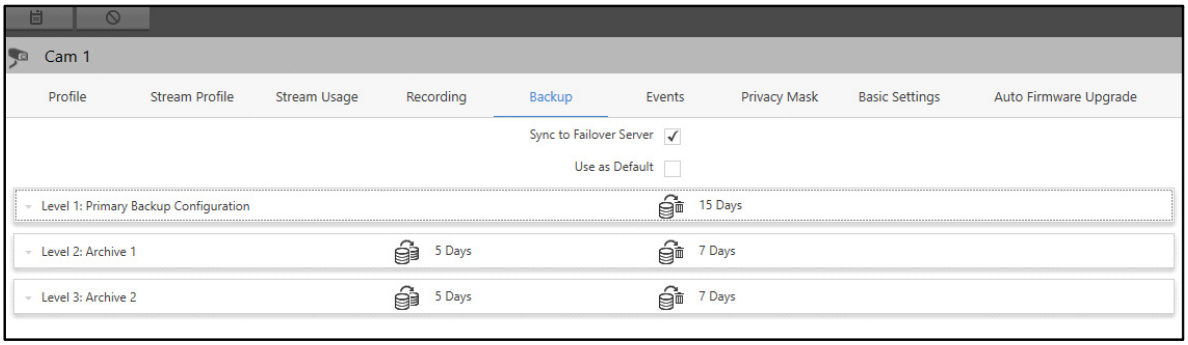
Video Data Grooming follows an archiving process. The Video Data Grooming tree comprises of three levels of archiving — Primary Backup Storage Level, Archive 1 and Archive 2.



This tab enables you to set the Backup configurations of a camera.

To view and configure camera Backup,

- Click the **Backup** tab.



Configure the following parameters:

- **Sync to Failover Server**: Select the check box to synchronize the configuration of the Recording Server's camera Backup page with the Failover Server's camera Backup page.
- **Use as Default**: Select the check box to copy the camera's Backup configurations to the Default Backup Settings.

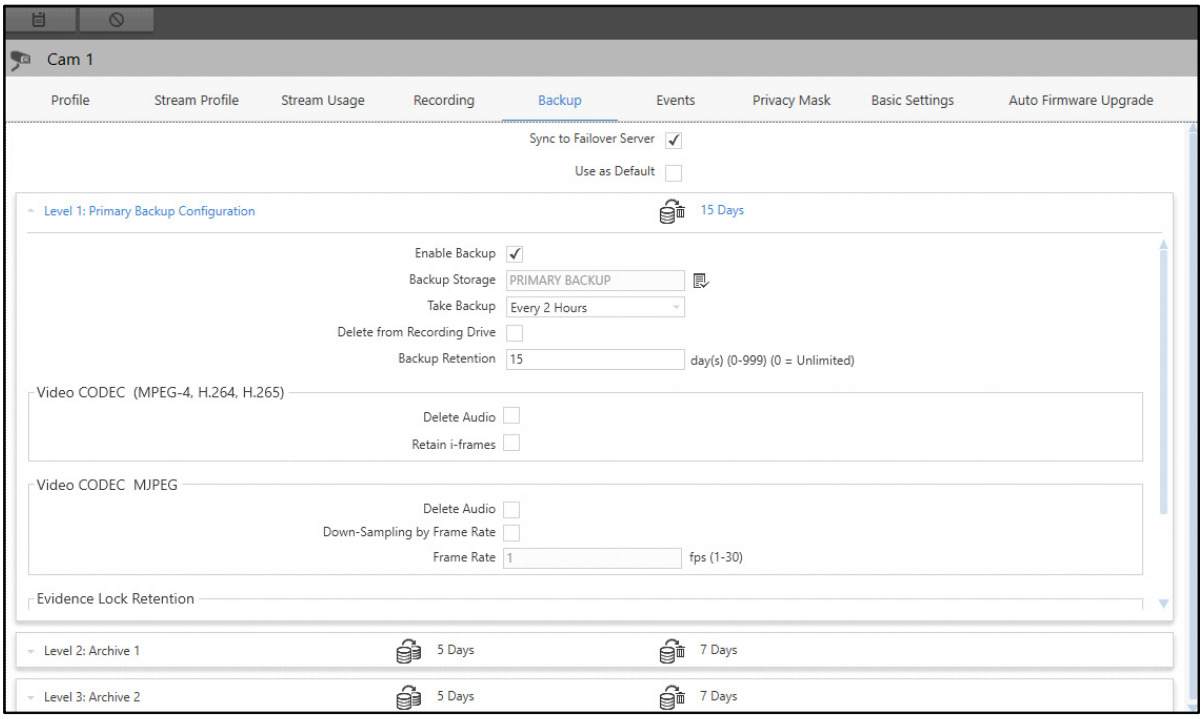
The Backup tab contains three collapsible panels — "Level 1: Primary Backup Configuration", "Level 2: Archive 1" and "Level 3: Archive 2".

Level 1: Primary Backup Configuration

This panel allows you to configure the Backup properties and Evidence Lock settings of the camera. In Primary Backup, the recorded data is retained in the Backup Storage till 15 days after it which it transfered to the Archive.

To view and edit the Primary Backup Configuration,

- Click the **Level 1: Primary Backup Configuration** collapsible panel.



- **Enable Backup:** Select the check box to enable the Backup for recorded files.
- **Backup Storage:** Select the desired Backup Storage location from a list of available Backup Drives using the **Backup Storage** picklist. Double-click to select the desired option.

*If you choose to select FTP Drive as the Primary Backup Storage, then you won't be able to configure the higher Backup levels i.e Archive1 and Archive2. If the **Sync to Failover Server** check box is enabled, the camera will be added into the FoS with Recording and Backup configuration with keeping the higher backup levels disabled. i.e Archive 1 and Archive 2.*

- **Take Backup:** Select the duration to schedule a Backup from the drop-down list.

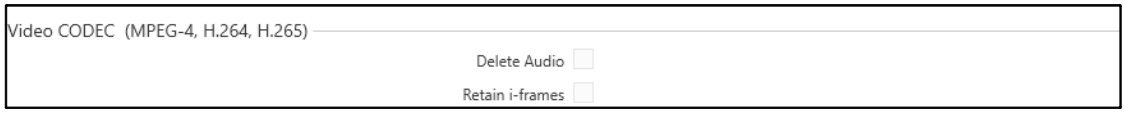
  For example, if the Take Backup duration is configured as Every 2 hours, the backup will be scheduled for after every 2 hours.
- **Delete from Recording Drive:** Select the check box if you wish to delete data from the recording drive while transferring it to the Primary Backup.
- **Backup Retention**: Specify the duration for which you wish to retain the Backup. This is time after which the data will be cleared from the Backup Drive. Enter 0, if the Backup is to be retained for an unlimited period. Valid Range: 0-999 days. Default: 15.

- Click **Save** to save the settings or **Cancel** to discard.

Video CODEC (MPEG-4, H.264, H.265)

Video CODEC (MPEG-4, H.264, H.265) is not applicable to Mobile Cameras.

This section allows you to configure the Recording data for the Primary Backup.

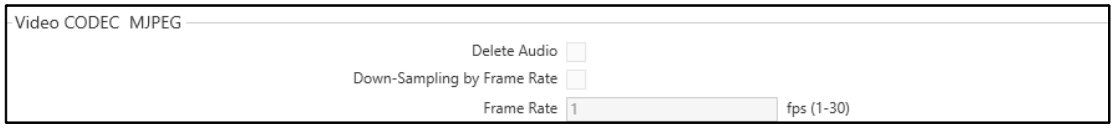


- **Delete Audio**: Select the check box to delete all the audio data from the Recording Storage Drive of higher hierarchy while moving the data to Backup Drive.
- **Retain i-frames**: Select the check box to retain only i-frames of the Recording data while storing it in the configured Backup Drive. When this check box is selected, all the p-frames get deleted, thereby decreasing the storage size of the recording data.

- Click **Save** to save the settings or **Cancel** to discard.

Video CODEC MJPEG

This section allows you to configure the Recording data for the Primary Backup.



- **Delete Audio**: Select the check box to delete all the audio data from the Recording Storage Drive of higher hierarchy while moving the data to Backup Drive.

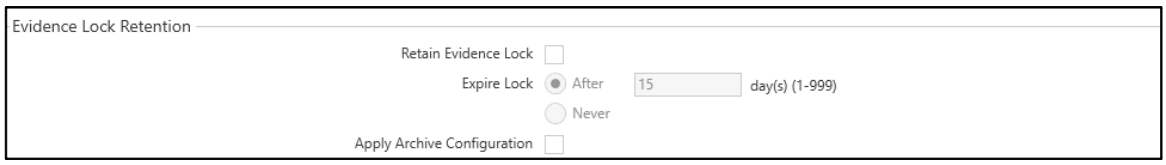
- **Down-Sampling by Frame Rate**: Select the check box to enable Down-Sampling on the basis of Frame Rate to reduce the recording data size. Down-Sampling is a method that reduces the size of the recording data by decreasing the Frame Rate of the Recording Data.

- **Frame Rate**: Specify the Frame Rate per second, if **Down-Sampling by Frame Rate** option is enabled. Valid Range: 1-30 fps. Default: 1.

- Click **Save** to save the settings or **Cancel** to discard.

Evidence Lock Retention

This section allows you to configure the Evidence Lock Retention settings for the Primary Backup.



- **Retain Evidence Lock:** Select the check box to keep the backed up Evidence locked within the Backup Drive, so that at the time of retention, those files are not deleted.

- **Expire Lock:** Select the Expire Lock option as **After** or **Never**. Specify the Lock Expiry days, if you select **After**. Valid Range: 1-999 days. Default: 15.

- **Apply Archive Configuration**: Select the check box to apply the Archive settings to the Evidence Lock Recording. If the check box is not selected, the Evidence Lock Recording configurations remain the same, i.e. Archive settings are not applied to the Evidence Lock Recording.

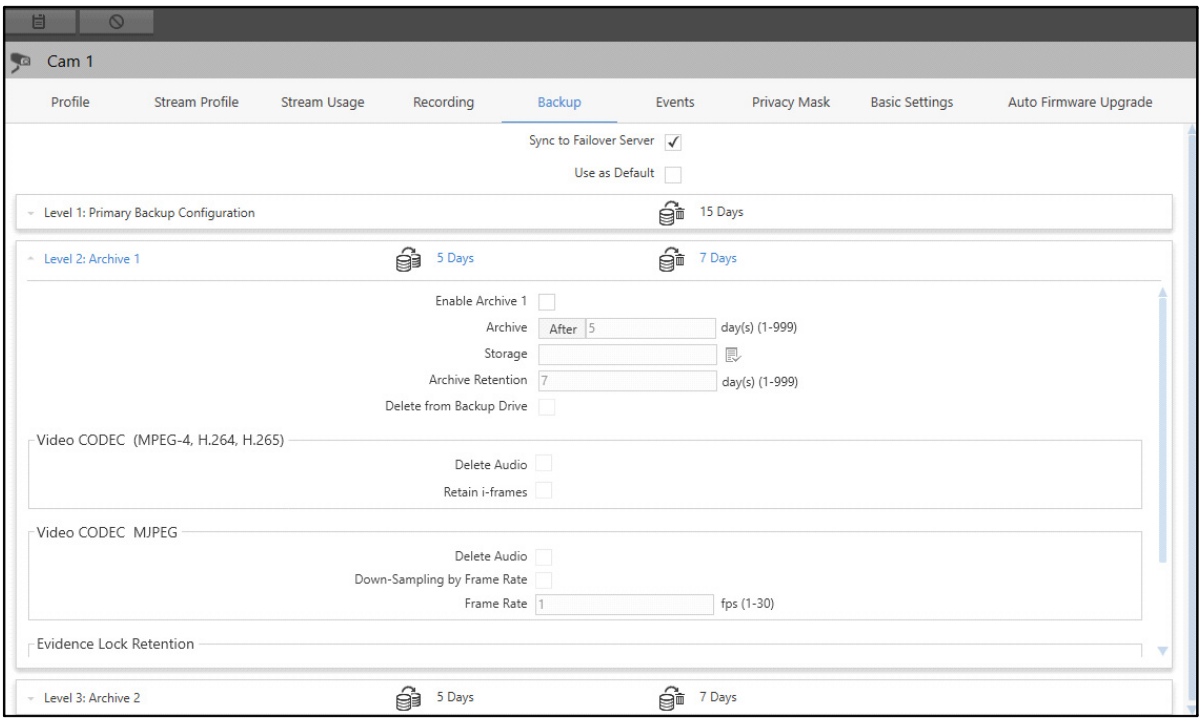
- Click **Save** to save the settings or **Cancel** to discard.

Level 2: Archive 1

This panel allows you to configure Archive 1 settings for the Backup. Archive 1 stores data that is older and moved from the Primary Backup Drive for retention. Archive 1 stores data of 5 days and retains it for 7 days. For example, if the Archive Duration is set as 5 days for Drive 1, and Retention Duration is set to 7 days, the Recording Server should start archiving Recording data from Archive 1 to Archive 2 after 5 days i.e. Archive Duration, and Recording Data shall be deleted from Archive 1 after 7 days i.e. Retention Duration.

To view and edit the Archive 1 Configuration,

- Click the **Level 2: Archive 1** collapsible panel.



- **Enable Archive 1:** Select the check box to store the recorded files from the Backup Drive to Archive 1.
- **Archive**: Specify the days after which the backup should be moved to Archive 2. Maximum 999 days of backup can be archived. Valid Range: 1-999 days. Default: 5.
- **Storage:** Select the Archive 1 Storage location using the **Storage** picklist. Double-click to select the desired option.

*If you choose to select FTP Drive as the Archive 1 Storage, you won't be able to configure the higher Backup levels i.e Archive2. If the **Sync to Failover Server** check box is enabled, then the camera will be added into the FoS with Recording and Backup configuration with keeping the higher backup levels disabled. i.e Archive 2.*

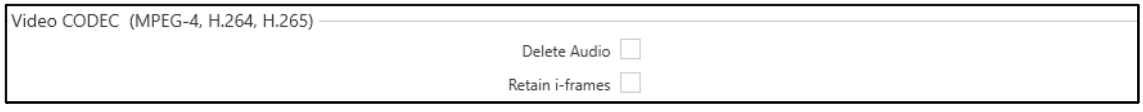
- **Archive Retention:** Specify the days for which the backup will be retained in Archive 1. Valid Range: 1-999 days. Default: 7.
- **Delete from Backup Drive**: Select the check box if you wish to delete the data from the Backup Drive while transferring it to Archive 1.

- Click **Save** to save the settings or **Cancel** to discard.

Video CODEC (MPEG-4, H.264, H.265)

Video CODEC (MPEG-4, H.264, H.265) is not applicable to Mobile Cameras.

This section allows you to configure the Recording data for the Archive 1 Backup.



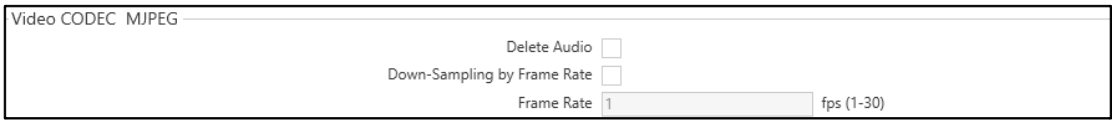
- **Delete Audio**: Select the check box to delete all the audio data from the Backup Drive while moving the data to Archive 1.

- **Retain i-frames**: Select the check box to retain only i-frames of the Backup Drive while storing it in the configured Archive 1. When this check box is selected, all the p-frames get deleted, thereby decreasing the storage size of the recording data.

- Click **Save** to save the settings or **Cancel** to discard.

Video CODEC MJPEG

This section allows you to configure the Recording data for the Archive 1 Backup.



- **Delete Audio**: Select the check box to delete all the audio data from the Backup Drive while moving the data to Archive 1.

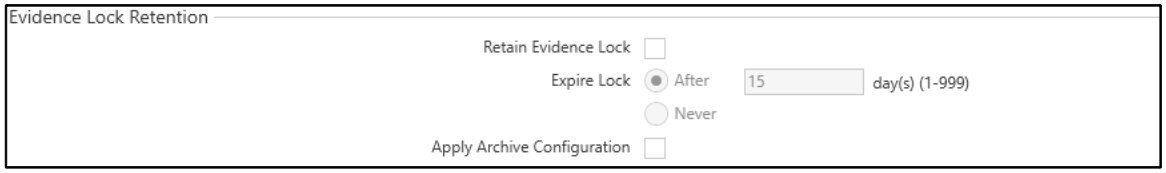
- **Down-Sampling by Frame Rate**: Select the check box to enable Down-Sampling on the basis of Frame Rate to reduce the recording data size. Down-Sampling is a method that reduces the size of the recording data by decreasing the Frame Rate of the Backup Data.

- **Frame Rate**: Specify the Frame Rate per second, if **Down-Sampling by Frame Rate** option is enabled. Valid Range: 1-30 fps. Default: 1.

- Click **Save** to save the settings or **Cancel** to discard.

Evidence Lock Retention

This section allows you to configure the Evidence Lock Retention settings for the Archive 1.



- **Retain Evidence Lock:** Select the check box to keep backed up Evidence locked within the Archive 1 drive, so that at the time of retention, those files are not deleted.

- **Lock Expiry days:** Select the Expire Lock option as **After** or **Never**. Specify the Lock Expiry days, if you select **After**. Valid Range: 1-999 days. Default: 15.

- **Apply Archive Configuration:** Select the check box to apply the Archive settings to the Evidence Lock Recording. If the check box is not selected, the Evidence Lock Recording configurations remain the same, i.e. Archive settings are not applied to the Evidence Lock Recording.

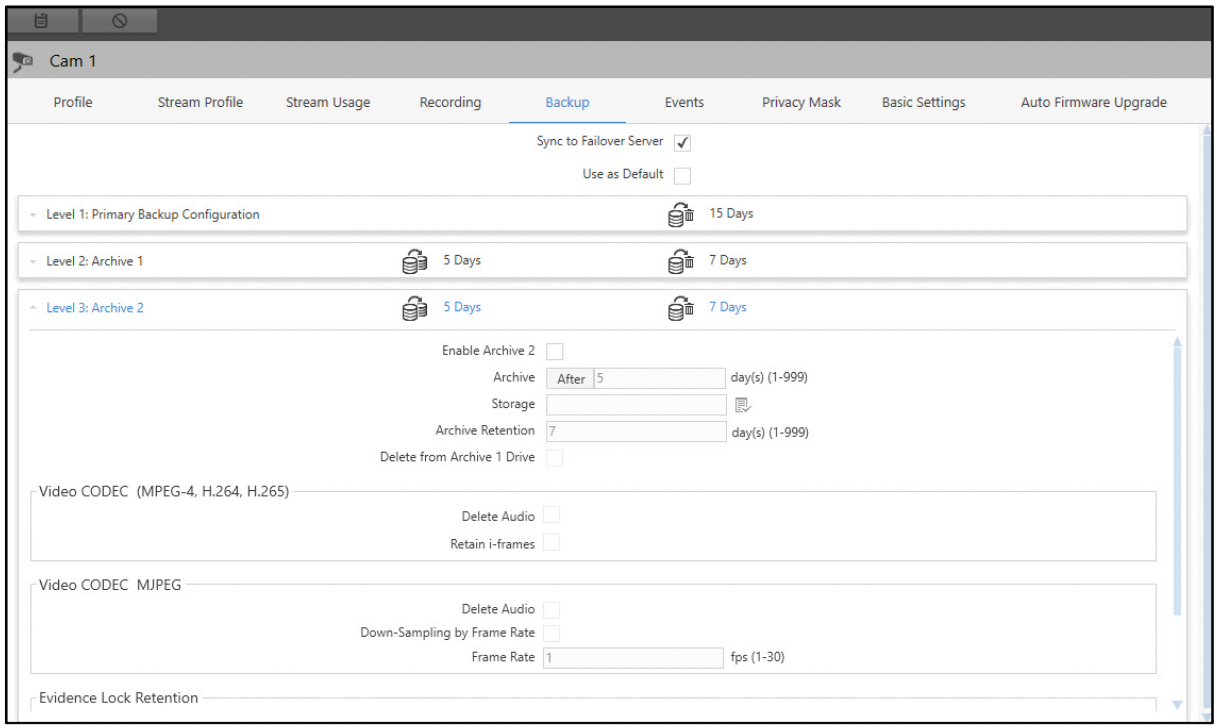
- Click **Save** to save the settings or **Cancel** to discard.

Level 3: Archive 2

This panel allows you to configure Archive 2 settings for the Backup.

To view and edit the Archive 2 Configuration,

- Click the **Level 3: Archive 2** collapsible panel.



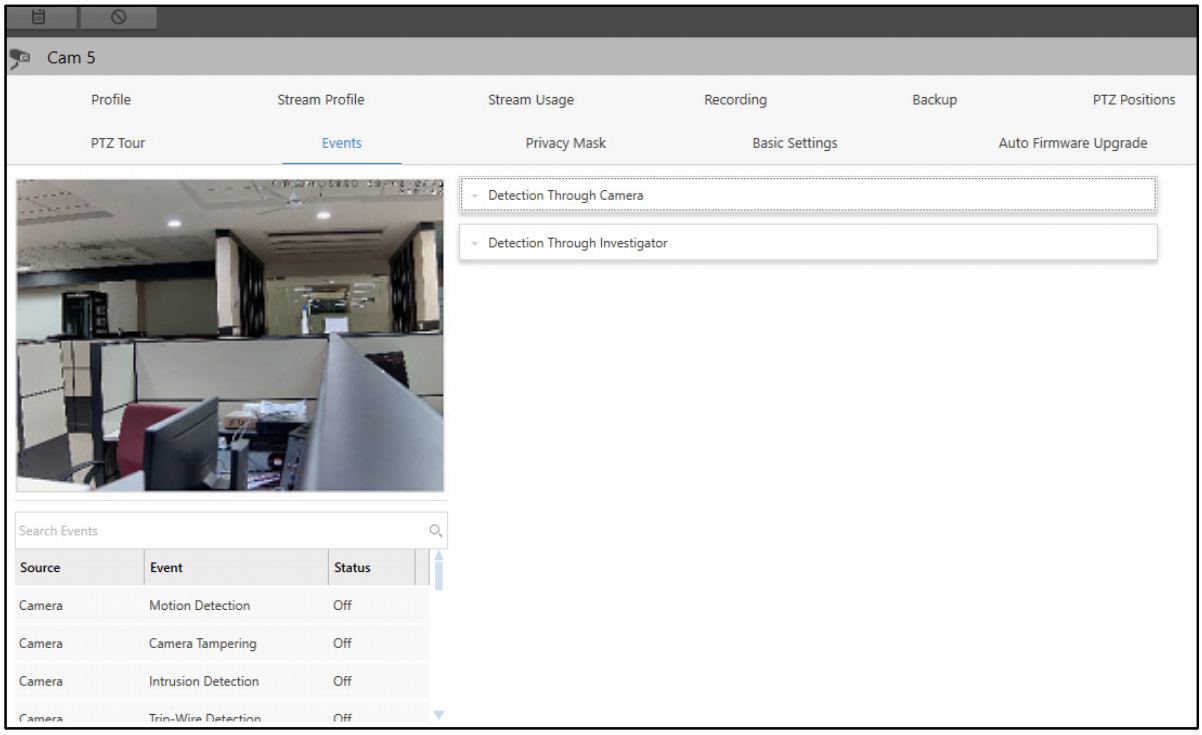
The configurations of Archive 2 are similar to the Archive 1. For details, refer to “Level 2: Archive 1”.

Events

Admin Client enables the detection of the Events through camera and investigator. This tab enables you to configure the Event configurations of a camera.

To view and configure camera Events,

- Click the **Event** tab.



The Events tab contains two collapsible panels — “Detection Through Camera” and “Detection Through Investigator”.

- **Detection Through Camera**

  This option allows you to detect the camera based Events such as Motion Detection, View Tampering, Intrusion Detection, Trip-Wire Detection etc. These Events are triggered by a camera and passed on to Admin Client.

  In Admin Client, cameras can be added via ONVIF as well as via Brand-Model configurations. The Events for the cameras depend on the features supported by the camera.

  For details, refer to “Detection Through Camera”.

Detection Through Camera is not applicable for Mobile Cameras.

- **Detection Through Investigator**

  Smart Client provides an effective alternative method for offline Event detection and analysis when the configured camera does not support these features. The in-built IVA Server in the Investigator uses video content analysis to detect Events such as People Counting, Vehicle Counting etc based camera recordings, irrespective of the camera specifications and configuration.

  SATATYA SAMAS provides the following license based IVA Events. The detailed explanation of each Event has been given in the **Event** tab of their respective modules.

  For details, refer to “Detection Through Investigator”.

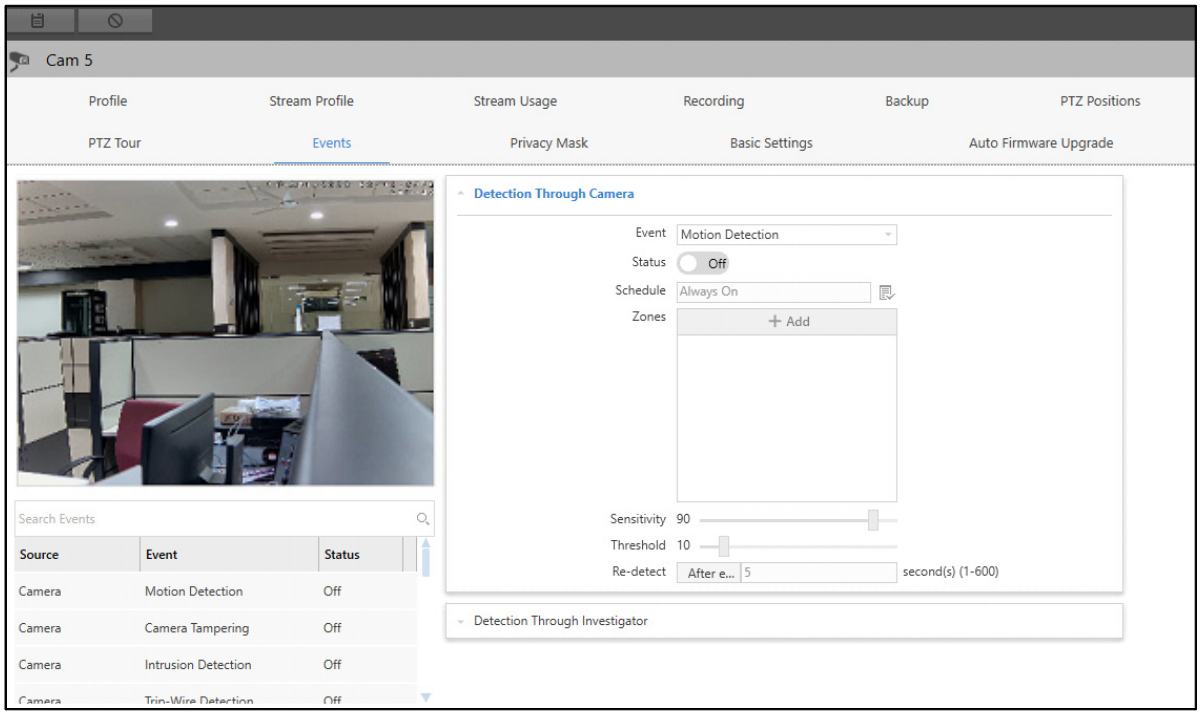
While configuring Events, the Status for two Events, one from **Detection Through Camera** and other from **Detection Through Investigator** can be switched On simultaneously.

Detection Through Camera

This panel displays the configurations for Events that can be detected by Camera. You can edit and configure the Events detected by Camera from this collapsible panel.

To view and edit Events,

- Click the **Detection Through Camera** collapsible panel.



Each configuration page of camera will depend on camera brand and model and how the camera has been added in Admin Client, that is, via Brand-model/ONVIF/Generic.

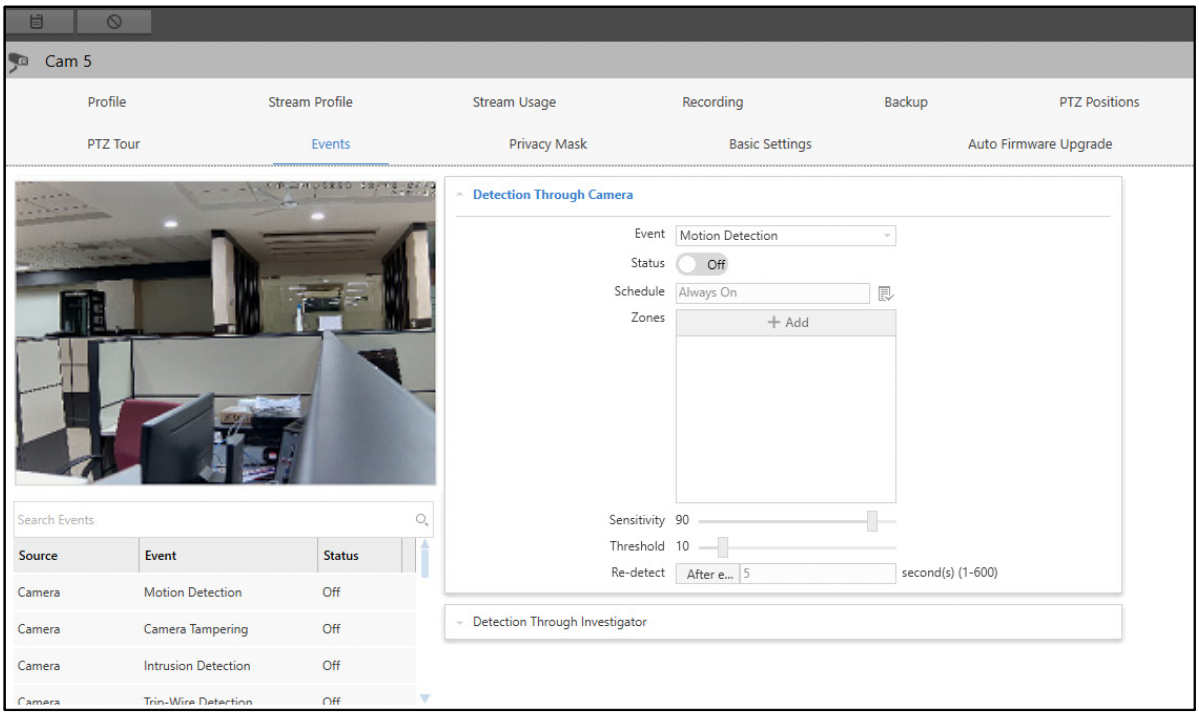
Refer to the following links for the configuration details of various Events.

- “Motion Detection”
- “Camera Tampering”
- “Intrusion Detection”
- “Trip-Wire Detection”
- “Audio Detection”
- “Object Counting”

Motion Detection

The Motion Detection feature enables the detection of any motion by an object or agent (such as people, vehicles etc.) in the configured zone. You can configure maximum 4 Motion Zones.

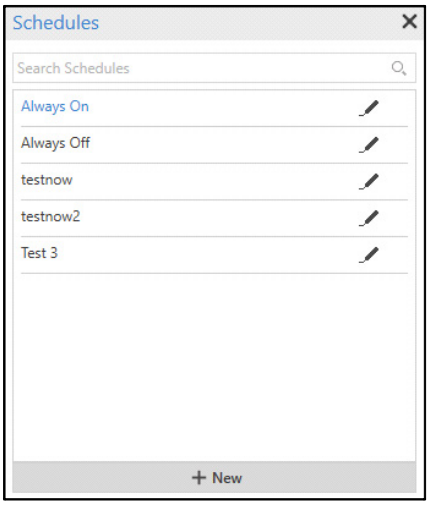
To configure Motion Detection,



Configure the following parameters:

- **Event**: Select the Motion Detection Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

  Once the Status switch is **On**, you can configure the remaining parameters.
- **Schedule**: Select the desired schedule which you wish to assign to the Event using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.

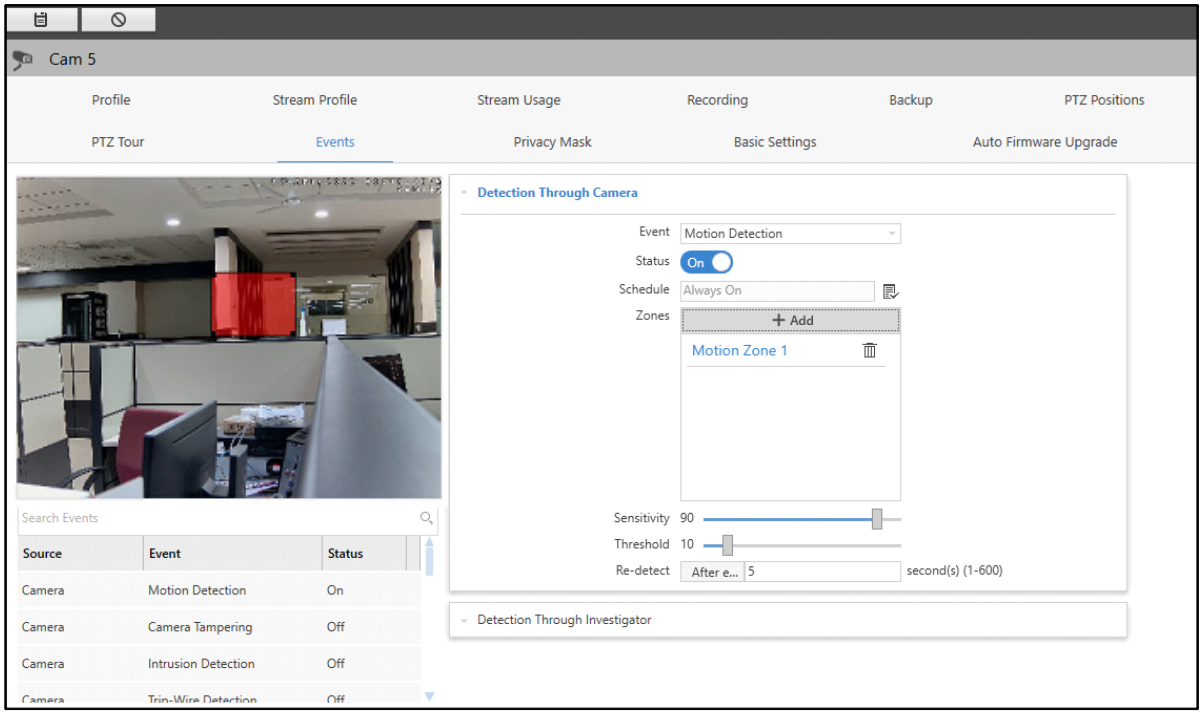


- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

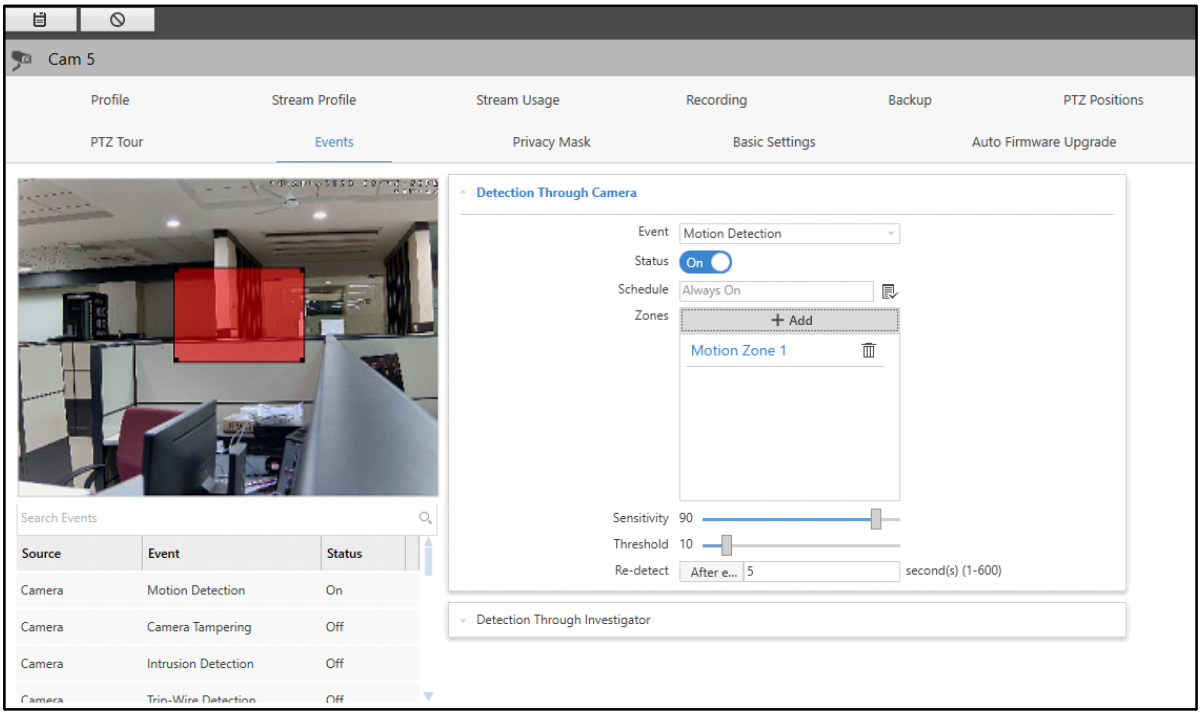
- **Sensitivity**: Drag the slider to set the desired sensitivity for the Motion Detection Event. Valid Range: 0-100. Default: 90. A higher Sensitivity will enable more precise detection.
- **Threshold**: Drag the slider to set the desired threshold for the Motion Detection Event. Valid Range: 0-100. Default: 10. A lower Threshold value will lead to motion detection even on slightest movement.
- **Re-detect**: Specify the Re-detect time after which the Motion Detection Event will be re-detected after the previous detection. Valid Range: 1-600 seconds. Default: 5.

Once these configurations are complete, you need to configure the Zones for the Event.

- Click **Add**.



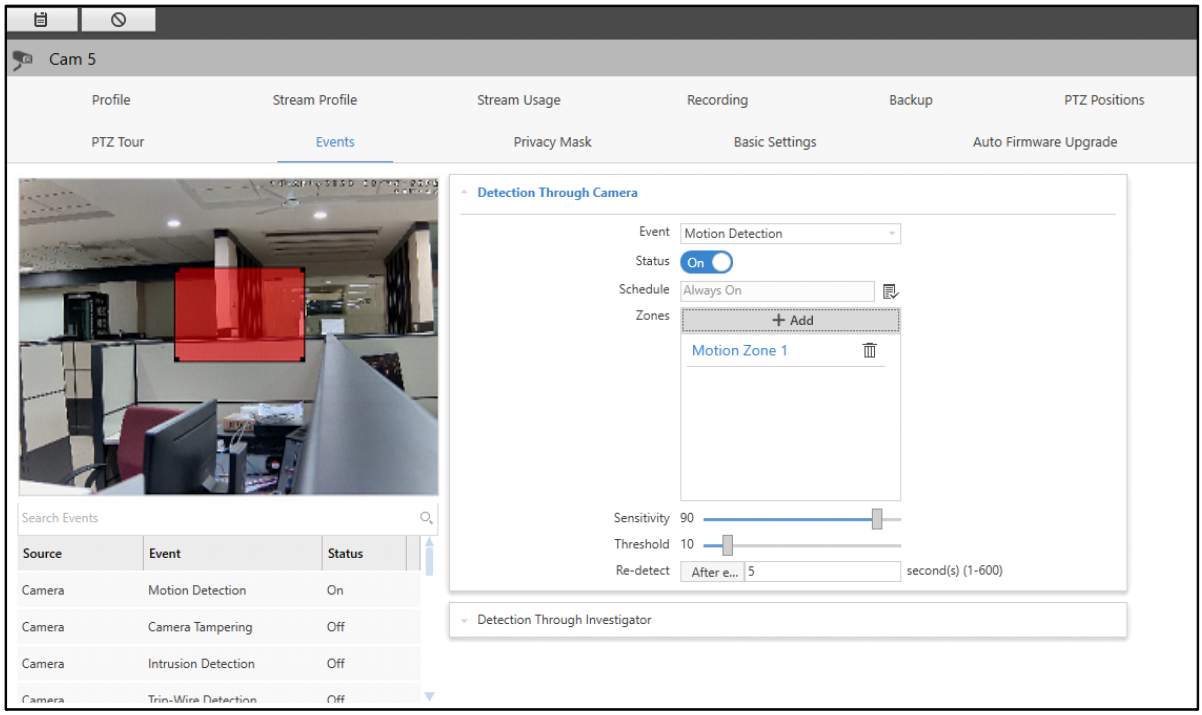
- Drag the corners and sides of the rectangle to configure the Zone.



- Click **Save** to save the settings or **Cancel** to discard.

The number of motion zones allowed to be configured will depend on the maximum number of motion zones supported by the camera brand. If no information is available on the same for the brand, a maximum of 4 zones can be defined.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event or delete the Zone.



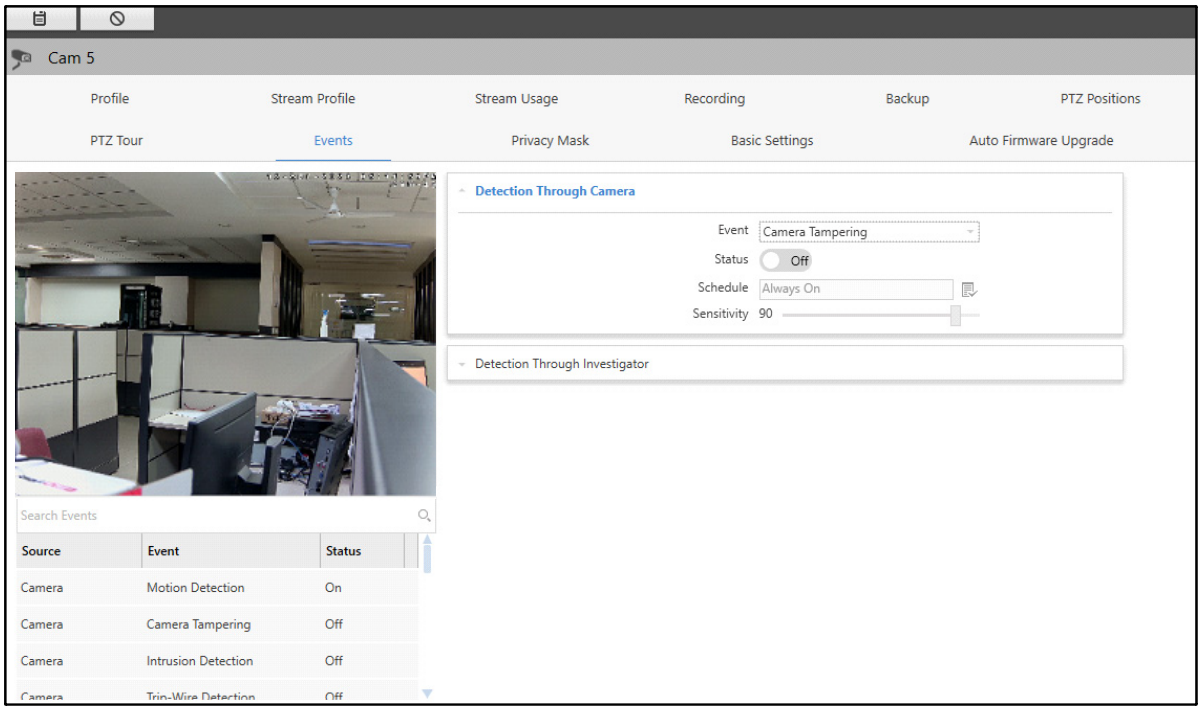
- Select the Event from the list and edit the configurations on the right hand side.

- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Zone.

Camera Tampering

The Camera Tampering feature enables you to monitor the live streaming of a camera and detects any attempts to impair the normal camera functioning.

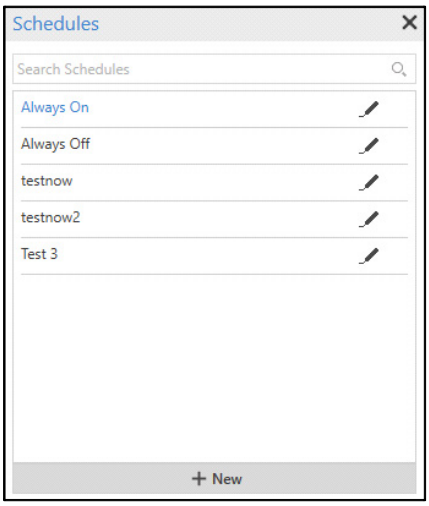
To configure Camera Tampering,



Configure the following parameters:

- **Event**: Select the Camera Tampering Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

  Once the Status switch is **On**, you can configure the remaining parameters.
- **Schedule**: Select the desired schedule which you wish to assign to the Event using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



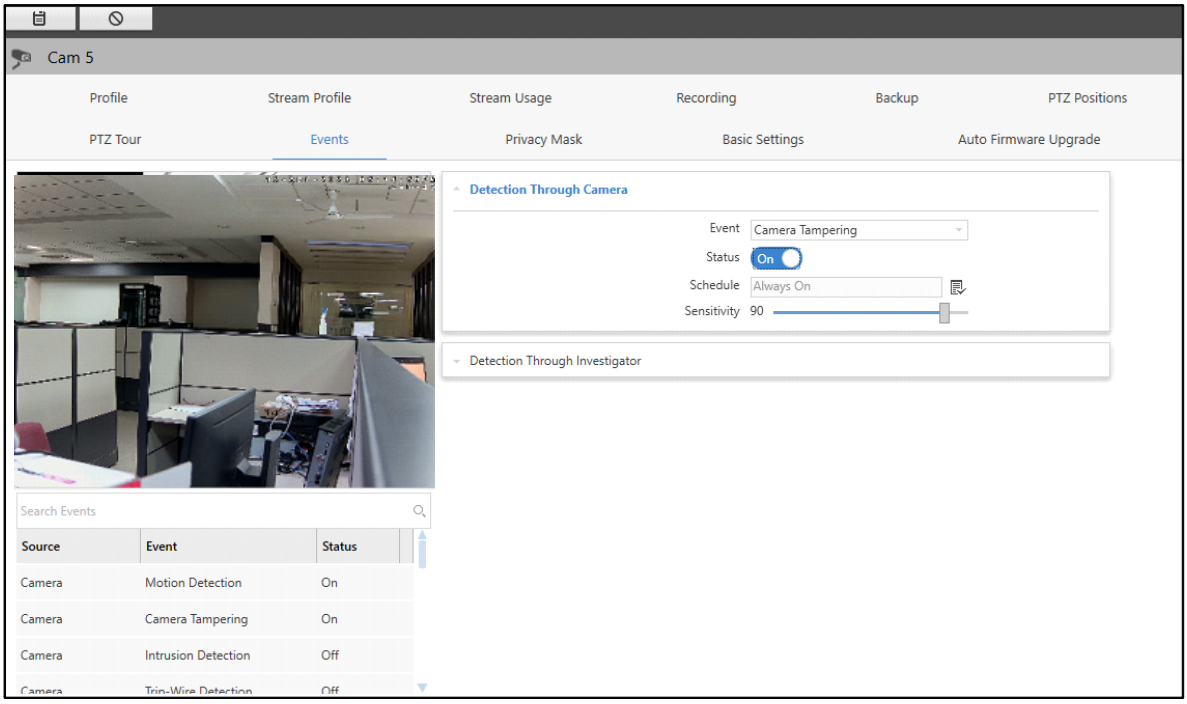
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Sensitivity**: Drag the slider to set the desired sensitivity for the Camera Tampering Event. Valid Range: 0-100. Default: 90. A higher Sensitivity will enable more precise detection.

- Click **Save** to save the settings or **Cancel** to discard.

The Event Status appears in a list below the live view of the camera.

You can edit the configurations of the Event, if required.



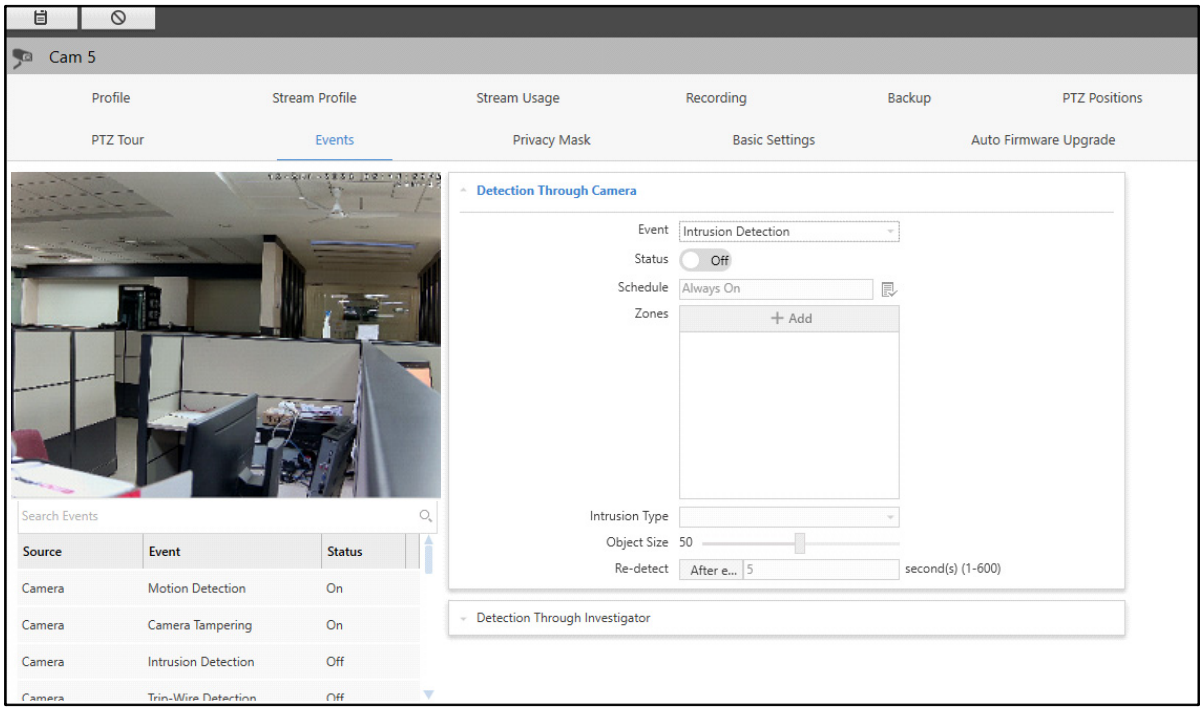
- Select the Event from the list and edit the configurations on the right hand side.

- Click **Save** to save the settings or **Cancel** to discard.

Intrusion Detection

The Intrusion Detection feature enables the detection of any new object or agent (such as people, vehicles etc.) entering or leaving an Intrusion Zone. You can configure maximum 4 Intrusion Zones.

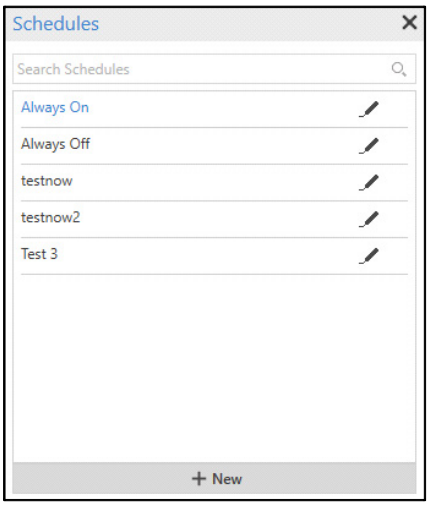
To configure Intrusion Detection,



Configure the following parameters:

- **Event**: Select the Intrusion Detection Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

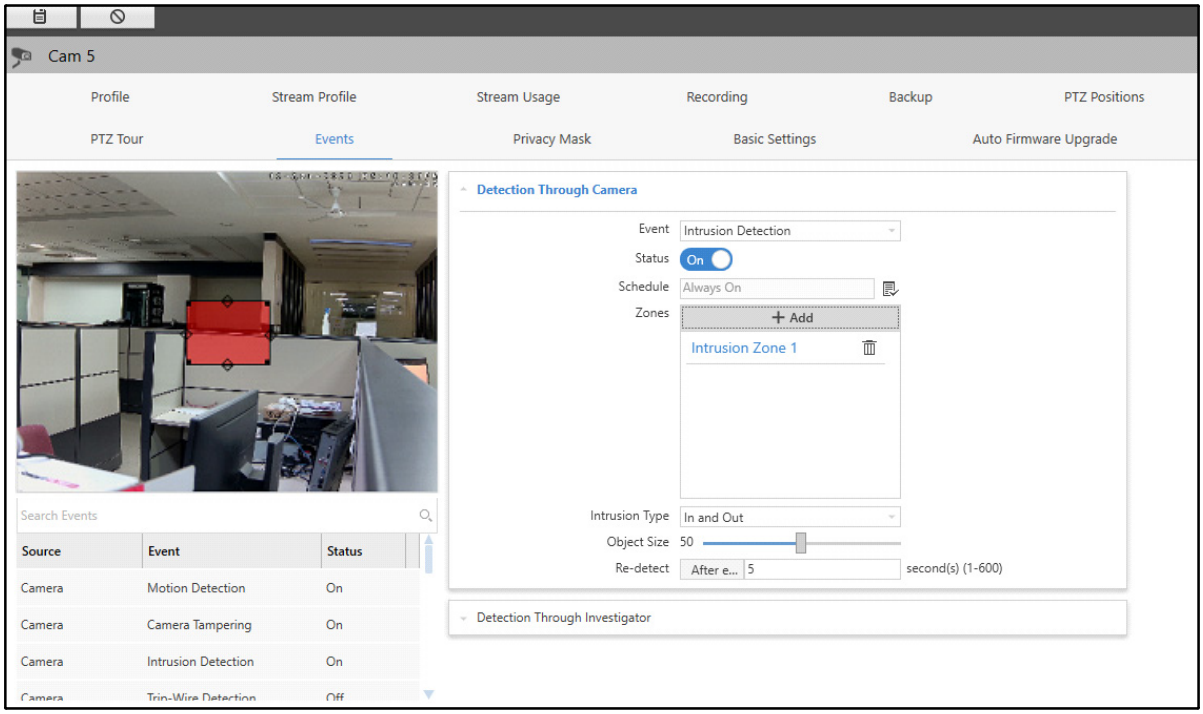
  Once the Status switch is **On**, you can configure the remaining parameters.
- **Schedule**: Select the desired schedule which you wish to assign to the Event using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



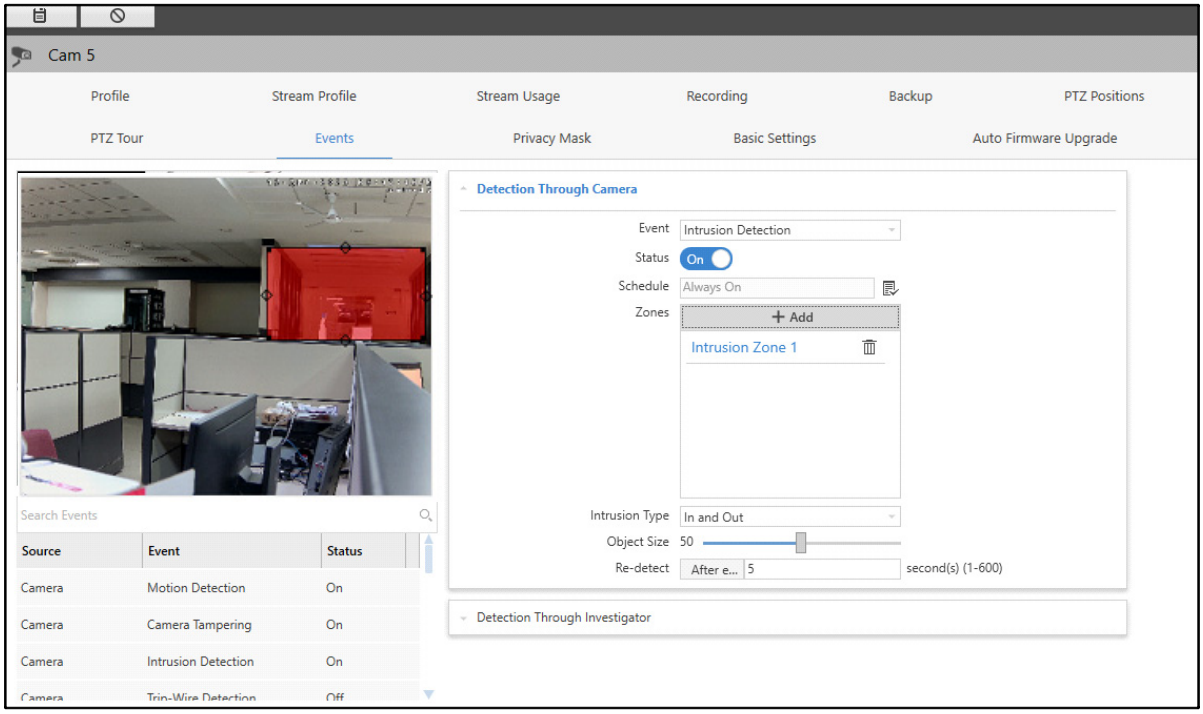
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

Once these configurations are done, you need to configure Zones for the Event and to enable the configuration of remaining parameters.

- Click **Add**.



- Drag the corners and sides of the rectangle to configure the Zone.



Once the Zone is configured, you can configure the remaining parameters.

- **Intrusion Type**: Select the direction of Intrusion from the drop-down list options — In, Out and In and Out.

  If you select **In**, the Event will occur when an object enters inside the configured zone.

  If you select **Out**, the Event will occur when an object leaves the configured zone.

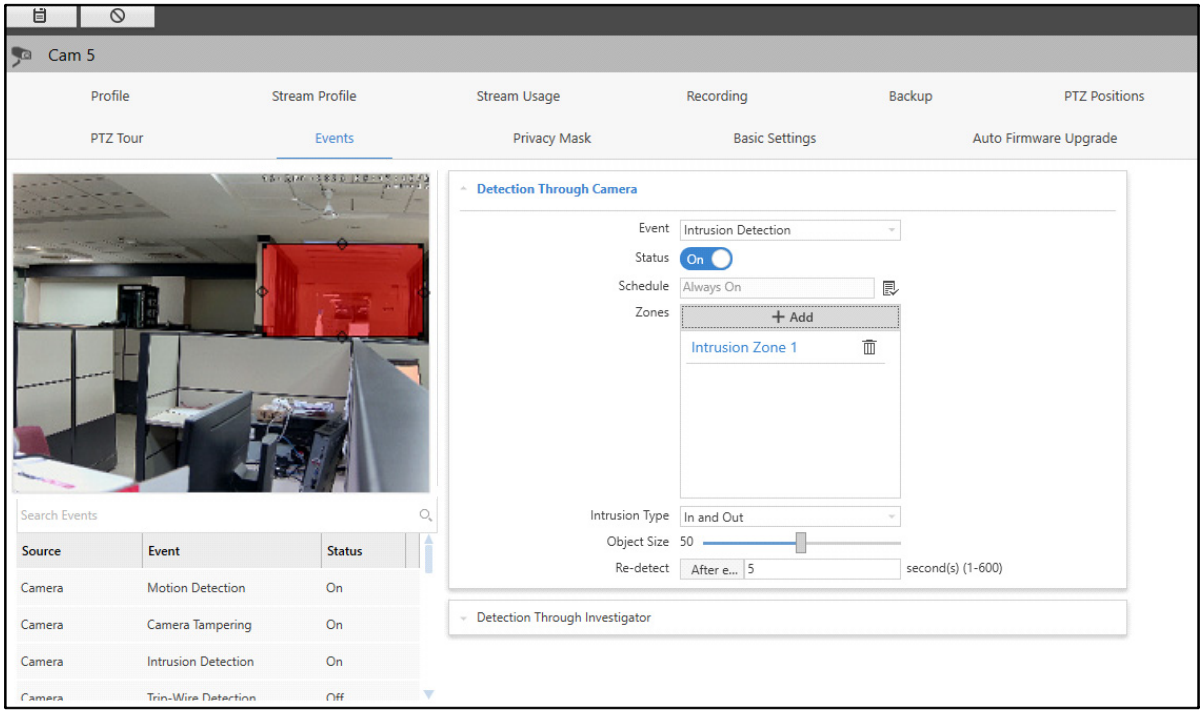
  If you select **In and Out**, the Event will occur either when an object enters or leaves the zone.

- **Object Size**: Drag the slider to set the desired Object Size for the Intrusion Detection Event. Valid Range: 1-100. Default: 50.

- **Re-detect**: Specify the Re-detect time after which the Intrusion Detection Event will be re-detected after the previous detection. Valid Range: 1-600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event or delete the Zone.

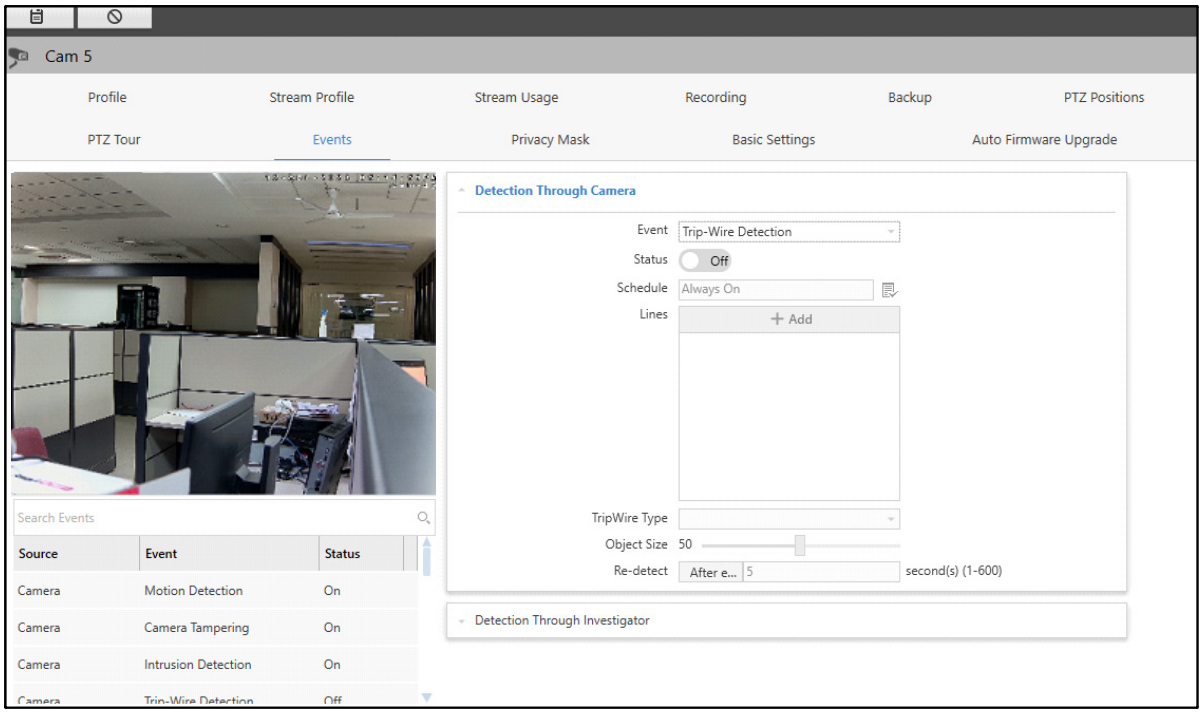


- Select the Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Zone.

Trip-Wire Detection

The Trip-Wire feature restricts a trespasser from crossing the line. You can configure maximum 3 Lines. Any object or person crossing the drawn line will generate an Event depending on the direction of intrusion.

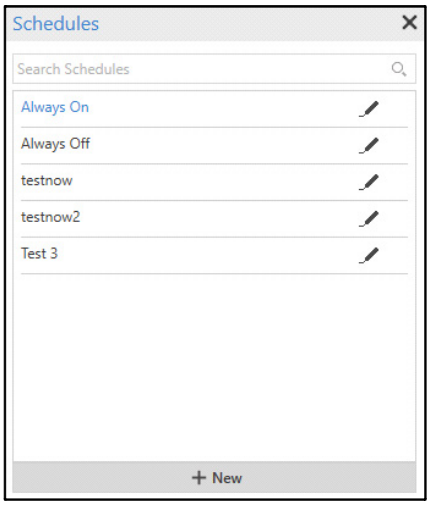
To configure Trip-Wire Detection,



Configure the following parameters:

- **Event**: Select the Trip-Wire Detection Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

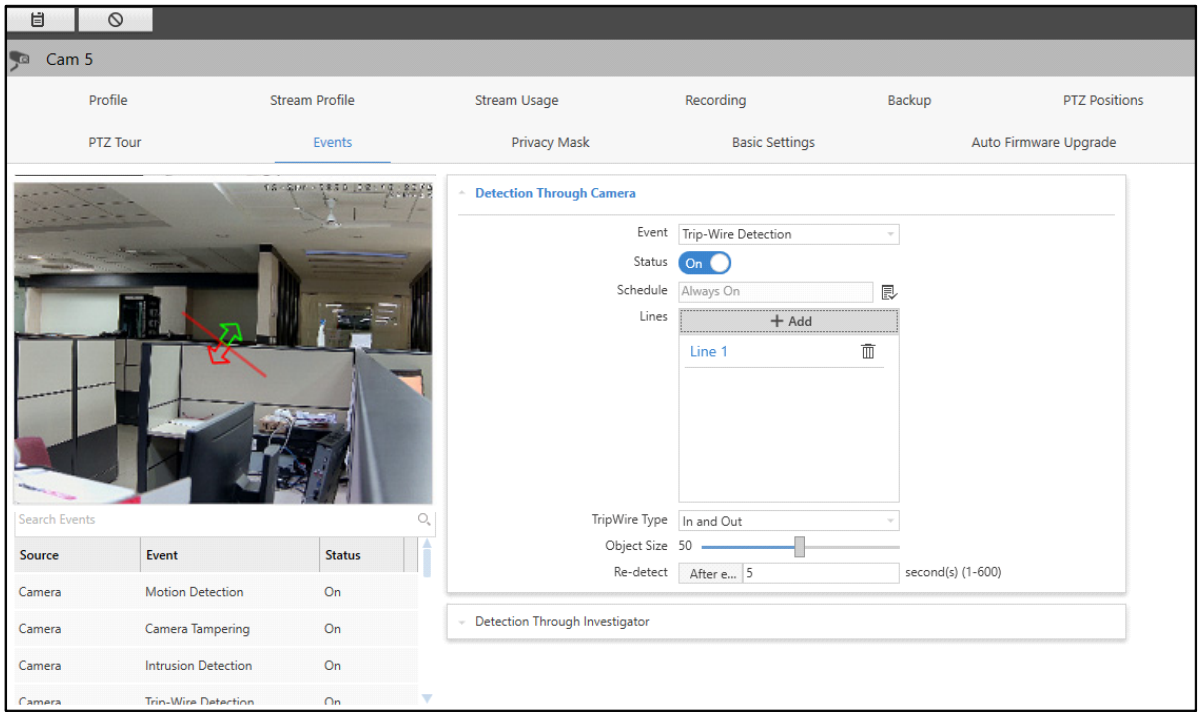
  Once the Status switch is **On**, you can configure the remaining parameters.
- **Schedule**: Select the check box to detect Event on a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



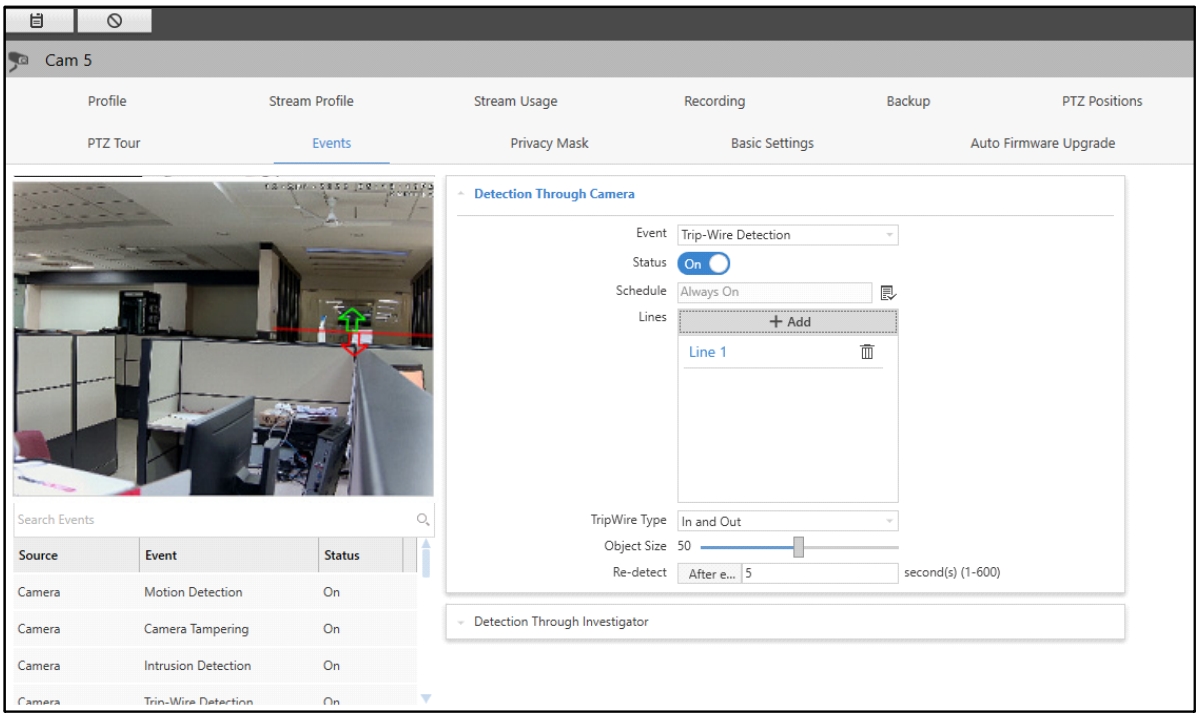
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

Once these configurations are done, you need to configure Lines for the Event and to enable the configuration of remaining parameters.

- Click **Add**.



- Drag the line to increase or decrease the length of the Line and set it as desired. You can also drag it to change the Entry (Green arrow) and Exit (Red arrow) direction.



Once the Line is configured, you can configure the remaining parameters.

- **Trip-Wire Type**: Select the Trip-Wire Type from the drop-down list options — In, Out and In and Out.

  If you select **In**, the Event will occur when an object crosses the line in the direction of green color.
  If you select **Out**, the Event will occur when an object crosses the line in the direction of red color.

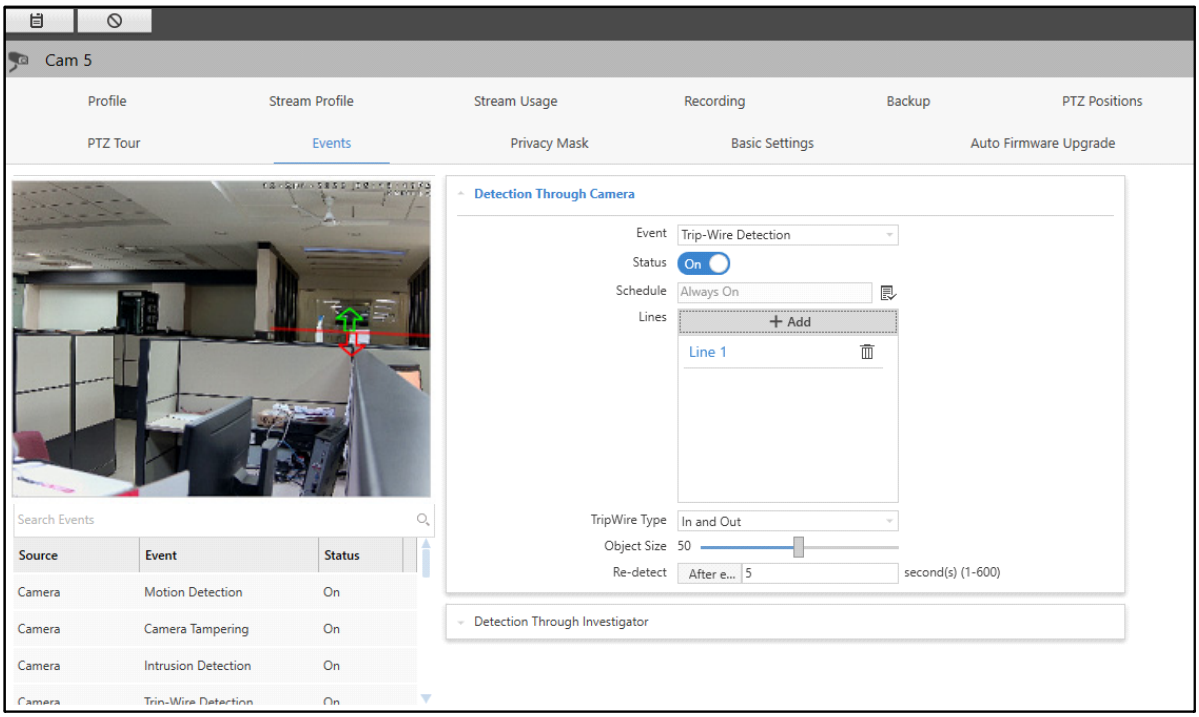
  If you select **In and Out**, the Event will occur either when an object crosses the line either in the direction of green or red color.

- **Object Size**: Drag the slider to set the desired Object Size for the Trip-Wire Detection Event. Valid Range: 0-100. Default: 50.

- **Re-detect**: Specify the Re-detect time after which the Trip-Wire Detection Event will be re-detected after the previous detection. Valid Range: 1-600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event or delete the Line.



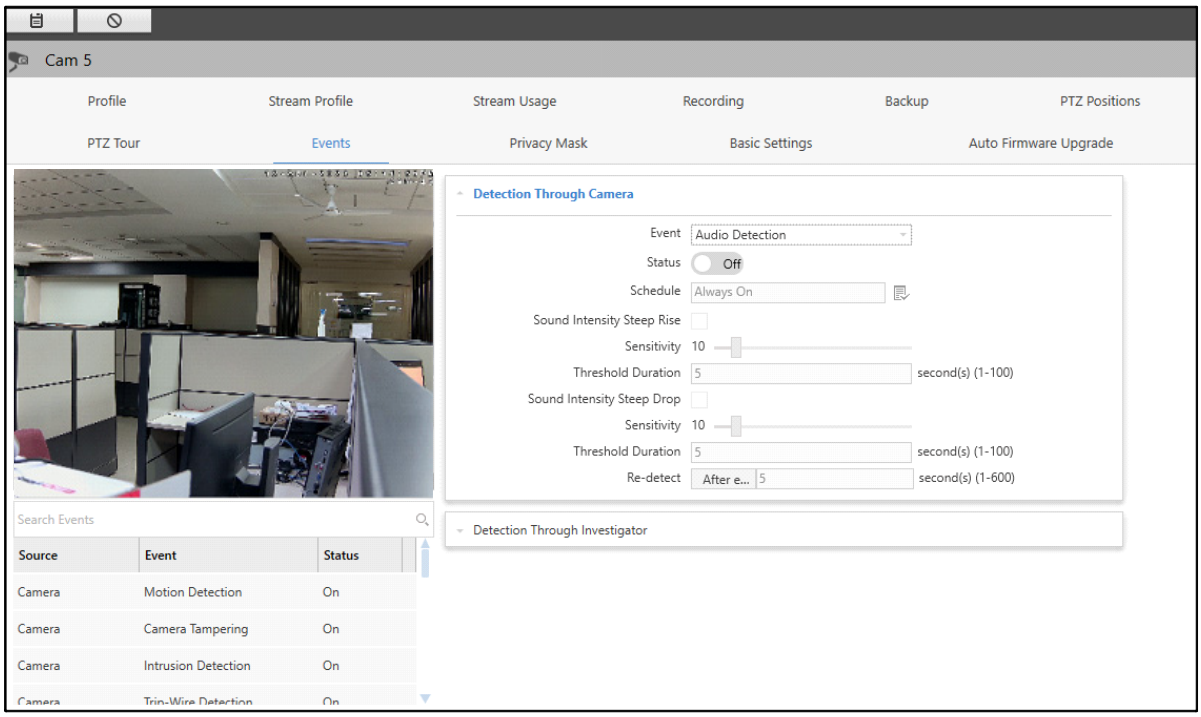
- Select the Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Line.

Audio Detection

Audio detection is a feature that enables to detect noise in a silent zone and take action accordingly. It is useful in places like hospitals, libraries, courts etc. where the intensity of sound should not go beyond a certain level. This helps in controlling the volume of sound.

This feature is supported with the cameras models supporting audio feature.

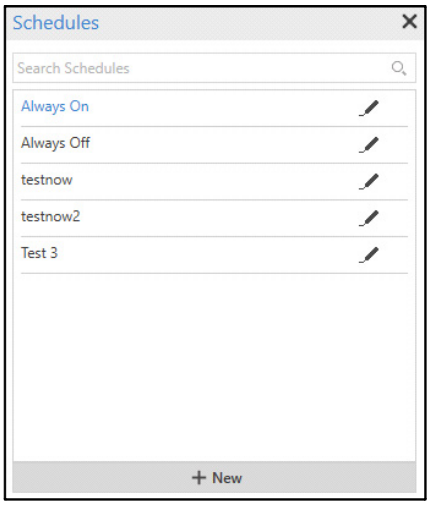
To configure Audio Detection,



Configure the following parameters:

- **Event**: Select the Audio Detection Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

  Once the Status switch is **On**, you can configure the remaining parameters.
- **Schedule**: Select the check box to detect Event on a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Sound Intensity Steep Rise**: Select the check box to configure the real time sound against high intensity of audio detection.

- **Sensitivity**: Drag the slider to set the desired sensitivity for the rise in intensity of noise. This sensitivity refers to the rise in intensity of noise that is to be detected in a received audio between 2 consecutive Audio signals received. Valid Range: 1-100. Default: 10.

  While at high sensitivity, the slightest variation in Audio signals would trigger an Audio Detection Event from the Camera. Lowering the sensitivity reduces the intensity of rise in signals to be detected in the audio.

- **Threshold Duration**: Specify the duration in seconds after which the rise in intensity of the audio would be detected. Valid Range: 1-100 seconds. Default: 5.

- **Sound Intensity Steep Drop**: Select the check box to configure the real time sound against low intensity of audio detection.

- **Sensitivity**: Drag the slider to set the desired sensitivity for the drop in intensity of noise. This sensitivity refers to the drop in intensity of noise that is to be detected in a received audio between 2 consecutive Audio signals received. Valid Range: 1-100. Default: 10.

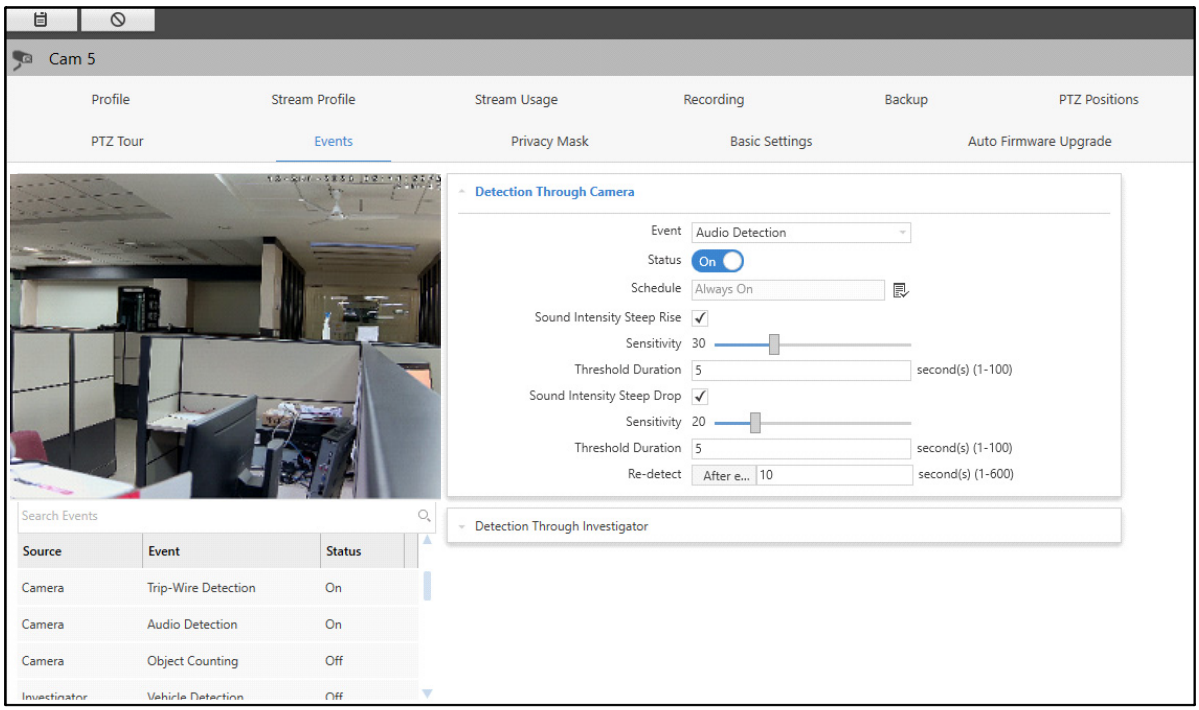
  While at high sensitivity the slightest variation in Audio signals would trigger an Audio Detection event from the Camera. Lowering the sensitivity reduces the intensity of drop in signals to be detected in the audio.

- **Threshold Duration**: Specify the duration in seconds after which the drop in intensity of the audio would be detected. Valid Range: 1-100 seconds. Default: 10.

- **Re-detect**: Specify the Re-detect time after which the Audio Detection Event will be re-detected after the previous detection. Valid Range: 1-600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event, if required.



- Select the Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

Object Counting

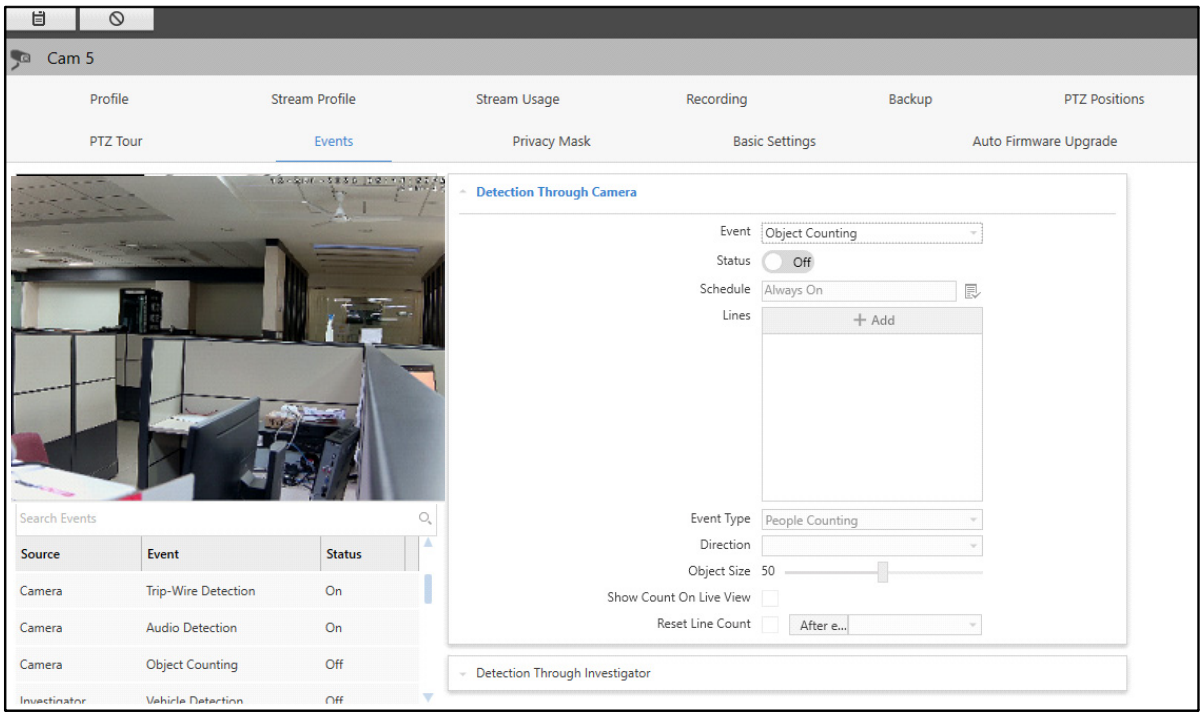
The Object Counting feature enables you to keep a track of the count of people or vehicles in the premises.

Object Counting includes People Counting and Vehicle counting Event types. This event is supported by **Matrix Professional IP Cameras** that are added via Brand Model name in the SATATYA SAMAS. Maximum 2 lines can be configured against each camera.

Vehicle Counting *event is available with VTPM license of SATATYA SAMAS. For detailed license information, refer to the SATATYA SAMAS Installation Guide*.

People Counting *event is available with PMTC license of SATATYA SAMAS. For detailed license information, refer to the SATATYA SAMAS Installation Guide*.

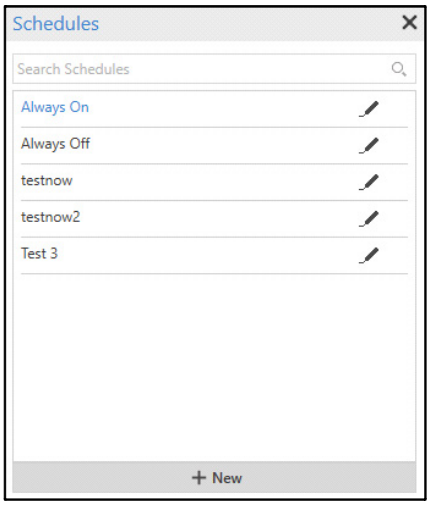
To configure Object Counting,



Configure the following parameters:

- **Event**: Select the Object Counting Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

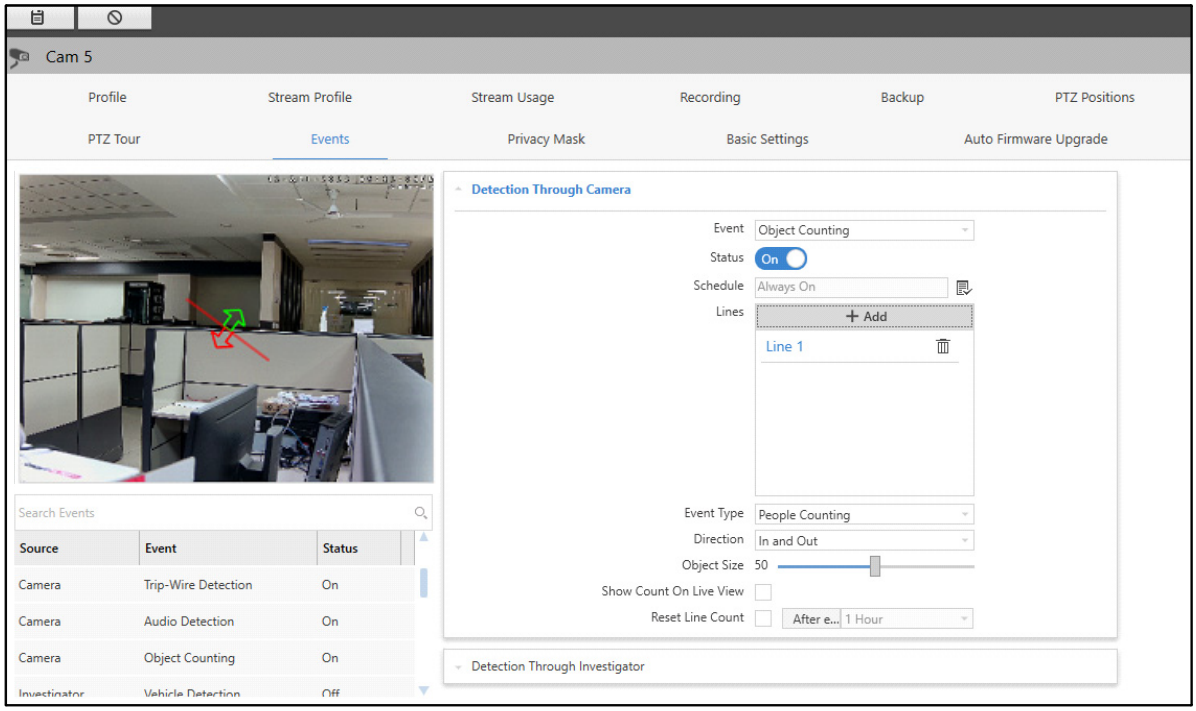
  Once the Status switch is **On**, you can configure the remaining parameters.
- **Schedule**: Select the check box to detect Event on a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



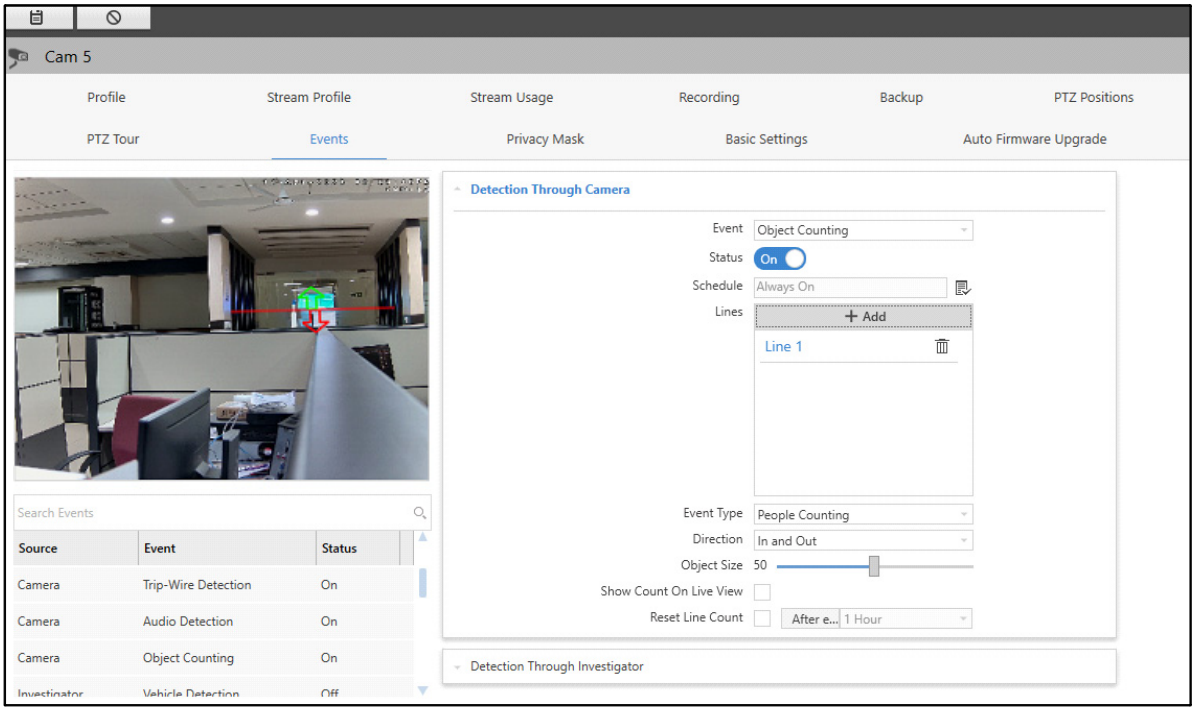
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

Once these configurations are done, you need to configure Lines for the Event and to enable the configuration of remaining parameters.

- Click **Add**.



- Drag the line to increase or decrease the length of the Line and set it as desired. You can also drag it to change the Entry (Green arrow) and Exit (Red arrow) direction.



Once the Line is configured, you can configure the remaining parameters.

- **Event Type**: Select the Event Type to be detected using the drop-down list options — People Counting or Vehicle Counting.
- **Direction**: Select the Direction from the drop-down list options — In, Out and In and Out.

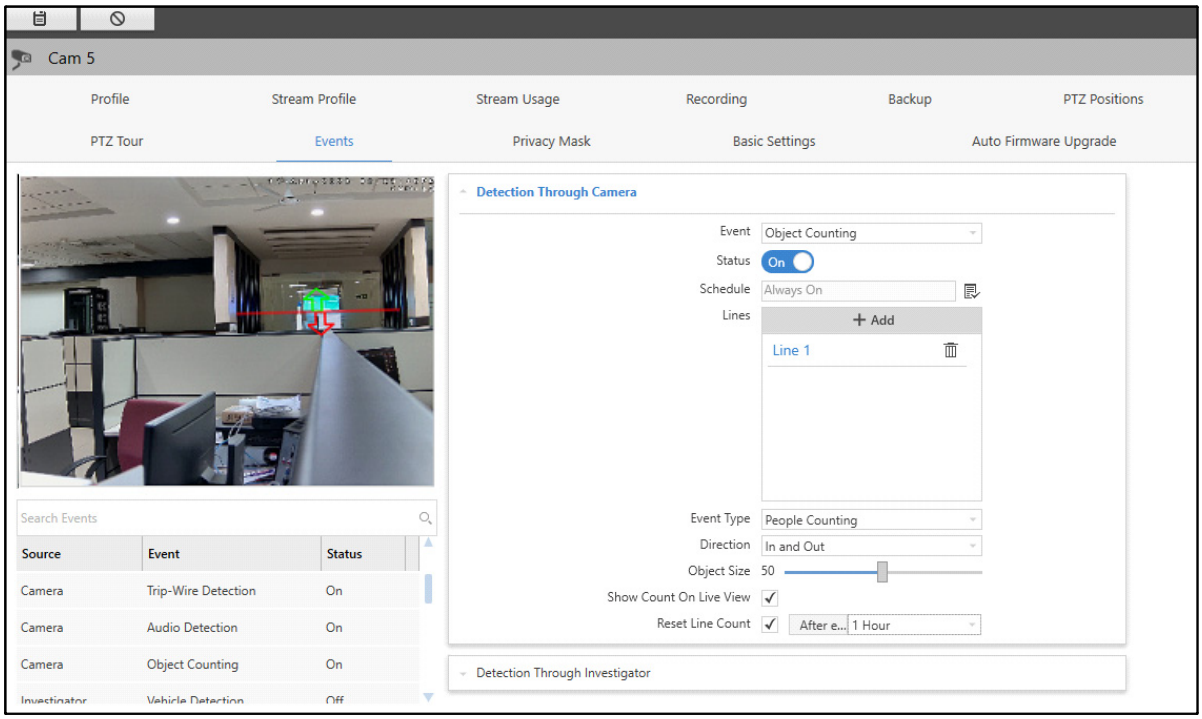
  If you select **In**, the Event will occur when an object crosses the line in the direction of green color.

  If you select **Out**, the Event will occur when an object crosses the line in the direction of red color.

  If you select **In and Out**, the Event will occur either when an object crosses the line either in the direction of green or red color.
- **Object Size**: Drag the slider to set the desired Object Size for the Object Detection Event. Valid Range: 1-100. Default: 50.
- **Show Count on Live View**: Select the check box to view the count of the objects on the live view of the camera.
- **Reset Line Count**: Select the check box to automatically reset the count of the Line to zero after the specified duration has elapsed. Specify the time after which the line count should be reset. For example, If the Reset Line Count is selected as After Every 1 hour, the line count will be set to zero after every 1 hour.

- Click **Save** to save the settings or **Cancel** to discard.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event or delete the Line.



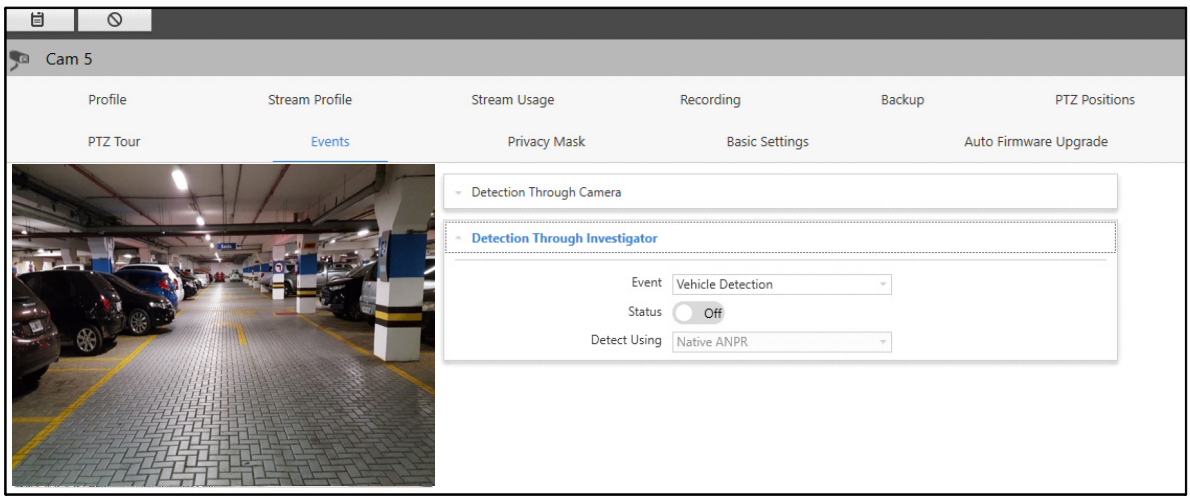
- Select the Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Line.

Detection Through Investigator

This panel displays the configurations for Events that can be detected through Investigator tab of Smart Client only when they are enabled in the Admin Client. These Events are fetched from the playback recordings of the cameras. You can edit and configure the Events detected by Investigator from this collapsible panel.

To view and edit Events,

- Click the **Detection Through Investigator** collapsible panel.



Each configuration page of camera will depend on camera brand and model and how the camera has been added in Admin Client i.e., via Brand-model/ONVIF/Generic.

Refer to the following links for the configuration details of various Events.

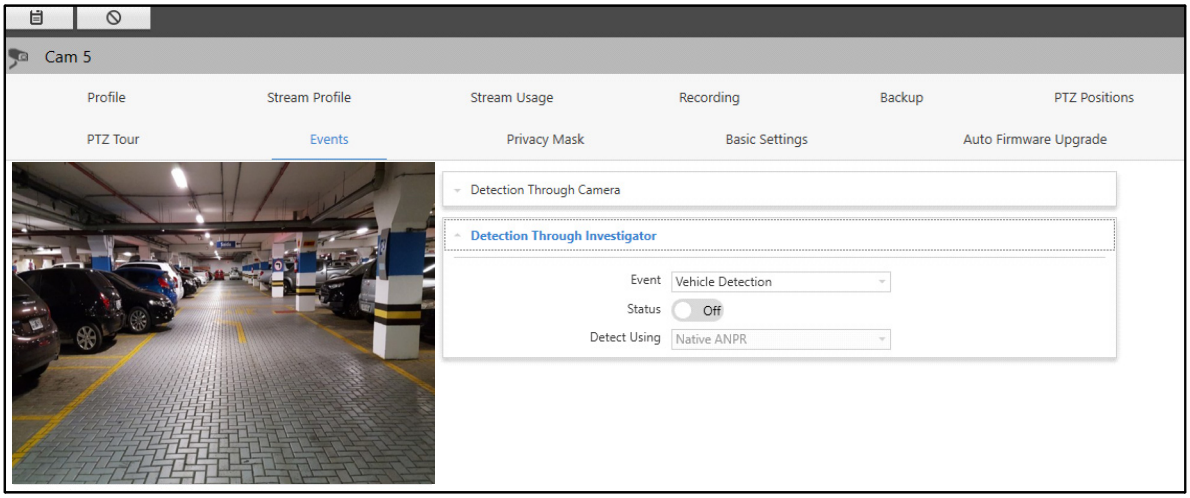
- “Vehicle Detection”
- “Face Detection”
- “People Counting”
- “Vehicle Counting”
- “Prohibited Parking”
- “Improper Parking”
- “Wrong Way Detection”
- “Unauthorized Parking”
- “Object Detection”
- “Premises Availability”

Detection through Investigator *feature will be supported as per the IVA License purchase. For detailed license information, refer to the* ***SATATYA SAMAS Installation Guide****.*

Vehicle Detection

The Vehicle Detection feature enables you to define the cameras on which investigation of Vehicle Detection should be performed. Once this Event is configured, you can detect vehicles in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Vehicle Detection,



Configure the following parameters:

- **Event**: Select the Vehicle Detection Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

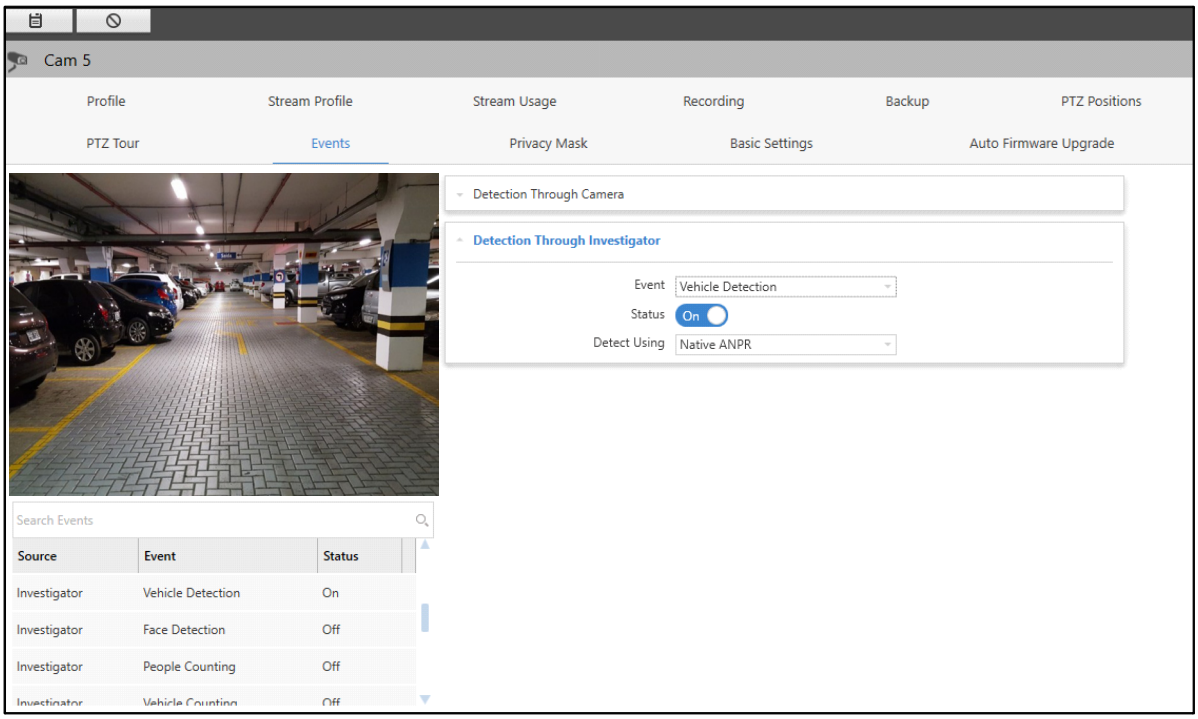
  Once the Status switch is **On**, you can configure the remaining parameters.
- **Detect Using**: Select the detection method from the drop-down list options — Native ANPR or CARMEN ARH.

Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Slot/Driveway/ Vehicle Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.

- Click **Save** to save the settings or **Cancel** to discard.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event

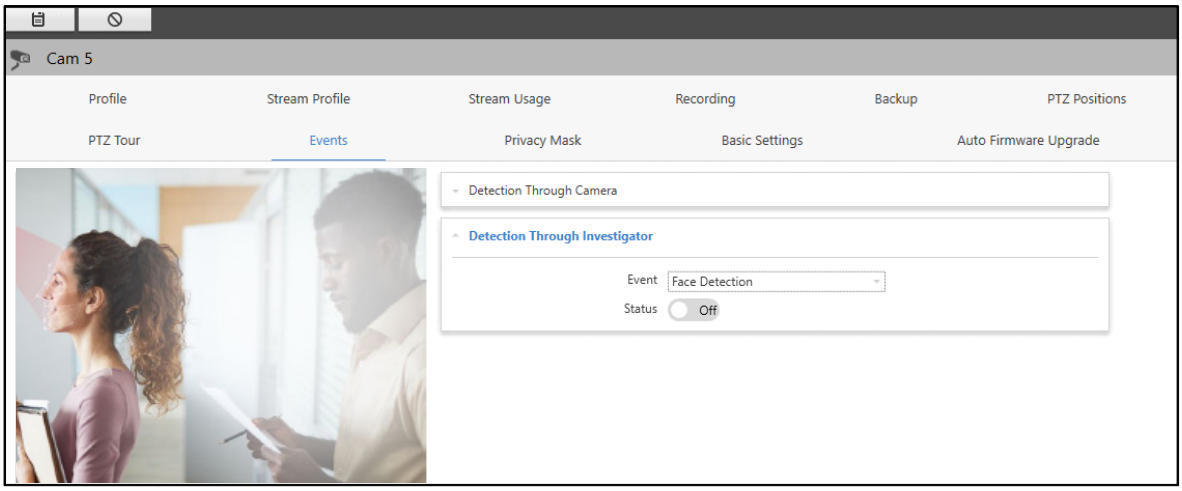


- Select the Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

Face Detection

The Face Detection feature enables you to define the cameras on which investigation of Face Detection should be performed. Once this Event is configured, you can detect the faces of individuals in the playback of the assigned cameras using the Smart Client **Investigator** tab.

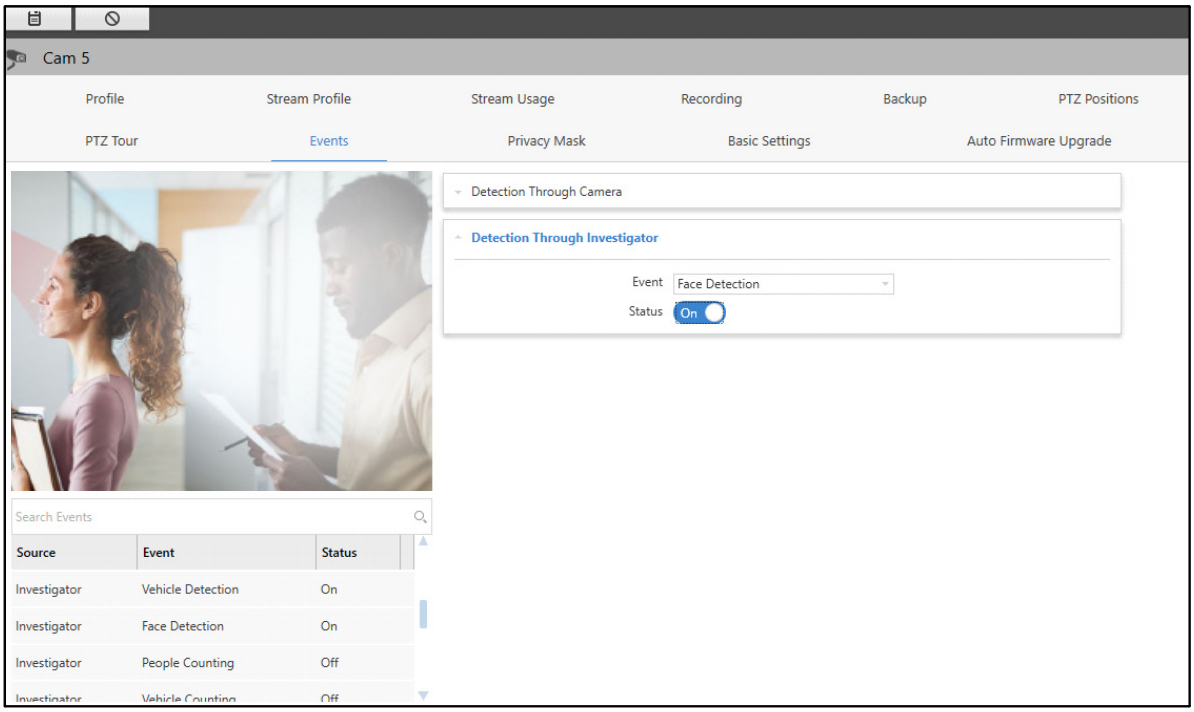
To configure Face Detection,



Configure the following parameters:

- **Event**: Select the Face Detection Event from the drop-down list.
- **Status**: Switch on the Status switch to enable the Event.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event



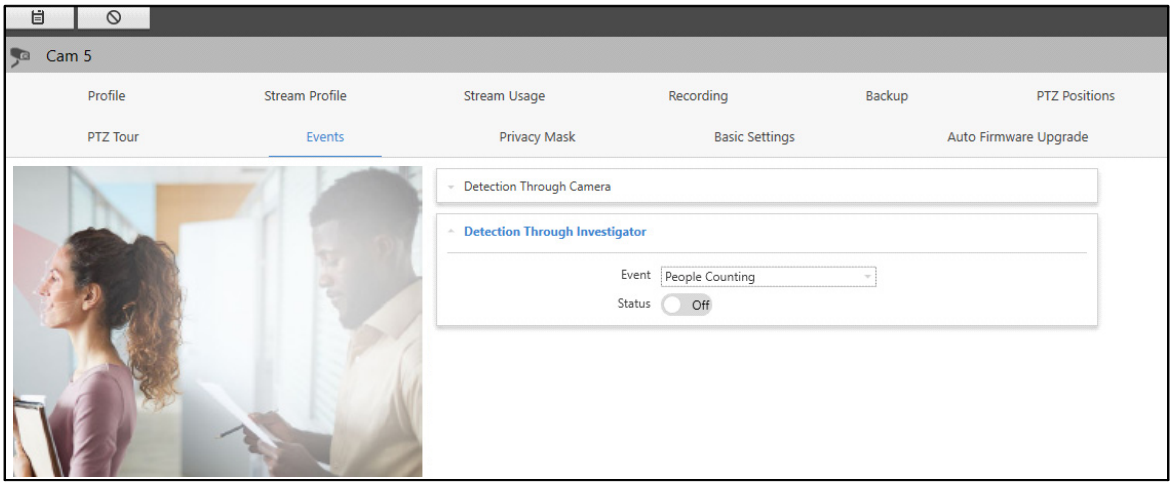
- Select the Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

Once the Event is enabled from the Admin Client, you can configure the Event from the **Investigator** tab of the Smart Client. For more details, refer to **SATATYA SAMAS Smart Client Manual**.

People Counting

The People Counting feature enables you to define the cameras on which investigation of People Counting should be performed. Once this Event is configured, you can keep a count of people in a premise in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure People Counting,

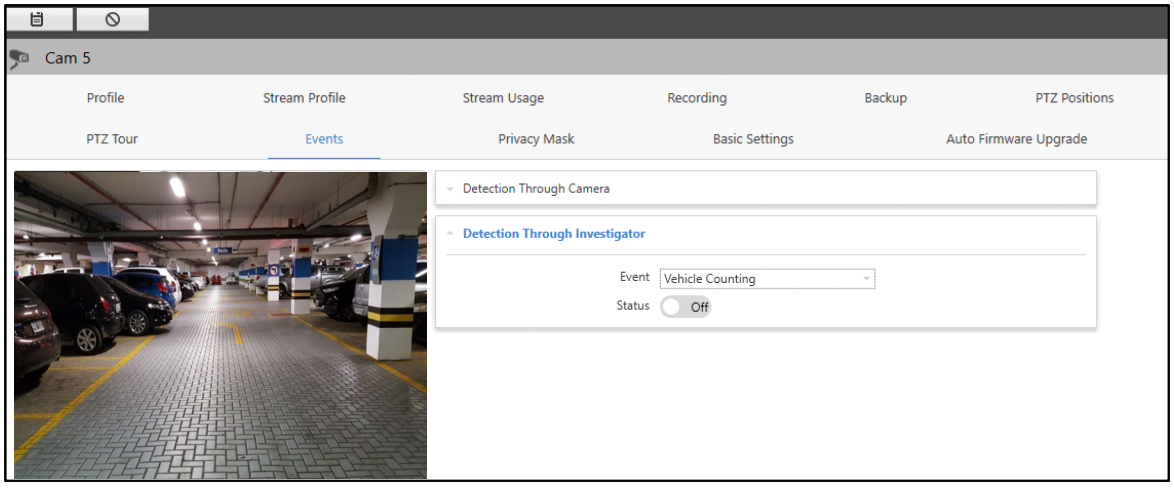


The configurations of People Counting Event are similar to the Face Detection. For more details, refer to “Face Detection”.

Vehicle Counting

The Vehicle Counting feature enables you to define the cameras on which investigation of Vehicle Counting should be performed. Once this Event is configured, you can keep a count of vehicles in a premise in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Vehicle Counting,

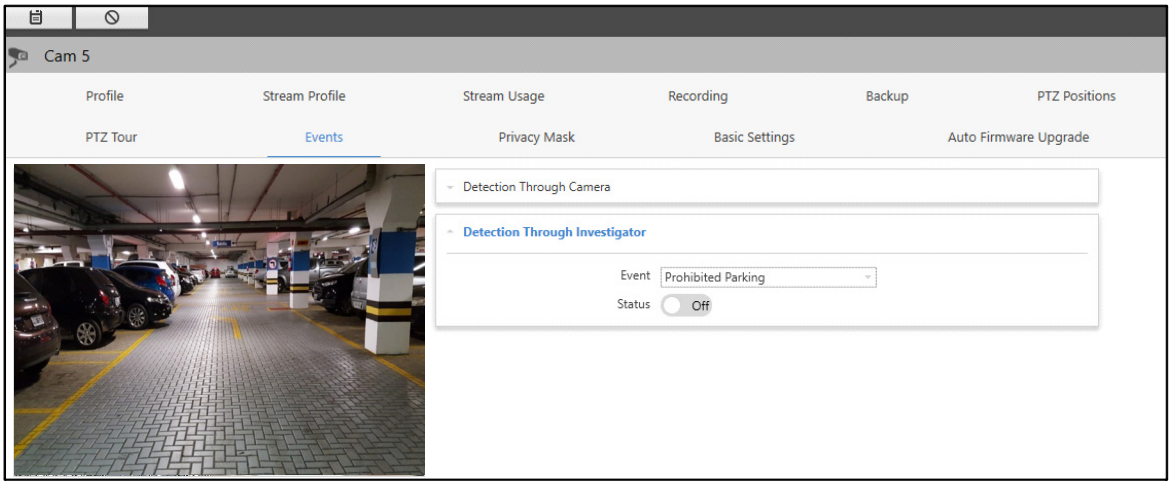


The configurations of Vehicle Counting Event are similar to the Face Detection. For more details, refer to “Face Detection”.

Prohibited Parking

The Prohibited Parking feature enables you to define the cameras on which investigation of Prohibited Parking should be performed. Once this Event is configured, you can keep a track of vehicles parked in a prohibited area in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Prohibited Parking,

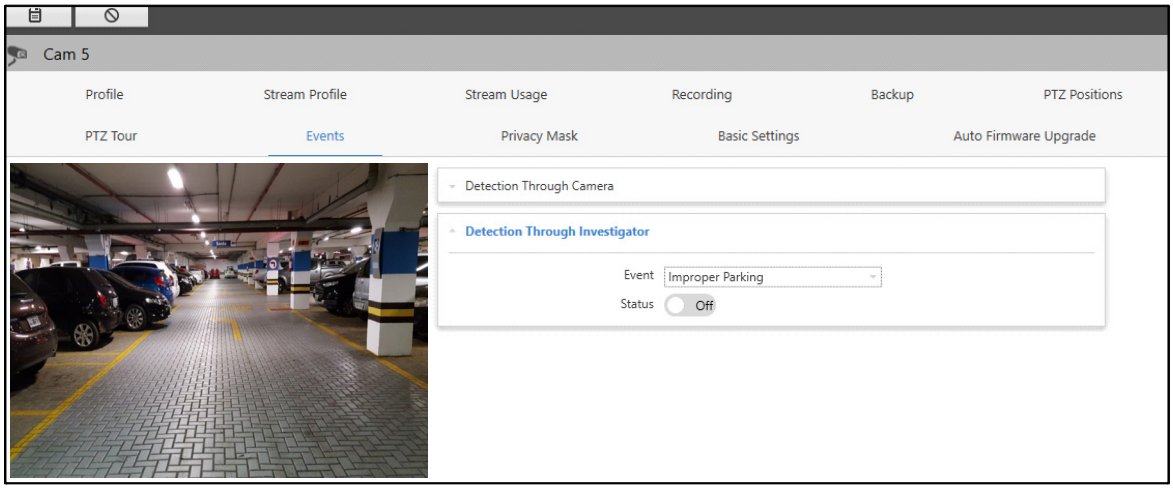


The configurations of Prohibited Parking Event are similar to the Face Detection. For more details, refer to “Face Detection”.

Improper Parking

The Improper Parking feature enables you to define the cameras on which investigation of Improper Parking should be performed. Once this Event is configured, you can keep a track of vehicles parked wrongly in an area in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Improper Parking,

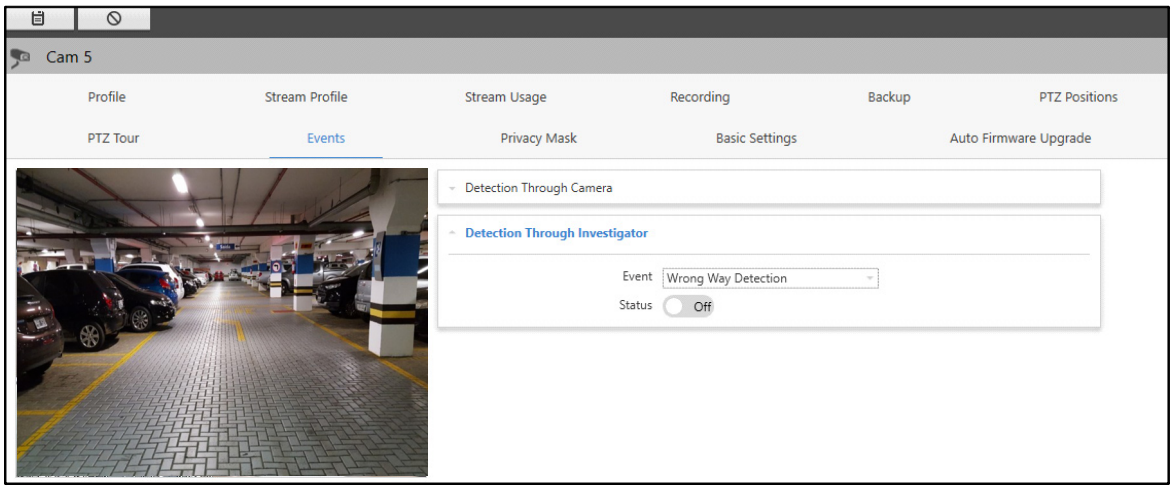


The configurations of Improper Parking Event are similar to the Face Detection. For more details, refer to “Face Detection”.

Wrong Way Detection

The Wrong Way Detection feature enables you to define the cameras on which investigation of Wrong Way Detection should be performed. Once this Event is configured, you can keep a track of vehicles entering from the wrong way in a premise in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Wrong Way Detection,

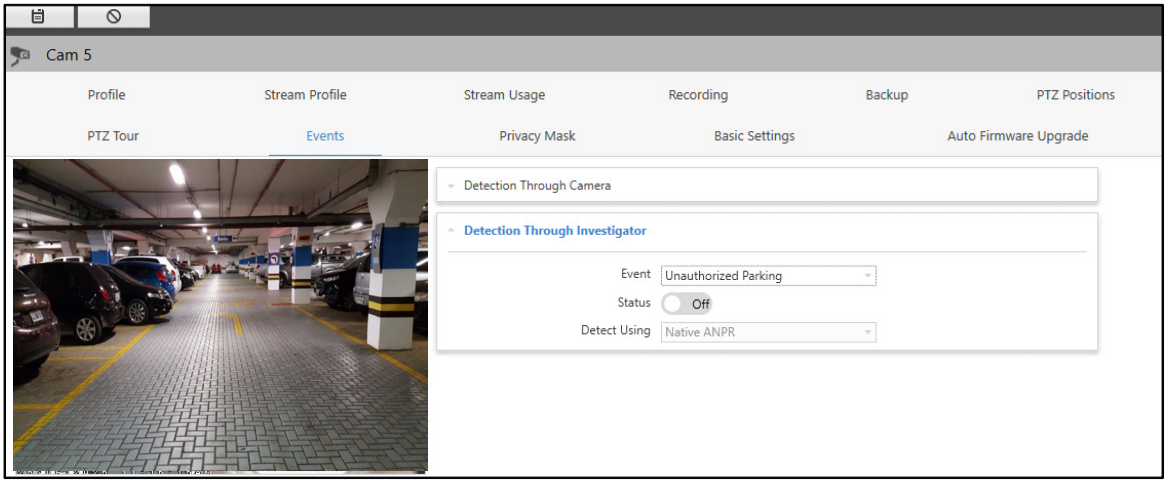


The configurations of Wrong Way Detection Event are similar to the Face Detection. For more details, refer to “Face Detection”.

Unauthorized Parking

The Unauthorized Parking feature enables you to define the cameras on which investigation of Unauthorized Parking should be performed. Once this Event is configured, you can keep a track of vehicles parked in an unauthorized premise in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Unauthorized Parking,

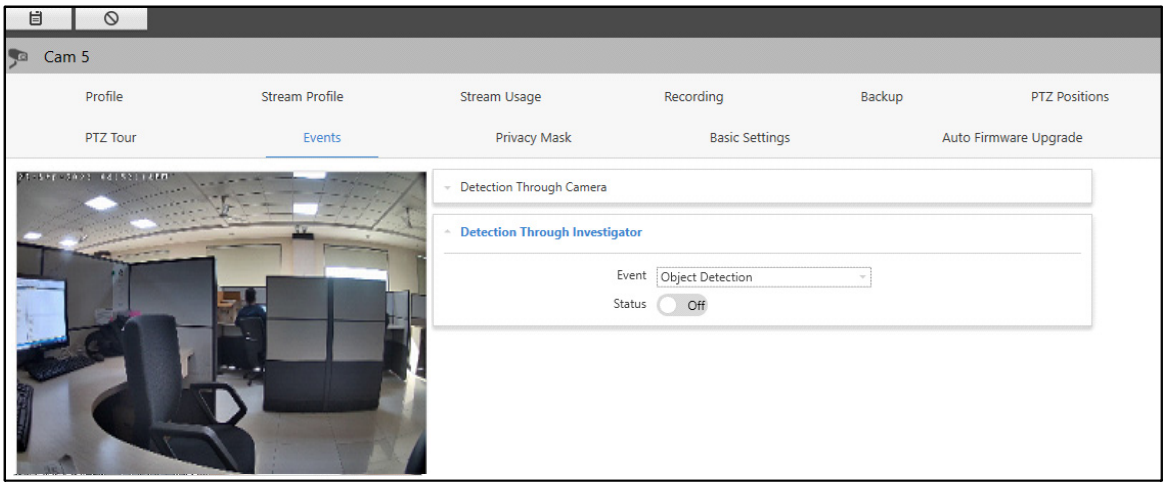


The configurations of Unauthorized Parking Event are similar to the Vehicle Detection. For more details, refer to “Vehicle Detection”.

Object Detection

The Object Detection feature enables you to define the cameras on which investigation of Object Detection should be performed. Once this Event is configured, you can detect the objects in a given zone in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Object Detection,

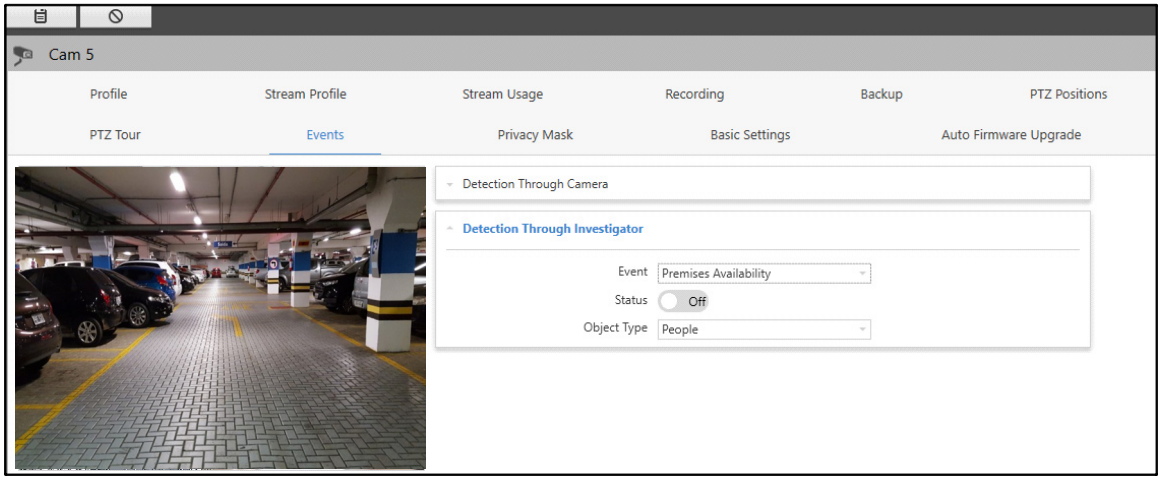


The configurations of Object Detection Event are similar to the Face Detection. For more details, refer to “Face Detection”.

Premises Availability

The Premises Availability feature enables you to define the cameras on which investigation of Premises Availability should be performed. Once this Event is configured, you can detect the availability of premises in the playback of the assigned cameras using the Smart Client **Investigator** tab.

To configure Premise Availability,



Configure the following parameters:

- **Event**: Select the Premise Availability Event from the drop-down list.

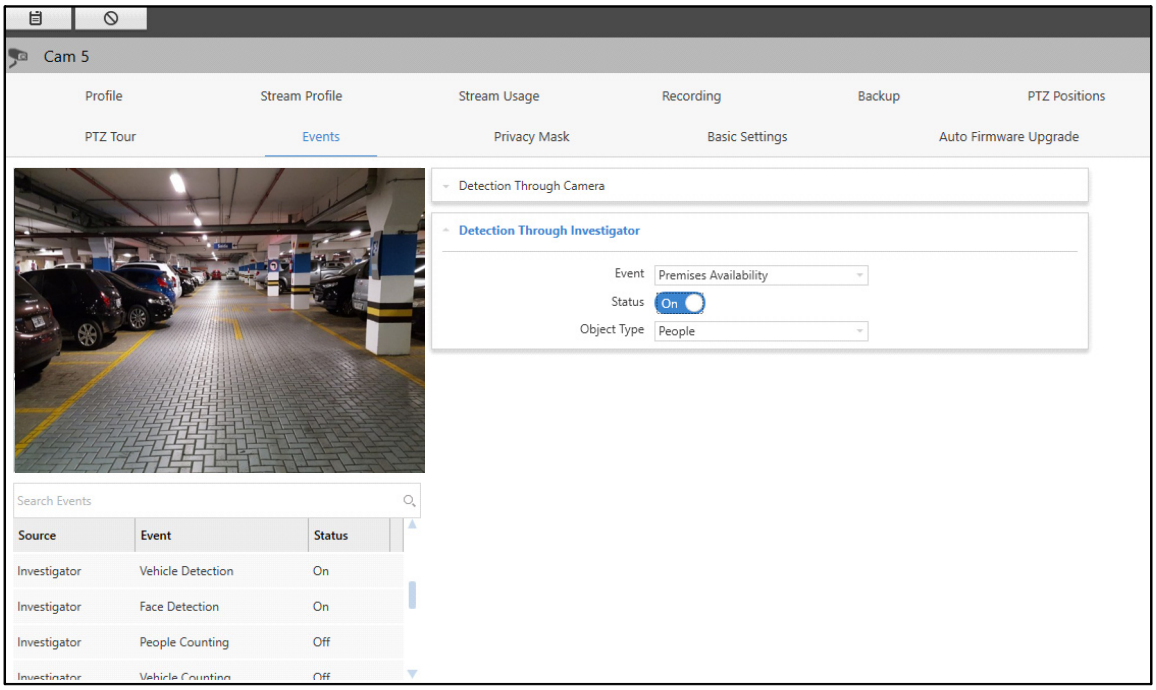
- **Status**: Switch on the Status switch to enable the Event.

  Once the Status switch is **On**, you can configure the remaining parameters.

- **Object Type**: Select the Object Type from the drop-down list options — People or Vehicle.

- Click **Save** to save the settings or **Cancel** to discard.

The Event Status appears in a list below the live view of the camera. You can change the configurations of the Event



- Select the Event from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

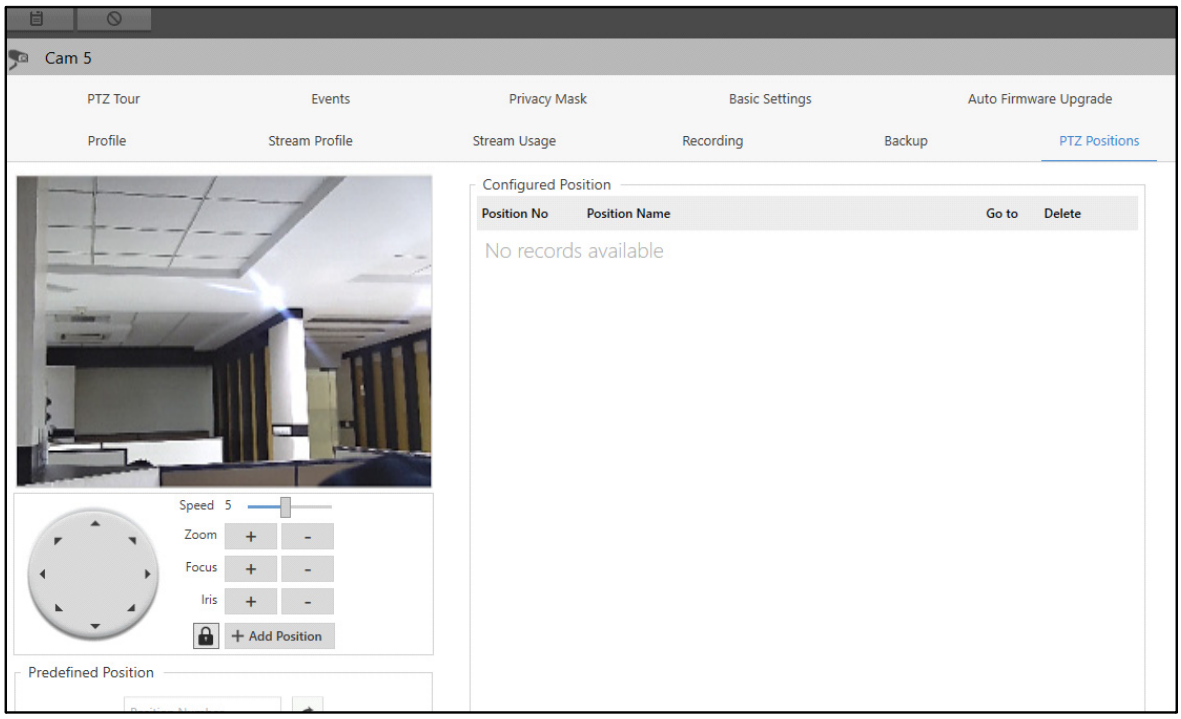
PTZ Positions

PTZ Positions is not applicable to Mobile Cameras.

This tab enables you to configure the Pan/Tilt/Zoom positions of a PTZ camera. For a network camera which supports the Pan/Tilt/Zoom (PTZ) functionality, it is possible to define which preset position the camera view will move to, when an event is triggered. A single preset position can be configured for each camera using this functionality. Preset positions can be set to move a PTZ camera to a desired preset location at the click of a button. Preset positions can also be used to design PTZ Tours.

To view and configure PTZ Positions,

- Click the **PTZ Positions** tab.

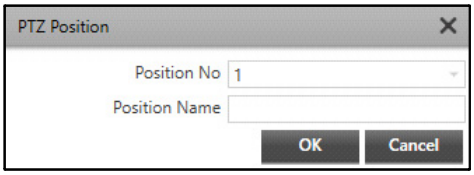


The live view of the camera is displayed on the left hand side. Referring to the live view, configure the following parameters:

By default, 300 PTZ Positions will be displayed. However, you can configure the PTZ Positions as supported by the camera.

- **Direction**: Set the camera direction using the arrow buttons on the PTZ Control to view the desired location.
- **Speed**: Set the camera speed by dragging the slider to left or right. This determines the speed at which the camera should move from one position to the next. Valid Range: 1-10. Default: 5.
- **Zoom**: Set the camera Zoom using the + and - buttons.
- **Focus**: Set the camera Focus using the + and - buttons.
- **Iris**: Set the camera Iris using the + and - buttons.

- Click **Add Position**. The **PTZ Position** pop-up appears.



Configure the following parameters:

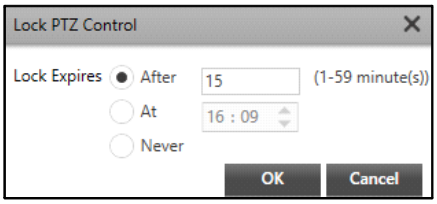
- **Position No**: Select the Position No. from the drop-down list.

- **Position Name**: Specify a suitable Position Name for the configured camera position. In Position Name, you can enter upto 50 characters. Default: Blank.

- Click **OK** to confirm or click **Cancel** to discard.

You can lock the configured PTZ Control according to the assigned PTZ Priority. For more details, refer to "Users".

- Click **Lock PTZ Control** . The **Lock PTZ Control** pop-up appears.



Configure the following parameter:

- **Lock Expires**: Select the desired option — After, At or Never.

  If you select **After**, specify the time in minutes after which the PTZ Lock should expire. After the lock expires lower priority users will be able to modify the PTZ Controls. Valid Range: 1-59 minutes. Default: 15.

  If you select **At**, set the time when the PTZ Lock should expire. After the lock expires lower priority users will be able to modify the PTZ Controls.

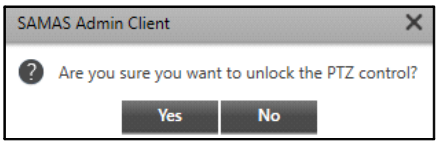
  If you select **Never**, the PTZ Lock will expire only after logout. The lock will never expire and the lower priority users will not be able to modify the PTZ Controls till logout of higher priority user.

- Click **OK** to confirm or click **Cancel** to discard.

Hover over the icon to view the details of the user who has locked the PTZ controls. The details displayed are — User Name and Lock Timer.

Once the PTZ Control is locked, the icon toggles to **Unlock**.

- Click **Unlock PTZ Control** **.** The following pop-up appears.



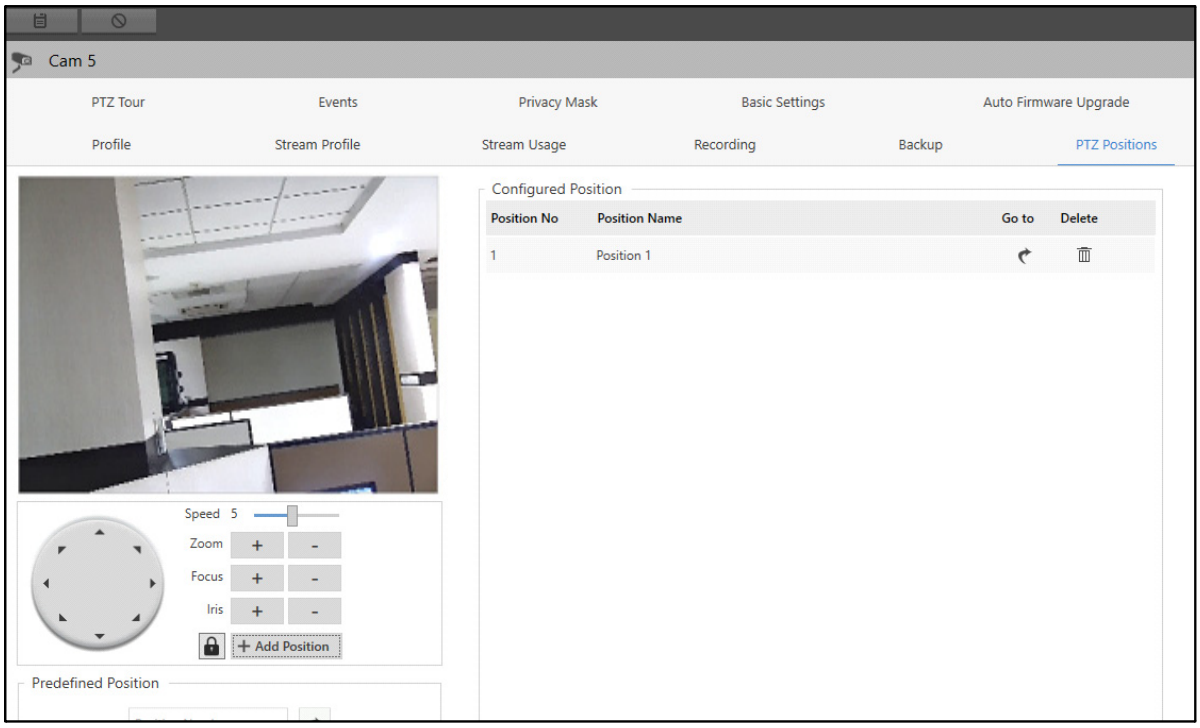
- Click **Yes** to confirm or click **No** to discard.

Only a user with higher or same priority as compared to the user who locked PTZ Controls can unlock the PTZ Controls before the timer expires. Once the PTZ Lock timer expires, all the users can perform PTZ Operations.

The PTZ Lock timer will reset if the Recording Server restarts or disconnects.

The PTZ Lock will not function if a PTZ Tour is running.

The new preset position appears in the Configured Positions list. You can configure these parameters — Go to, Delete and Predefined Position.



- **Go to**: Click **Go to** to move the camera view to this position.
- **Delete**: Click **Delete** to delete the position.
- **Predefined Position**: Specify the Position No and click **Go to** to move the camera to the preset position.

- Click **Save** to save the settings or **Cancel** to discard.

*Admin Client supports the Manufacturer defined preset positions for PTZ Cameras. You can move the camera to a preset position pre-defined by the Camera Manufacturer by entering the Position Number in **Predefined Position**. Pre-defined **Configured Positions** list can be found in the respective Manufacturer's Manual.*

*For example, say, a manufacturer has pre-defined Position No **255** for the **Auto Scan** function. Moving to Position No 255 for that camera shall move the camera to the defined position and also initiate Auto Scan function in the camera.*

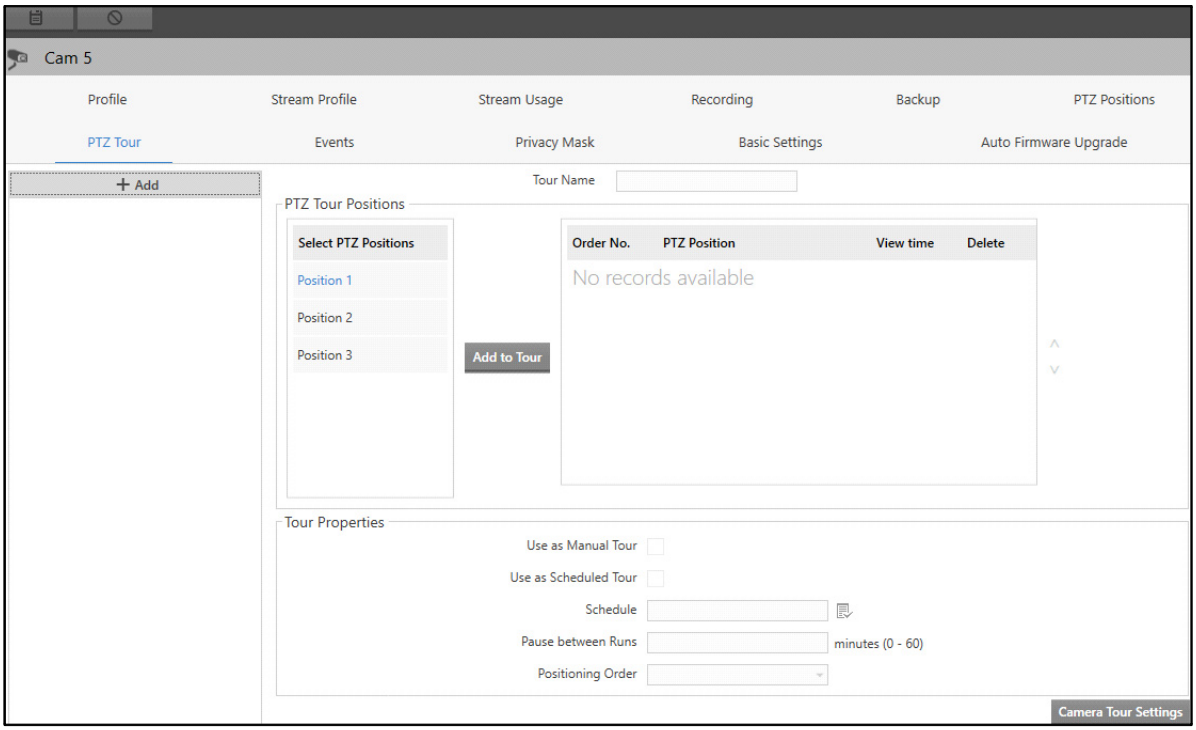
PTZ Tour

PTZ Tour is not applicable to Mobile Cameras.

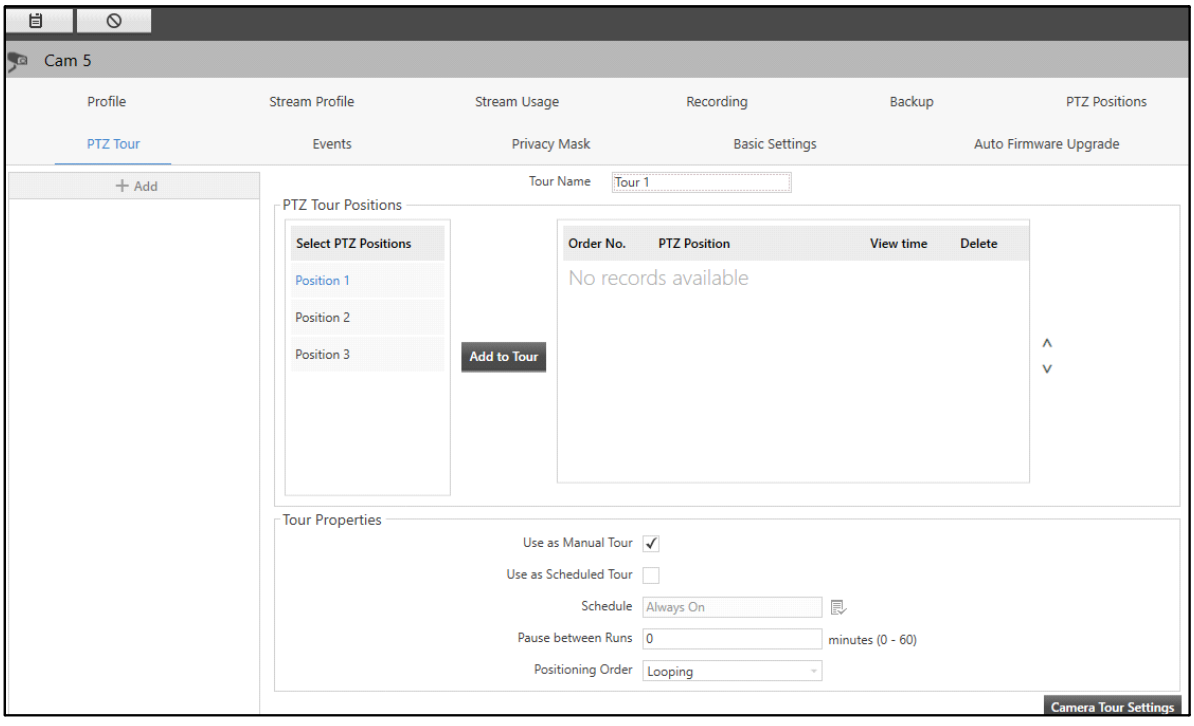
This tab enables you to configure the Pan/Tilt/Zoom Tour of a PTZ camera. A PTZ Tour is a configured sequence of preset positions to be followed by a PTZ camera.

To view and configure PTZ Tour,

- Click the **PTZ Tour** tab.



- Click **Add**.



*If **PTZ Priority Delay Time** is configured, you can add a PTZ Tour but it cannot be accessed by any Smart Client user until the delay time expires or a higher priority user makes a change in the PTZ operations.*

The PTZ Lock will not function if a PTZ Tour is running.

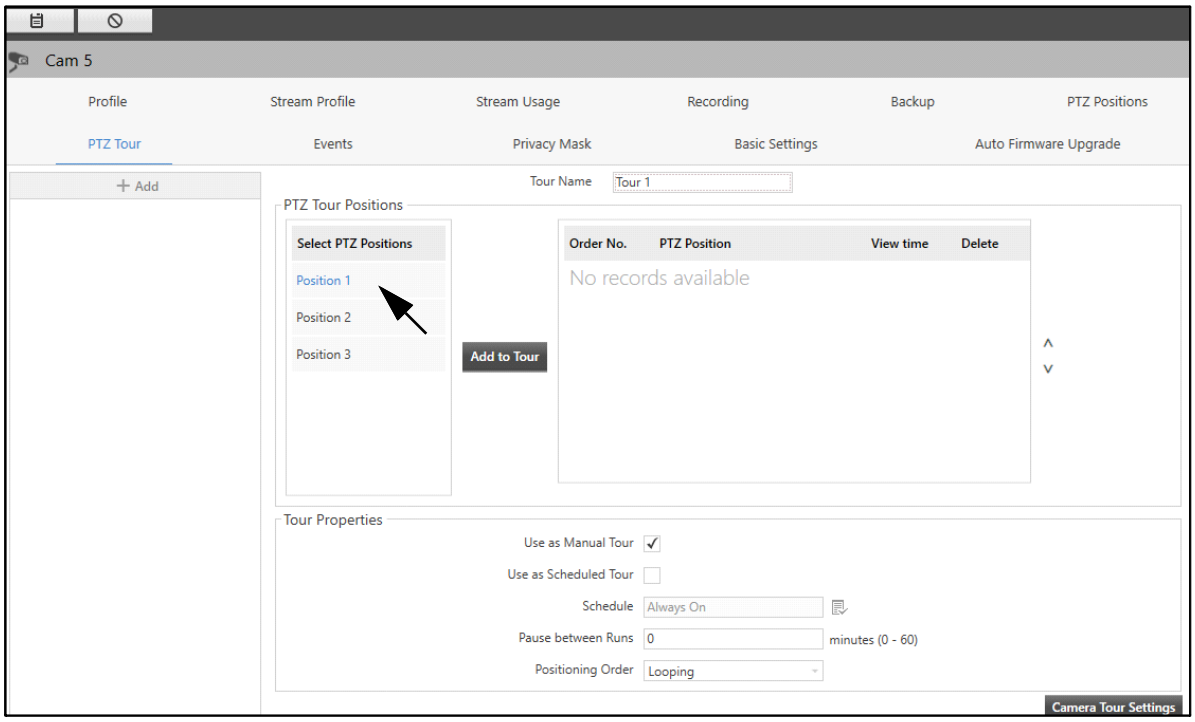
- **Tour Name**: Specify a suitable Tour Name. In Tour Name, you can enter upto 50 characters. Default: Blank.

The PTZ Tour configurations consist of two sections — "PTZ Tour Positions" and "Tour Properties".

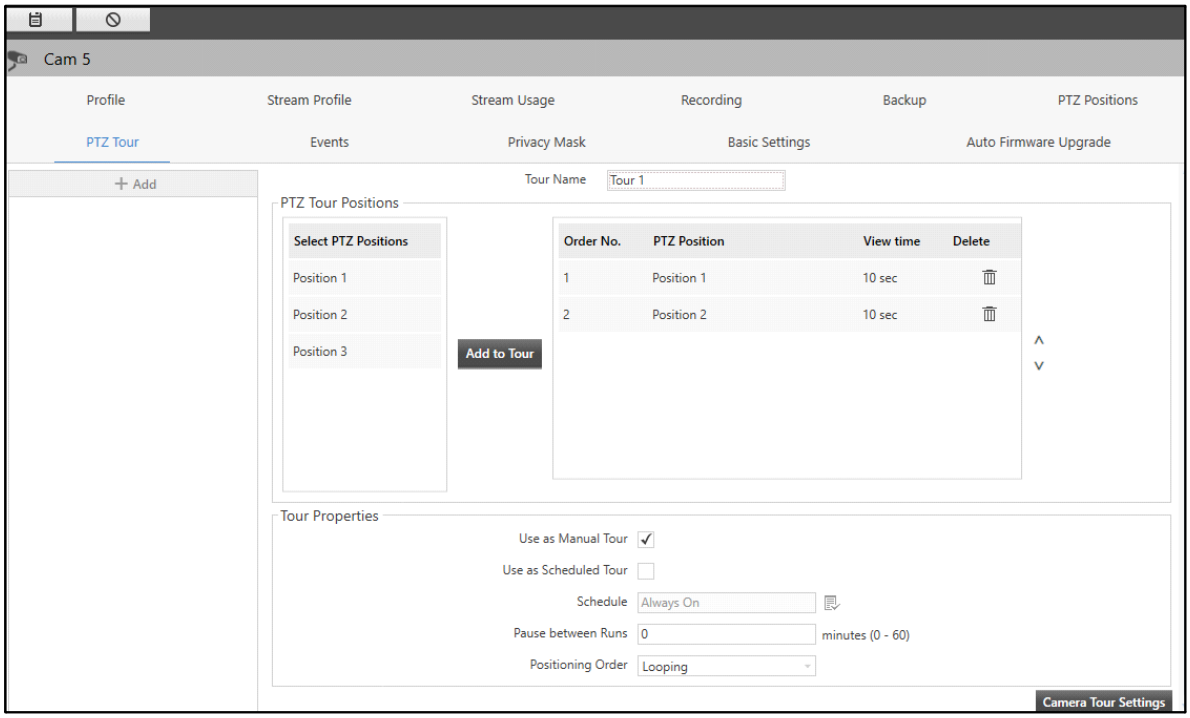
PTZ Tour Positions

This section allows you to configure the PTZ Positions to be displayed in the PTZ Tour.

- Select the PTZ Positions from the **Select PTZ Positions** list. Upto 20 positions can be added in a Tour. The order in which positions are added in a Tour will define the sequence in which the positions will be displayed during the Tour.

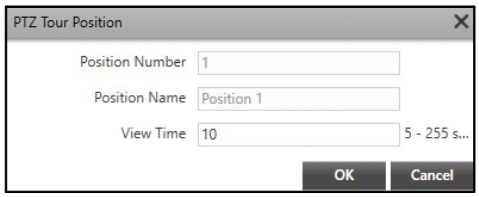


- Click **Add to Tour**. The selected positions appear in a list on the right hand side.



These Position details are displayed — Order No., PTZ Position, View time and Delete. You can configure the View time of the position or Delete it.

- Double-click on the PTZ Position to change the **View time**. The **PTZ Tour Position** pop-up appears.



  - Specify the View Time duration for which the position should be displayed in the Tour. Valid Range: 5-255 seconds. Default: 10.

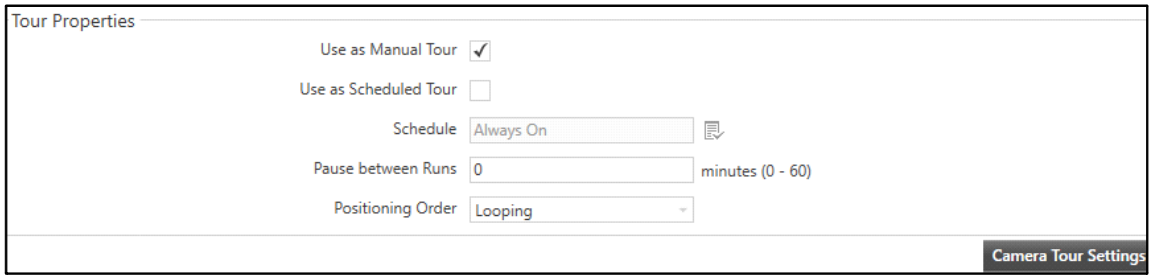
- Click **OK** to confirm or click **Cancel** to discard.
- Click **Delete** corresponding to any PTZ position to delete it.

  You can reorder the sequence of PTZ positions after adding them to the Tour. Drag the positions up or down the list to reorder the sequence.

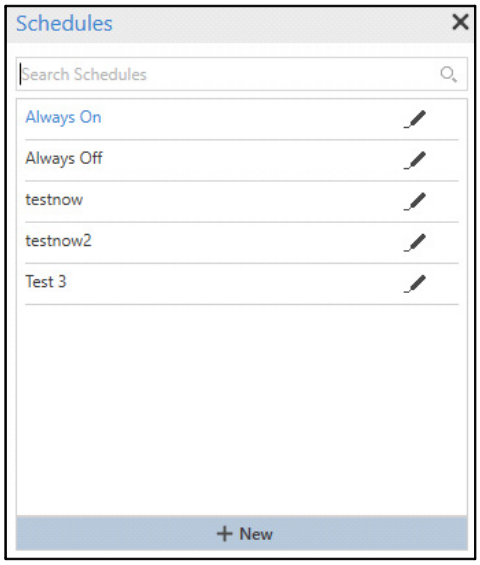
- Click **Save** to save the settings or **Cancel** to discard.

Tour Properties

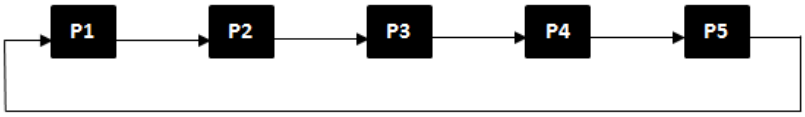
This section allows you to configure the settings of the PTZ Tour.



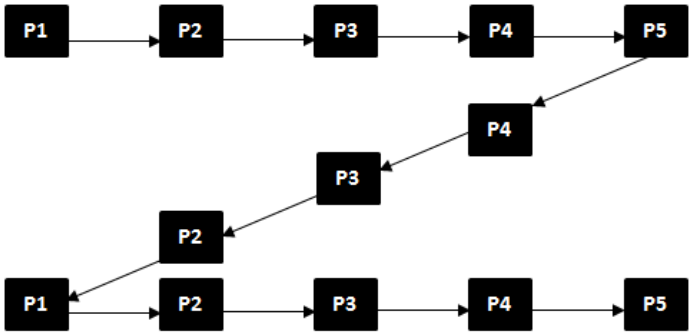
- **Use as Manual Tour**: Select the check box to run this Tour manually.
- **Use as Scheduled Tour**: Select the check box to run this Tour as per a specific schedule.
- **Schedule**: Select the desired Schedule of the PTZ Tour using the **Schedules** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".
- **Pause between Runs**: Specify the duration for which there will be a pause between two consecutive runs of the same tour. Valid Range: 0-60 minutes. Default: 0.
- **Positioning Order**: Select a Positioning Order from these options in the drop-down list — Looping, Zigzag and Random.
  - **Looping**: The Tour runs in a fixed order from the first preset position to the last preset position and then starts from the first position again.

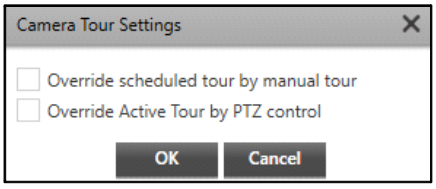


- **Zigzag**: The Tour runs in a fixed ordered loop from the first preset position to the last preset position and backwards; from the last preset position to the first.



- **Random**: The Tour runs in a random order of positions.

- Click **Camera Tour Settings**. The **Camera Tour Settings** pop-up appears.



- **Override scheduled tour by manual tour**: Select the check box if you wish to start manually triggered PTZ Tour even when the scheduled Tour is running.

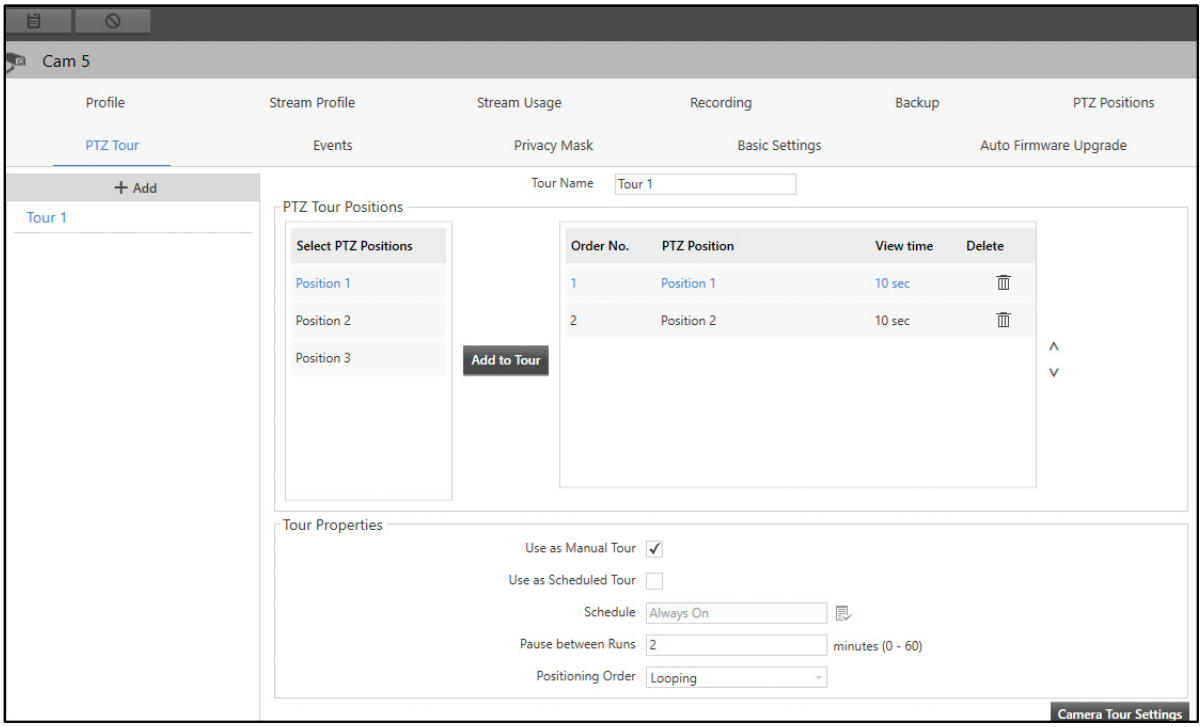
- **Override Active Tour by PTZ control**: Select the check box if you wish the camera to move to the preset positions even when the PTZ Tour is running.

- Click **OK** to confirm or click **Cancel** to discard.
- Click **Save** to save the settings or **Cancel** to discard.

*If **Override Active Tour by PTZ control** is enabled and a user moves the camera to a preset position, the system will override the tour as per the assigned PTZ Priority.*

*If **Override Active Tour by PTZ control** is disabled and a tour is running, the PTZ requests will not be served.*

The configured PTZ Tour appears on the left hand side.



Once the PTZ Tour configuration is complete, you can log into Smart Client to view/manually operate the PTZ Tour.

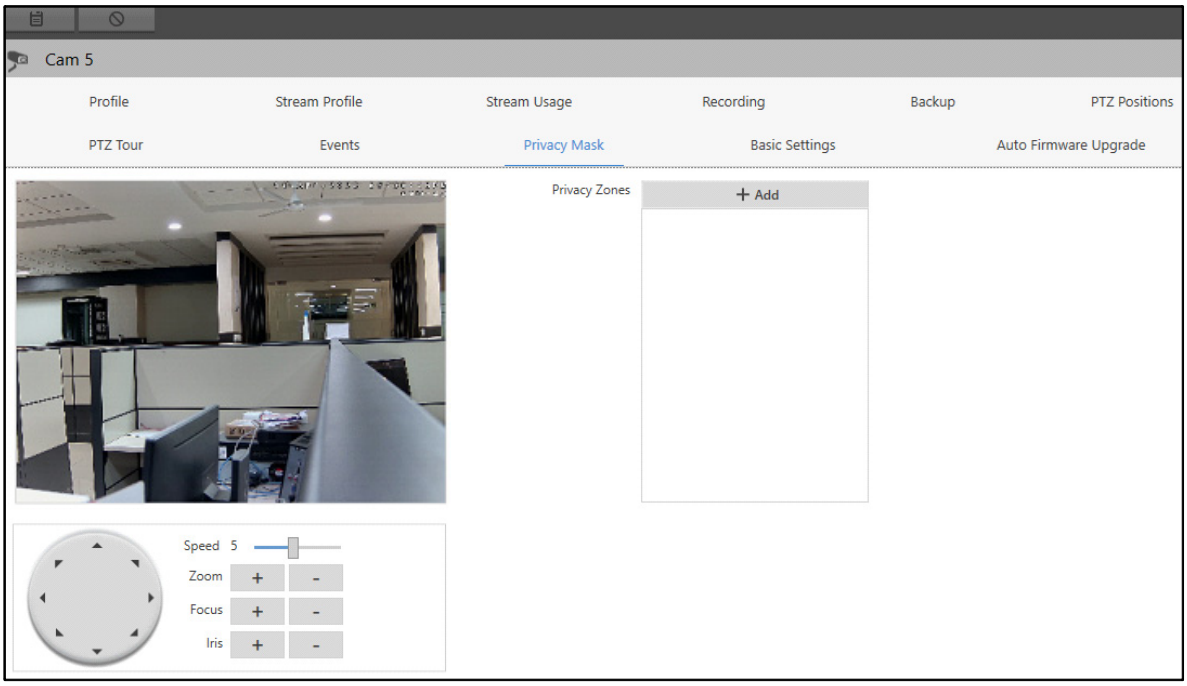
Privacy Mask

Privacy Mask is not applicable to Mobile Cameras and for cameras added via ONVIF.

This tab enables you to configure privacy zones for the live view of a camera so that the view is blocked for certain areas which are to be kept private from any surveillance. The number of privacy zones allowed to be configured will depend on the maximum number of privacy zones supported by the camera brand. If no information is available on the same for the brand, a maximum of 4 zones can be defined.

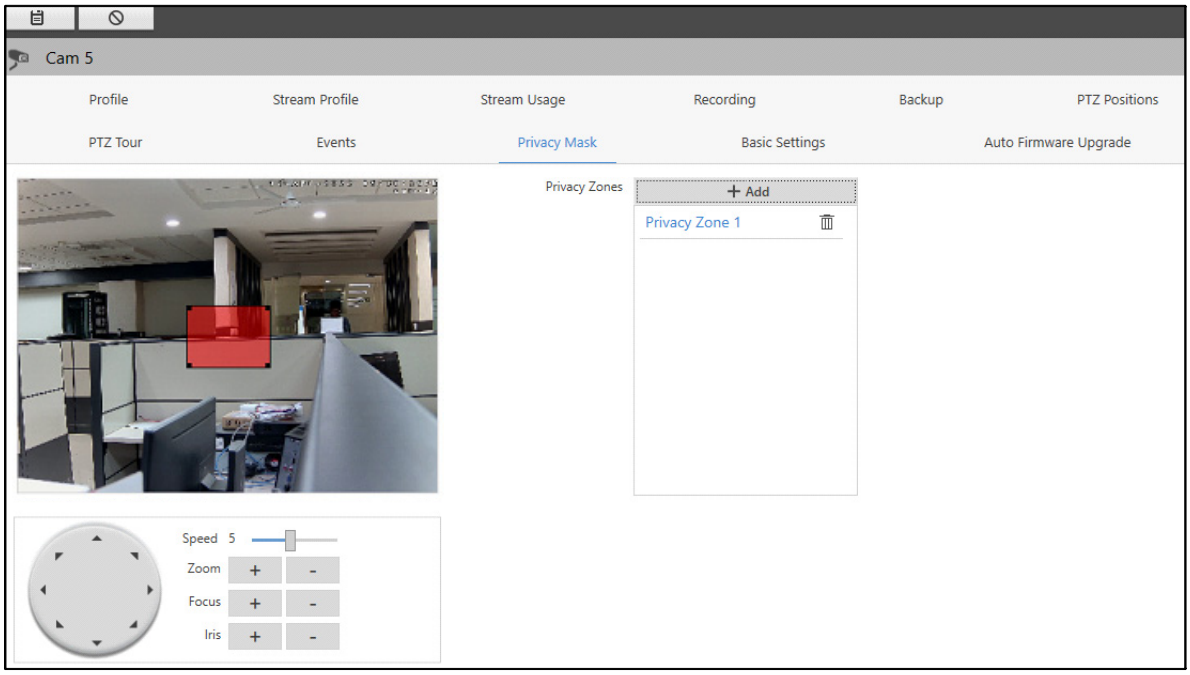
To view and configure Privacy Mask,

- Click the **Privacy Mask** tab.

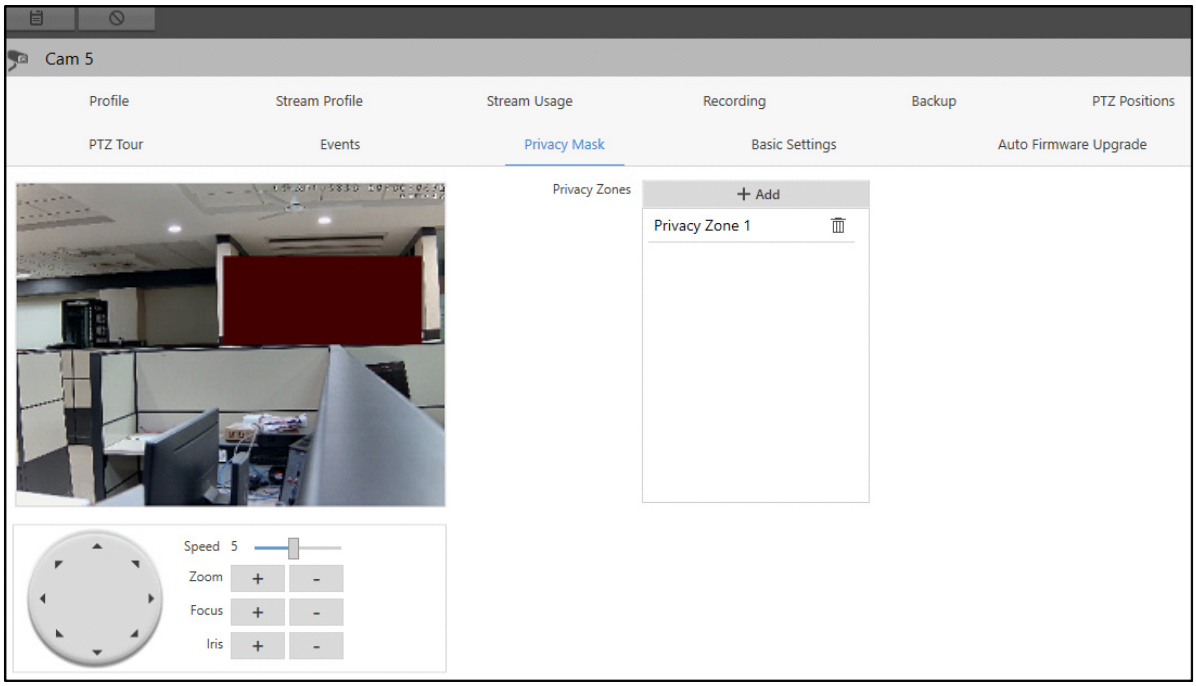


Before configuring a Privacy Mask for Matrix PTZ cameras, you can set the desired camera angle using the PTZ Control. For details, refer to "PTZ Positions".

- Click **Add**. Drag the mouse across the camera live view to select area of the view for which Privacy Mask is to be enabled.



The configured Privacy Zones appear in a list on the right hand side. The configured area will appear blank.



- Click **Delete** corresponding to the Privacy Zone to delete it.
- Click **Save** to save the settings or **Cancel** to discard.

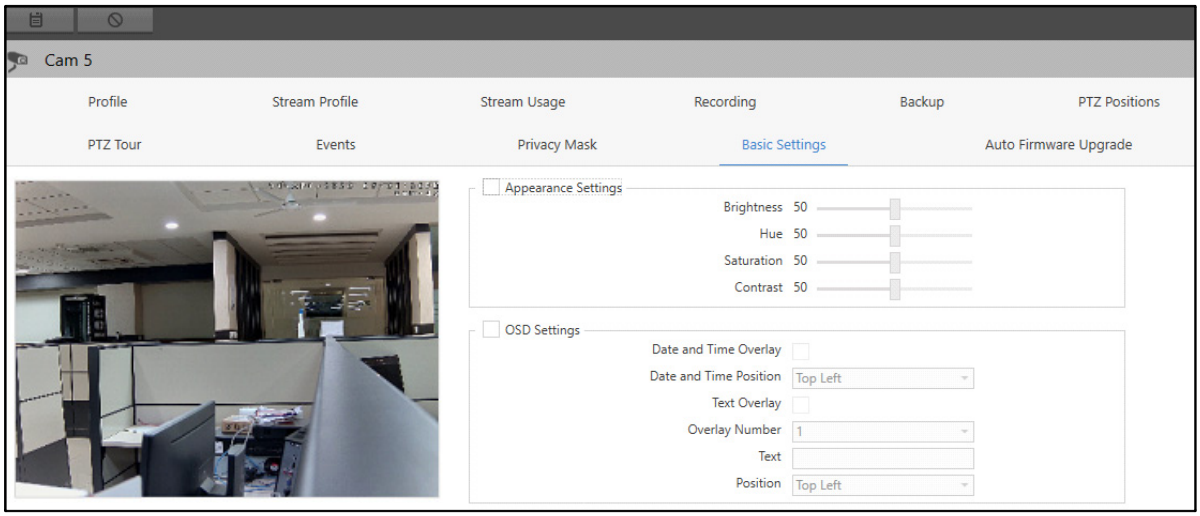
Basic Settings

Basic Settings is not applicable to Mobile Cameras.

This tab enables you to configure the Appearance Settings and On-Screen Display (OSD) settings of a camera.

To view and configure Basic Settings,

- Click the **Basic Settings** tab.



The live view of the camera is displayed on the left hand side. Referring to the live view, Configure the following parameters:

Appearance Settings

- Select the Appearance Settings check box to enable the configuration of Appearance Settings parameters.
    - **Brightness**: Set the Brightness by dragging the slider to left or right. Valid Range: 0-100. Default: 50.
    - **Hue**: Set the Hue by dragging the slider to left or right. Valid Range: 0-100. Default: 50.
    - **Saturation**: Set the Saturation by dragging the slider to left or right. Valid Range: 0-100. Default: 50.
    - **Contrast**: Set the Contrast by dragging the slider to left or right. Valid Range: 0-100. Default: 50.
- Click **Save** to save the settings or **Cancel** to discard.

OSD Settings

The OSD Settings parameters will depend on how camera has been added, that is, via specific brand, ONVIF or Generic. The parameters also depend on the camera brand and model.

- Select the OSD Settings check box to enable the configuration of OSD Settings parameters.
    - **Date and Time Overlay**: Select the check box to display the Date and Time on the live view of the camera.
    - **Date and Time Position**: Select the position of the date and time to be displayed on the live view of the camera from the drop-down list.
    - **Text Overlay**: Select the check box to display text on the live view of the camera.
        - **Overlay Number**: Select the Overlay Number for which you wish to configure the text to be displayed. The Overlay Numbers that appear depend on the camera variant that you have selected.
        - **Text**: Specify the text to be displayed on the live view of the camera for the selected Overlay Number. In Text, you can enter upto 20 characters. Default: Blank.
        - **Position**: Select the position of the text from the drop-down list.
- Click **Save** to save the settings or **Cancel** to discard.

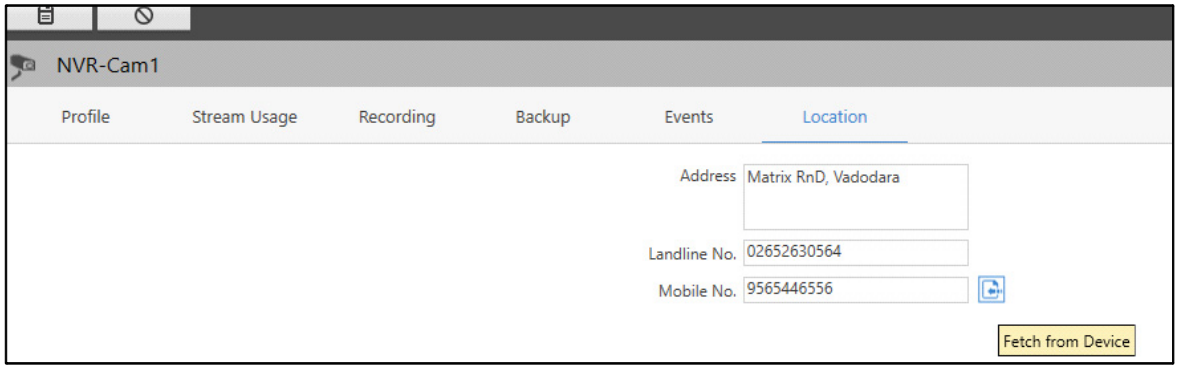
Location

This option will be visible for cameras that are added to a Device such as NVR.

This tab enables you to configure the location information of a camera.

To view and configure the location,

- Click the **Location** tab.



Configure the following parameters:

- **Address**: Specify the address where the camera is located. In Address, you can enter upto 150 characters. Default: Blank.
- **Landline Number**: Specify the Landline Number of the place where the camera is located. In Landline Number, you can enter upto 15 characters. Default Blank.
- **Mobile Number**: Specify the Mobile Number of the place where the camera is located. In Mobile Number, you can enter upto 15 characters. Default Blank.

If you are accessing a camera that has been added in a device, you can fetch the details from the respective device.

- Click on **Fetch from Device** . The location details are fetched from the device.

- Click **Save** to save the location details or **Cancel** to discard.

Using the location information provided here, you can make a call from the SATATYA SAMAS mobile application, that is, SATATYA VISION while viewing the live view of the camera.

This location information will also be displayed in the Event details in the Smart Client.

Auto Firmware Upgrade

This tab is applicable for Matrix IP Cameras added via Brand and Model method only. This tab is not applicable to cameras added to HVR/DVR/NVR.

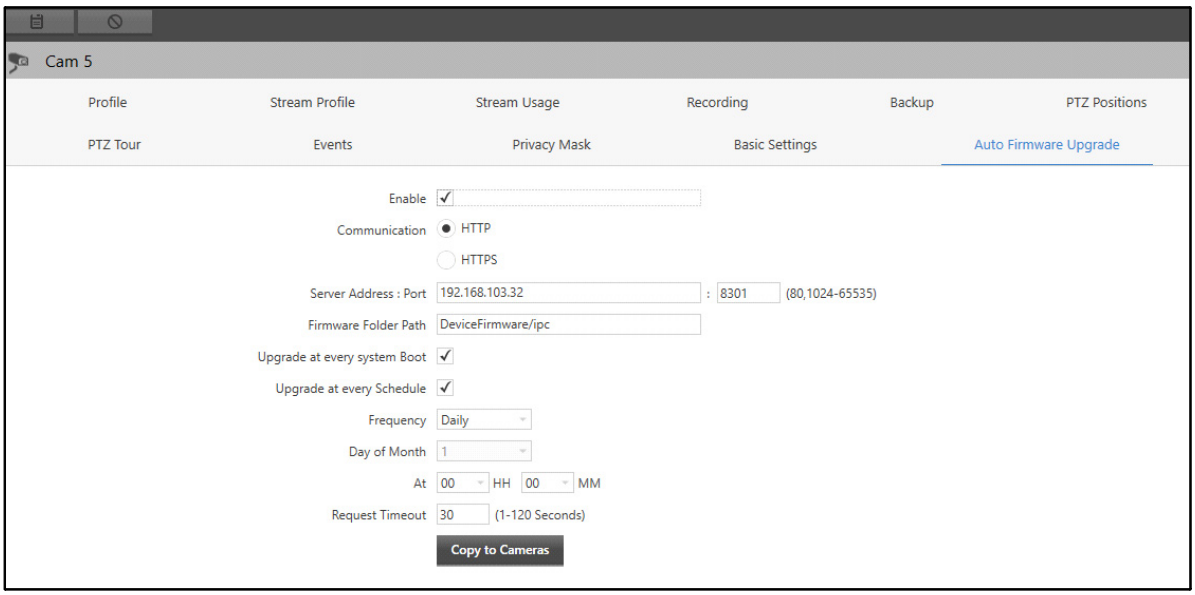
Make sure you note down the configurations of this tab if you are upgrading the camera firmware from "Device Firmware Management" page and you wish to restore the original configurations of the camera.

This tab enables you to configure the Auto Firmware parameters for a camera. By default, the configuration set on the camera webpage is displayed here. When you upgrade the camera firmware from "Device Firmware Management", the configuration on the camera webpage will be overwritten with the configuration set in "Device Firmware Management" for the selected cameras.

If you wish to restore the Auto Firmware Upgrade configuration of the cameras as per their original configurations, you need to re-configure the parameters in this tab with the information you have already noted earlier. On saving the configuration in this tab, the same will be then set on the camera webpage.

To view and configure camera Auto Firmware Upgrade,

- Click the **Auto Firmware Upgrade** tab.



Configure the following parameters:

- **Enable**: Select the check box to enable the Auto Firmware Upgrade configuration.
- **Communication**: Select the desired protocol for firmware upgrade — HTTP, HTTPS.
- **Server Address : Port**: Specify the IPv4/IPv6 Server Address and Port from where the firmware file is to be fetched. Specify the port as per the selected protocol for firmware upgrade. For Server Address, you can enter upto 39 characters. For Port, Valid Range: HTTP/HTTPS 1024-65535.
- **Firmware Folder Path**: Specify the path on the Server where the firmware files are stored. In Firmware Folder Path, you can enter upto 100 characters.
- **Upgrade at every System boot**: Select the check box if you wish the camera should check for updates in firmware files on every system boot.
- **Upgrade at every Schedule**: Select the check box if you wish the camera should check for updates in firmware files as per the configured schedule.

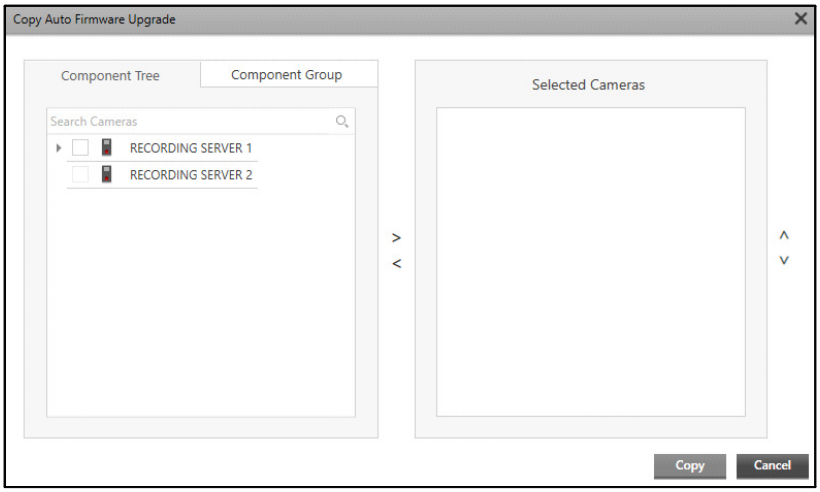
  If you select the **Upgrade at every Schedule** check box, configure the following:

- **Frequency**: Select the desired option for firmware upgrade schedule from the drop-down list — Daily, Monthly.
- **Day of Month**: If you select Frequency as **Monthly**, select the day of the month on which you wish to upgrade the camera firmware.
- **At**: Select the desired time in HH:MM format.
- **Request Timeout**: Specify the duration in seconds for which you wish the camera should wait for the Server to respond. Valid Range: 1-120 seconds.

- Click **Save** to save the settings or **Cancel** to discard.

You can copy the Auto Firmware Upgrade configurations to other cameras as well.

- Click **Copy to Cameras**. The **Copy Auto Firmware Upgrade** pop-up appears.

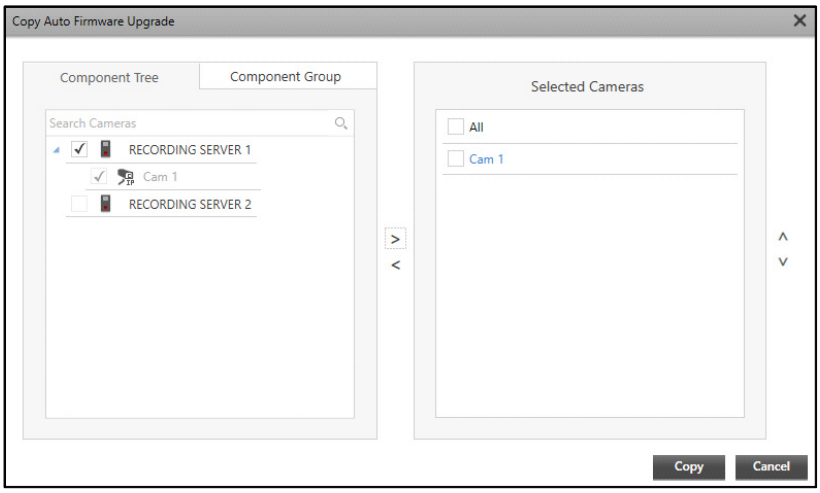


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to "Component Group". Select the check boxes of the those cameras whose Auto Firmware Upgrade configurations you wish to copy from in the Component Tree or Component Group tabs.

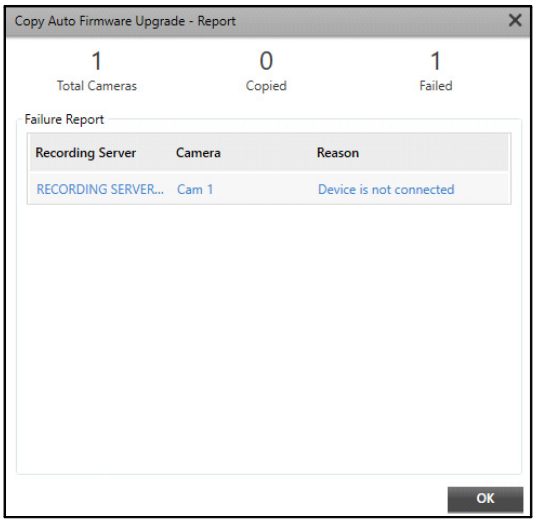
  Click the right arrow button to add these cameras to the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the desired check boxes for the cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.

  You can change the sequence of the cameras in the Selected Cameras list. To do so, select the check box of the desired cameras and click the up or down button as per your requirement.



- Click **Copy** to copy the Auto Firmware Upgrade parameters to the selected cameras. The **Copy Auto Firmware Upgrade - Report** appears.



The report displays the total number of cameras, the number of cameras to which the configurations have been copied successfully and the number of cameras to which the configurations were not copied along with the reason for failure.

- Click **OK**.

Advanced Settings

This tab enables you to configure the Advanced Parameters for Object Tracking when you have selected **Object Type** while configuring events. Depending on your installation scenario, event and profile configurations and detection environment, it may be possible that Object Detection results are not proper. In such cases, to get optimum results, you need to contact Matrix Support Team. The Team will configure or guide you to configure these parameters with respect to your installation scenario to fine-tune the algorithm and reduce variations in detection results.

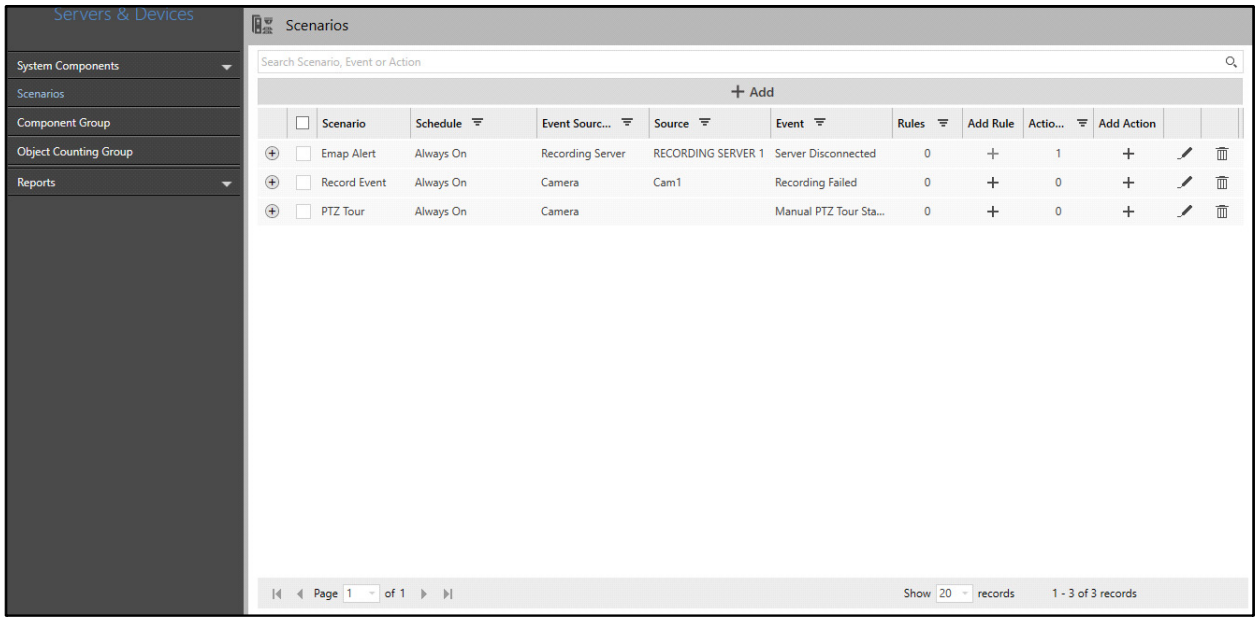
These parameters are not intended to be configured by user. These are intended to be configured in consultation with Matrix Support Team only when the desired detection results are not achieved.

Servers and Devices-Scenarios

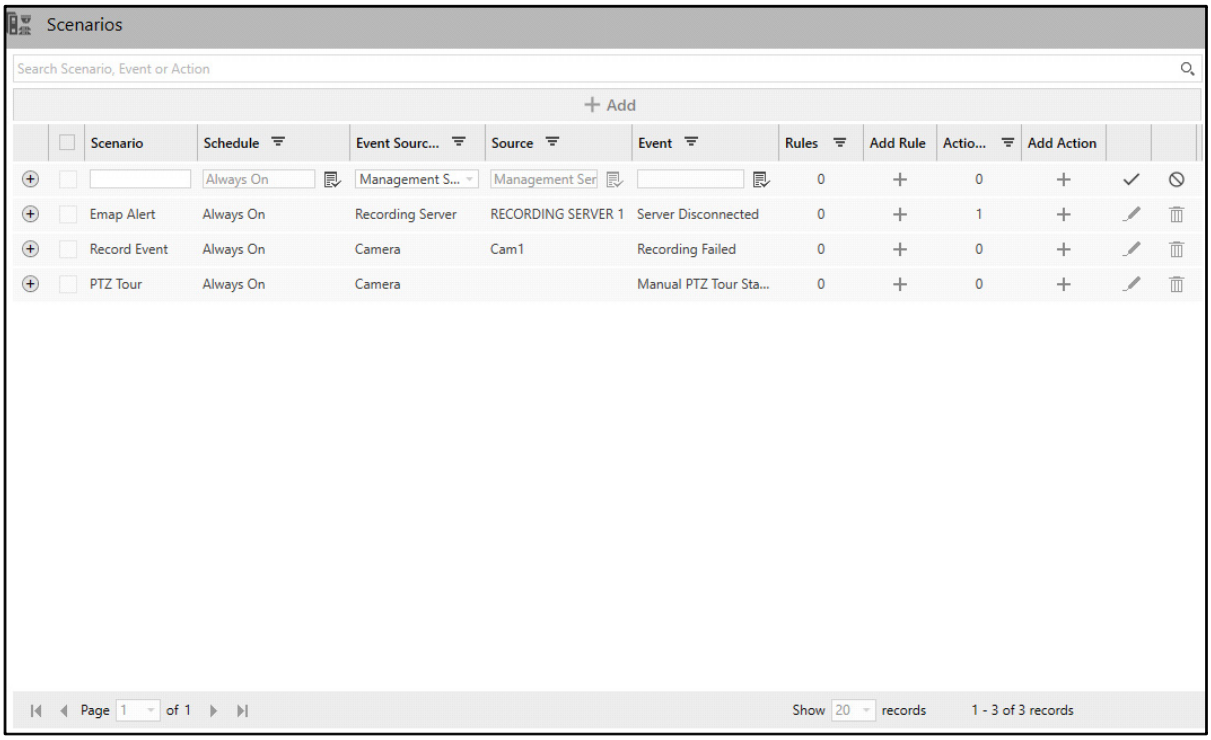
You can configure scenarios to trigger a set of actions (for example, Send SMS) on the occurrence of events at certain sources (for example, Storage Memory Low). The Scenarios page displays all the Scenarios configured for Servers and Devices. You can view and configure the Scenarios for all the Servers and Devices.

To configure Scenarios,

- Click **Servers & Devices > Scenarios**.



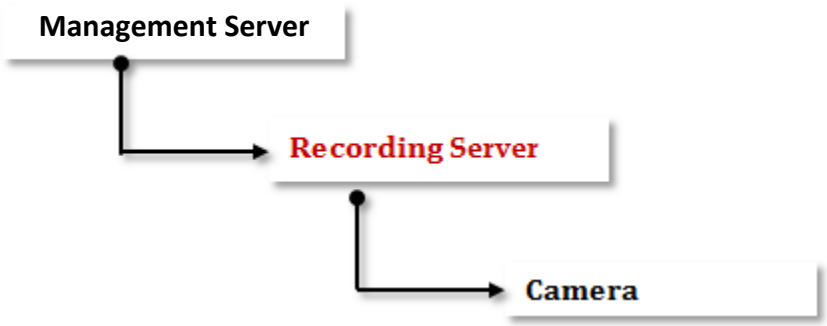
- Click **Add**.



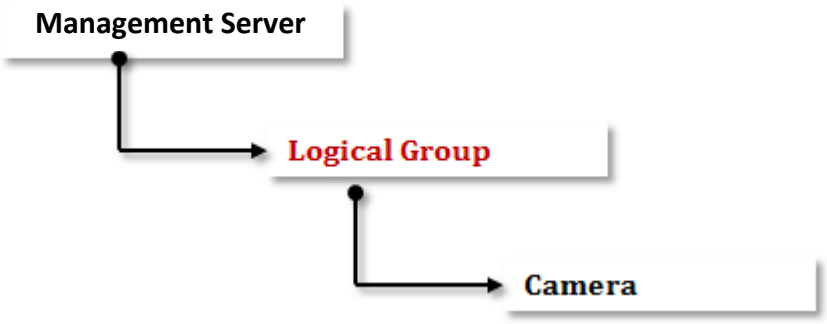
The configurations of Scenarios for Servers and Devices are similar to the configurations of the Basic Scenario. For details, refer to “Basic Scenario”.

Component Group

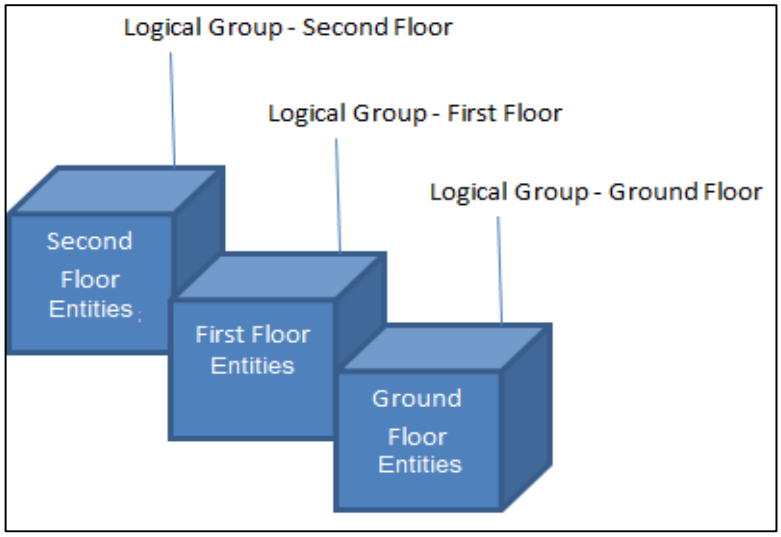
The Admin Client enables grouping of cameras based on a Server- Device hierarchy.



However, a user may want to bypass this pre-defined physical hierarchy and create a custom camera group based on logical operation. The **Component Group** in the Admin Client enables you to create camera groups and add selected cameras to it, such as floor-wise camera groups, department-wise camera groups, area-wise camera groups etc.



You can also add the entities (Camera, Alarm and Sensor) into a custom group from different Recording Servers. Hence, this type of grouping is independent of the Server-Device hierarchy inherent to SATATYA SAMAS. However, each entity can be associated with only one group at a time. If you try to add the same entity in the second group, that entity would be removed from the first group.

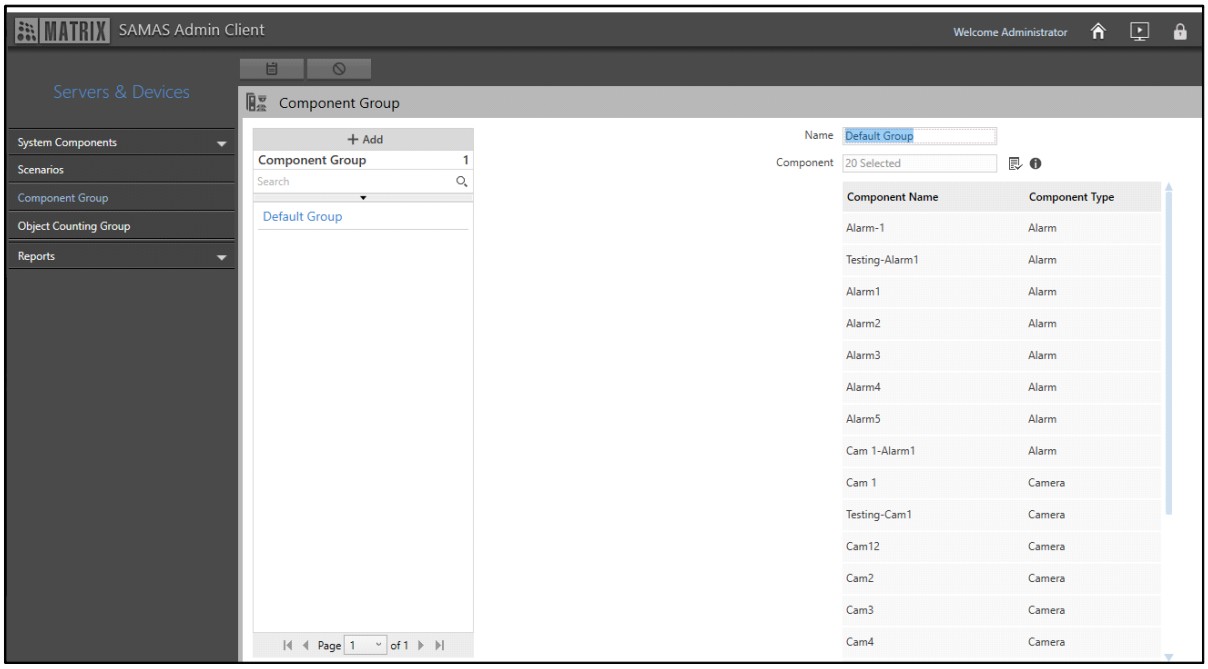


Creating a Group

The Component Group page displays all the configured Component Groups. You can view and configure the Component Groups, add new Camera Groups, Alarm Groups as well as Sensor Groups.

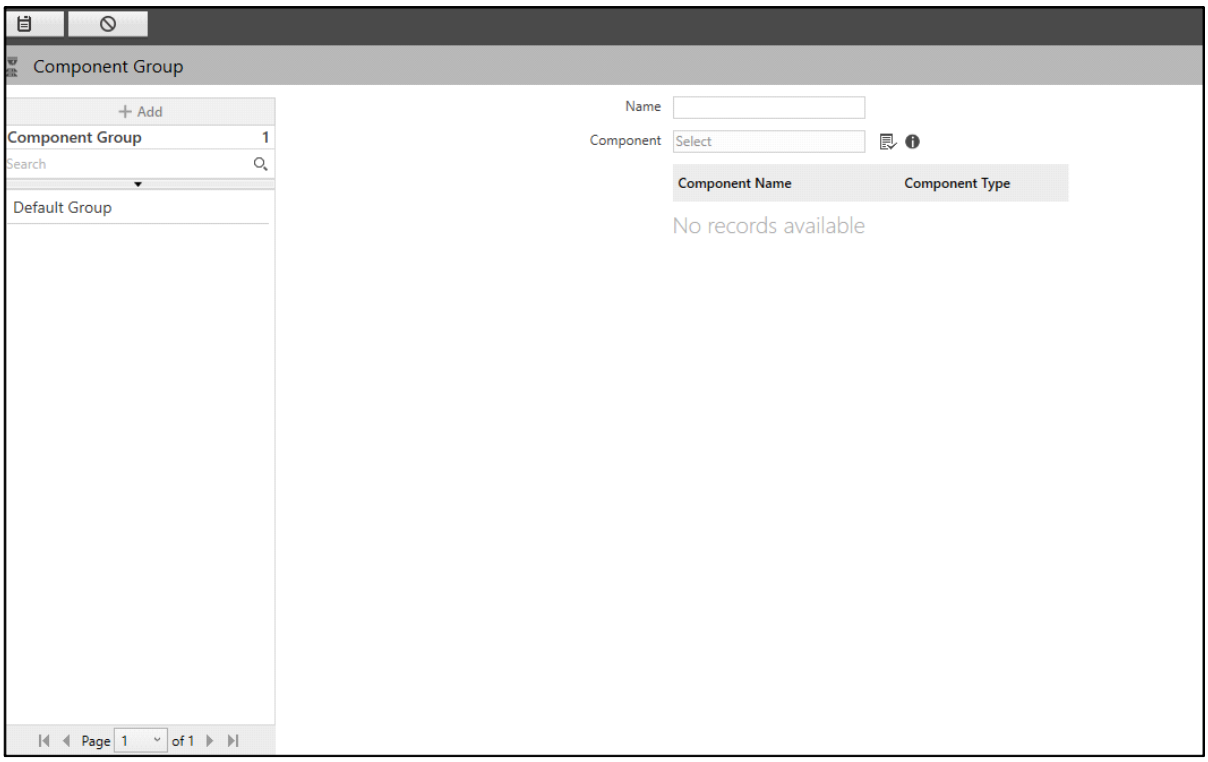
To create a new Group,

- Click **Servers and Devices > Component Group**.



*The **Component Group** page will always have a **Default Group**. You can only edit its parameters. This Default Group cannot be deleted.*

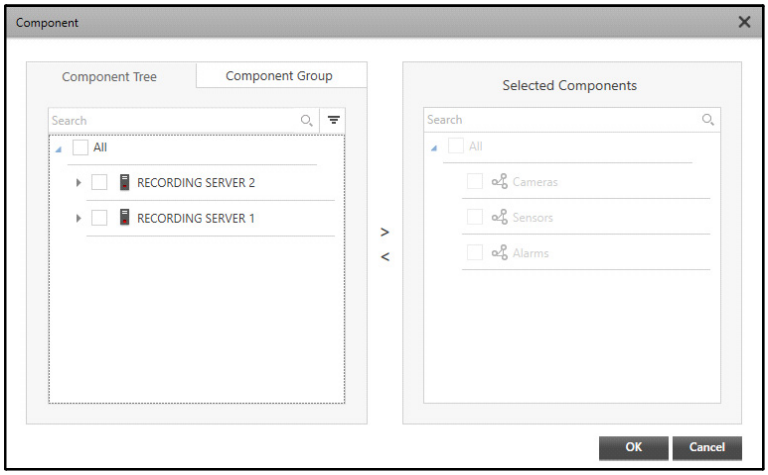
- Click **Add**.

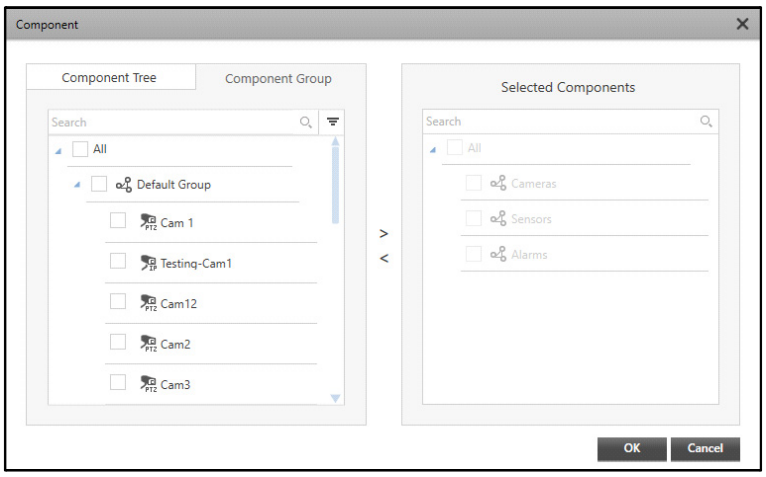


Configure the following parameters:

- **Name**: Specify a suitable Name for the Component Group based on the grouping criteria (for example: Alarm Output Group, Parking Lot Cameras, Server Alarm Group, Security Sensors Group, Cafeteria Group, PTZ Cameras etc.). In Name, you can enter upto 50 characters. Default: Blank.
- **Component**: Select the desired Components which you wish to add to the Component Group using the **Component** picklist.
  - Click **Component** picklist. The **Component** pop-up appears.

The Component details are displayed in two tabs — Component Tree and Component Group.





You can view the components of the Component Groups based on the "Entity Rights"of assigned to your User Group.

Component Groups having only Alarms and/or Sensors will not be visible in the Smart Client.

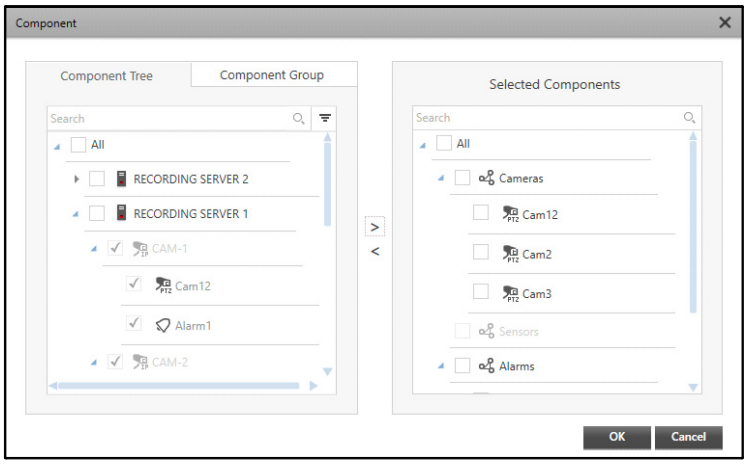
The **Component Tree** tab displays the Recording Servers along with the components — Cameras, Alarms and Sensors. Whereas, the **Component Group** tab displays the Groups with list of all the components — Cameras, Alarms and Sensors irrespective of the Recording Server they belong to.

- Select the check boxes of the desired components you wish to add from the Component Tree or Component Group tabs. Click the right arrow button to add those components in the **Selected Components** list.

  You can search for the desired components using the search bar.

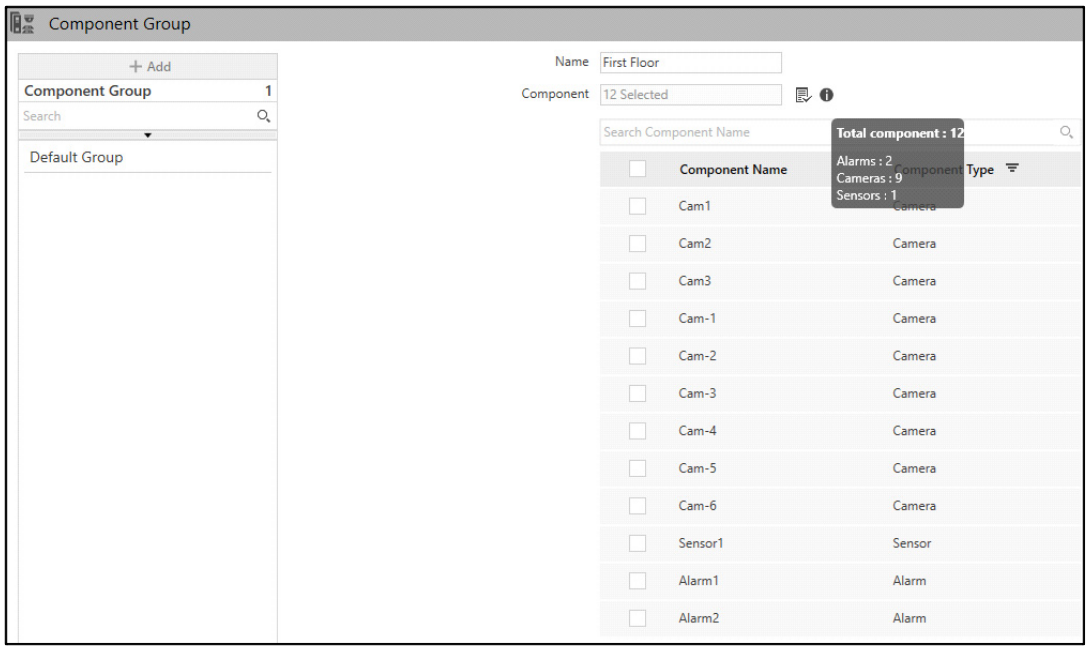
  You can also apply filters to the components by clicking on **Filter** .

  To remove the components, select the check boxes of the desired components you wish to remove from the Selected Components list. Click the left arrow button to remove the components from the Selected Components list.



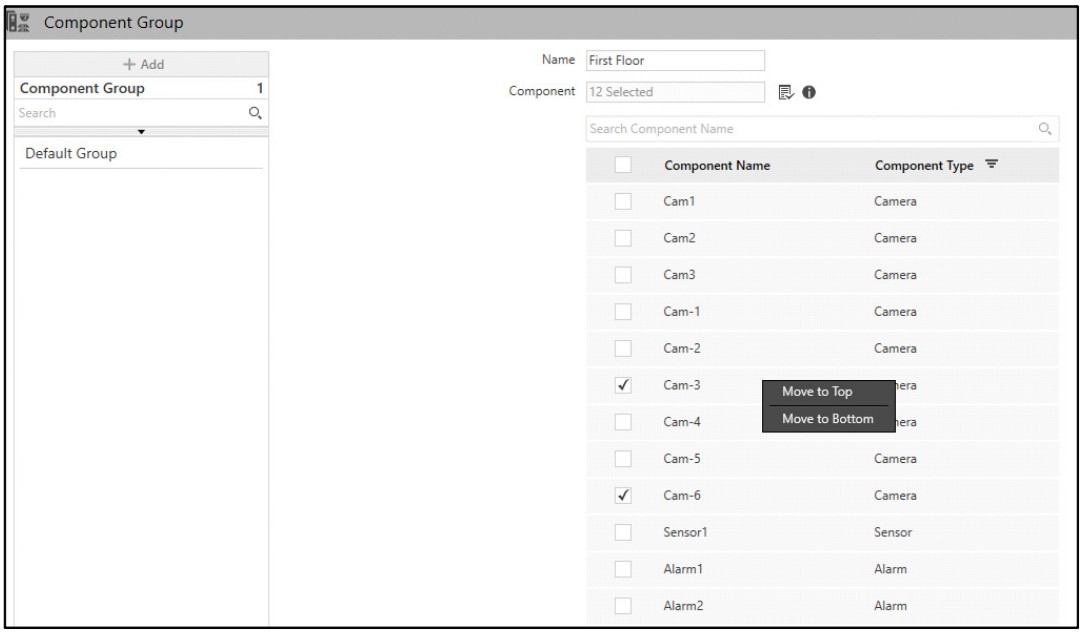
In the Selected Components list, the selected components appear in three distinct Groups by default — Cameras, Sensors and Alarms. All the cameras you select appear under the **Cameras** group. All the sensors and alarms appear under the **Sensors** and **Alarms** groups respectively.

- Click **OK** to confirm or click **Cancel** to discard.
- You can hover the cursor over the Component **Info** icon to view the Component Group details.



You can change the order of the components by moving them to the top or bottom of the list.

- Select the check boxes of the components that you wish to move. You can also search for the desired components using the **Search Component Name** search bar. Right-click on the list. The following options appear — **Move to Top** and **Move to Bottom**.



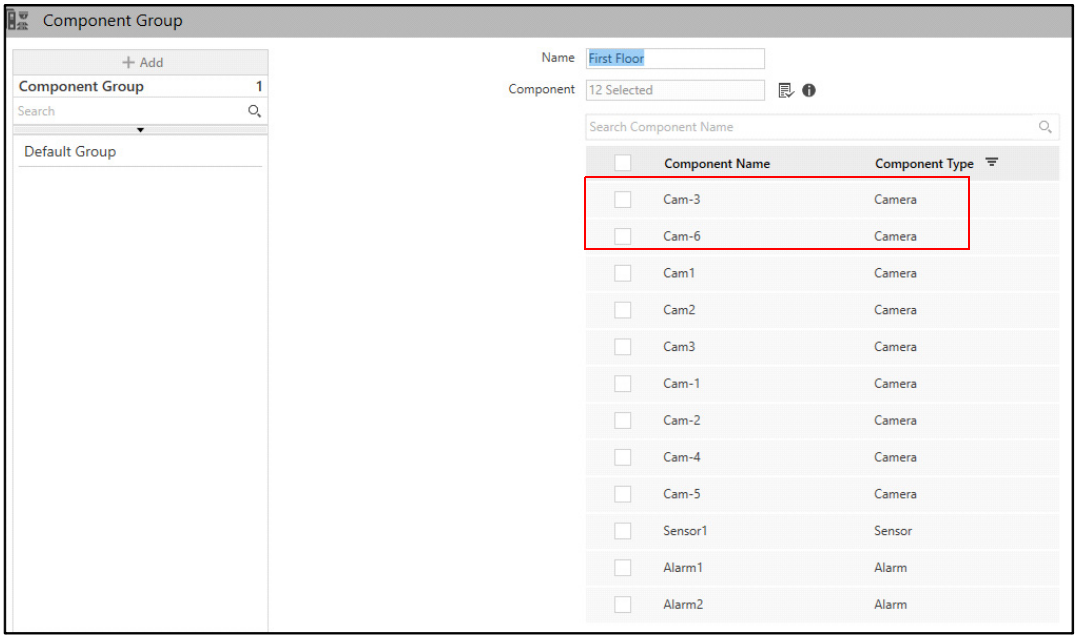
- Select **Move to Top** to move the selected components on the top of the list. Similarly, select **Move to Bottom** to move the components to the bottom of the list. The components are arranged in the order as they appear in the list when either moved to top/bottom.

  OR

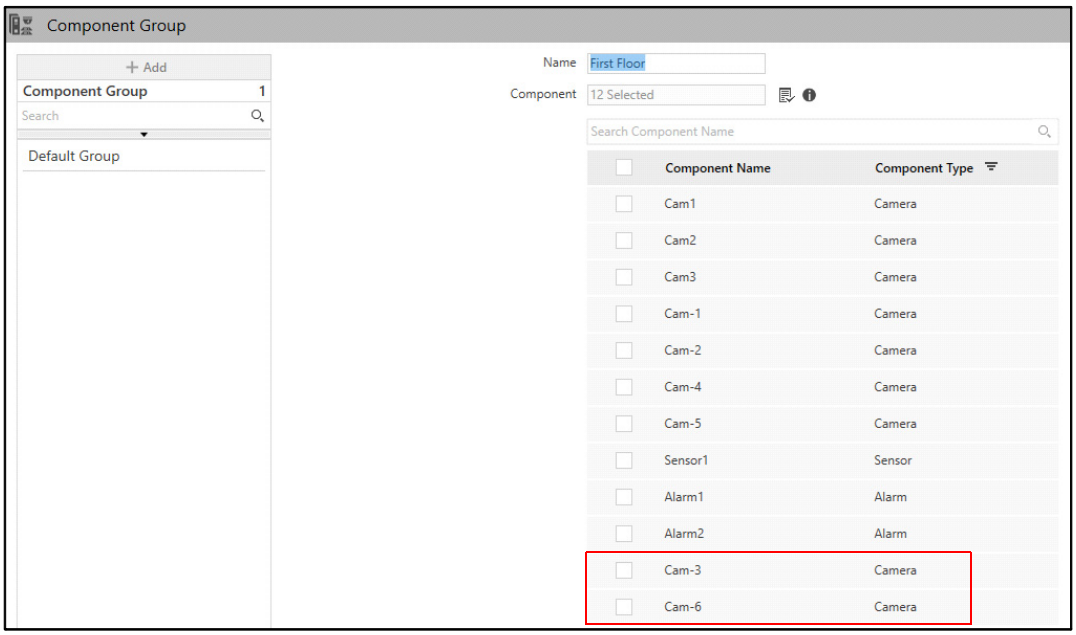
  You can also drag and drop the selected components across the list to move them to the desired position on the list. To do so, select the desired components and drag them to the desired position and then drop them there in the list. If the selected components are dropped over an existing component, then they will be added above that component.

  For example,

  If two components Cam-3 and Cam-6 are moved to the top, they are arranged in the order as they appear in the list at the top of the list.

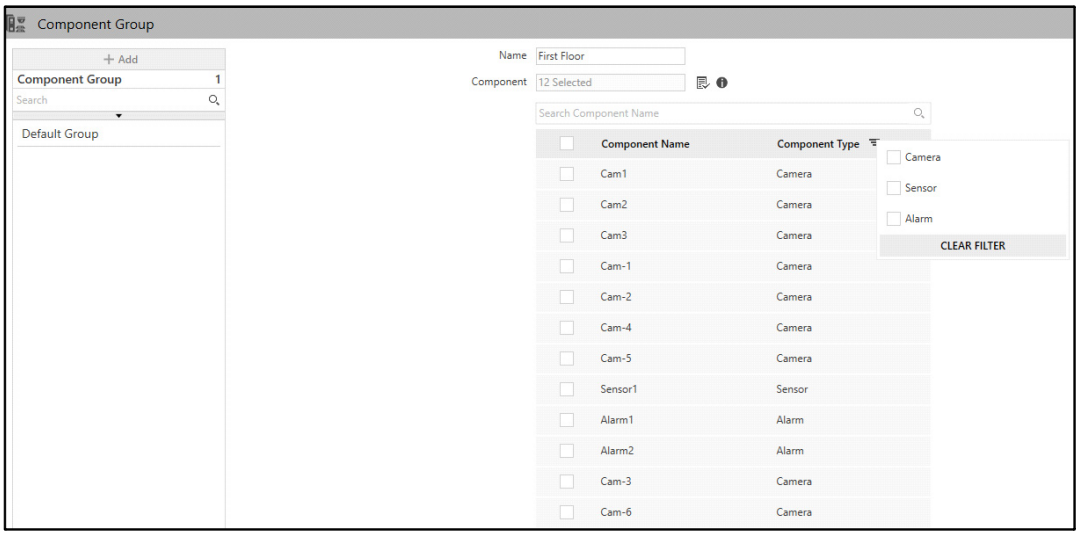


If the same components are moved to the bottom, they are arranged in the order as they appear in the list at the bottom of the list.



You can also filter the components as per your requirement. To do so,

- Click **Filter** to apply filters to the components. The filter options are— Camera, Sensor and Alarm.
- Select the desired option to filter the components.

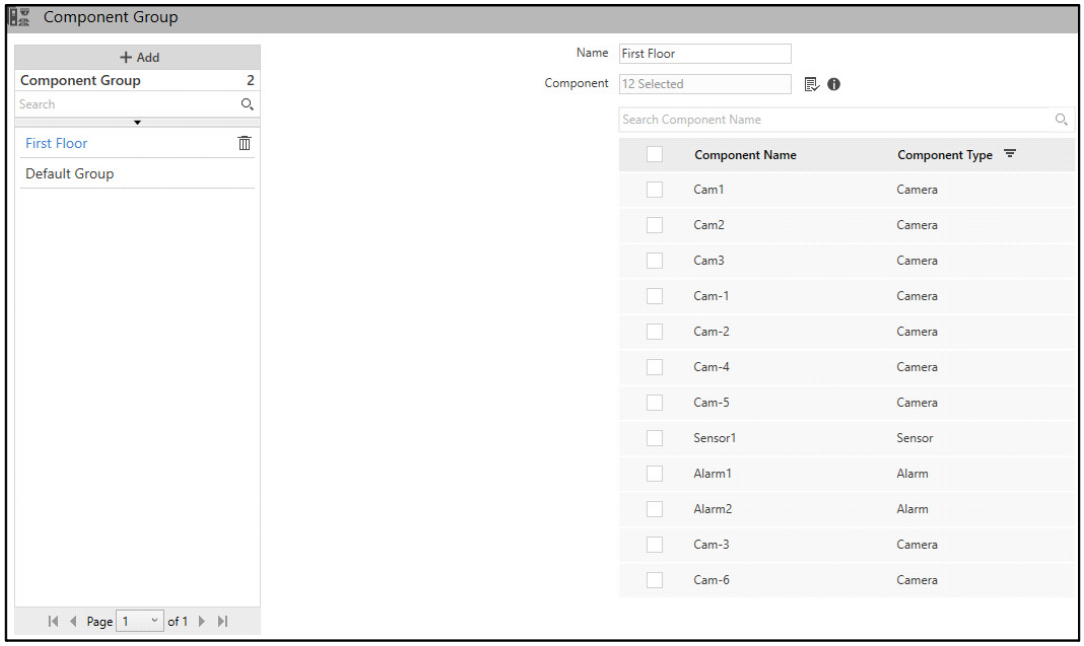


- Click **CLEAR FILTER** to clear the set filter.

- Click **Save** to save the configurations of the new Component Group.

The new Component Group will appear on the left hand side.

You can view, edit or delete these Component Groups.



- **Edit**: Click the desired Component Group from the left hand side list. The details appear on the right. You can edit these as per your requirement.

- **Delete**: Click **Delete** corresponding to the desired Component Group to delete it.

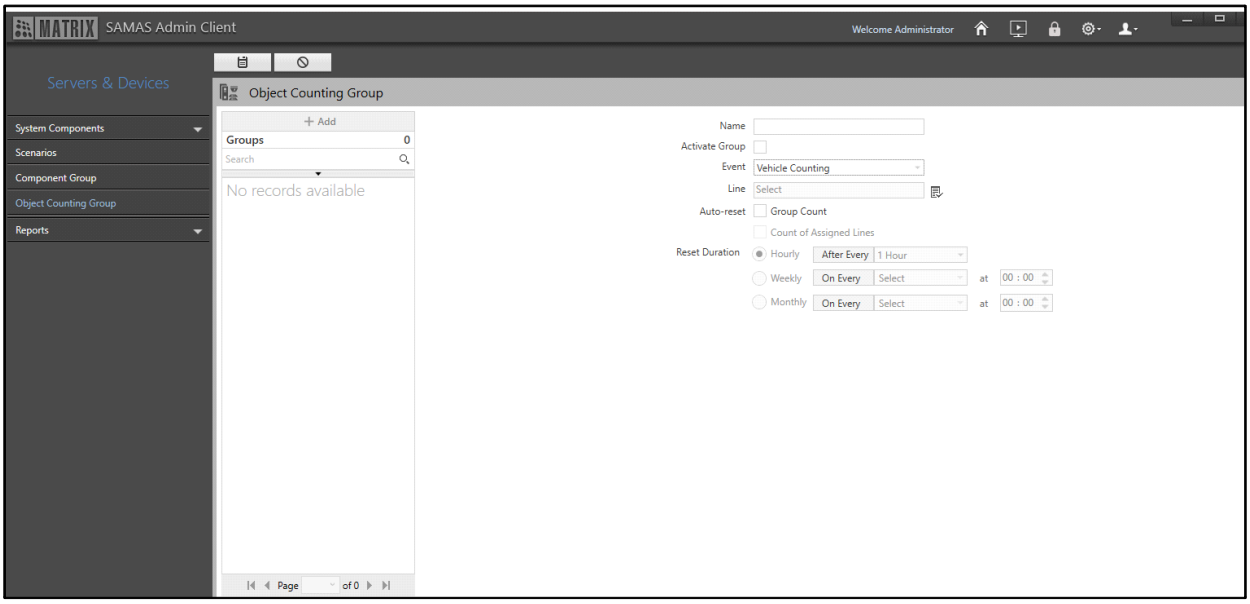
Object Counting Group

Object Counting Groups are the logical groups of lines configured for the Object Counting Events such as People Counting and Vehicle Counting. This feature is useful in a situation where an organization has different entry and exit gates and the user needs a cumulative sum of all these entry and exit points. This helps the user to get a clear view of the number of objects entering and exiting the premise. An object can either be a vehicle or a person.

The Object Counting Group page displays all the configured Object Counting Groups. You can view and configure Object Counting Groups for People Counting or Vehicle Counting.

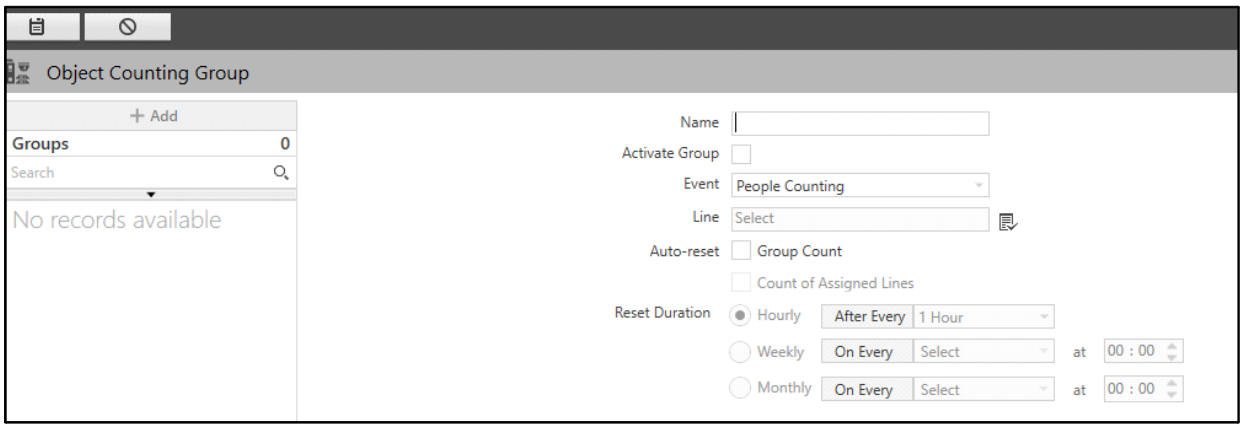
To configure Object Counting Group,

- Click **Servers & Devices > Object Counting Group**.



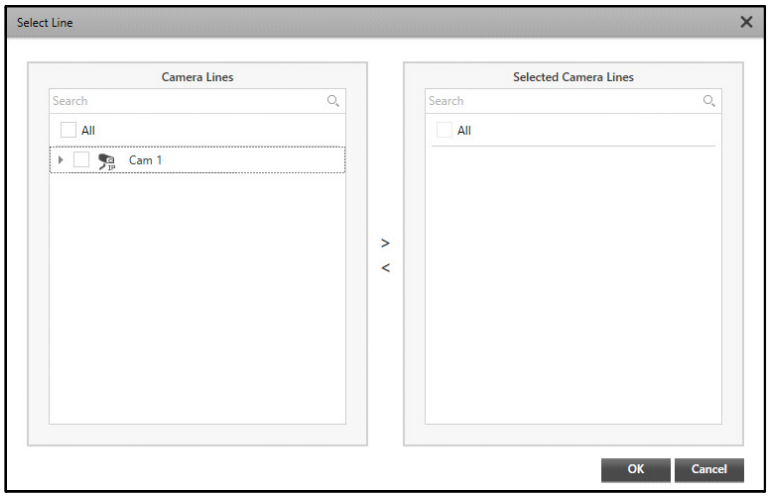
*The **Add** button is disabled when you are configuring Object Counting Group for the first time. You can directly configure the parameters and save the Object Counting Group.*

- Click **Add**.

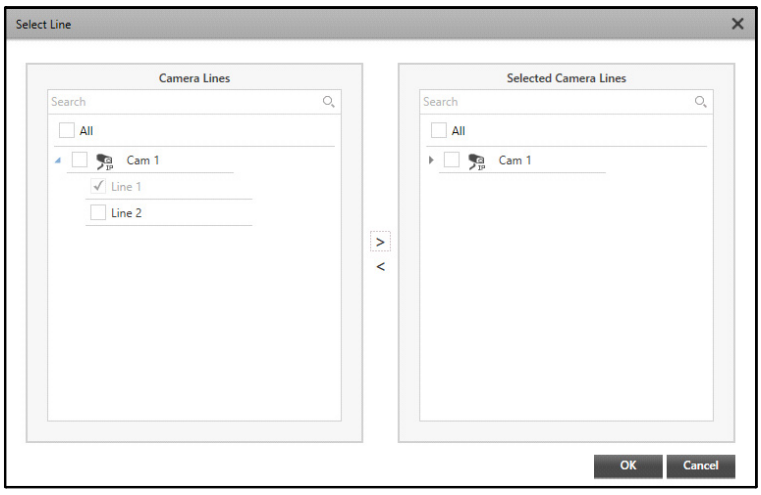


Configure the following parameters:

- **Name:** Specify a suitable name for the Object Counting Group. For example, Entry Group. In Name, you can enter upto 50 characters. Default: Blank.
- **Activate Group:** Select the check box to activate the group. If enabled, the Event will be generated and sent to the Smart Client. If disabled, Events will not be generated for the group.
- **Event:** Select the desired Event — Vehicle Counting or People Counting. Vehicle Counting will give the group count of the vehicles while People Counting will give the group count of the people.
- **Line:** Select the Lines to be included in the group using the **Lines** picklist. The Lines depend on the Event selected. The lines displayed in the picklist are configured in the **Event** tab of the respective Camera. For more details, refer to “Object Counting”.
  - Click **Lines** picklist. The **Select Line** pop-up appears.



  - Select the check boxes of the desired Lines you wish to add from the **Camera Lines** list. Click the right arrow button to add these Lines in the **Selected Camera Lines** list. You can search for the desired Lines using the search bar.



To remove the Lines, select the check boxes of the desired Lines you wish to remove from the Selected Camera Lines list. Click the left arrow button to remove the Lines from the Selected Camera Lines list.

- Click **OK** to confirm or click **Cancel** to discard.

Auto-reset

- **Group Count**: Select the check box to automatically reset the group count of the Vehicle Counting or People Counting Events.

- **Count of Assigned Lines**: Select the check box to automatically reset the count of the Lines assigned to the group. If the same Lines are assigned to other groups, the Line counts will be reset for the other groups as well.



If Auto-reset check box is not enabled, then the counter will never reset. In this case, reset can be done either manually or by the Management Server when the counter reaches its limit, that is, till 999999999 for the selected group.

- **Reset Duration**: Select the desired Reset Duration — Hourly, Weekly or Monthly to Auto-reset the group or line counter.

  - **Hourly:** Select this option to Auto-reset the group or line counter hourly. Select the desired interval from the drop-down list. The group or line counter will be Auto-reset hourly as per the selected interval.

    For example, if you select **1 Hour**, from the drop-down list, then group/line counter will be reset after every 1 Hour.

  - **Weekly:** Select this option to Auto-reset the group or line counter on a particular day of the week and at the set time. You can select multiple days of week. Select the desired day from the drop-down list. Specify the desired time.

    For example, if you select **Monday** and **Wednesday** from the drop-down list and set the time as 18:00, the group or line counter will be reset on every Monday and Wednesday of the week at 6 PM.

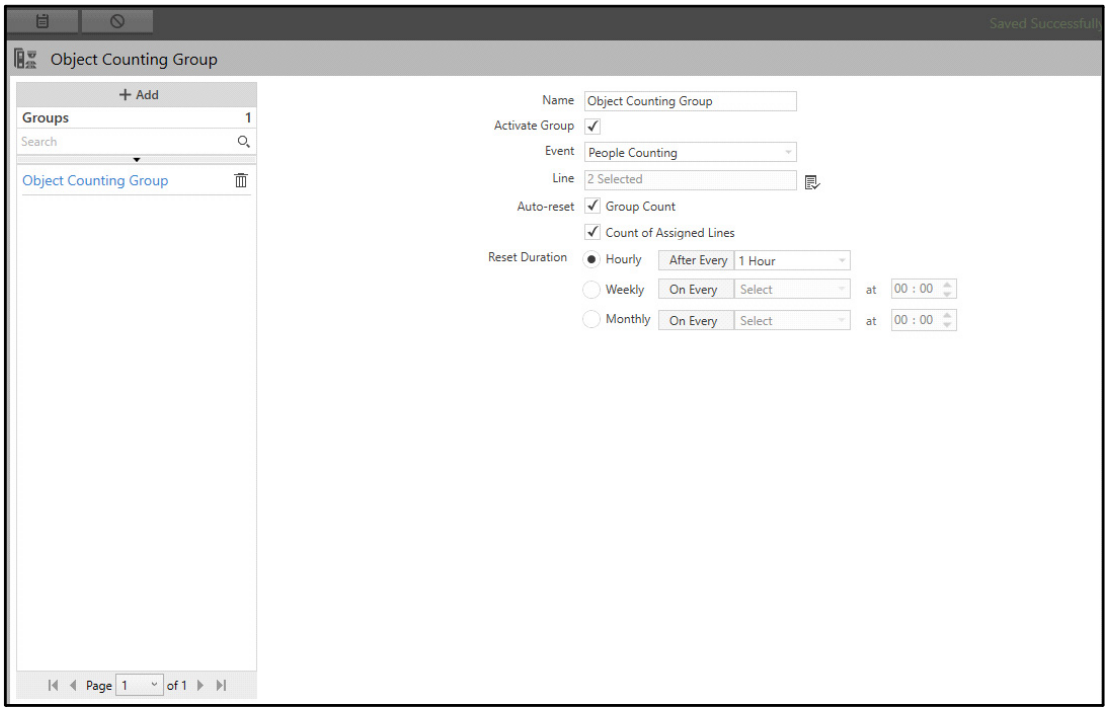
  - **Monthly:** Select this option to Auto-reset the group or line counter on a particular date of the month and at the set time. You can select multiple dates of the month. Select the desired date from the drop-down list. Specify the desired time.

    For example, if you select 1st and 25th date from the drop-down list and set the time as 18:00, the group or line counter will be reset on every 1st and 25th date of the month at 6 PM.

- Click **Save**  to save the settings or **Cancel**  to discard.

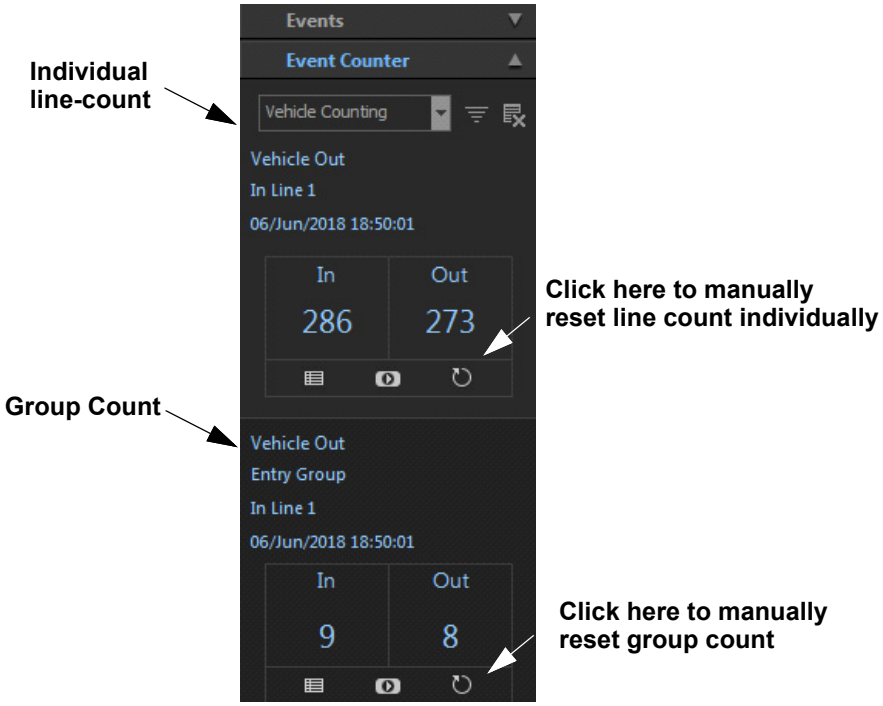
The Object Counting Group appears in the list on the left hand side.

You can change the configurations of the Object Counting Group or delete it.



- To edit, select the desired Object Counting Group from the list on the left hand side. The details appear on the right hand side. Edit the configurations as per your requirement.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** against the desired group to delete the Object Counting Group.

When any Event such as People Counting or Vehicle Counting occurs, the Object Counting Group is displayed in the Smart Client in the Event Counter Panel.



Servers and Devices - Reports

Vehicle Counting Report

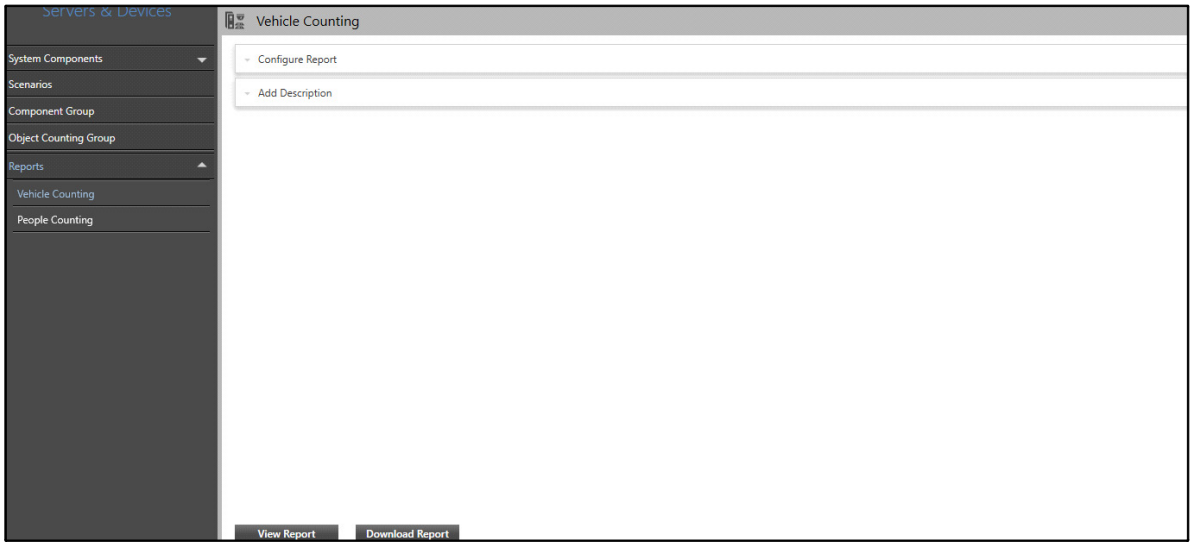
Vehicle Counting Report provides tabular as well as graphical statistics on vehicle congestion. These statistics can be useful in managing the traffic at various locations by sitting at one place. It allows the user to track the number of vehicles passing by within the defined duration at any place. The report includes the count of vehicles detected at camera across multiple entries/exits.

For example, consider a shop having various outlets at different locations. Based on this report, the user can track the number of vehicles entering and exiting the various outlets by sitting at one place. If traffic increases at a particular outlet, it can be managed by taking the appropriate action.

The Vehicle Counting Report page enables you to configure parameters for Vehicle Counting Reports. You can view and configure Vehicle Counting Reports on Yearly, Monthly, Weekly, Daily, Hourly and Peak Hour basis.

To configure Vehicle Counting Report parameters,

- Click **Servers & Devices > Reports > Vehicle Counting**.



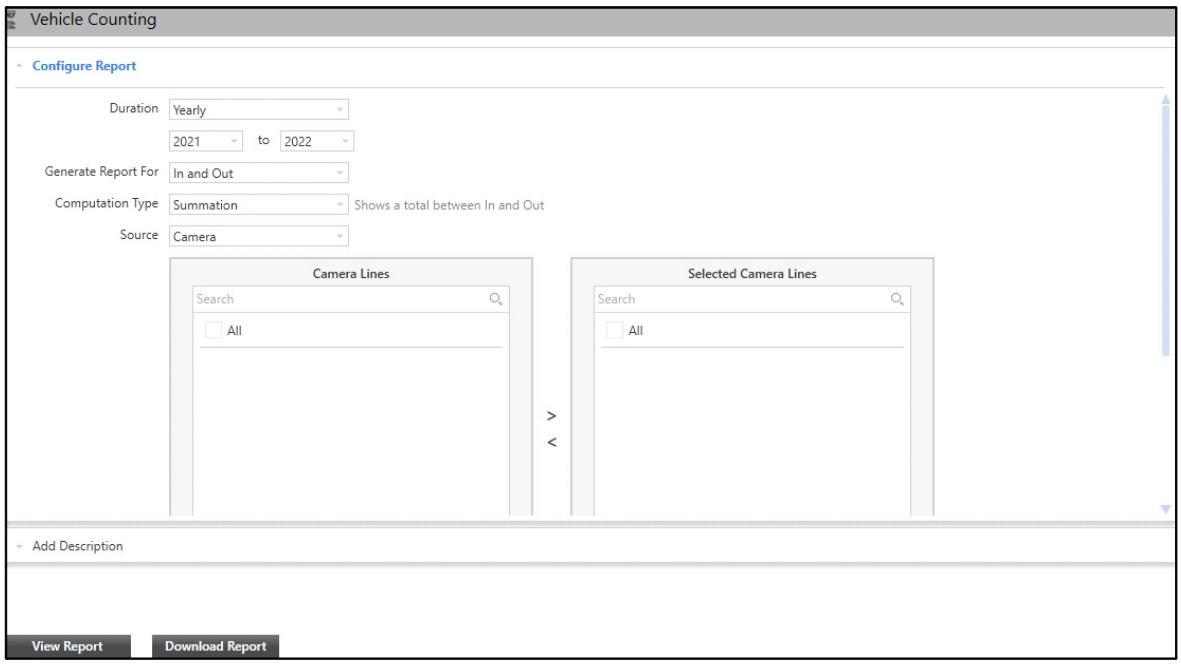
The Vehicle Counting page contains two collapsible panels — “Configure Report” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Vehicle Counting Report from this collapsible panel.

To configure the report parameters,

- Click the **Configure Report** collapsible panel.



- **Duration**: Select the Duration from the drop-down list — Yearly, Monthly, Daily, Hourly, Weekly and Peak Hour Reports.
    - **Yearly**: Select this option to generate yearly reports. Select the desired From and To year from the drop-down lists.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
    - **Weekly**: Select this option to generate weekly reports. Select the desired From and To dates from the calendar. Select the day of the week from when you wish the weekly report to begin in **Start Week From** drop-down list.
    - **Peak Hour**: Select this option to generate reports for the peak hours. Select the period for which you wish to generate the report from the **Period** drop-down list. Select the desired option year, month or daily and configure their respective parameters. In **Peak Period,** set the desired duration.
- **Generate Report For**: Select the parameter for which you wish to generate the report from the drop-down list — In, Out and In and Out.
    - If you select **In**, the report will include only **In** counts of the vehicles from various locations.
    - If you select **Out**, the report will include only **Out** counts of the vehicles from various locations.
    - If you select **In and Out,** the report will include both **In** and **Out** counts of the vehicles from various locations.

- **Computation Type**: Select the type of computation for the report from the drop-down list — Summation, Differentiation and Maximum Count. The data will be processed according to the selected computation type option.

    - **Summation**: This report will give you the total counts between In and Out for the selected Camera Lines or Group.

    - **Differentiation**: This report will give you difference between In and Out count for the selected Camera Lines or Group.

    - **Maximum Count**: This report will give the maximum count In or Out count for the selected Camera Lines or Group.

- **Source**: Select the source from the drop-down list — Camera Lines or Groups.



    - Select the check boxes of the desired Camera Lines or Groups you wish to select for the report from the **Camera Lines** or **Groups** list. Click the right arrow button to add these Camera Lines or Groups in the **Selected Camera Lines** or **Selected Groups** list. You can also search for the desired Camera Lines or Groups using the search bar.

      To remove Camera Lines or Groups, select the check boxes of the desired Camera Lines or Groups you wish to remove from the Selected Camera Lines or Selected Groups list. Click the left arrow button to remove the Camera Lines or Groups from the list.



- **Representation Format**: Select the format in which you wish the report to be generated from the drop-down list — Tabular, Graphical.

- **Graph Type**: If you have selected **Graph** as the **Representation Format**, select the Graph Type from the drop-down list — Column, Bar, Line.

- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.

- **Language**: Select the Language in which you wish to generate the report from the drop-down list.

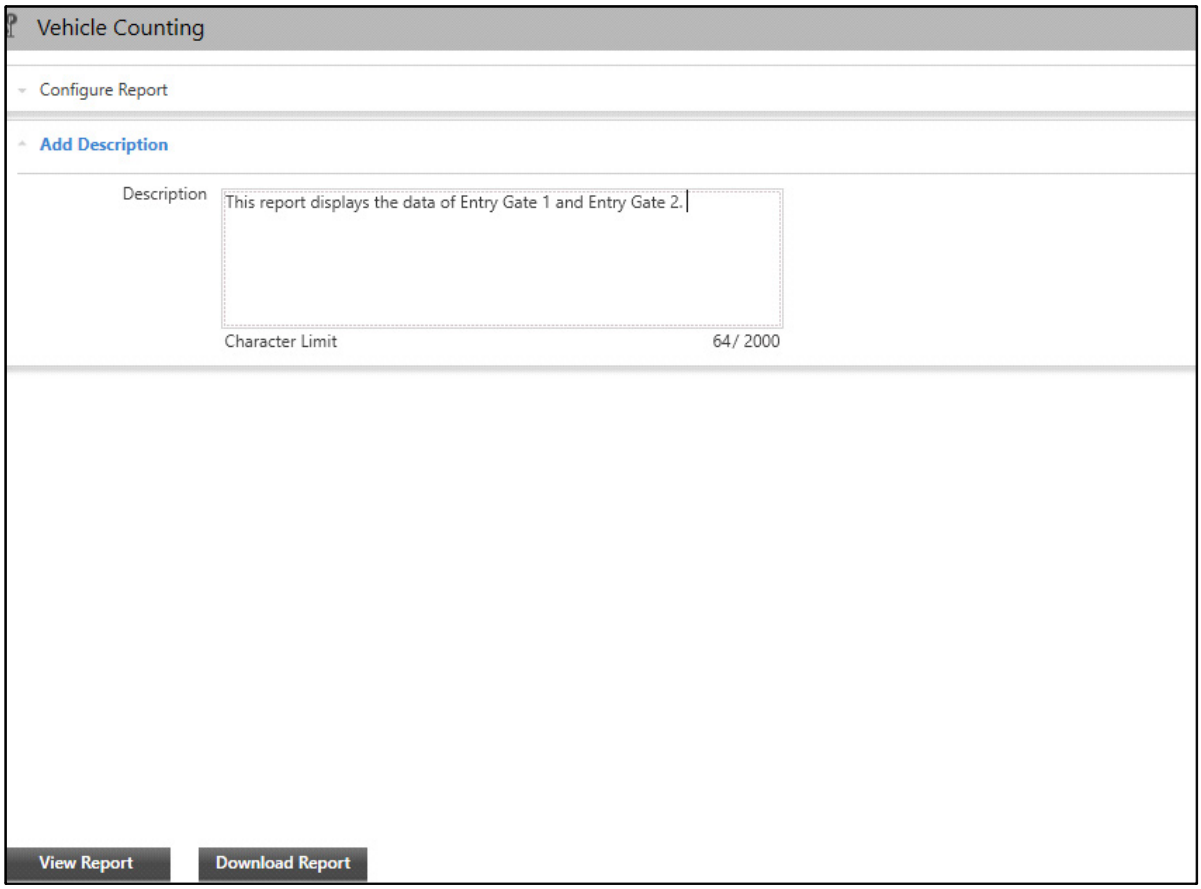
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Description

This panel allows you to add a description for the Vehicle Report once the report configurations are done. This description is visible in the generated report.

To add the description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. The Description can be of upto 2000 characters only and it is displayed on the second page of the report.

Once the report configurations are done and the description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

People Counting Report

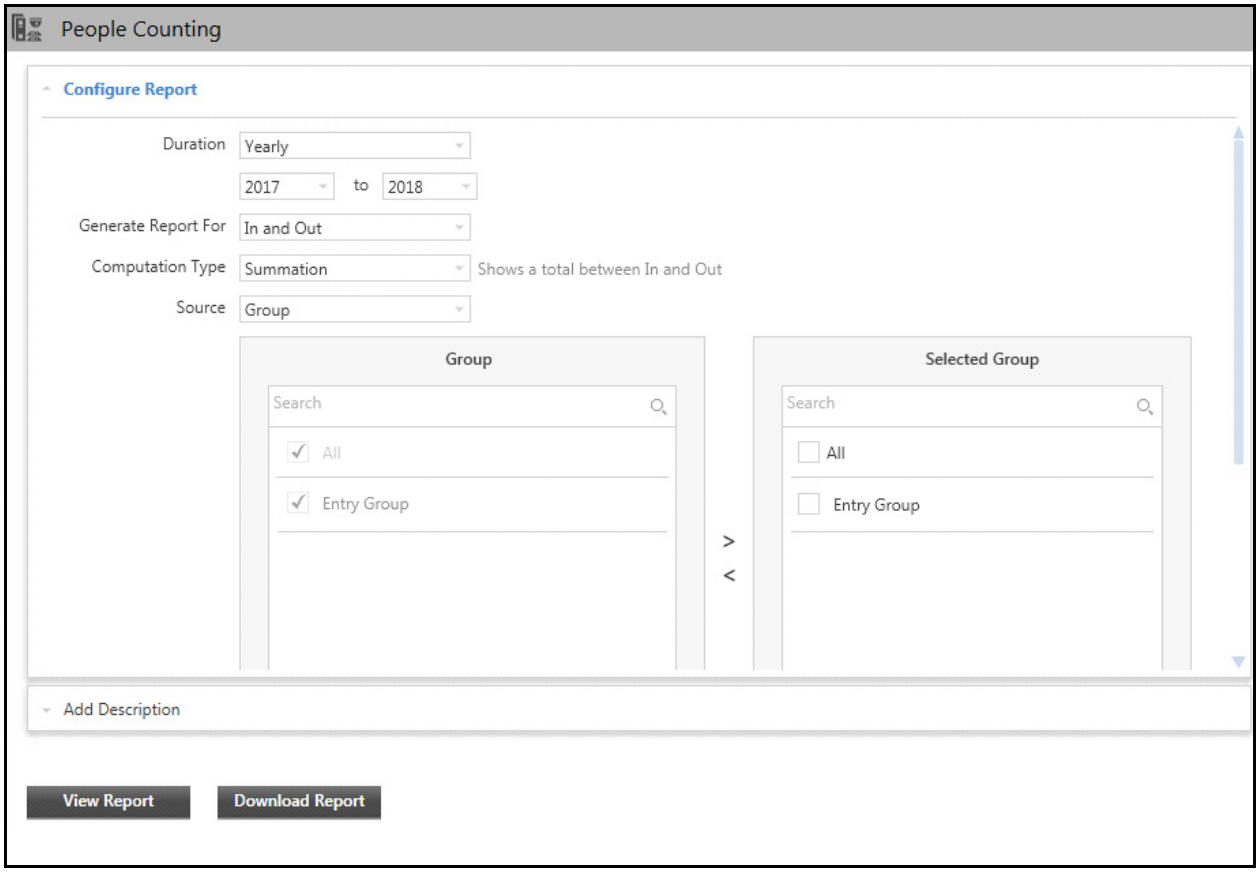
People Counting Report provides tabular as well as graphical statistics on crowd behavior. These statistics can be useful in managing the crowd at various locations from one place. It allows the user to track the number of people passing by within the defined duration at any place. The report includes the count of people across multiple entries/ exits.

For example, consider a shop having various outlets at different locations. Based on this report, the user can track the number of people entering and exiting various outlets by sitting at a place. If the crowd increases at a particular outlet, it can be managed by taking the appropriate action.

The People Counting Report page enables you to configure parameters for People Counting Reports. You can view and configure People Counting Reports on Yearly, Monthly, Weekly, Daily, Hourly and Peak Hour basis.

To configure People Counting Report parameters,

- Click **Servers & Devices > Reports > People Counting**.



Configurations of People Counting Report are similar to that of the Vehicle Counting Report. For more details, refer to “Vehicle Counting Report”.

CHAPTER 6

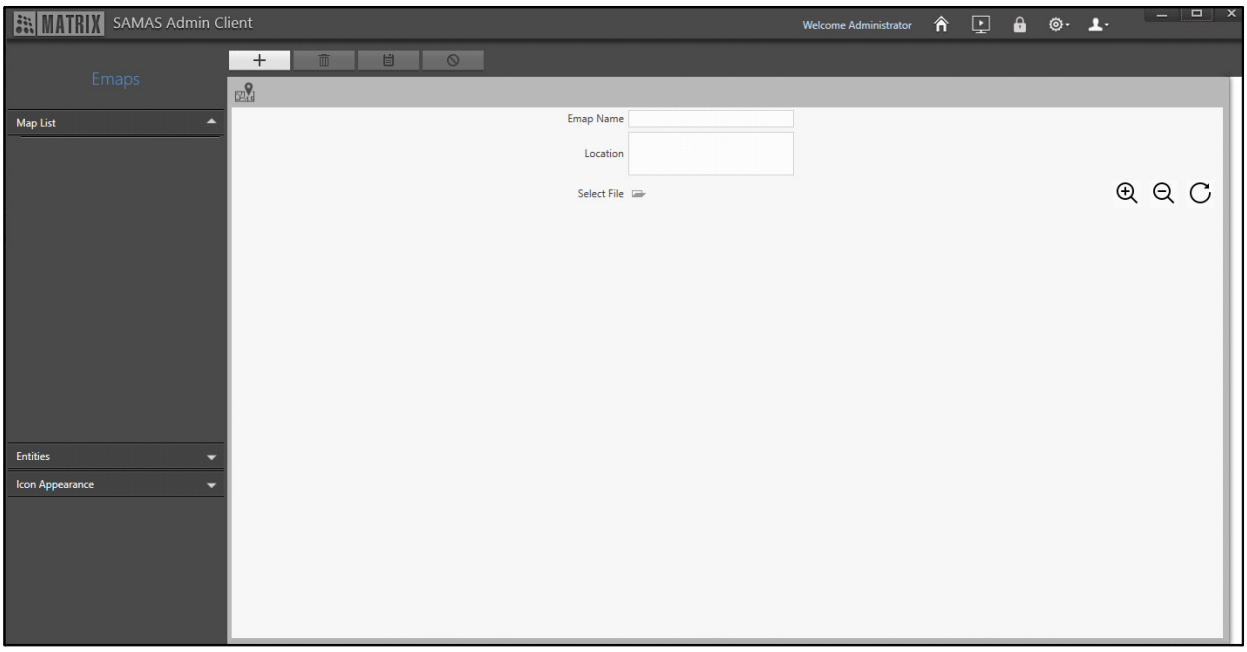
Emaps

The Emaps module enables you to indicate the location of various devices in your premises using an Electronic Map. This functionality is used to define Electronic Maps in.jpg,.bmp and .pdf formats in the Admin Client. Such Emaps can be used for indicating the location of cameras, sensors and other entities, as positioned for surveillance purposes. You can add alarm spots or camera locations on these maps for live monitoring.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure Emaps,

- Click **Emaps**.



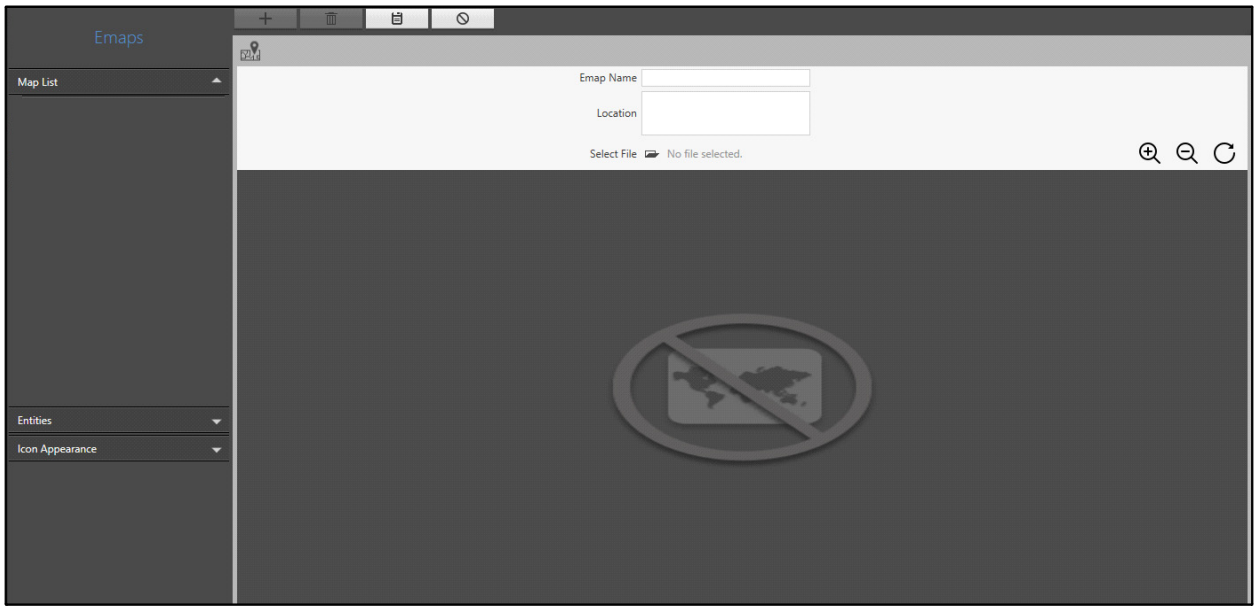
The Emaps module contains these pages — "Map List", "Entities" and "Icon Appearance".

Map List

The Map List page displays all the configured Emaps. You can view, add and configure the Emaps from this page.

To configure Emap,

- Click **Emaps**. The **Map List** page appears by default.
- Click **Add** .



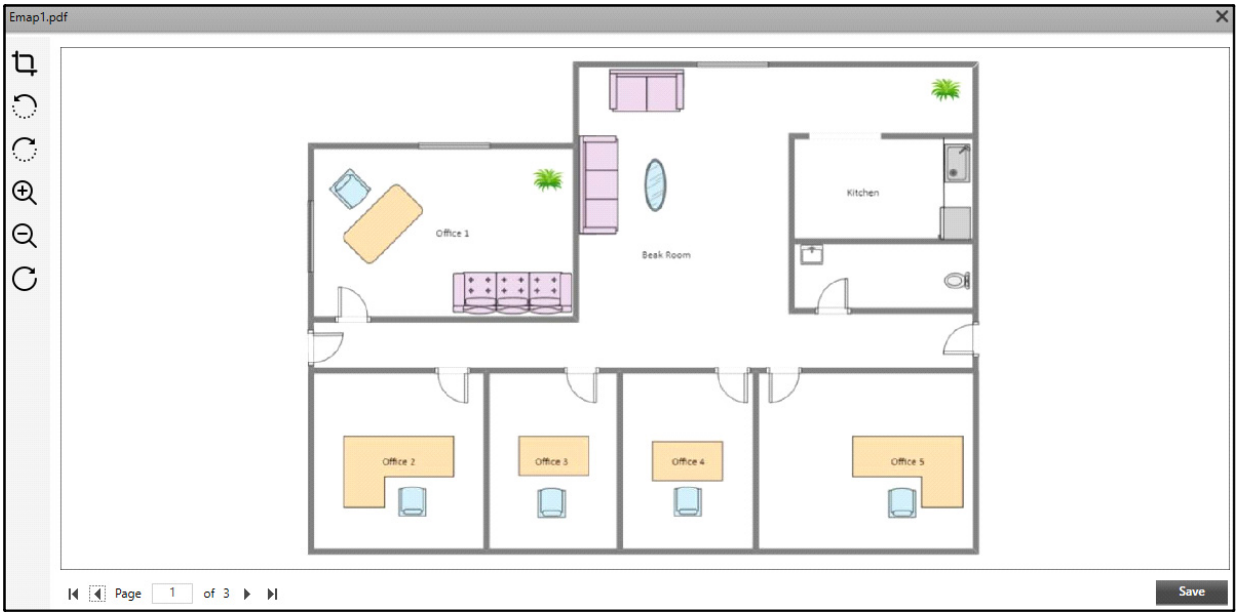
Configure the following parameters:

- **Emap Name**: Specify a suitable name for the Emap. In Emap Name, you can enter upto 50 characters. Default: Blank.
- **Location**: Specify the location of the Emap. In Location, you can enter upto 150 characters. Default: Blank.
- **Select File**: You need to browse the path in the selected drive where you have saved the Emap image or file. Click **Browse** . It displays all folders which are in the drive. Select the desired folder to select the desired file. Supported formats — .jpg .bmp, .pdf. The maximum size of the file can be 50 MB.

Once you upload the file successfully, the **File Name** (For example: Emap) pop-up appears.



If you are uploading a pdf, you can navigate to the desired page by entering the page number in the text box or using the navigation arrows.



The preview in the pop-up will be based on the file format selected. Hence, it can either be the uploaded image or the selected image from the pdf file.

You can drag the image to adjust its position and edit the image using the following functionalities:

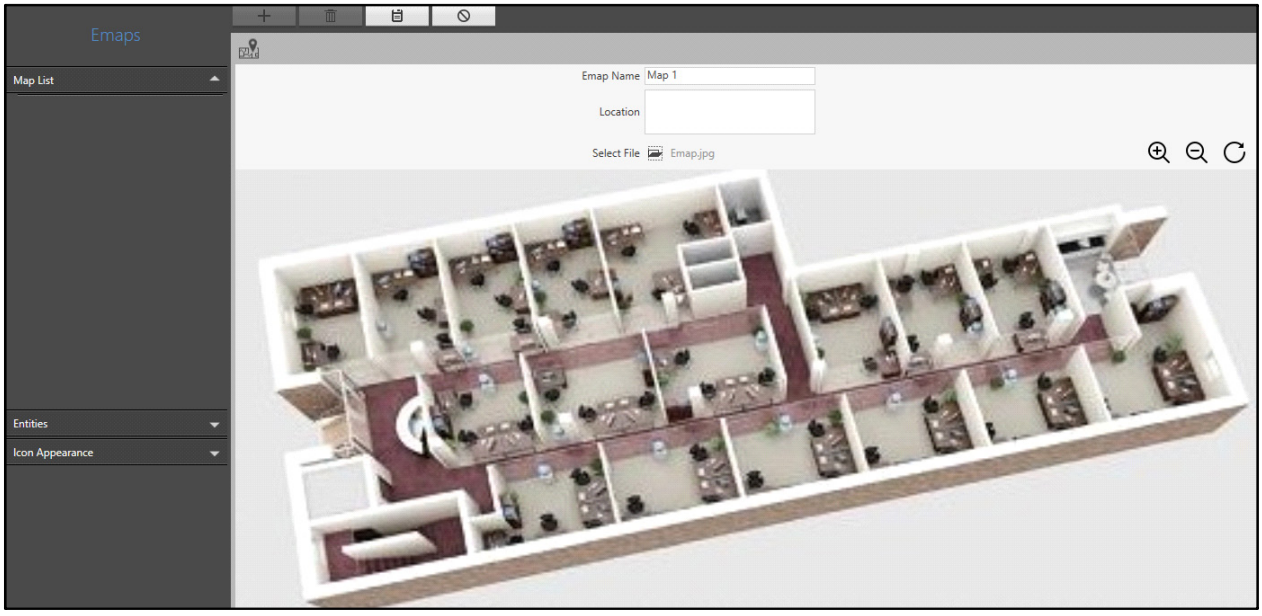
- **Crop**: Click **Crop** and adjust the area to be cropped.



- Click **Save** ✓ to save the selection or click **Cancel** ✕ to discard. Once you click **Save**, this cropped area will be used as the final Emap.

- **Rotate Left**: Click **Rotate Left** to rotate the image to the left.
- **Rotate Right**: Click **Rotate Right** to rotate the image to the right.
- **Zoom In**: Click **Zoom In** to zoom into the image. You can also scroll upwards using the mouse to zoom in.
- **Zoom Out**: Click **Zoom Out** to zoom out of the image. You can also scroll downwards using the mouse to zoom out.
- **Reset Zoom**: Click **Reset Zoom** to set the zoom configurations to default.

- Click **Save** to save the configurations. The Emap will be saved as per the above configurations and the **Emap** pop-up closes. You return to the Emap page.



You can adjust the Emap using the following functionalities:

- **Zoom In**: Click **Zoom In** to zoom into the Emap. You can also scroll upwards using the mouse to zoom in.
- **Zoom Out**: Click **Zoom Out** to zoom out of the Emap. You can also scroll downwards using the mouse to zoom out.
- **Reset Zoom**: Click **Reset Zoom** to set the zoom configurations to default.

Once the Emap configurations are done, you need to place "Entities" before saving the Emap.

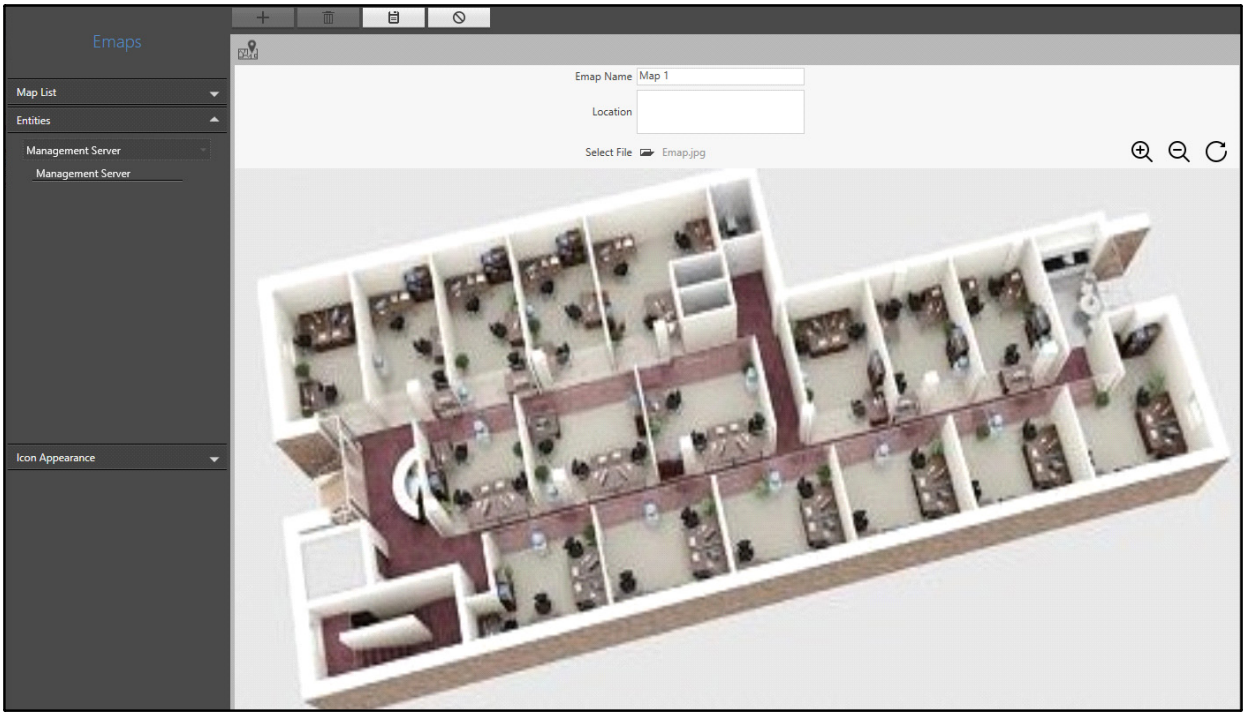
If you wish to change the Emap image to a pdf file or vice versa after placing the entities, you can do so.In this case the entity placement will not be affected. However, the Emap will be changed.

Entities

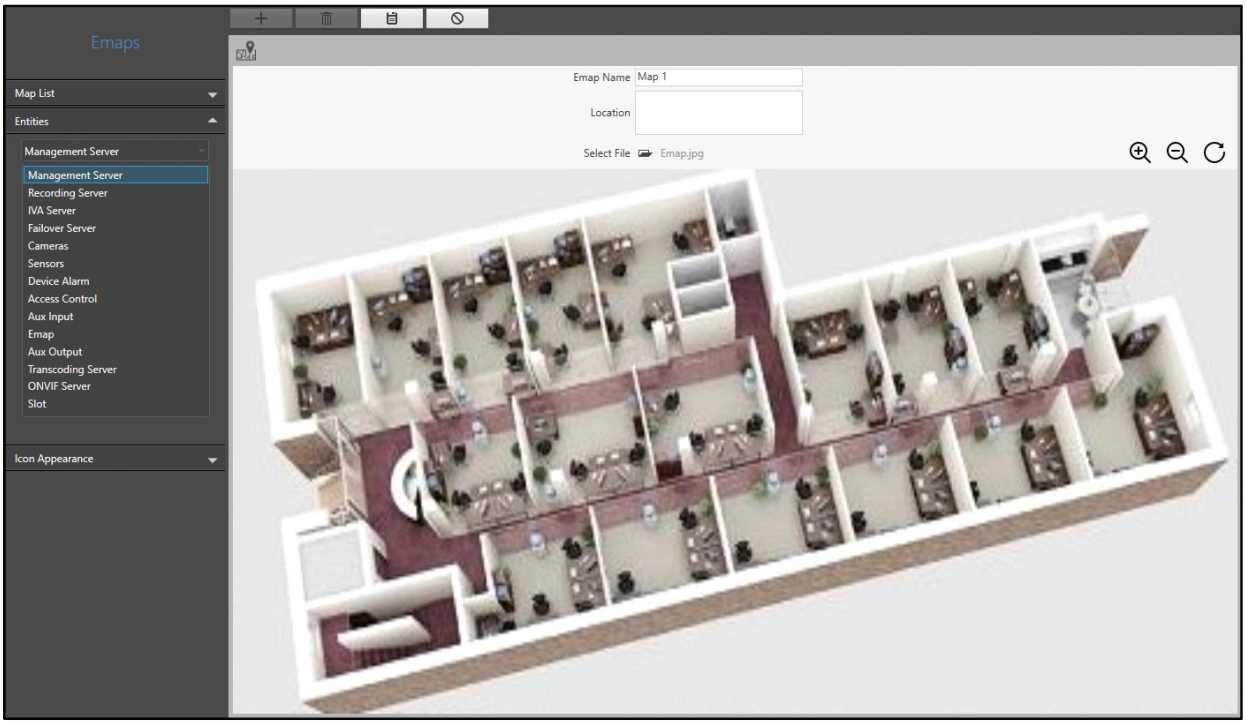
The Entities page displays all the entities on the configured Emaps. You can view and place different Servers, Cameras, Sensors and Alarms on the Emap.

To configure Entities,

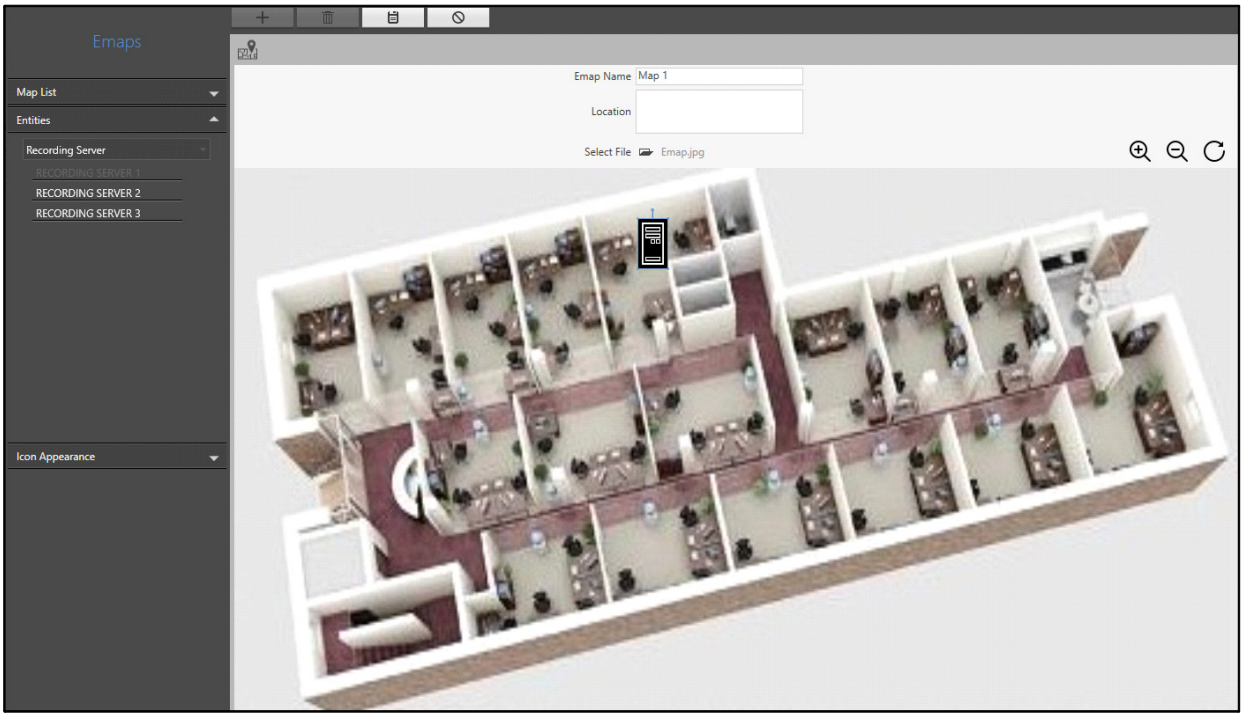
- Click **Emaps > Entities**.



- Select the desired entity from the drop-down list.



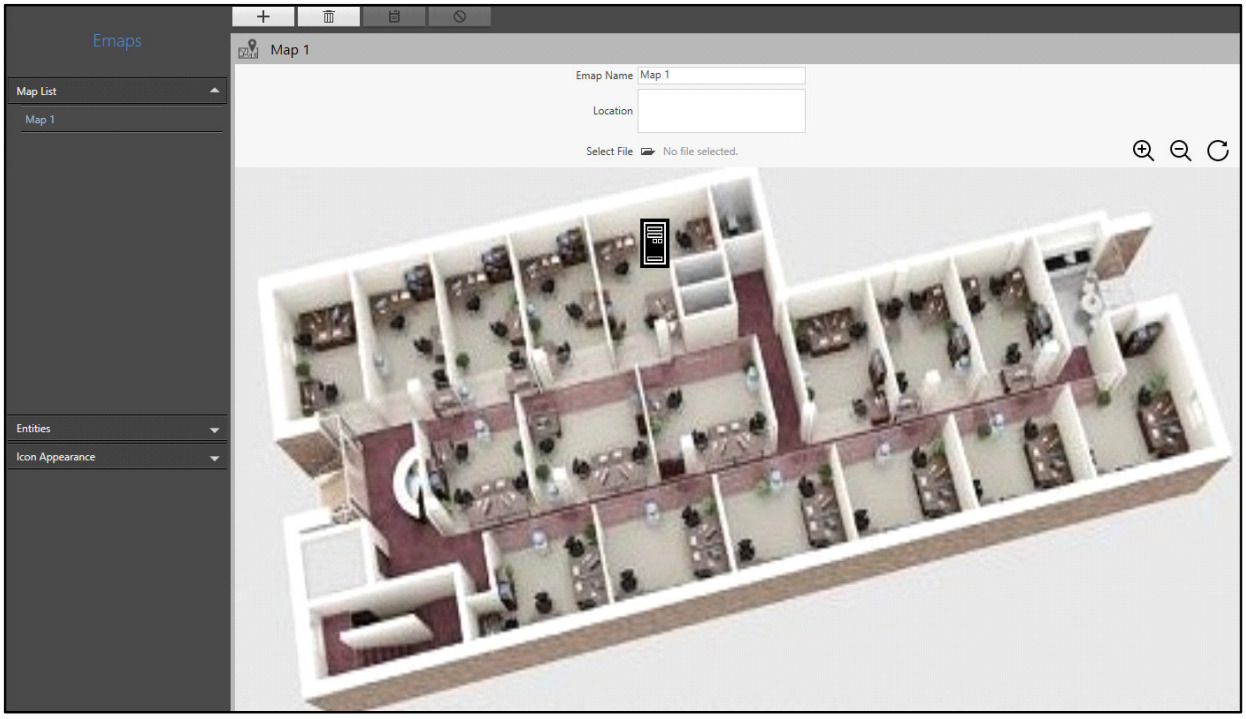
- All the active entities under the selected **Entity** type appear in a list. For example, if you select Recording Server as Entity type, all the active Recording Servers will appear in a list. Select an entity (For example, Recording Server) and drag and place it on the Emap at its appropriate location.



- Click **Save** to save the settings or **Cancel** to discard.

The new Emap appears in the **Map List**.

You can change the configurations of the saved Emaps or delete them.



- To edit, select the desired Emap from the list and edit the details on the right hand side.

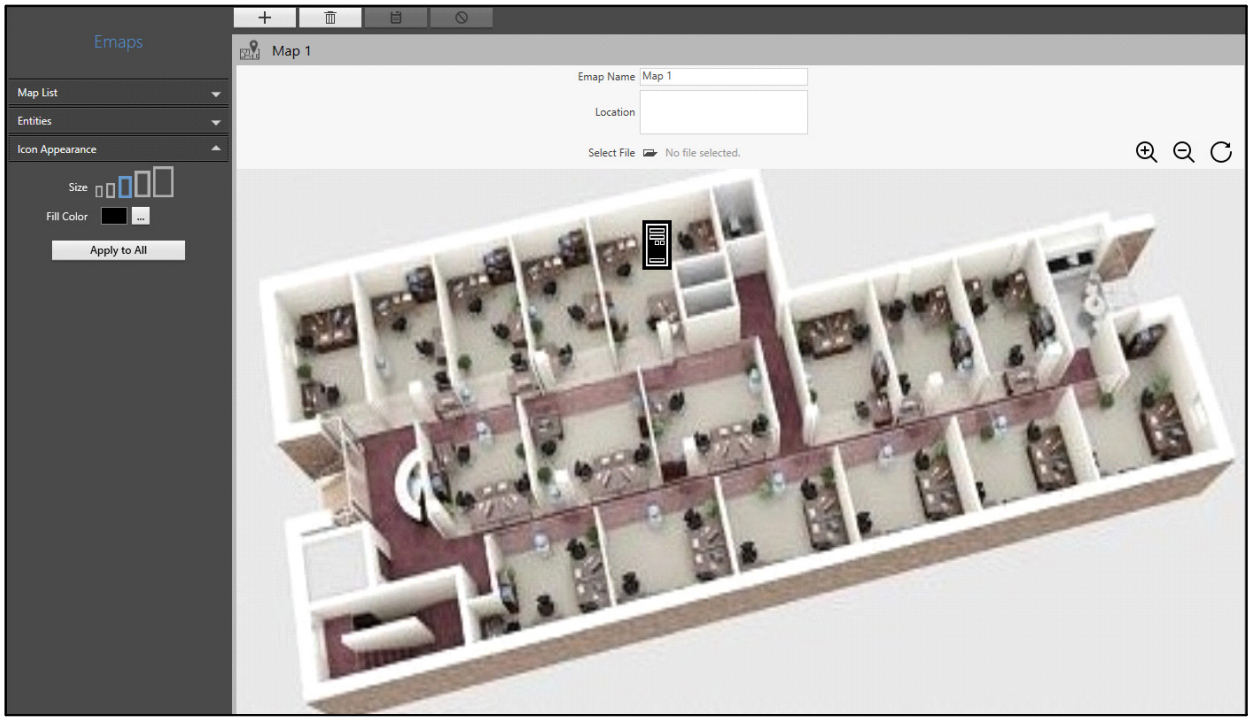
- Click **Save** to save the settings or **Cancel** to discard.
- To delete, select the desired Emap from the list and click **Delete** .

Icon Appearance

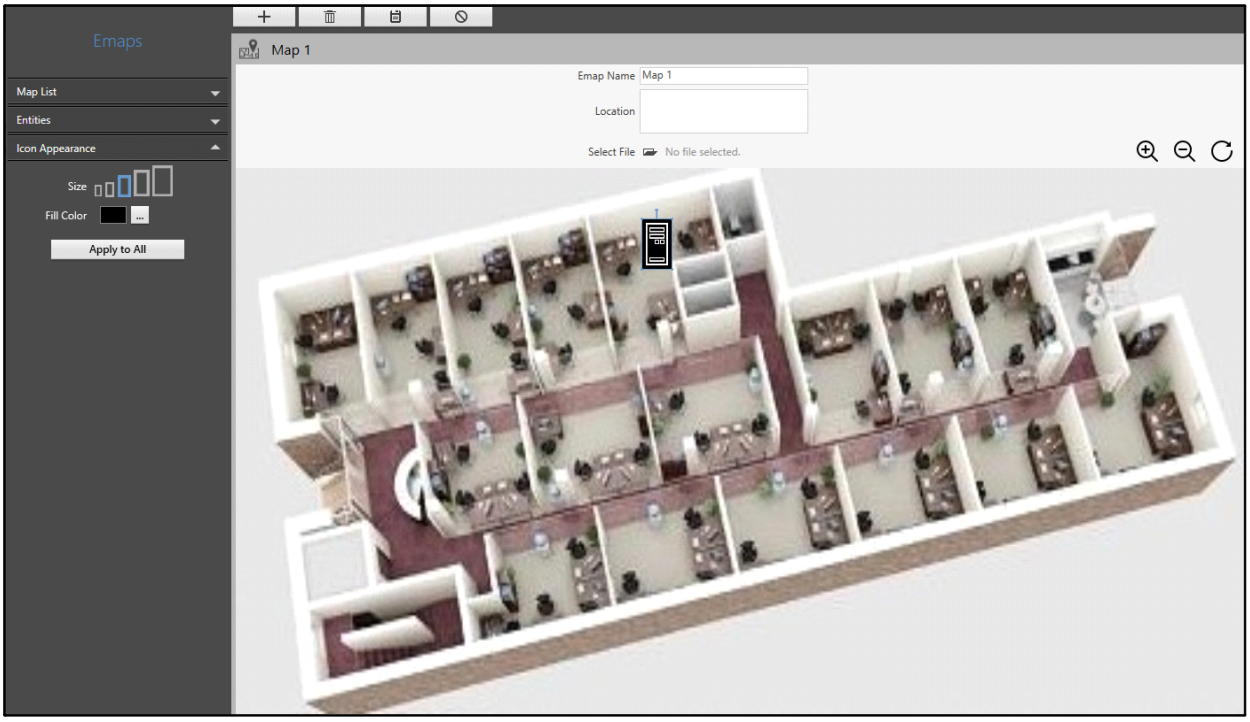
The Icon Appearance page allows you to change the appearance of the entities placed on the Emap. You can view and configure the size and color of entity icons.

To configure Icon Appearance.

- Click **Emaps > Icon Appearance**.



- Select the desired entity icon on the Emap.



Configure the following parameters:

- **Size**: Select the size of the entity icon from the options — Extra Small, Small, Medium, Large and Extra Large. Default: Medium.
- **Fill Color**: Click on ... to select the color of the selected entity icon. The **Color** pop-up appears. Default: Black.

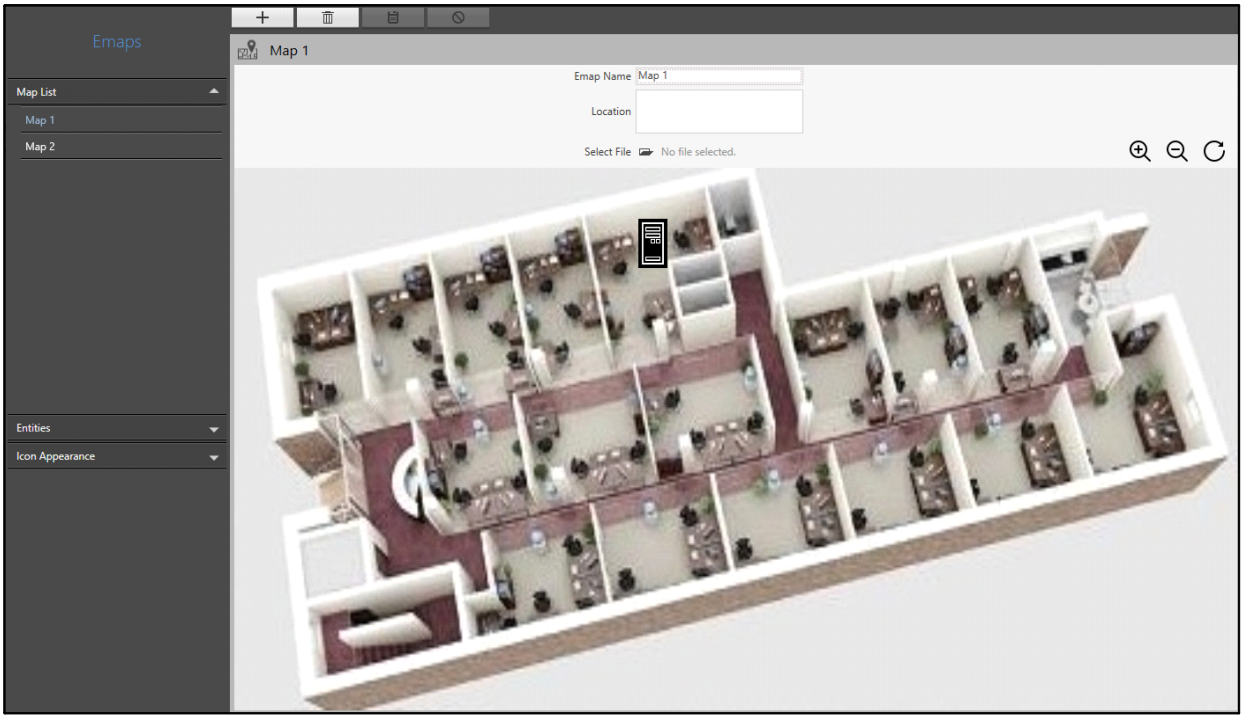


  - Select the desired color.
  - Click **OK** to confirm or click **Cancel** to discard.
- Click **Apply to All** if you wish to apply these settings to all the entity icons.

- Click **Save** to save the settings or **Cancel** to discard.

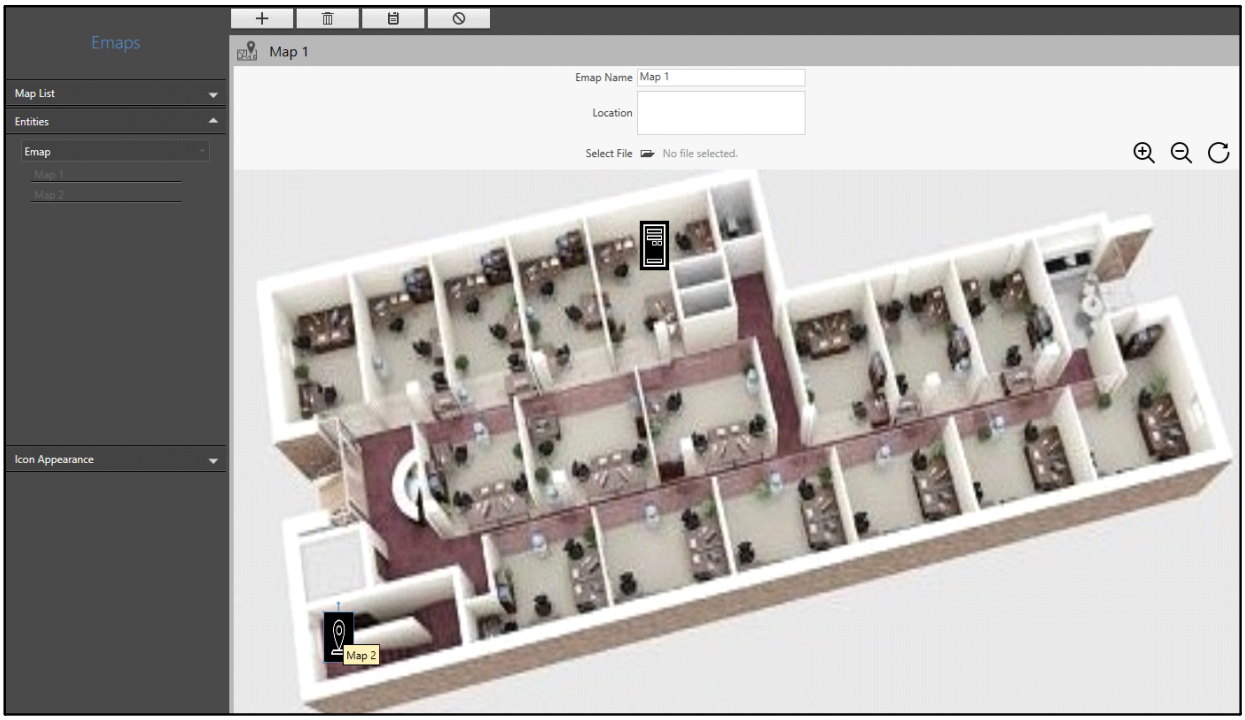
You can also assign a pre-configured Emap as a child entity to a new Map. To do so,

- Select the Emap which you wish to keep as the Parent Map.



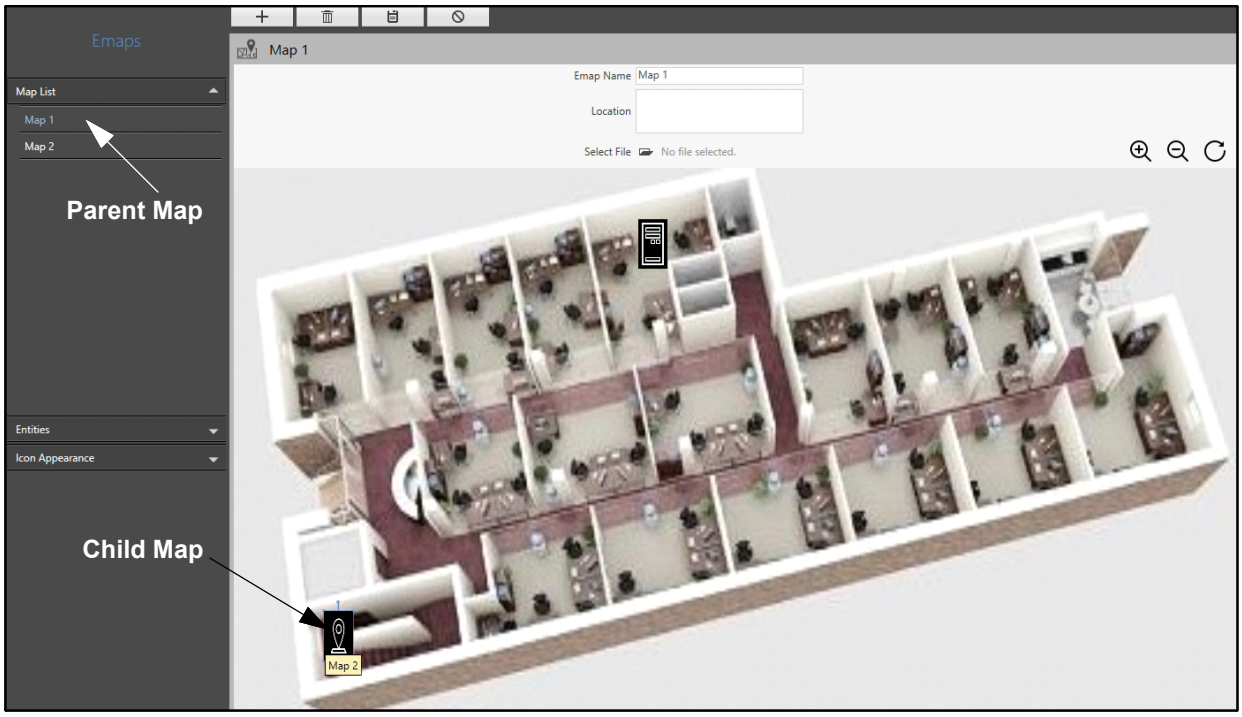
- In **Entities**, select the Entity Type as Emaps. Select the Emap which you wish to place as the child entity and drag it to place on the Parent Emap.

If the Emap selected in Entity Type is higher than the loaded Emap in hierarchy, it cannot be assigned as a child entity to the currently loaded Emap.

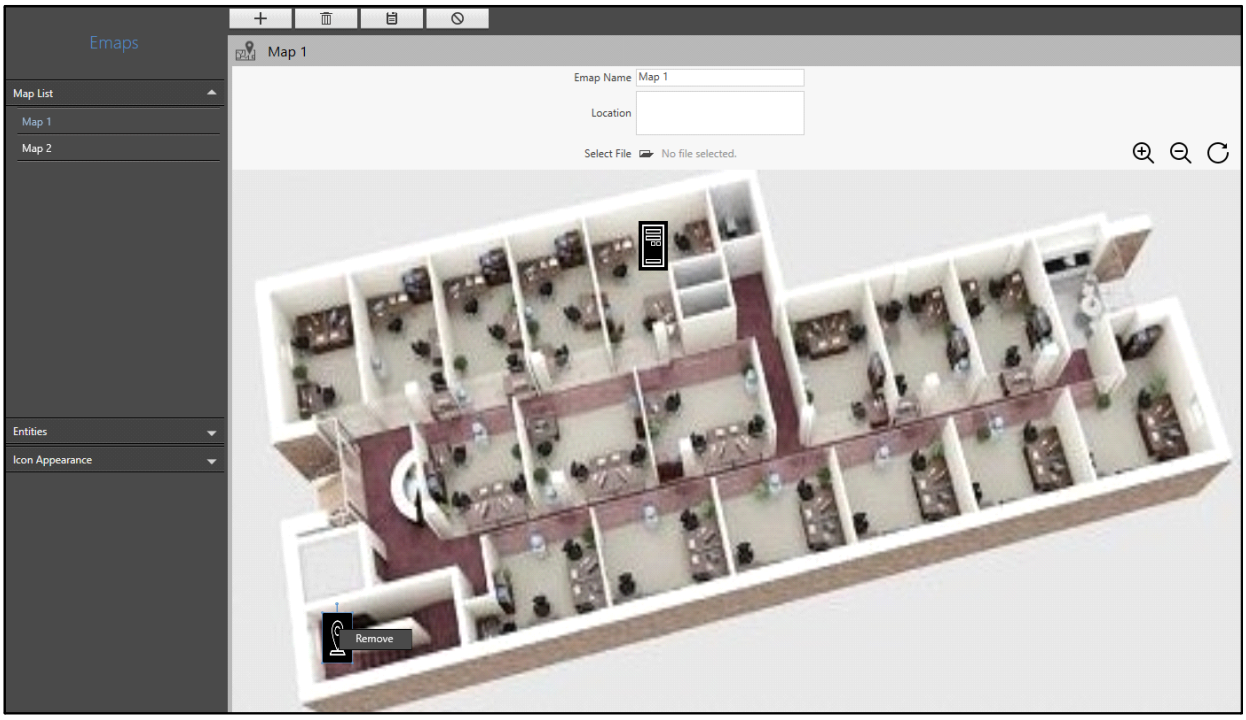


- Click **Save** to save the settings or **Cancel** to discard.

The Child Map appears on the Parent Map in the form of Emap entity.



- Hover the cursor over the Emap entity to view its name. You can drag the entity to change its position on the Emap.
- To remove an Emap entity, right click on it. The **Remove** option appears.



- Click **Remove** to remove the Emap entity.

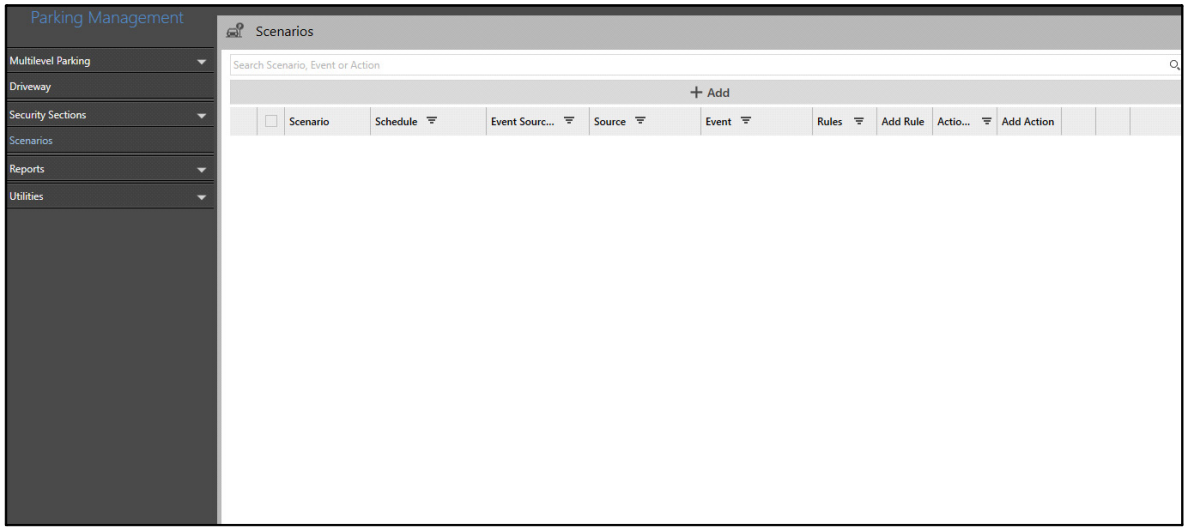
Configuring Event Notifications for the Emap Entity

You can configure Event Notifications to get an Emap alert on the Smart Client everytime the Event occurs. For example, you can configure Event Notifications for Parking Slot availability and get Emap alerts for the same.

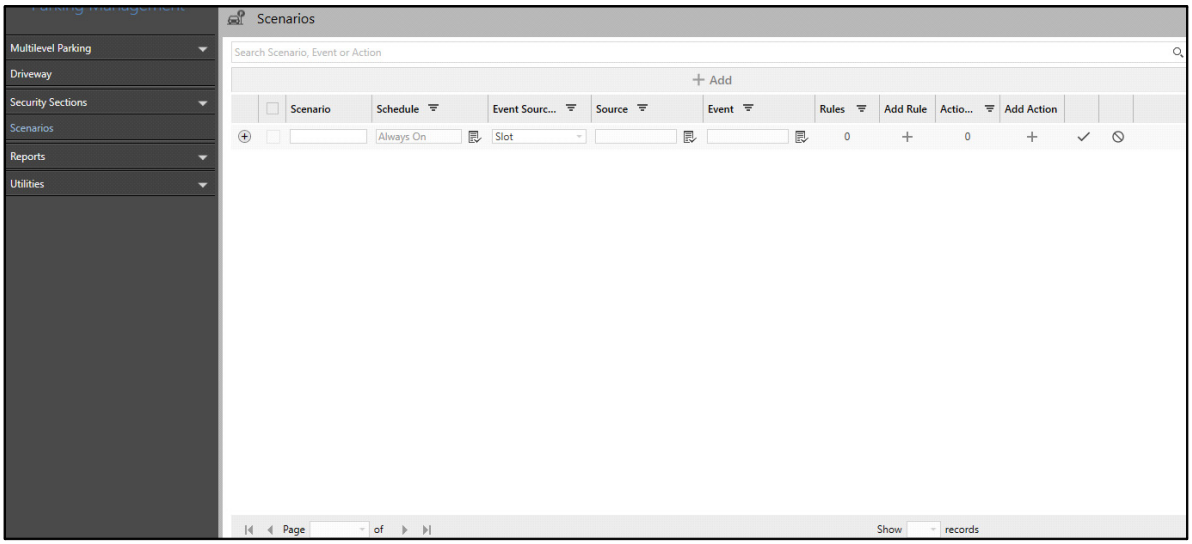
For example: Admin Client provides a facility to indicate the Status of the Parking Slot — Available or Occupied. This status is visible once you configure the Event Notification for Parking Slot availability to get Emap alerts.

To configure Event Notification for Parking Slot Availability,

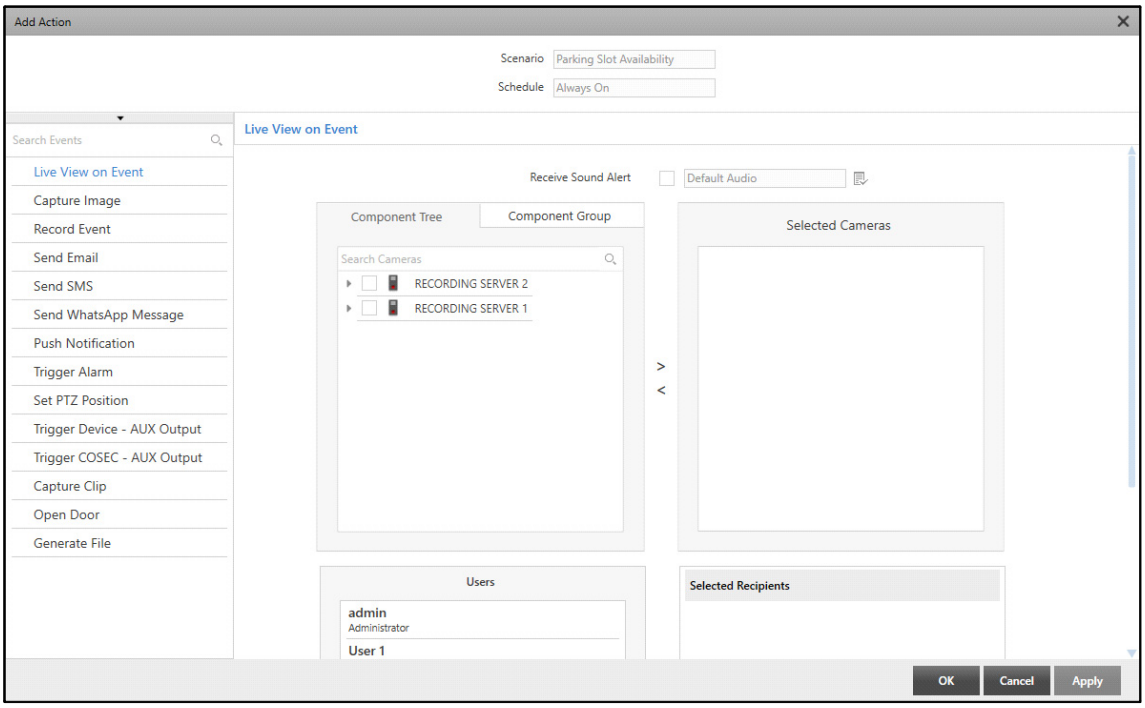
- Click **Parking Management > Scenarios**.



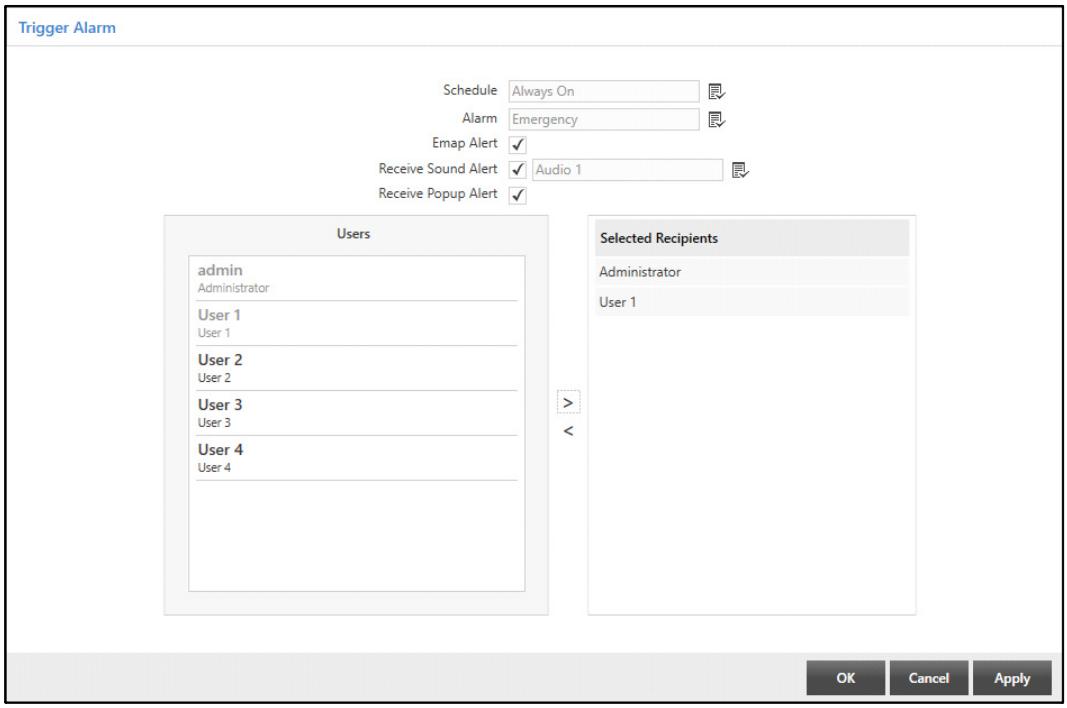
- Configure the Scenario **Parking Slot Availability** with the Event Source Type as **Slot** and the Event as **Slot Available**. For detailed Scenario configurations, refer to “Configure Scenarios”.



- Click **Add Action** + . The **Add Action** pop-up appears.



- Select **Trigger Alarm** from the list. Select the **Emap Alert** check box. For detailed configurations of action, refer to “Trigger Alarm”.



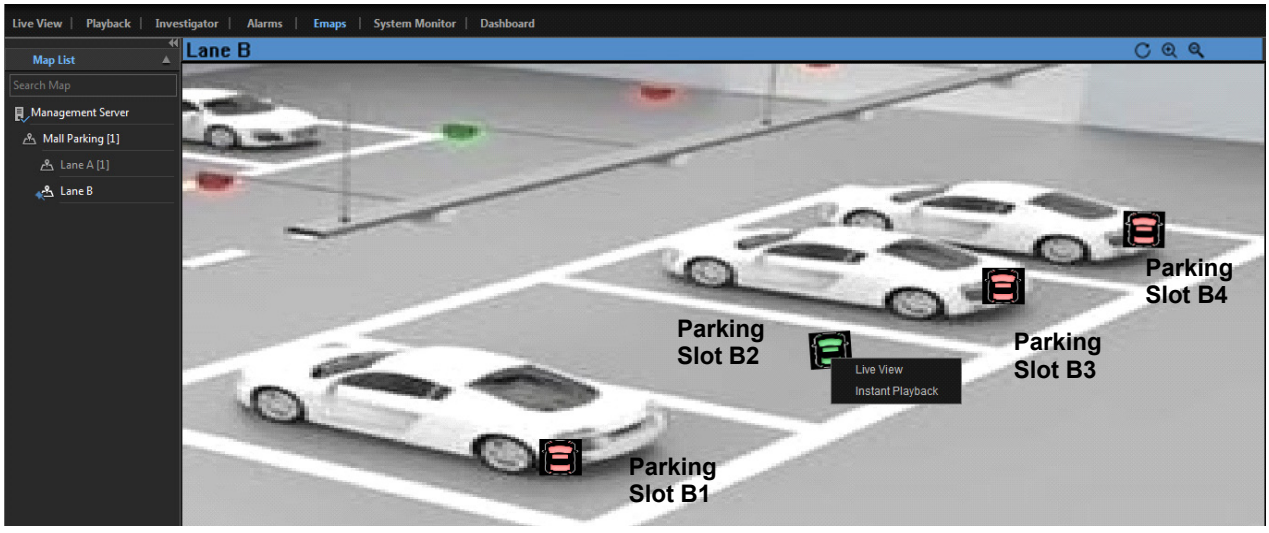
- Click **OK** to save the Action.

Emap Alerts are not supported for following Event Source Type — Device, Parking-Group, Parking-Lane, Parking-Area, Parking-Level, Parking-Facility and Custom Events.

- Once the Event is configured, you can view an Emap Alert in the Smart Client everytime that Event occurs.

Along with configuring the Event Notifications, you need to add the Parking Slot entities on the Emap for which you wish to receive alerts. To know more about adding entities, refer to “Entities”.

The Parking Slots configured on the Emap are displayed in the Smart Client. The Parking Slots B1, B3 and B4 are occupied, so they are indicated in red color. Whereas, the Parking Slot B2 is Available, so it is indicated in green color on the Emap.



Similarly, you can add various Actions and configure Event Notifications to receive Emap alerts for them.

CHAPTER 7

Access Control

Access Control System can detect and report intrusion, access to warehouse, cash rooms in banks, R&D departments in corporate, troubled conditions or any other place, where unauthorized access needs to be monitored.

Access Control Systems can grant, record, deny, detect and report access to facilities, services, information and other assets that need to be protected from mass access.

The Access Control module enables you to configure the integration of the COSEC Access Control Management System with the SATATYA SAMAS (via the COSEC Web Server). This integration is useful in enhancing the intelligence of a video surveillance system by enabling the detection of events on COSEC Devices to initiate appropriate actions in the Admin Client. You can integrate and configure Access Control System and add devices.

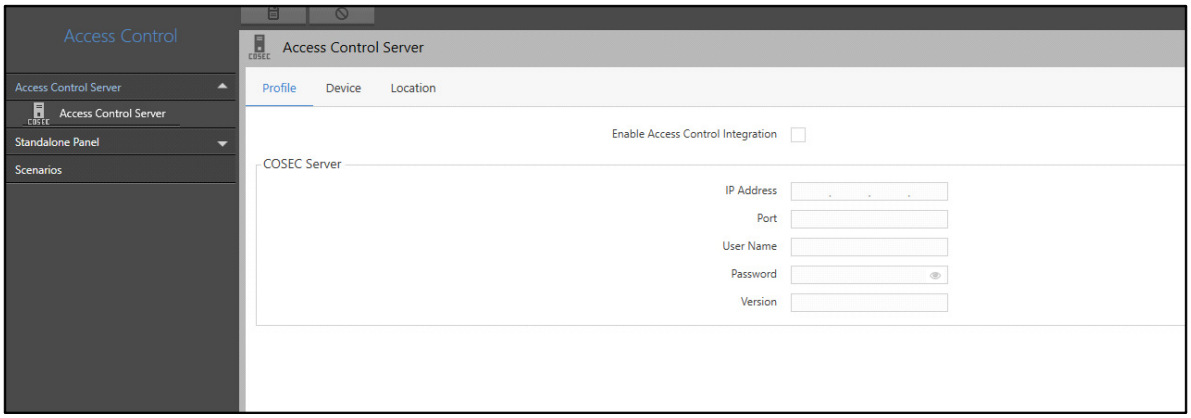
The Access Control module also provides a platform to integrate the COSEC Standalone Panel with SATATYA SAMAS. For details refer to “Standalone Panel”.

If you wish to integrate Access Control Server or Standalone Panel with SAMAS, make sure you only configure IPv4 addresses.

The user’s accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to “User Groups”.

To configure Access Control,

- Click **Access Control**.



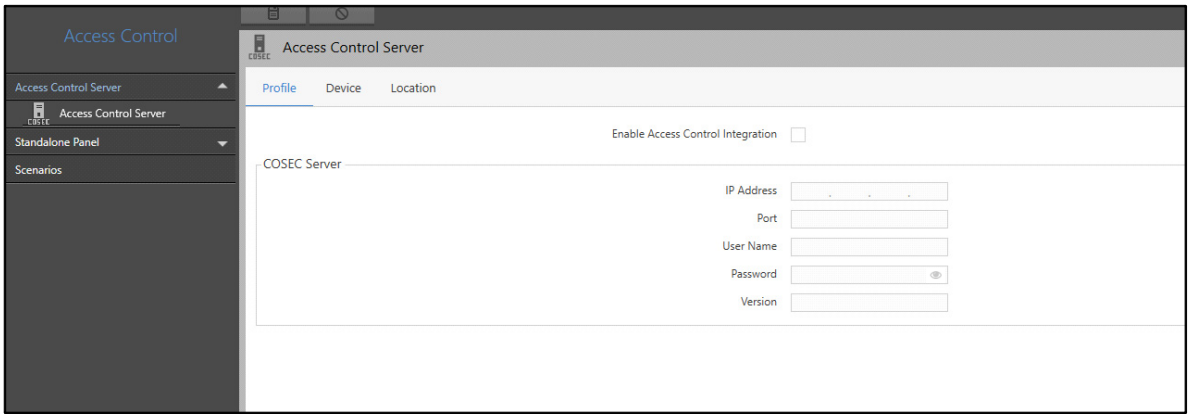
The Access Control module contains these pages — “Access Control Server”, “Standalone Panel” and “Scenarios - Access Control”.

Access Control Server

The Access Control Server page displays the COSEC Server configurations, configured devices and the location details. You can view and configure the Server, devices and location details from this page.

To configure Access Control Server,

- Click **Access Control**. The **Access Control Server** page appears by default.



The Access Control Server page consists of the following tabs.

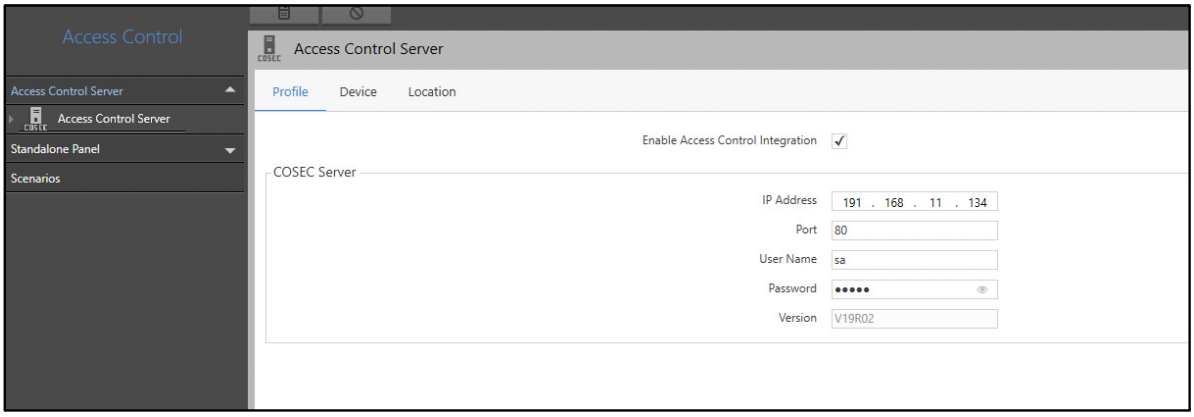
- “Profile”
- “Device”
- “Location”

Profile

This tab enables you to integrate the Access Control Server with the Admin Client and configure its network settings.

To configure the Profile settings,

- Click **Access Control Server**. The **Profile** tab appears by default.



Configure the following parameters:

- **Enable Access Control Integration**: Select the check box to enable the integration of COSEC Access Control Management System and SATATYA SAMAS.

COSEC Server

- **IP Address**: Specify the IP Address of the COSEC Server with which integration is to be done. In IP Address, you can enter upto 15 characters. Default: Blank.
- **Port**: Specify the Port number of the COSEC Server at which the MS will request for the COSEC data. Valid Range: 1-65535. Default: Blank.
- **User Name**: Specify the User Name for authentication of the COSEC Server. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password**: Specify the Password for authentication of the COSEC Server. In Password, you can enter upto 50 characters. Default: Blank.

  Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.

- **Version**: The Firmware Version of the COSEC Server appears by default.

- Click **Save** to save the settings or **Cancel** to discard.

To view events through the Smart Client, make sure you have also configured the following in **COSEC Admin Portal** as well as **COSEC Server**:

- To access the **Admin Portal** web page, enter the COSEC Server IP address followed by /cosecadmin (for example: 192.168.103.88/cosecadmin)
- Click C**ompany Configuration** > **Monitor Configuration**. The Monitor Configuration page appears.
- Select the Monitor Service from the right pane.
- Under **Optional Parameters**, configure the following:
  - **Export Events:** Select **All** from the drop-down list.
  - **IP Address:** Configure the **IP Address of the Management Server.**
  - **Port:** Configure the port as **8086**.
  - **Re-Try Count** :Configure this as **5**.
  - **Polling Interval:** Configure this as **5**.

For more details refer to the **Admin Mgt Portal User Guide.**

- To create users, enroll their credential and assign devices, access COSEC Server, that is 192.168.103.88/cosec/login. For more details refer to the **User Guide**.

The same events can also be viewed from the Monitor Utility. For details refer to the **Monitor User Guide**.

The documents can be downloaded from the website: **www.matrixcomsec.com/support/acta-product-manuals/ Folder: COSEC CENTRA.**

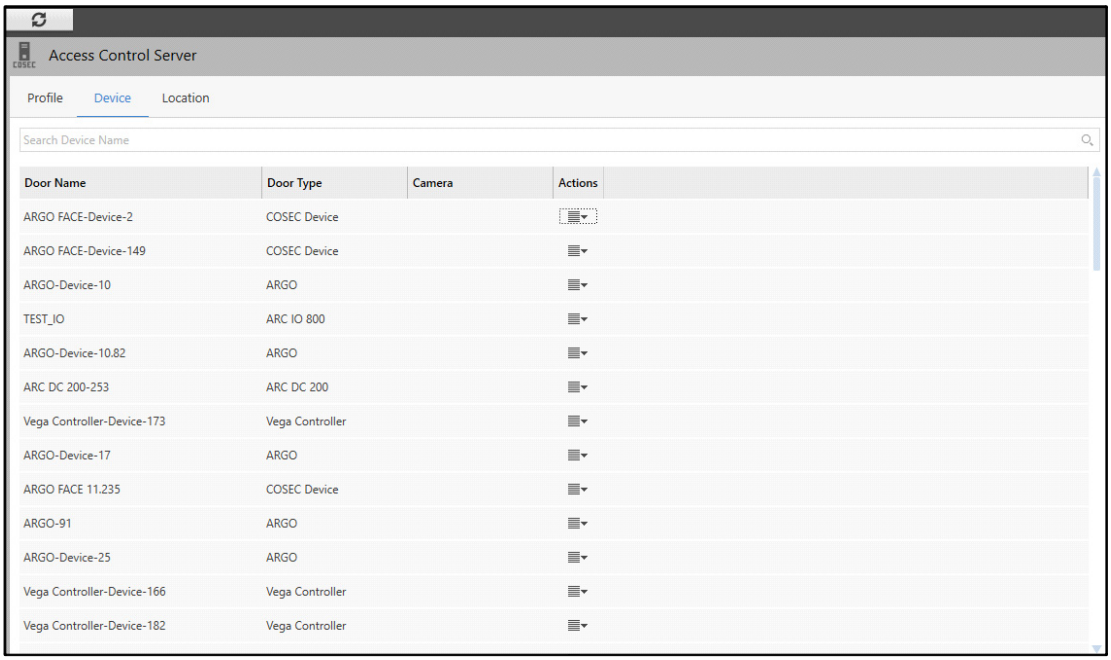
Once you have configured the details, the Admin Client will automatically sync and fetch the connected devices from the COSEC Server. To Sync the data manually, refer to “Device”.

Device

This tab enables you to view the devices added in the COSEC Server and configure them.

To configure the Device settings,

- Click the **Device** tab.



The COSEC Doors must be added to the COSEC Server before integration with the Admin Client.

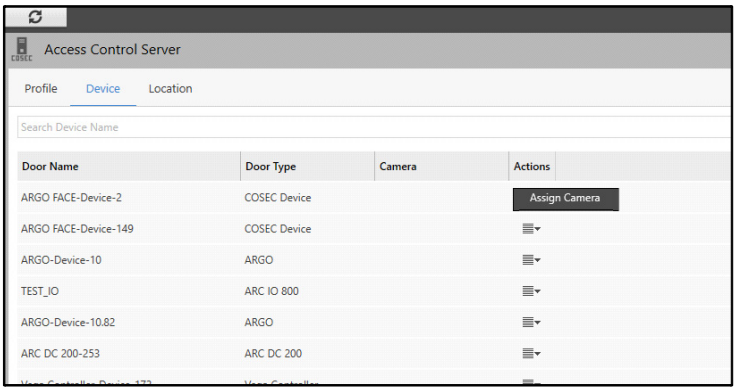
- To manually sync the data with the COSEC Server, click **Sync** . The connected devices will be displayed.

- The assigned devices/doors are also displayed to the left side by expanding the **Access Control Server** tab. You can search for the desired device using **Search Device Name** search bar.

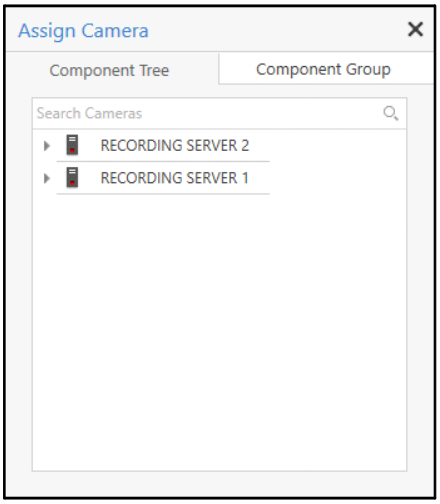
All the devices configured with the COSEC Server appear under this tab. The following Device details are displayed — Door Name, Door Type, Camera and Actions. You can also configure the settings of individual devices. For details, refer to “COSEC Device Details”.

You can also assign cameras to the individual COSEC Door. To do so,

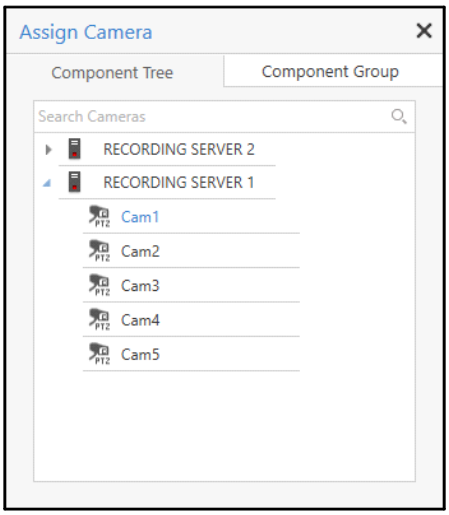
- Click **Actions** . The **Assign Camera** option appears.



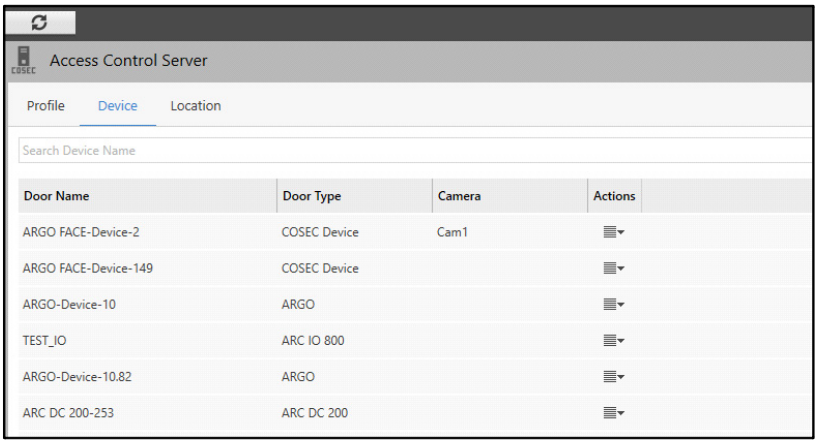
- Click **Assign Camera**. The **Assign Camera** pop-up appears.



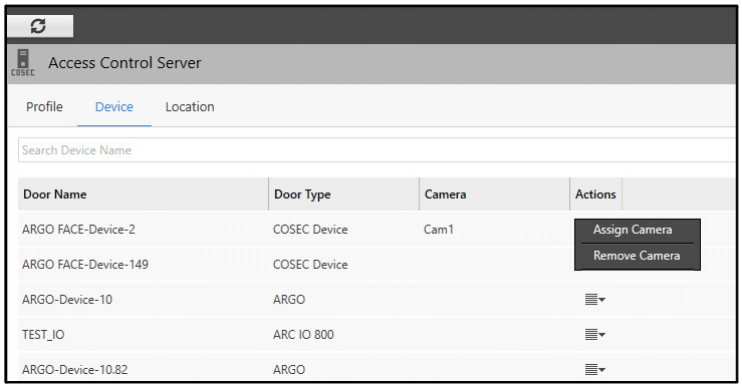
- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Double-click the desired camera to assign it to the COSEC Door. You can also search for the desired cameras using the **Search Cameras** search bar.



- The assigned camera appears corresponding to the COSEC Door under the device details.



- To remove the camera, click **Actions** . The **Remove Camera** option appears.



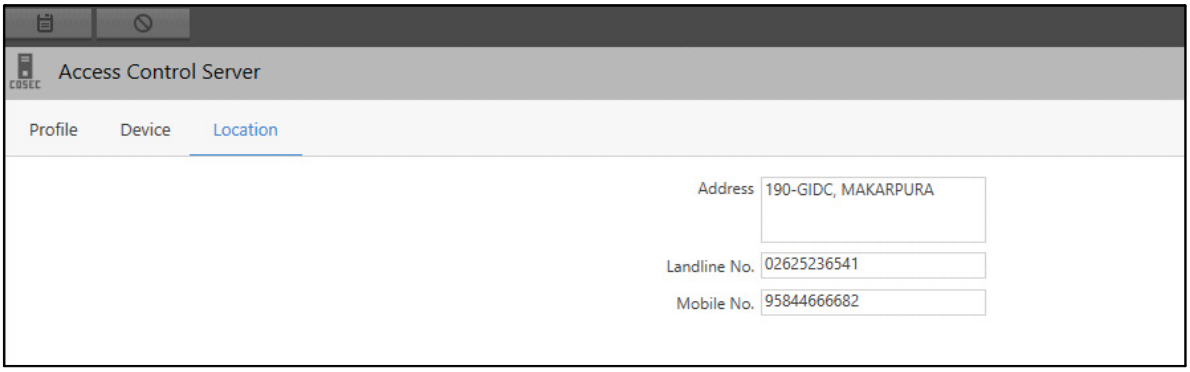
- Click **Remove Camera** to remove the assigned camera from the COSEC Door.

Location

This tab enables you to view and configure the location information of the Access Control Server.

To configure the Location,

- Click the **Location** tab.



The configurations of Location Settings in Access Control Server are similar to that of the Management Server. For details, refer to “Location”.

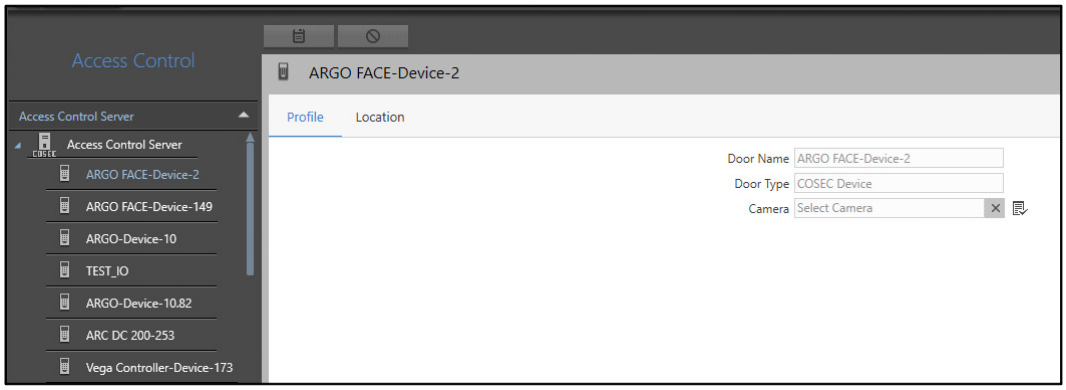
Whenever the Access Control Events are generated by Admin Client, you will be able to see the configured location information of the Access Control Server and/or relevant device from the Event Panel in the Smart Client.

COSEC Device Details

This page allows you to view the details of the device, along with the assigned cameras and the location details.

To view the device details,

- Select the desired device.



Each device consists of the following tabs:

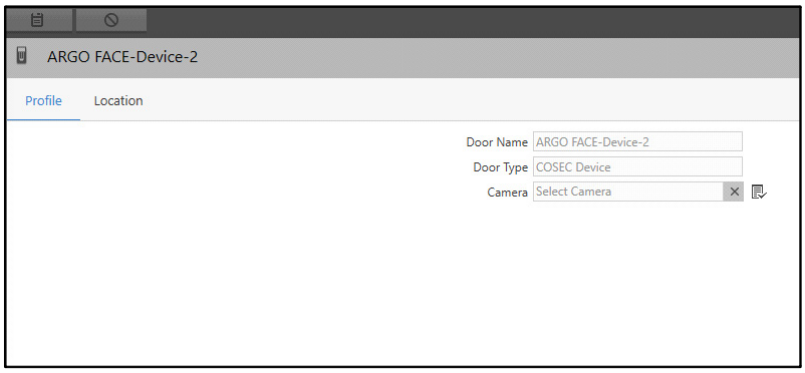
- “Profile”
- “Location”

Profile

This tab enables you to view the Device Profile, including assigned cameras. You can configure the assigned cameras under this tab.

To configure Device Profile,

- Select the desired device. The **Profile** tab appears by default.

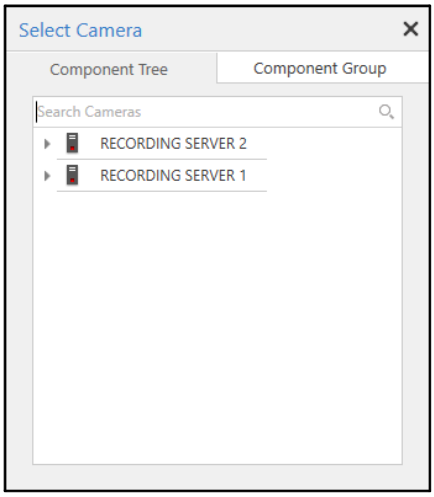


The following device details are displayed — Door Name, Door Type and Camera. You can only assign or remove the camera.

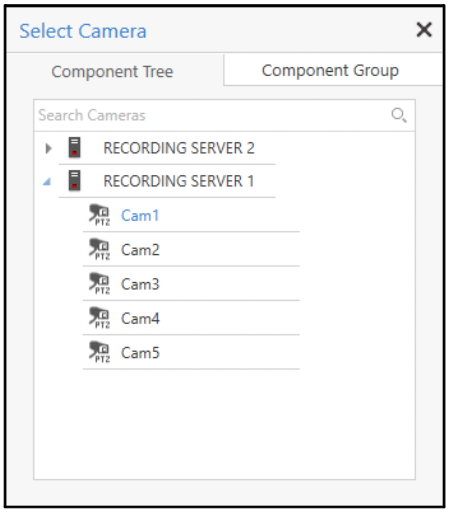
Assigning/Removing Cameras

To assign a camera,

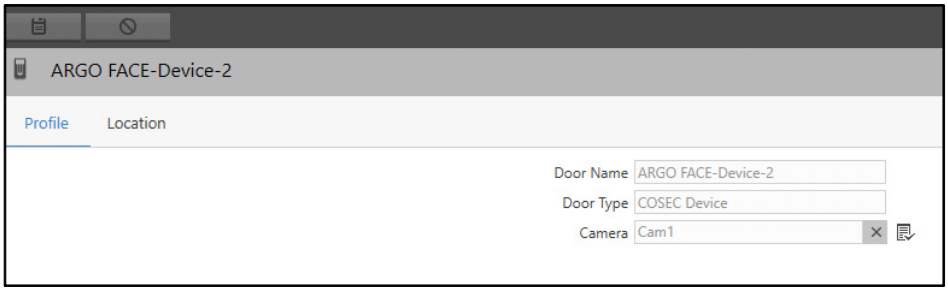
- Click **Camera** picklist. The **Select Camera** pop-up appears.



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Double-click the desired camera to assign it to the COSEC Door. You can also search for the desired cameras using the **Search Cameras** search bar.



- The selected camera appears against the **Camera** parameter.



- Click **Save** to save the settings or **Cancel** to discard.

Once you have added the camera to the COSEC Device, you can also remove it. To do so,

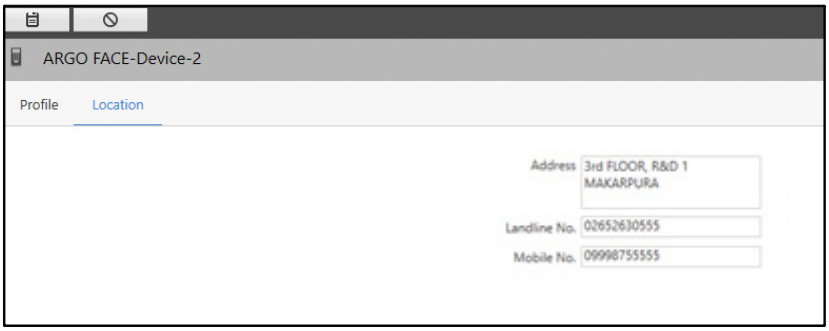
- Click **Remove** to remove the camera from the COSEC Device.
- Click **Save** to save the settings or **Cancel** to discard.

Location

This tab enables you to view and configure the location information of the device.

To configure the Location,

- Click the **Location** tab.



The configurations of Location Settings of a device are similar to that of the Management Server. For details, refer to “Location”.

Standalone Panel

The Access Control module provides a platform to integrate the COSEC Standalone Panel with SATATYA SAMAS. This integration allows detection of the Events and notifies you about the same by triggering alarm or by visual representation.

For example, an Occupied Parking Slot can be indicated by red LED or by triggering an alarm while a Vacant Parking Slot can be indicated by green LED.

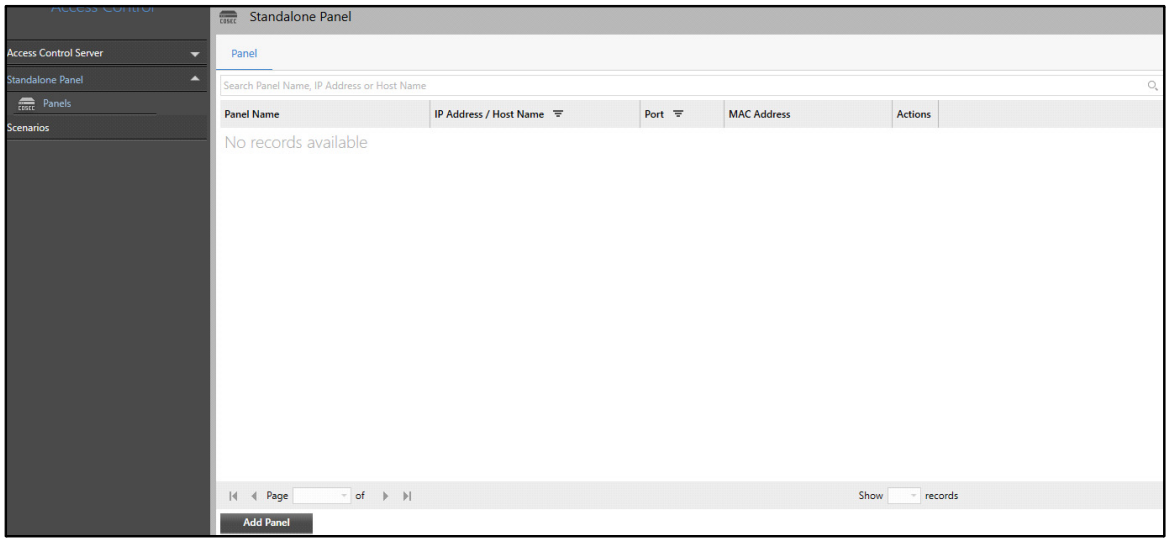
The COSEC Standalone Panel provides the facility to add 255 IO Controllers. Each IO Controller supports 8 Aux Outputs and 8 Aux Inputs.

- At AUX Inputs, you can connect sensors to detect the availability of slot in the parking facility. These sensors' AUX Inputs can be assigned to the slots from the Parking Management module. For the detailed configuration, refer to "Profile".
- At Aux Output, you can connect devices such as alarms or LEDs to indicate the Panel Events.

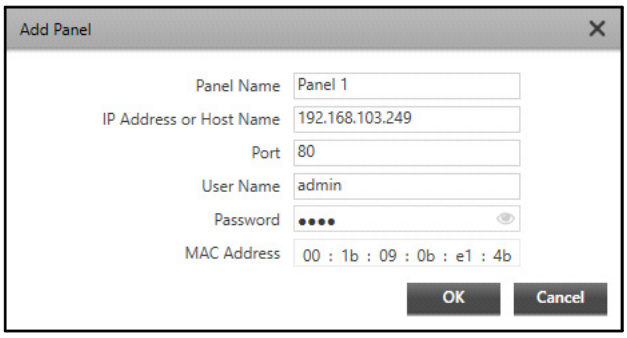
The Standalone Panel page displays all the configured Panels. You can view and configure the Standalone Panels from this page.

To configure Standalone Panel,

- Click **Access Control > Standalone Panel**. The **Panel** tab appears by default.



- Click **Add Panel**. The **Add Panel** pop-up appears.

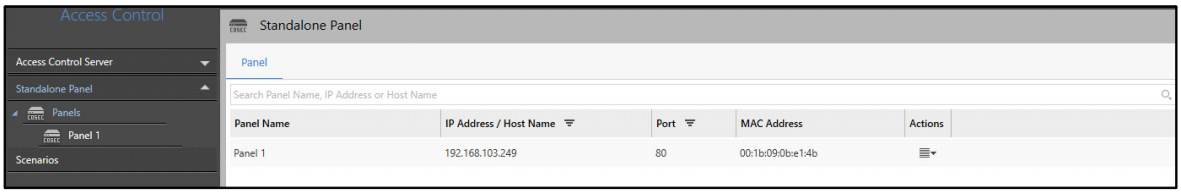


Configure the following parameters:

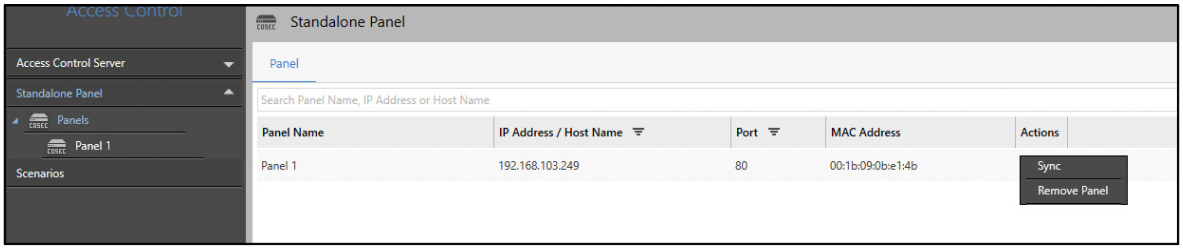
- **Panel Name:** Specify the name of the Panel which you wish to integrate with the Admin Client. In Panel Name, you can enter upto 30 characters. Default: Blank.
- **IP Address or Host Name:** Specify the IP Address or Host Name of the Panel. You cannot add a Panel with same IP address/Host Name twice. In IP Address or Host Name, you can enter upto 253 characters. Default: Blank.
- **Port:** Specify the Port which will be used to communicate with the COSEC Standalone Panel. Valid Range: 1-65535. Default: 80.
- **User Name**: Specify the User Name of the Panel for authentication. In User Name, you can enter upto 50 characters. Default: Blank.
- **Password:** Specify the Password of the Panel for authentication. In Password, you can enter upto 16 characters. Default: Blank.Click **Show** to view the password. The icon toggles to **Hide** . Click **Hide** to hide the password.
- **MAC Address:** Specify the MAC Address of the COSEC Standalone Panel. This will allow to get the Panel Events via the specified Port. In MAC Address, you can enter upto 17 characters. Default: Blank.

- Click **OK** to confirm or click **Cancel** to discard.

The new Standalone Panel appears in a list under the Panel tab. After adding the Panel the following details are displayed — Panel Name, IP Address/Host Name, Port, MAC Address and the Actions.



Click **Actions** , you can perform the following — Sync and Remove Panel.



- **Sync**: Click **Sync** to check if the configurations are valid. It also syncs all the IO Controllers configured in the Standalone Panel.
- **Remove Panel**: Click Remove Panel to remove the configured Panel from the Admin Client.
- **Filter:** Click **Filter** of the respective parameter in the header row.

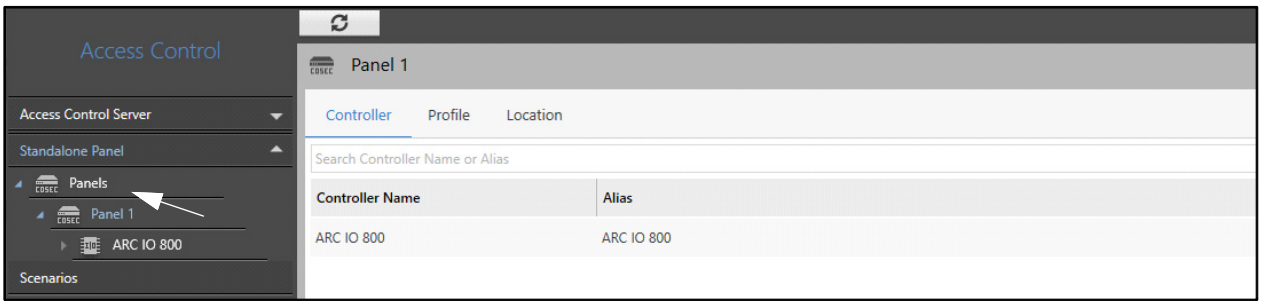
Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR FILTER**.

- **Sort:** You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

You can also configure the settings of individual Panels.

- Double-click the desired Panel.



Each Panel consists of the following tabs.

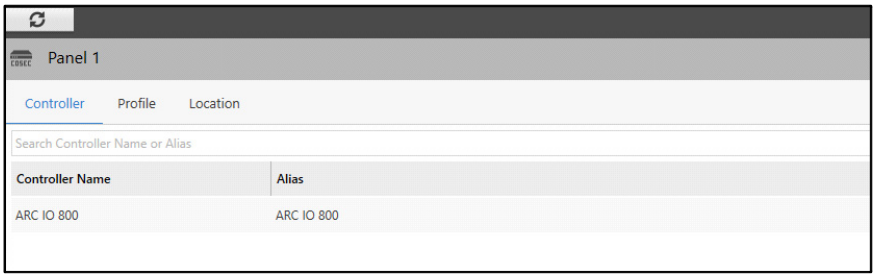
- "Controller"
- "Profile"
- "Location"

Controller

This tab enables you to view and configure the synchronized Controllers. You can view the Controllers only if they are added to the Panel through its web page. To know more about adding Controllers to a Panel, refer to **COSEC Panel200 System Manual**.

To configure the Controllers,

- Click the **Controller** tab.



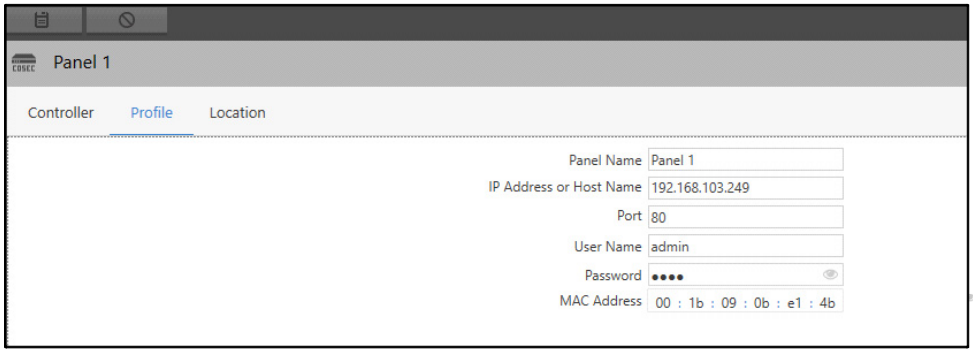
This tab displays two device parameters — Controller Name and Alias. You can also view and configure individual Controllers. For details, refer to "Controller Details".

Profile

This tab enables you to view and configure the Panel Profile.

To configure Profile,

- Click the **Profile** tab.



The details specified when adding the Panel are displayed under the Profile tab. You can make changes to these parameters, if required. For details, refer to “Standalone Panel”.

Location

This tab enables you to view and configure the location information of the Panel.

To configure the Location,

- Click the **Location** tab.



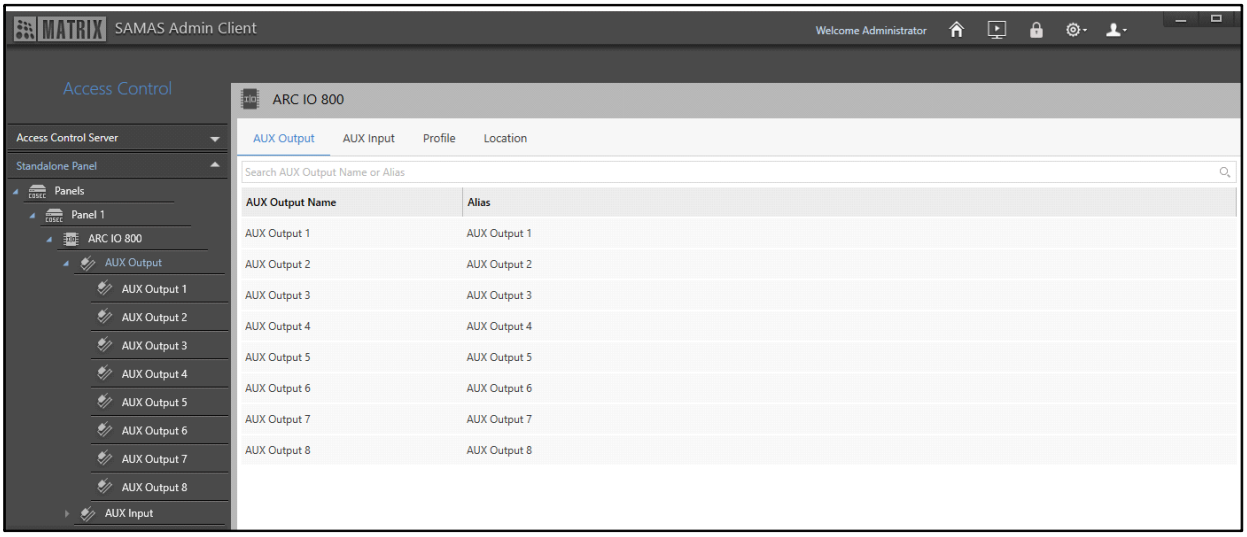
The configurations of Location Settings of a Panel are similar to that of the Management Server. For details, refer to “Location”.

Controller Details

This page allows you to view the details of the Controller, along with the Profile and location details.

To view the Controller details,

- Select the desired Controller.



Each Controller consists of the following tabs.

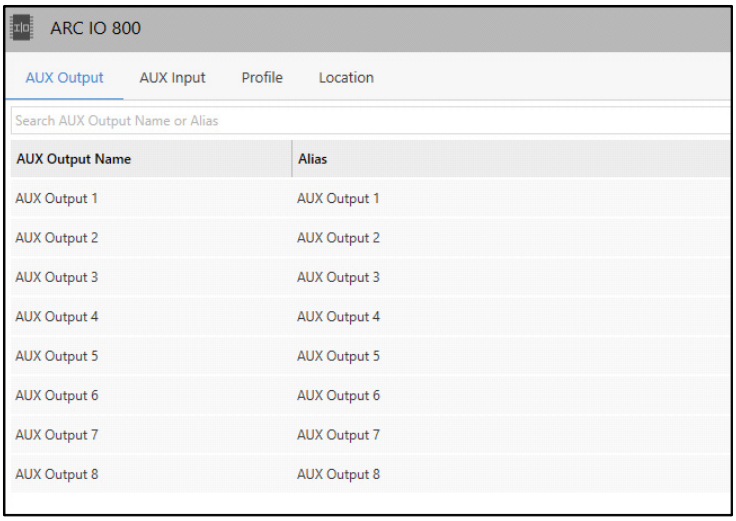
- "AUX Output"
- "AUX Input"
- "Profile"
- "Location"

AUX Output

This tab enables you to view the AUX Outputs of the Controller.

To view the AUX Output,

- Select the desired Controller. The **AUX Output** tab appears by default.



The following details are displayed — AUX Output Name and Alias.

AUX Output - Profile

This tab enables you to view and configure the Aux Output Profile.

To configure Profile,

- Double-click the desired Aux Output.
- The **Profile** tab appears.



The following details are displayed — Aux Output Name and Alias. You can only configure the Alias.

- **Alias**: Specify the Alias or alternative name you wish to assign to the Aux Output. In Alias, you can enter upto 50 characters. Default: same as the Aux Output Name.

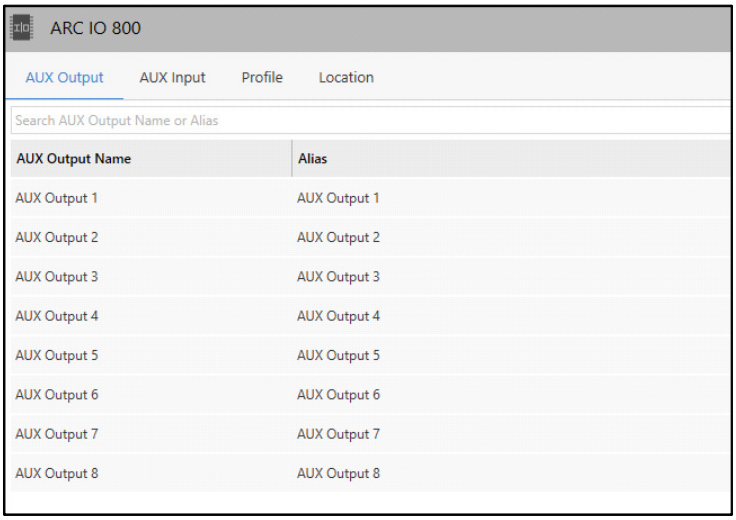
- Click **Save** to save the settings or **Cancel** to discard.

AUX Input

This tab enables you to view the AUX Inputs of the Controller.

To view the AUX Output,

- Click the **AUX Input** tab.



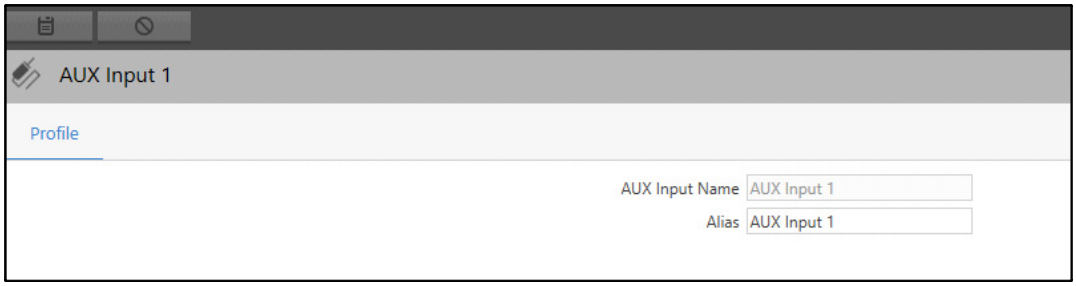
The following details are displayed — AUX Input Name and Alias.

AUX Input - Profile

This tab enables you to view and configure the Aux Input Profile.

To configure Profile,

- Double-click the desired Aux Input.
- The **Profile** tab appears.



The following details are displayed — Aux Input Name and Alias. You can only configure the Alias.

- **Alias**: Specify the Alias or alternative name you wish to assign to the Aux Input. In Alias, you can enter upto 50 characters. Default: same as the Aux Input Name.

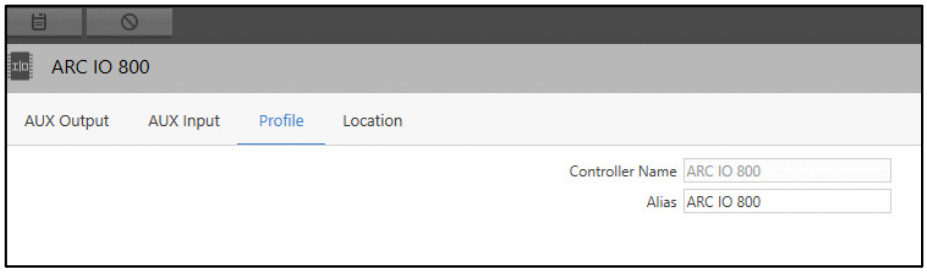
- Click **Save** to save the settings or **Cancel** to discard.

Profile

This tab enables you to view and configure the Controller Profile.

To configure Profile,

- Click the **Profile** tab.



The following Controller details are displayed — Controller Name and Alias. You can only configure the Alias.

- **Alias**: Specify the Alias or alternative name you wish to assign to the Controller. In Alias, you can enter upto 50 characters. Default: same as the Controller Name.

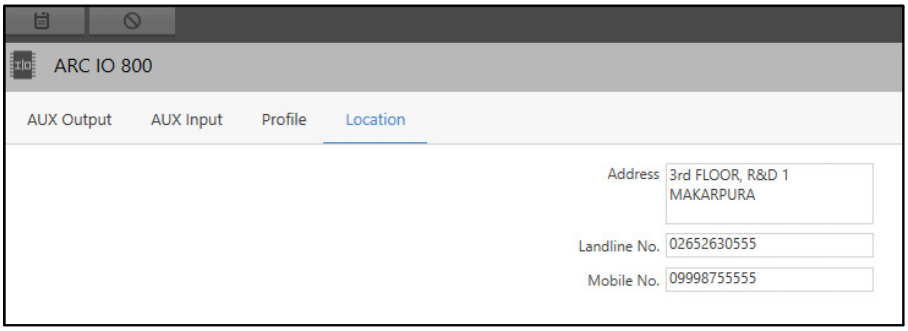
- Click **Save** to save the settings or **Cancel** to discard.

Location

This tab enables you to view and configure the location information of the Controller.

To configure the Location,

- Click the **Location** tab.



The configurations of Location Settings of a Controller are similar to that of the Management Server. For details, refer to “Location”.

Whenever the AUX Input Event is generated by Admin Client, you will be able to see the configured Location information of the IO Controller from the Event Panel in the Smart Client.

Configuring Event Notifications for Standalone Panel

You can configure Event Notifications using a Standalone Panel to trigger an alarm on the occurrence of particular events. For example, you can configure Event notifications to trigger alarm when a Parking Slot is occupied.

Let us understand this with the help of an example: Consider a Scenario of Smart Parking Facility where an Admin Client user wants to trigger an alarm when Slot is occupied.

Follow the steps below to achieve this scenario:

- “Add the Standalone Panel: COSEC Panel200 to SAMAS”
- “Add COSEC ARC IO800 Controller to Standalone Panel”
- “Configure the Parking Slot Profile”
- “Configure Scenarios and Actions to indicate about the Event”

Add the Standalone Panel: COSEC Panel200 to SAMAS

From the Access Control module, add the Standalone Panel. For detailed configurations, refer to “Standalone Panel”.

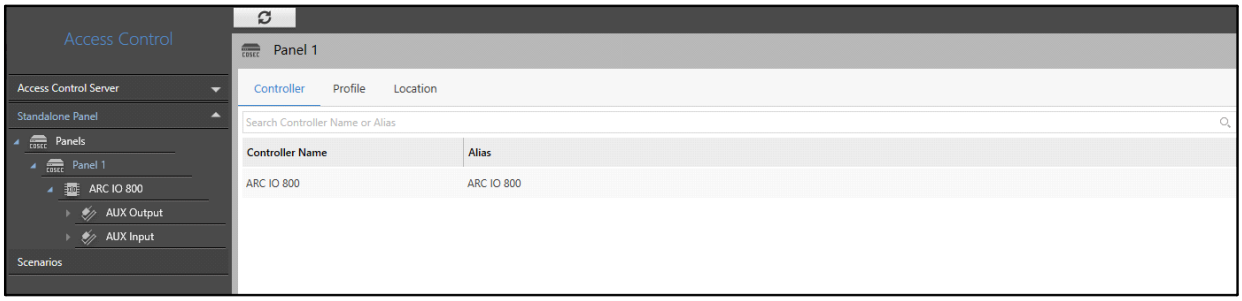


Add COSEC ARC IO800 Controller to Standalone Panel

Add the COSEC ARC IO800 to the Standalone Panel by accessing the web page of COSEC Panel200.

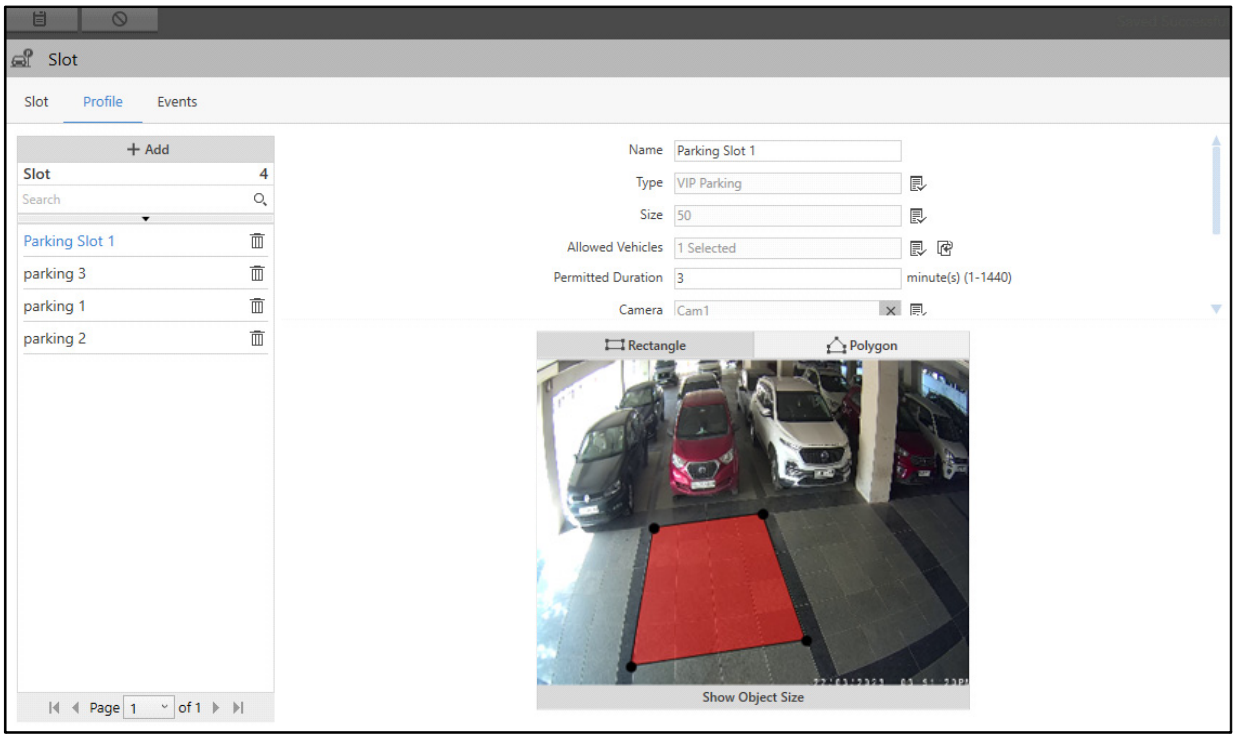
On the web page of Standalone Panel, click the **Configuration** tab. Click **Devices > Door Configuration** and click **Add** to add the ARC IO800. For more information, refer to **COSEC Panel200 System Manual**.

Now from Admin Client, sync the added Standalone Panel to fetch the configured IO Controllers to Admin Client. For detailed configuration, refer to “Standalone Panel”.



Configure the Parking Slot Profile

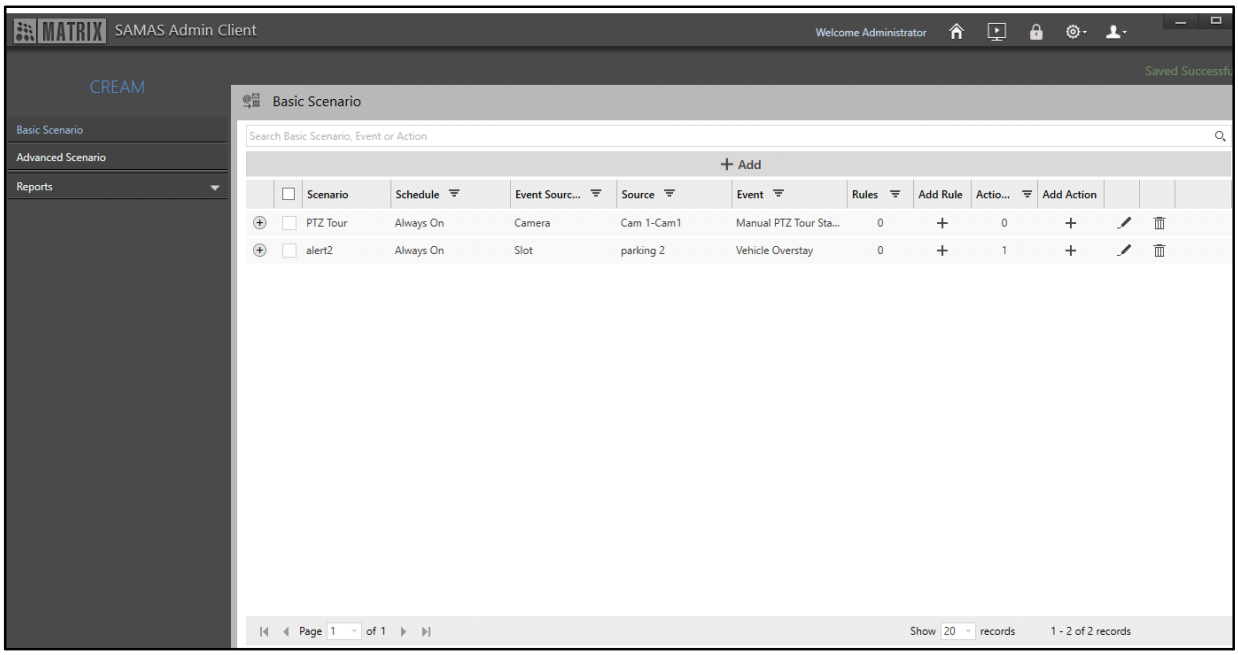
To detect the availability of a slot, you need to configure the Slot Profile from the Parking Management module. For detailed configuration, refer to “Profile”.



Configure Scenarios and Actions to indicate about the Event

To indicate the slot occupancy Event, you need to configure a Basic Scenario from CREAM module.

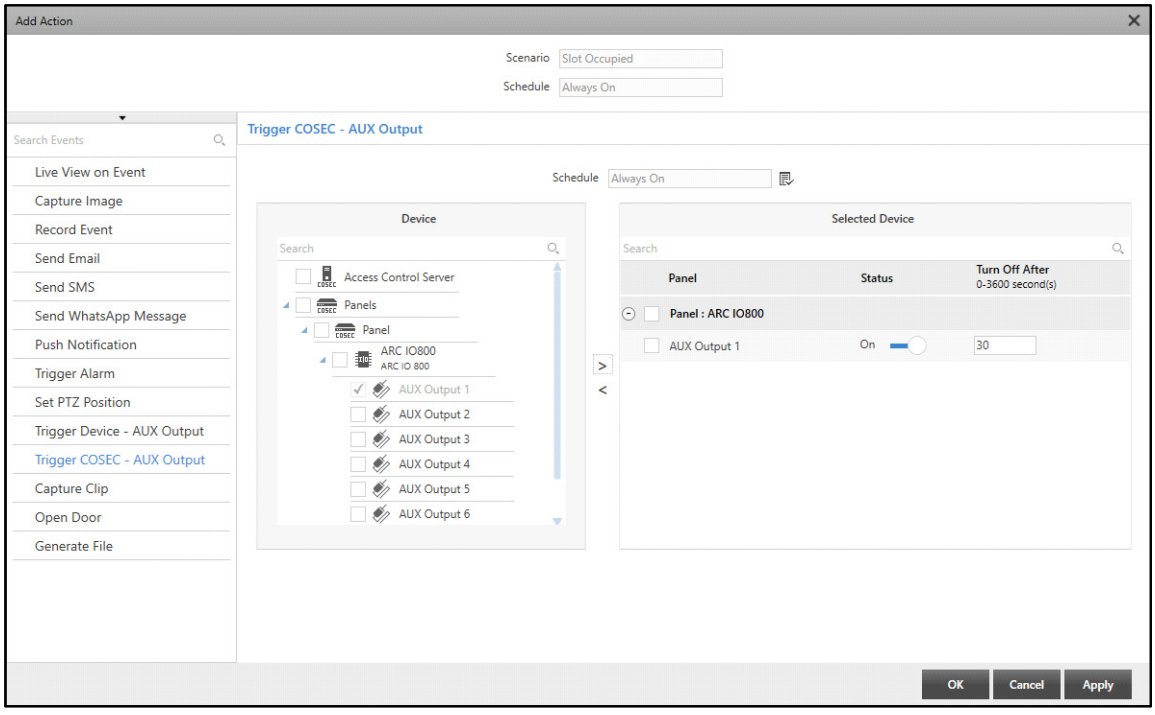
- Configure the Scenario **Slot Occupied** with the Event Source Type as **Slot** and the Event as **Slot Occupied**. For detailed Scenario configurations, refer to “Configure Scenarios” in “Basic Scenario”.



- Click **Save** ✓ to save the Scenario.

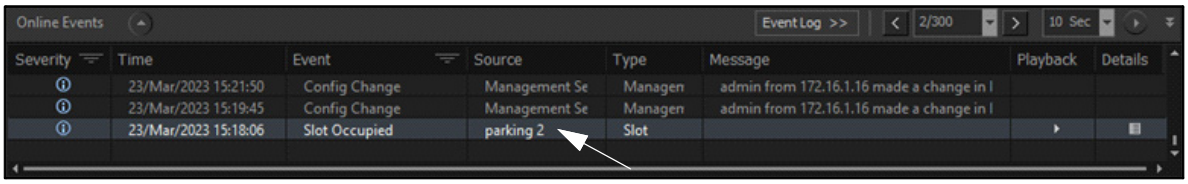
  You can also configure the same Scenario from **Parking Management > Scenarios** also**.**

- Click **Add Action** + to add the action for triggering the alarm. Select **Trigger COSEC- AUX Output** from the list. Select the desired schedule and add the desired ARC IO800 AUX Output Port from the **Device** list. For detailed configuration of Actions, refer to “Trigger COSEC - AUX Output”.



- Click **Apply** and **OK** to save the settings.

Now, when Slot 1 is occupied, LED or Alarm configured with IO AUX Output port will be triggered. You can also view the Event Log in the Smart Client as shown below.

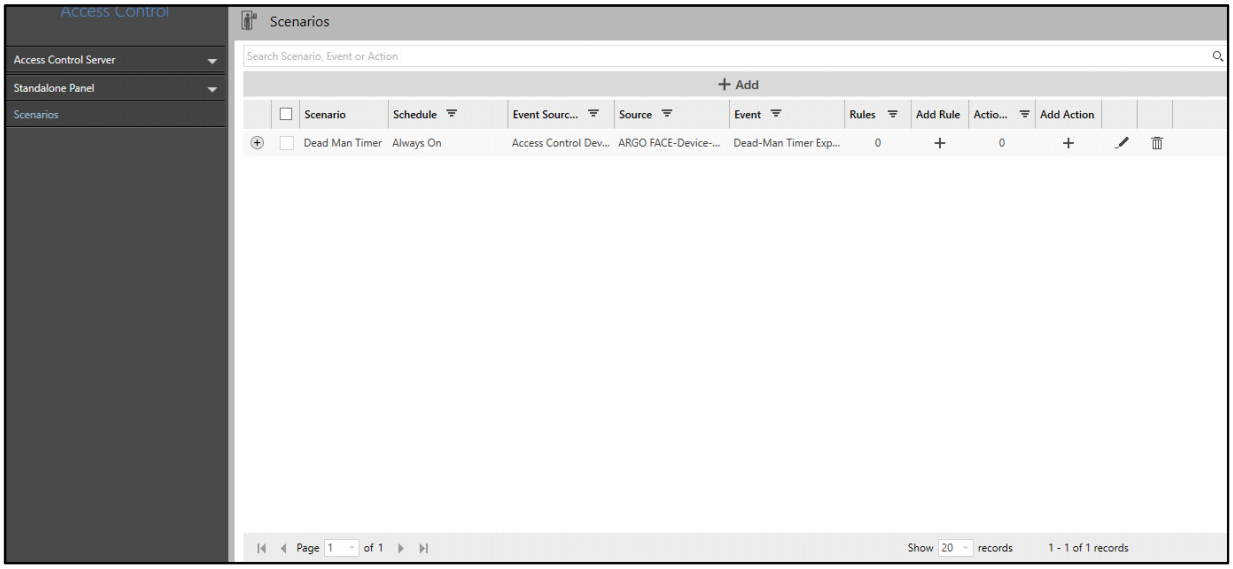


Scenarios - Access Control

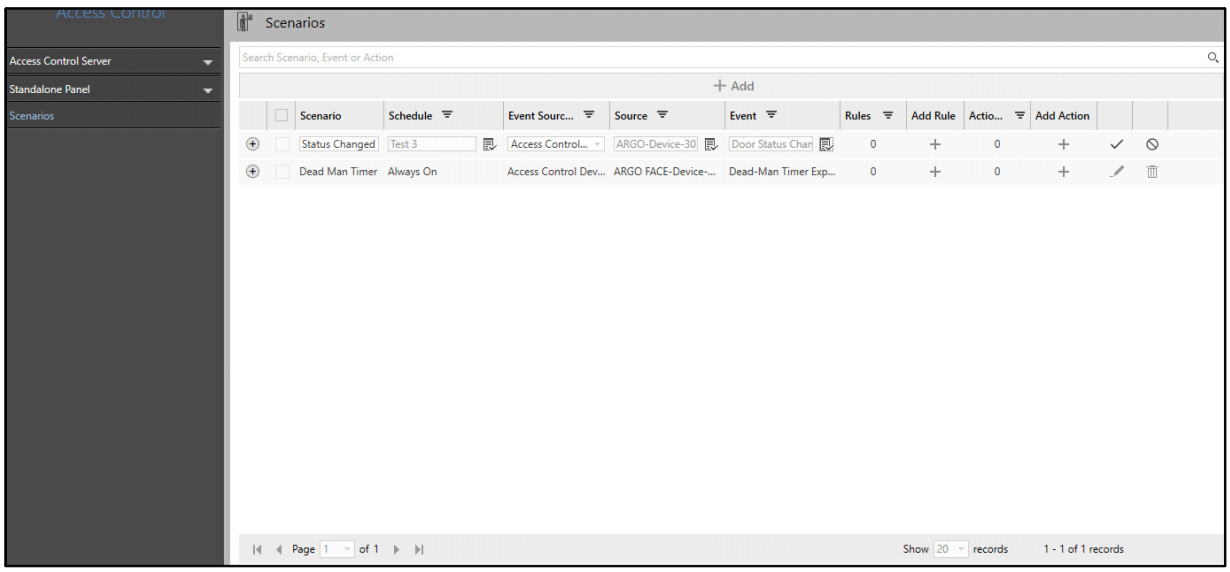
In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send Email) on the Event occurring at certain sources (For example, User Allowed, Door Status Changed, Duress Detection etc). The Scenarios page displays all the Scenarios configured for the Access Control Module. You can view and configure the Scenarios for all the Events related to Access Control.

To view and configure Scenarios,

- Click **Access Control > Scenarios**.



- Click **Add**.



The configurations of Scenarios for Access Control are similar to the Basic Scenario. For details, refer to “Basic Scenario”.

CHAPTER 8

Cognitive Response Engine with Automated Monitoring

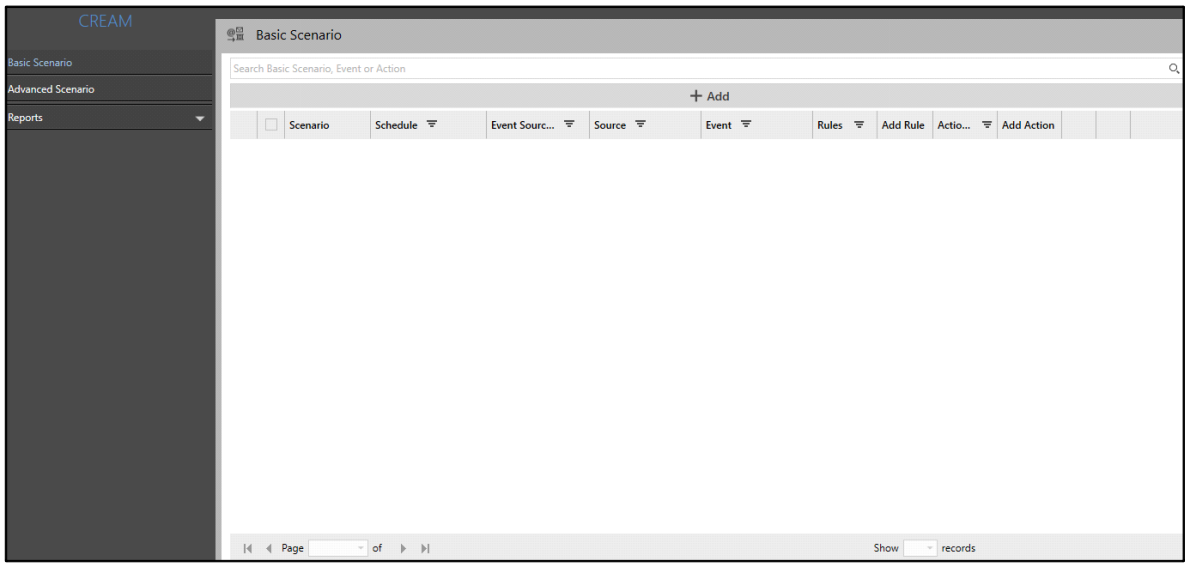
The CREAM (Cognitive Response Engine with Automated Monitoring) module enables you to configure Basic and Advanced Scenarios for monitoring and analysis. You can also view and configure Evidence Reports from this module.

Basic Scenario** feature is available with Basic License of SATATYA SAMAS. For **Advance Scenarios,** you need to upgrade your license. For detailed license information, refer to the **SATATYA SAMAS Installation Guide.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure CREAM,

- Click **CREAM**.



The CREAM module contains these pages — "Basic Scenario", "Advanced Scenario" and "CREAM - Report".

For scenarios configured in the CREAM module, actions are executed through Scenarios according to the Entity Rights and Event Monitoring Rights of active users.

For example, consider an Admin has configured the following action for a Scenario; Start Live View of Camera 1 and Camera 2 on execution of the action **Live View on Event**. The user for whom this action is enabled from Event

Monitoring Rights can view the live view of Camera 1 and Camera 2 in the Smart Client. But, if the user has entity rights for Camera 1 only, then the live view of Camera 1 only will start on the execution of the action, because the user does not have entity rights for Camera 2.

In **Basic Scenario**, if the user has Entity Rights of the configured **Event Source Type** entity and the Event Monitoring Rights of the configured Event, then only the user will get Event details in Smart Client and Scenario Initiated Event Log in Smart Client. For configuring Basic Scenarios, refer to “Basic Scenario”.

In **Advance Scenario**, if the user has entity rights of any one camera of the configured Scenario and Event Monitoring Rights of the configured Events or Wait action Event, the user will get **Scenario Initiated**, **Scenario Waiting**, **Scenario Resumed** and **Scenario Failed** Event Logs in the Smart Client. For configuring Advanced Scenarios, refer to “Advanced Scenario”.

Basic Scenario

In CREAM (Cognitive Response Engine with Automated Monitoring) module, the **Basic Scenario** page displays all the Basic Scenarios. You can view and configure set of actions (for example, Send SMS) for Events (for example, Storage Memory Low) occurring at certain sources (for example, Management Server).

In Basic Scenario, single Event can be configured and multiple actions can be taken on it.

For the Basic Scenario you must:

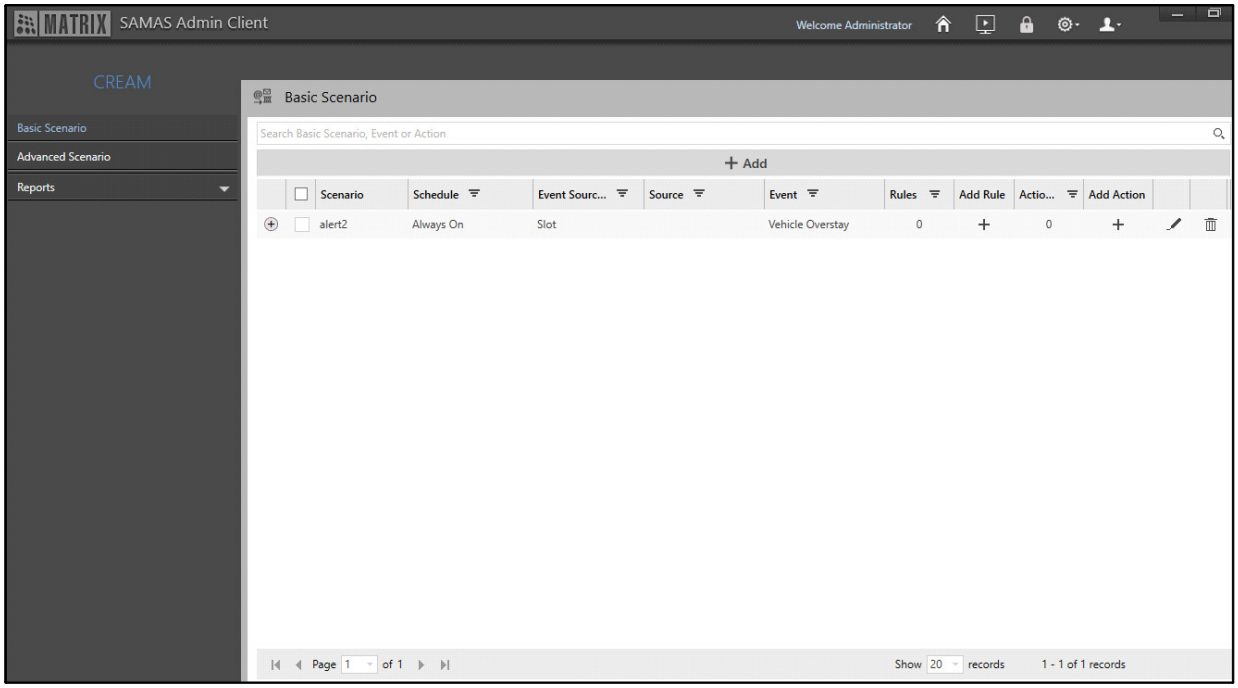
- "Configure Scenarios"
- "Add Rule"
- "Add Action"

Configure Scenarios

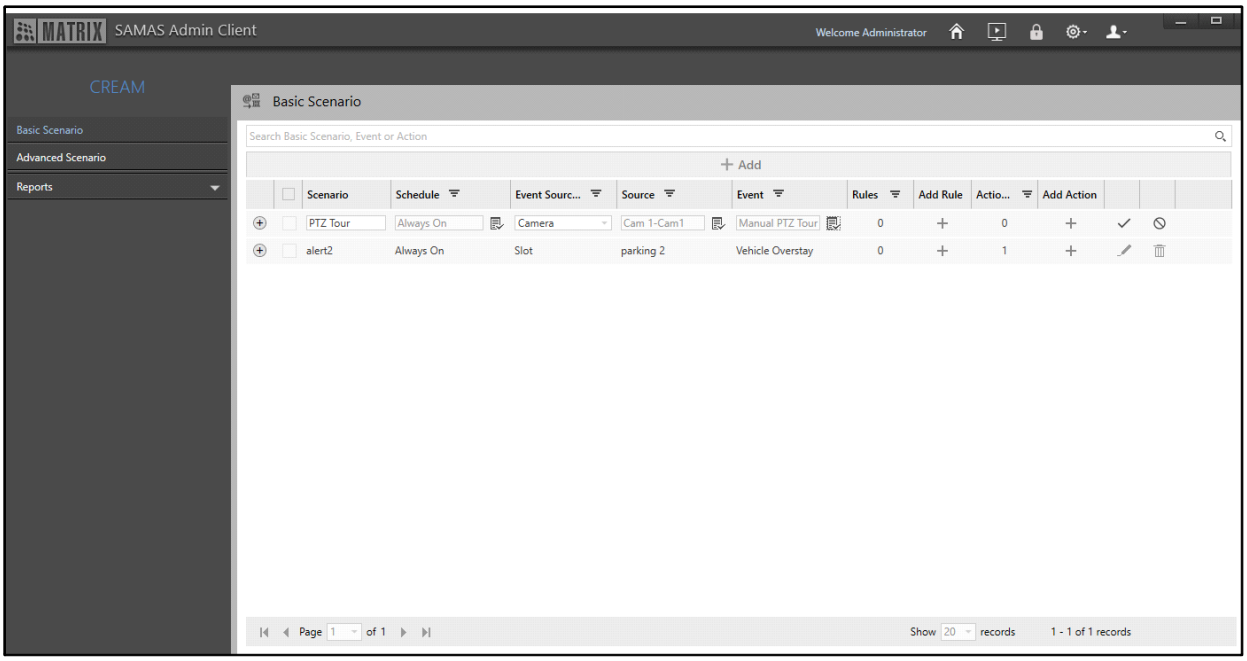
The Basic Scenarios page displays all the configured Scenarios. You can view and configure the Scenarios from this page.

To configure Basic Scenario,

- Click **CREAM**. The **Basic Scenario** page appears by default.



- Click **Add**

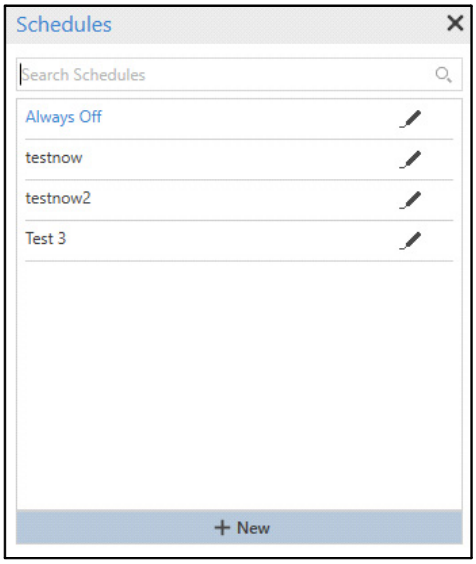


Configure the following parameters:

- **Scenario**: Specify a suitable name for the new Scenario. In Scenario, you can enter upto 100 characters. Default: Blank.

Due to Windows limitation, make sure you do not configure any of the following — CON, PRN, AUX, NUL, COM1 to COM9, LPT1 to LPT9 — as the name of the ***Scenario.***

- **Schedule**: Select the desired Schedule which you wish to assign to the Scenario using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



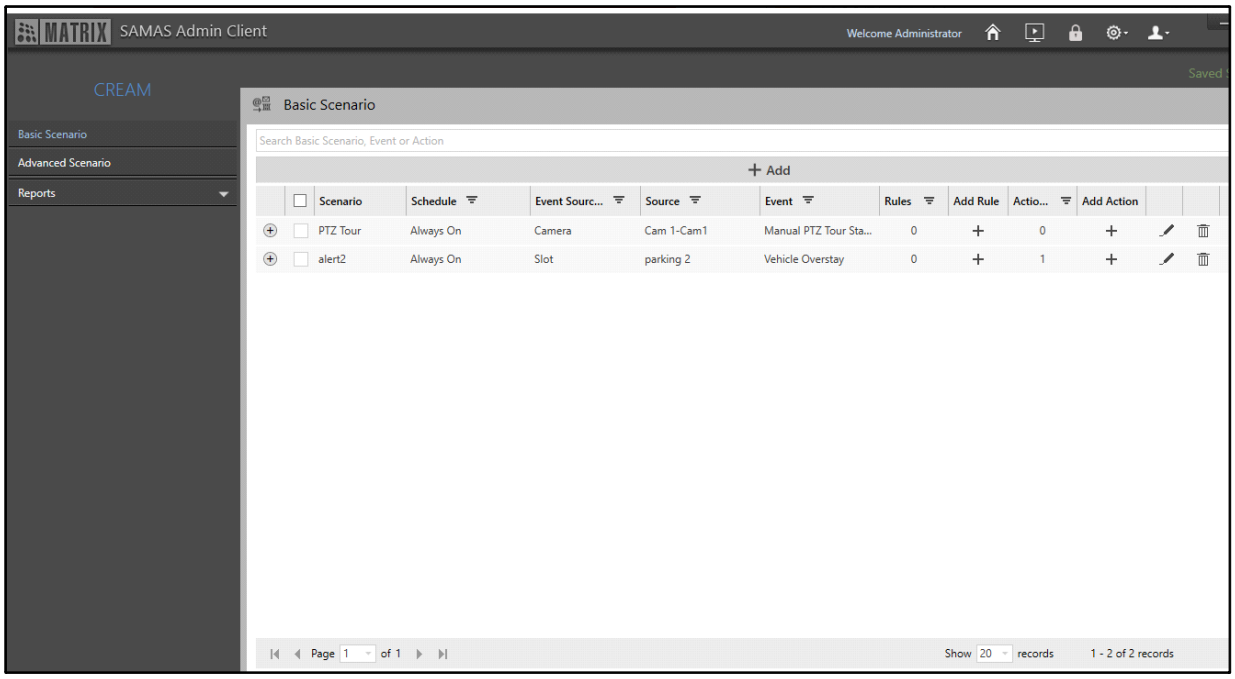
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Event Source Type**: Select the type of Event Source for which you wish to configure an Event and Action from the drop-down list.
- **Source**: Select the Source where the Scenario has to be initiated using the **Source** picklist. The Source depends on the selected Event Source Type. For example, if you select Camera as the Event Source Type, a list of all the configured cameras appear in the **Source** picklist. Double-click to select the desired option.
- **Event**: Select the desired Event for which you wish to configure an Action using the **Event** picklist. The Event depends on the selected Event Source Type and Source. Double-click to select the desired option.

- Click **Save** to save the Scenario or click **Cancel** to discard.

The configured Scenario appears in a list.

You can edit the configured Scenario or delete it.



- Click **Edit** to edit the Scenario configurations.
- Click **Delete** to delete the Scenario.
- Click **Filter** of the respective parameter in the header row.
  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

Once a Scenario is configured, you can add a Rule and Action to the Scenario.

Add Rule

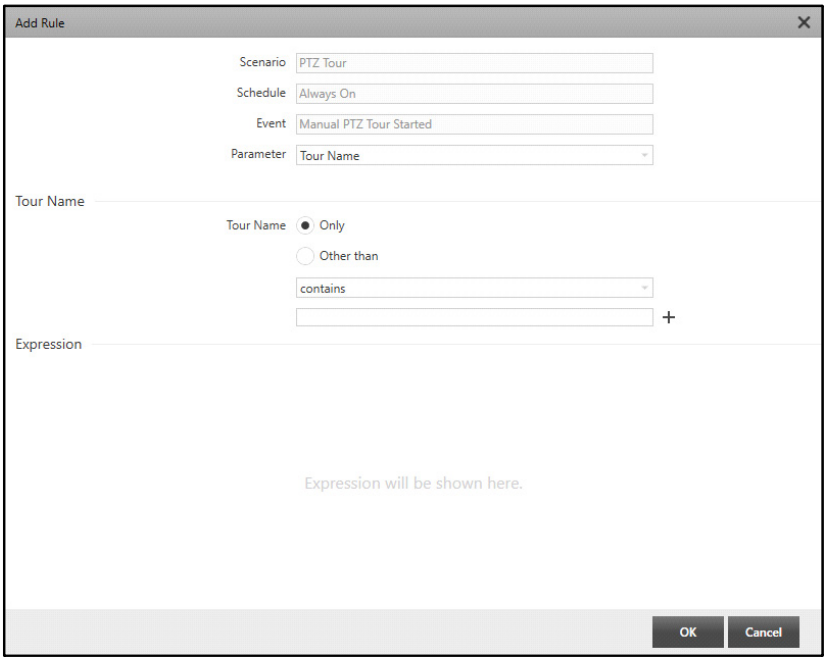
This option allows you to add a Rule for the configured Scenario. Only when the conditions for the Rule are satisfied, the Scenario will be executed.

You can configure Rules only for selected Events.

The Rules can be configured only for the specific Event Parameter.

To add a Rule,

- Click **Add Rule** + to add Rules. The **Add Rule** pop-up appears.



The Scenario details displayed are— Scenario Name, Schedule and Event.

Configure the following parameters:

- **Parameter**: Select the desired Parameter from the drop-down list. For example, Tour Name.

  The selected Parameter can be configured in the Parameter (Tour Name) section. All the further conditions are explained in accordance with the selected Parameter (Tour Name).

The list of parameters depends on the type of Event selected. Also, the type of expressions/conditions for the Rule changes as per the selected parameter.

*For the applicable Event (for example, User Login), if you select Parameter as **IP Address**, then you can configure IPv4/IPv6 address.*

- **Tour Name**: Select the desired condition for the **Parameter** from the options — Only or Other than.

  Select **Only**, if the Rule is to be configured only for the specified expression value.

  Select **Other than**, if the Rule is to be configured for all the values except the specified expression value.
- Select the desired condition from the drop-down list — contains, starts with or matches.

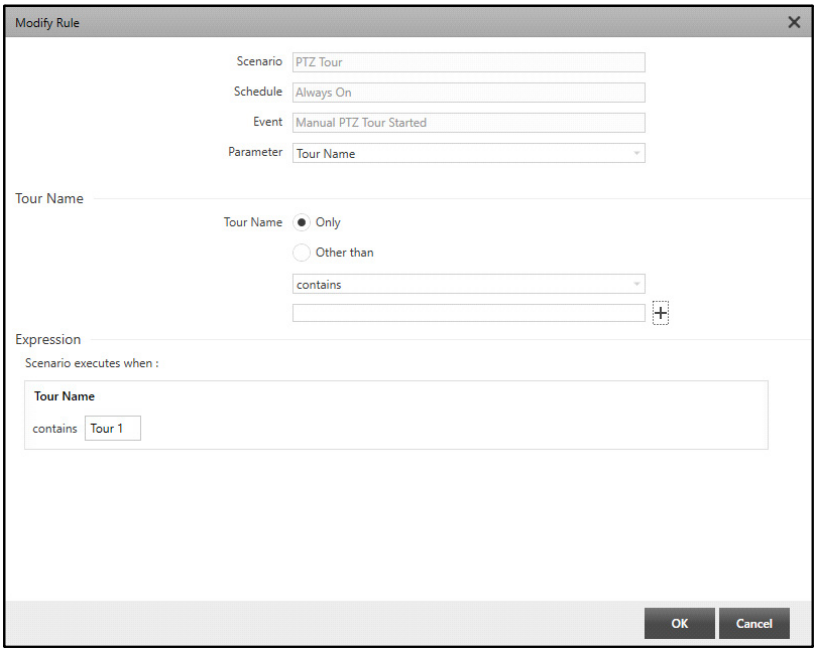
  Select **contains** to specify the value which contains a particular name.

  Select **starts with** to specify the value which starts with a particular name or letter.

  Select **matches** to specify the value that matches exactly with the name of the configured Tour.

- Specify the condition details as per the selected conditions for the Rule.

- Click **Add** + . The Expression of the Rule will be displayed with the defined conditions in the **Expression** section.

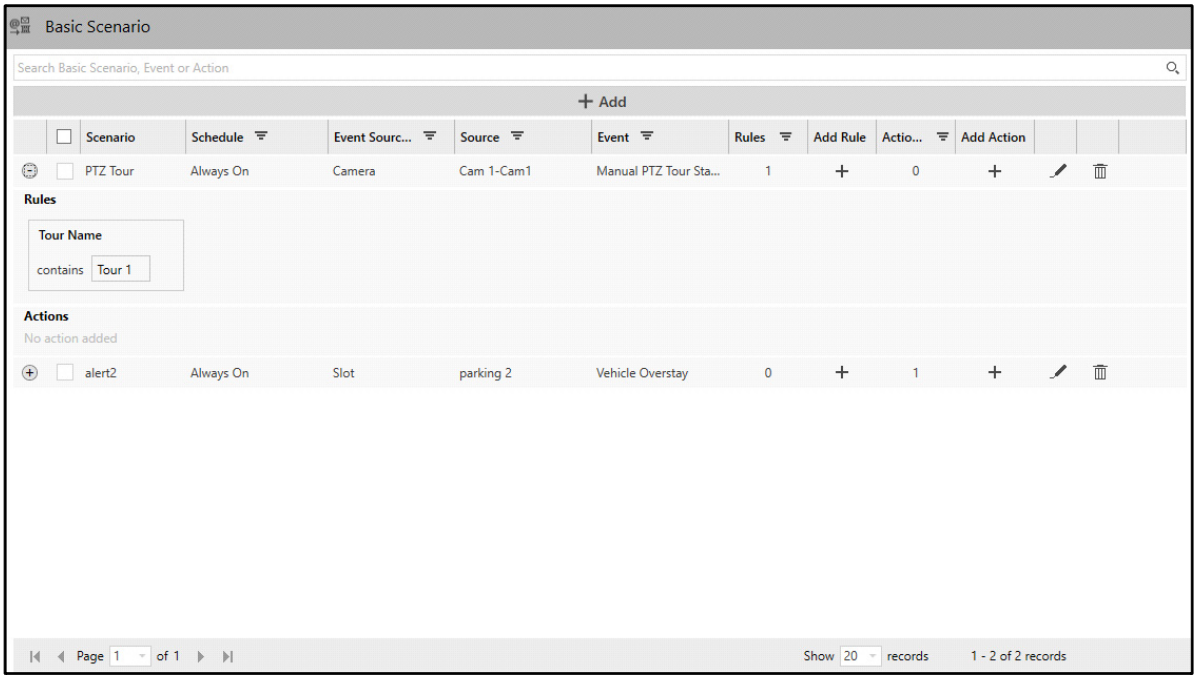


The Scenario **PTZ Tour** with the Event **Manual PTZ Tour Started** will be executed if the Parameter **Tour Name** only contains Tour 1.

- Click **OK** to confirm or click **Cancel** to discard.

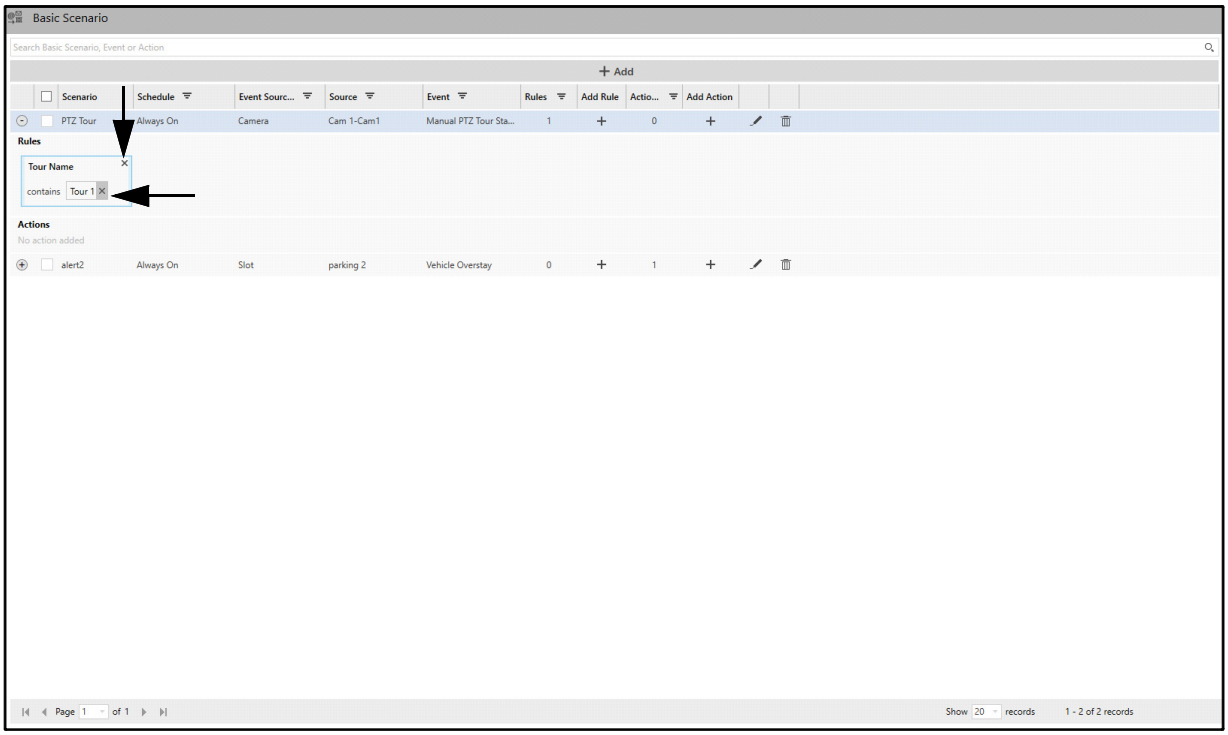
The configured Rule appears in the Scenario details. To view the Rule details:

- Click **Show** .



- The Rule and Actions details are displayed.

  Hover the cursor over the configured Rule. The **Remove** ✕ option appears.



- Click **Remove** ✕ to remove the Rule.

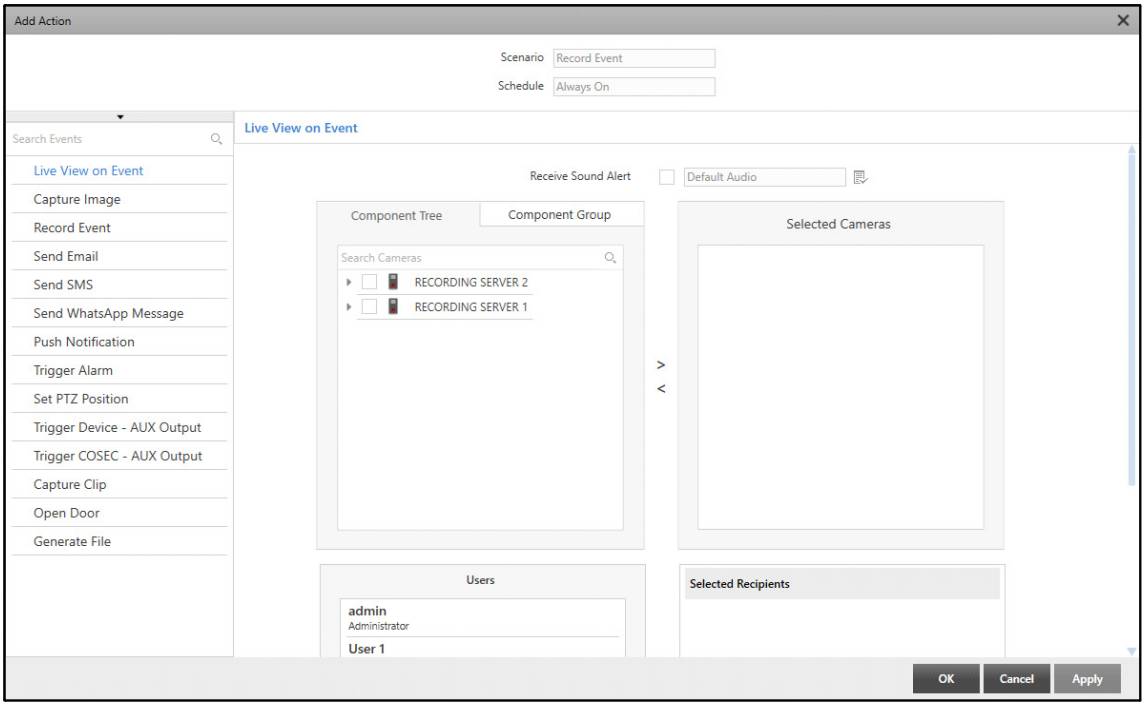
Add Action

This option allows you to add an Action to the configured Scenario. The Action is triggered when the Scenario is executed.

The configurable Actions change as per the selected Event. Also, the configurable parameters differ from Action to Action.

To add an Action,

- Click **Add Action** + . The **Add Action** pop-up appears.

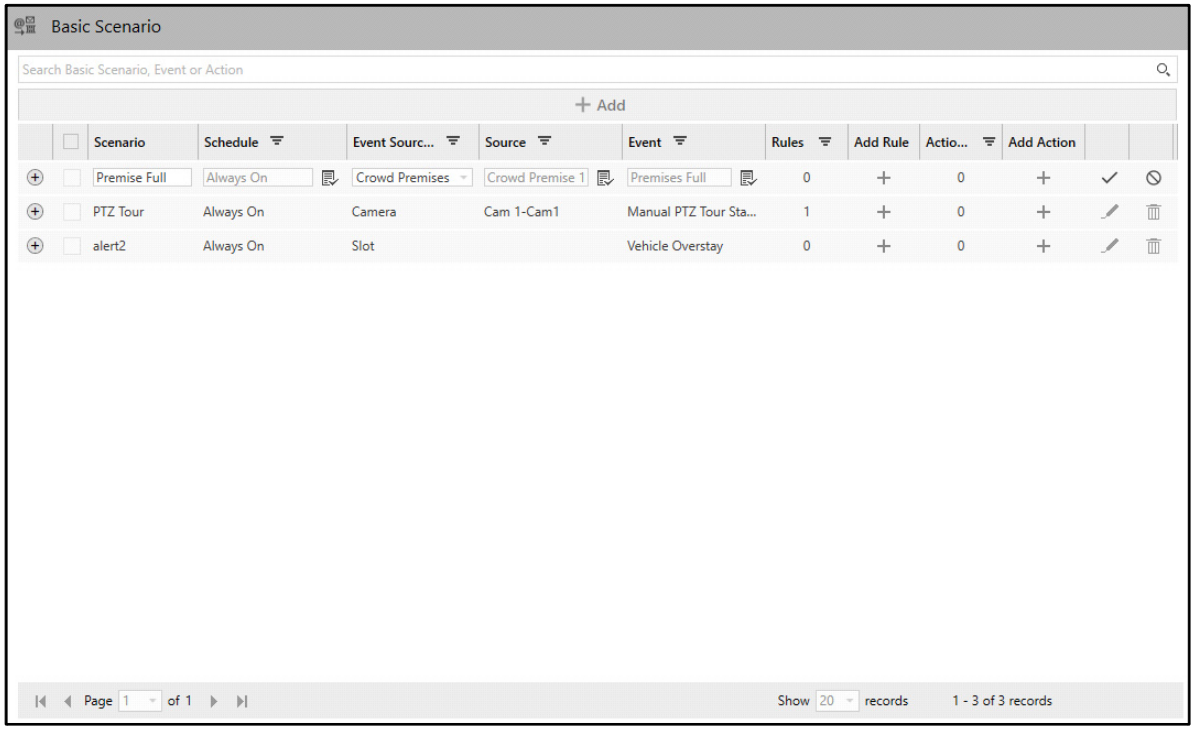


For detailed configuration of Actions, refer to “Configuring Actions for Events”.

Consider the following examples for which you can configure different conditional rules for the Basic Scenario to be executed.

Example 1: Whenever the Hall or Premise is full and reaches its maximum capacity, the Scenario will be executed.

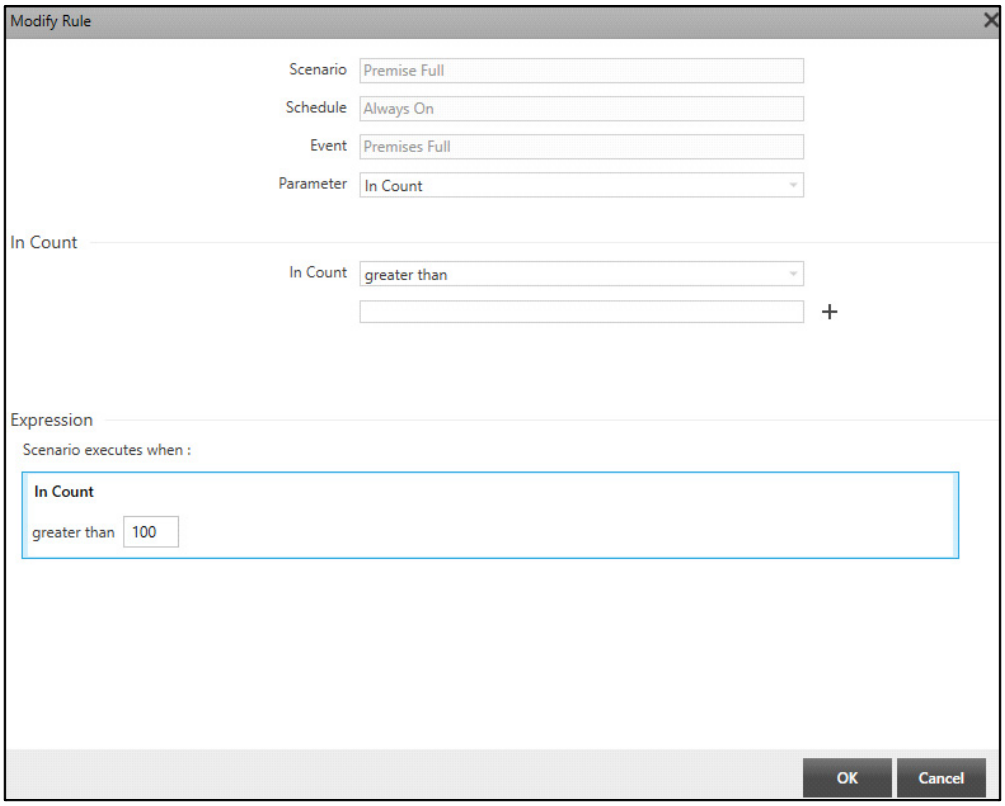
- Configure the Scenario **Premise Full** with the Event Source Type as **Crowd Premise** and the Event **People In**. For detailed Scenario configurations, refer to “Configure Scenarios”.



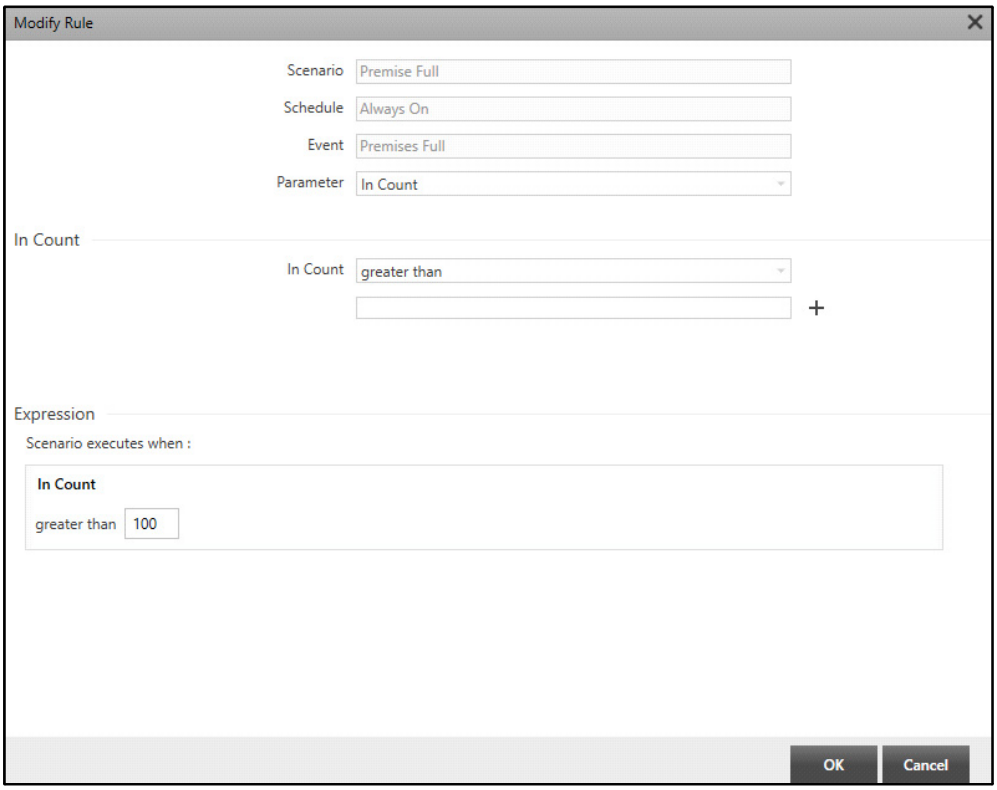
- Click **Save** ✓ to save the Scenario.

  You can also configure the same Scenario from **Crowd Management > Scenarios.**

- Click **Add Rule** + to add the rule for maximum people capacity. Select the Parameter as **In Count**. Select the condition for In Count from the drop-down list as **greater than**. Specify the number of people to define the maximum capacity, that is, 100 in this case. For detailed configuration of Rules, refer to “Add Rule”.



- Click **Add** + . The Expression for the condition with the defined rules appears in the **Expression** section.



- Click **OK**.

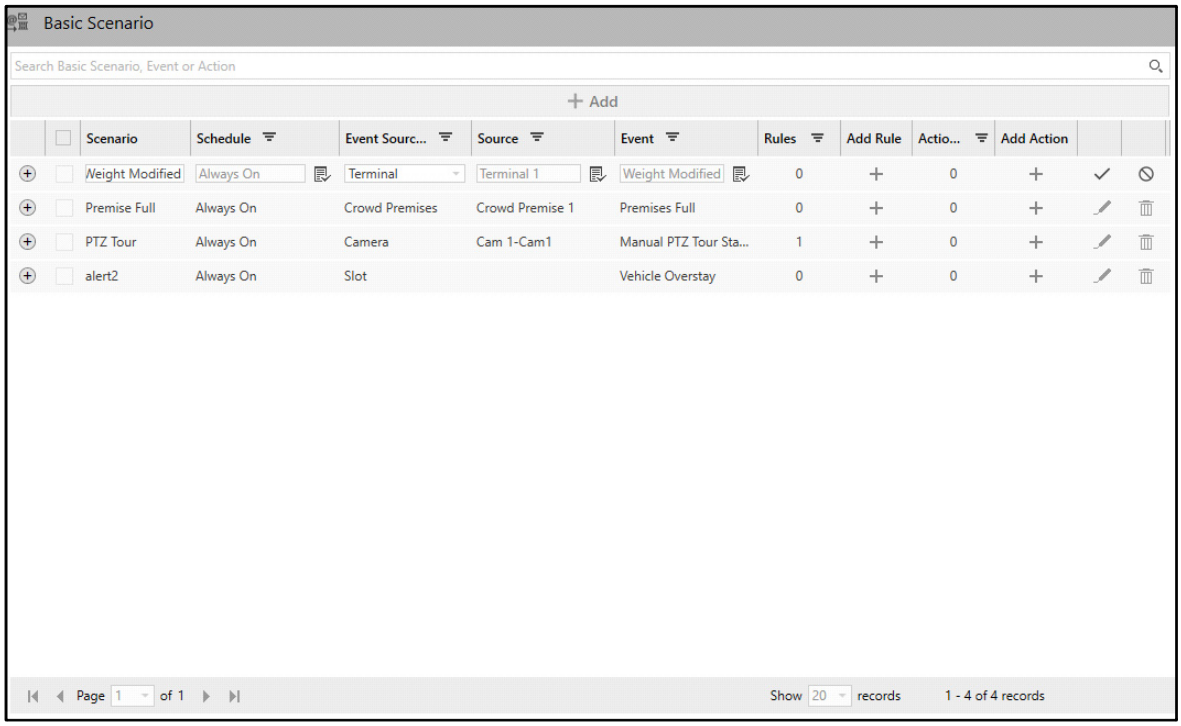
The maximum capacity of people in the premise is 100. The parameter is selected as **In Count** and the condition is selected from the drop-down list as **greater than** with its value 100.

Now, whenever a person entering into the premise is detected under the **People In** Event, Admin Client will check for the total **In Count** whether it has reached 100 or not. Once the total In Count reaches 100 and then a person is detected under **People In** Event, the Scenario will be executed.

You can also add the various actions to be performed with the execution of a Scenario. For example, Trigger Alarm, Open Door, Capture Image etc. To know more about configuring actions, refer to “Configuring Actions for Events”.

Example 2: The Scenario will be executed whenever the detected weight at Weighbridge terminal is modified to be less than 2000 for the old weight which was in between 1900 to 1999.

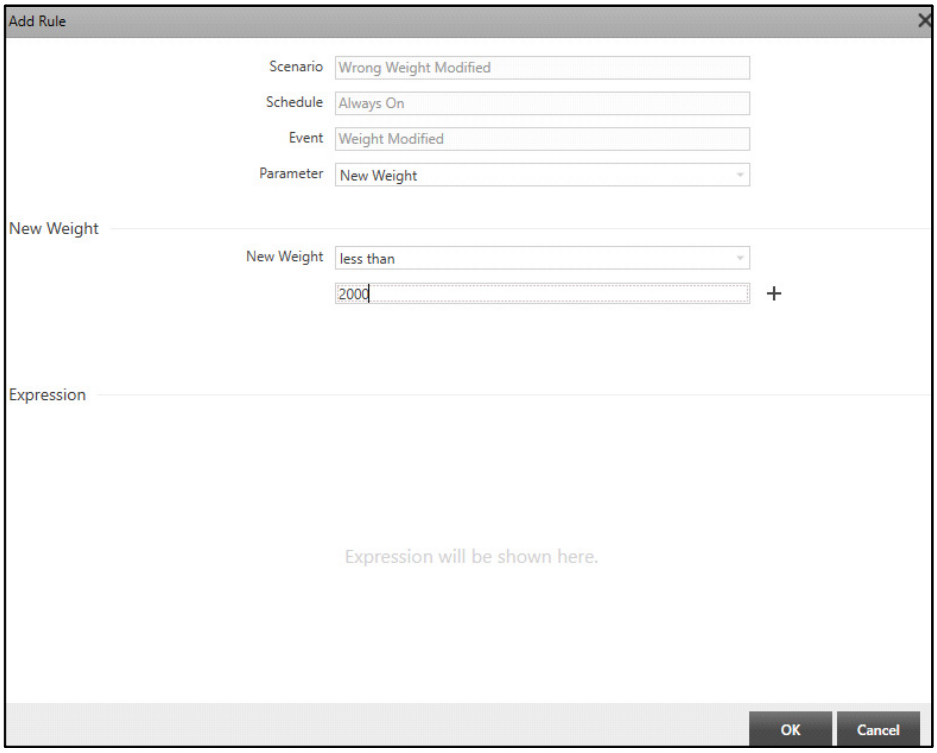
- Configure the Scenario **Wrong Weight Modified** with the Event Source Type as **Terminal** and the Event **Weight Modified**. For detailed Scenario configurations, refer to “Configure Scenarios”.



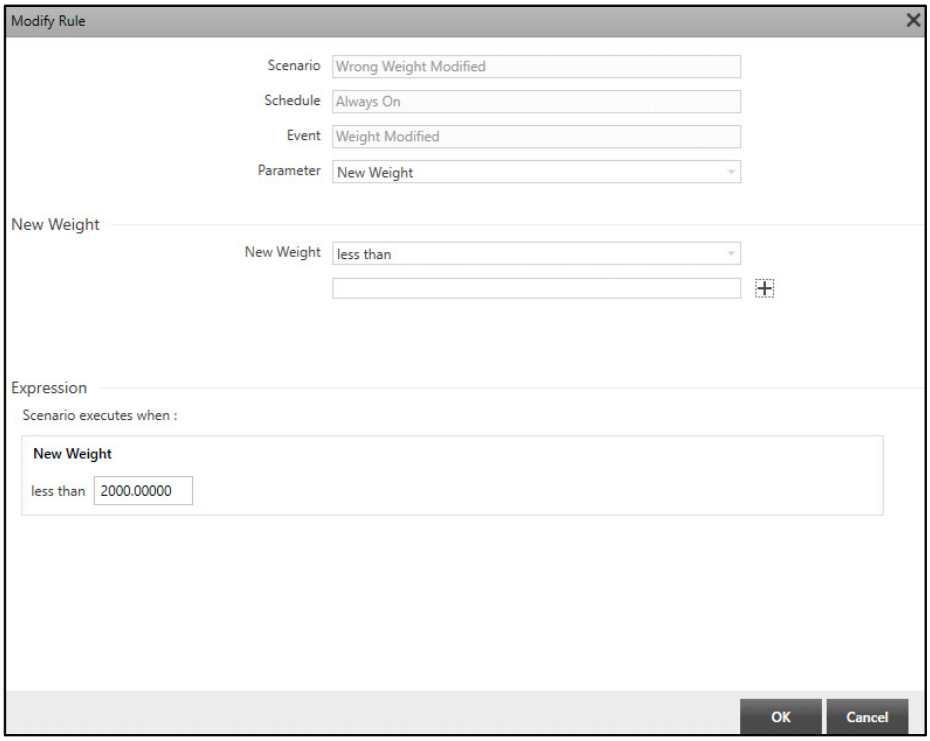
- Click **Save** ✓ to save the Scenario.

  You can also configure the same Scenario from **Weighbridge Application > Scenarios.**

- Click **Add Rule** + to add the rule for modified weight. Select the Parameter as **New Weight**. Select the condition for New Weight from the drop-down list as **less than**. Specify the weight, that is, 2000 in this case. For detailed configuration of Rules, refer to “Add Rule”.

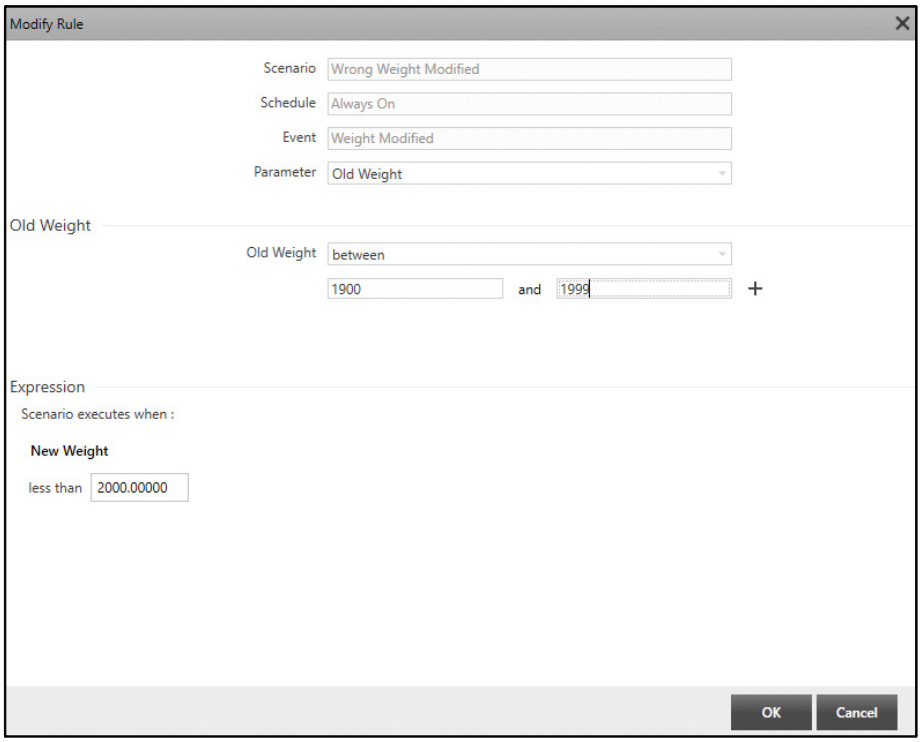


- Click **Add** + . The Expression for the condition with the defined rules appears in the **Expression** section.

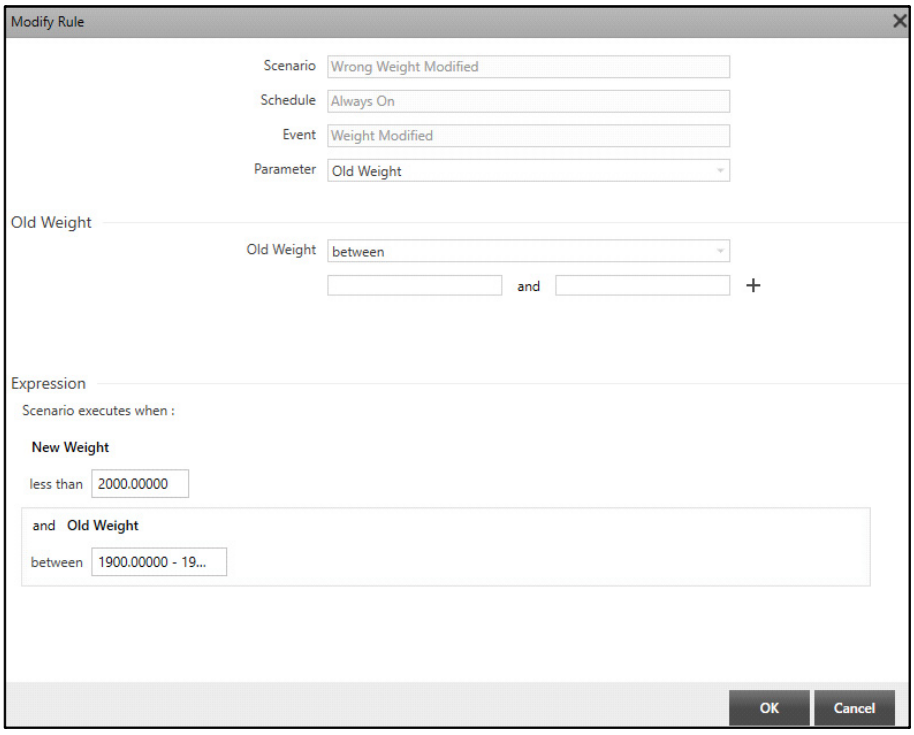


- Click **OK**.

- Click **Add Rule** + to add the second rule for old weight. Select the Parameter as **Old Weight**. Select the condition for Old Weight from the drop-down list as **between**. Specify the weight range, that is, 1900 to 1999 in this case. For detailed configuration of Rules, refer to “Add Rule”.



- Click **Add** + . The Expression for the condition with the defined rules appears in the **Expression** section.



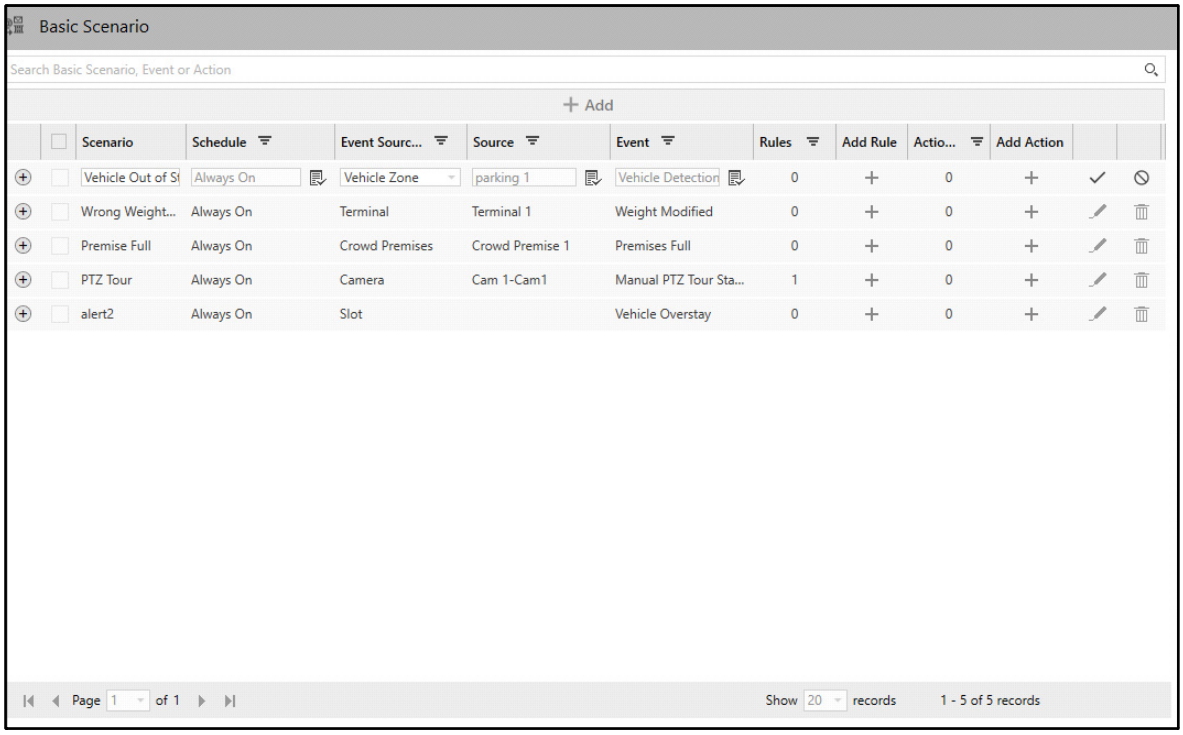
- Click **OK**.

Now, as per the above configured rule, the **Wrong Weight Modified** Scenario will be executed under the **Weight Modified** Event when the **New Modified Weight** is less than 2000 for the **Old Weight** which is in between 1900 to 1999.

You can also add the various actions to be performed with the execution of a Scenario. To know more about configuring actions, refer to “Configuring Actions for Events”.

Example 3: The Scenario will be executed whenever any other state vehicles except Gujarat are detected in the parking premises.

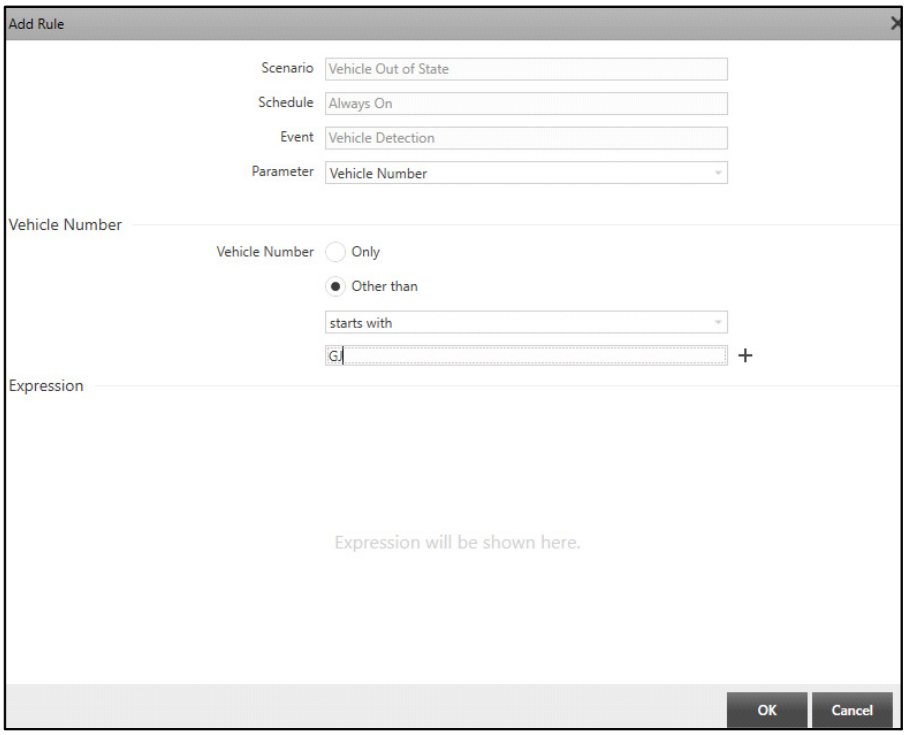
- Configure the Scenario **Vehicle Out of State** with the Event Source Type as **Vehicle Zone** and the Event **Vehicle Detection**. For detailed Scenario configurations, refer to “Configure Scenarios”.



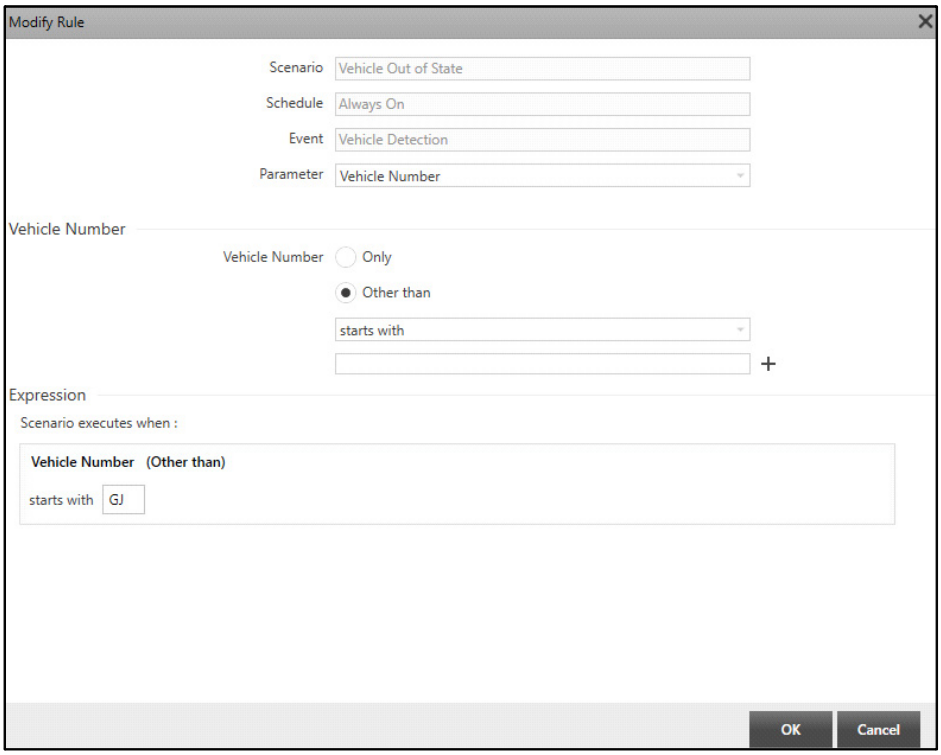
- Click **Save** ✓ to save the Scenario.

  You can also configure the same Scenario from **Vehicle Management > Scenarios.**

  Click **Add Rule** + to add the rule for vehicle detection. Select the Parameter as **Vehicle Number**. Select the condition for Vehicle Number as **Other Than** and **starts with** from the drop-down list. Specify the state code, that is, GJ in this case. For detailed configuration of Rules, refer to “Add Rule”.



- Click **Add** + . The Expression for the condition with the defined rules appears in the **Expression** section.



- Click **OK**.

Now, whenever the vehicles are detected under the **Vehicle Detection** Event, the Admin Client will check for the vehicles whose vehicle number starts with any initials except GJ. If found, the Scenario will be executed.

Advanced Scenario

The Advanced Scenario page displays all the configured Scenarios with their Actions and Events. This page allows you to configure multiple actions against different combinations of Events. You can configure Scenarios wherein you can delay the configured actions for a certain amount of time after Event occurrence using the **Wait** feature. You can also schedule multiple actions to be executed on Event occurrence in a logical manner.

- *Multiple actions (maximum 999 actions) can be configured in a Scenario.*
- *Single Action can be configured for multiple times in a Scenario.*
- *All actions of Scenario will be executed in predefined sequence only.*

*At a time, multiple instances of same Scenario can be generated. One Scenario can be in multiple states, that is, if one instance of Scenario is **Scenario Waiting** then new instance can be started with **Scenario Initiated**.*

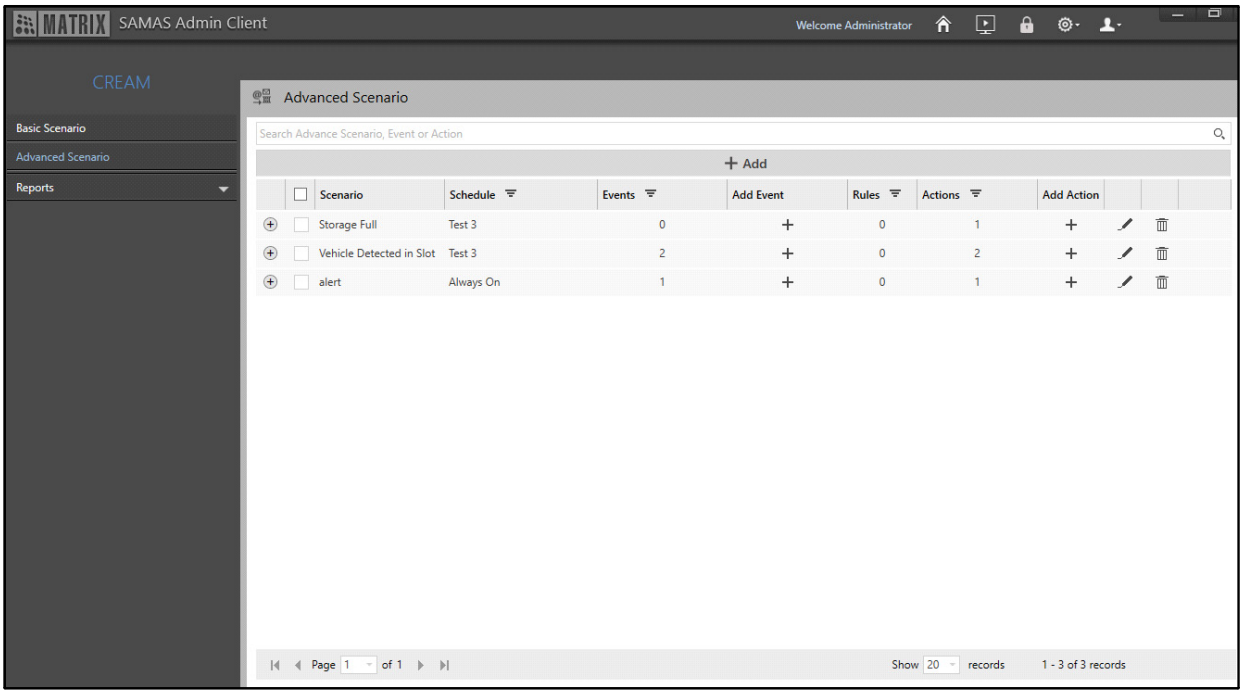
For the Advanced Scenario you must:

- “Configure Scenarios”
- “Add Event”
- “Add Action”

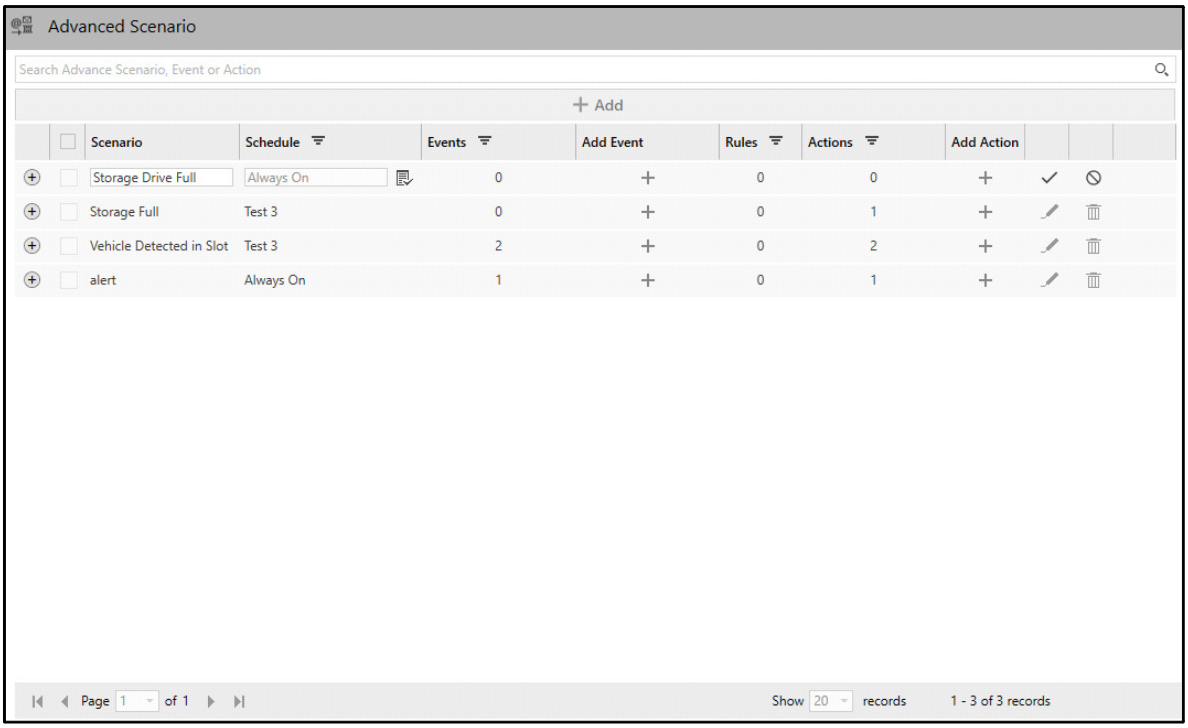
Configure Scenarios

To configure Advanced Scenario,

- Click **CREAM > Advanced Scenario**.



- Click **Add**.

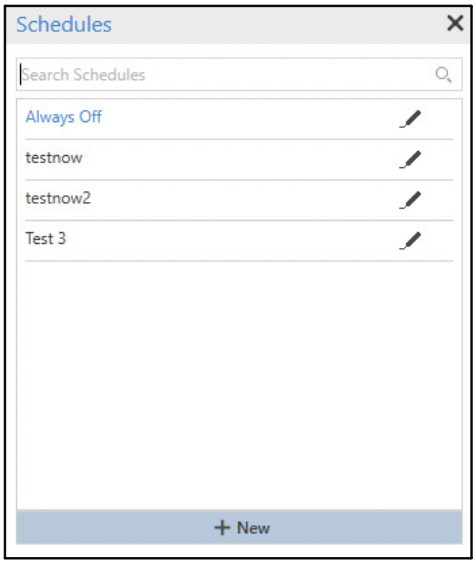


Configure the following parameters:

- **Scenario**: Specify a suitable name for the new Scenario. In Scenario, you can enter upto 100 characters. Default: Blank.

Due to Windows limitation, make sure you do not configure any of the following — CON, PRN, AUX, NUL, COM1 to COM9, LPT1 to LPT9 — as the name of the ***Scenario.***

- **Schedule**: Select the desired Schedule which you wish to assign to the Scenario using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.

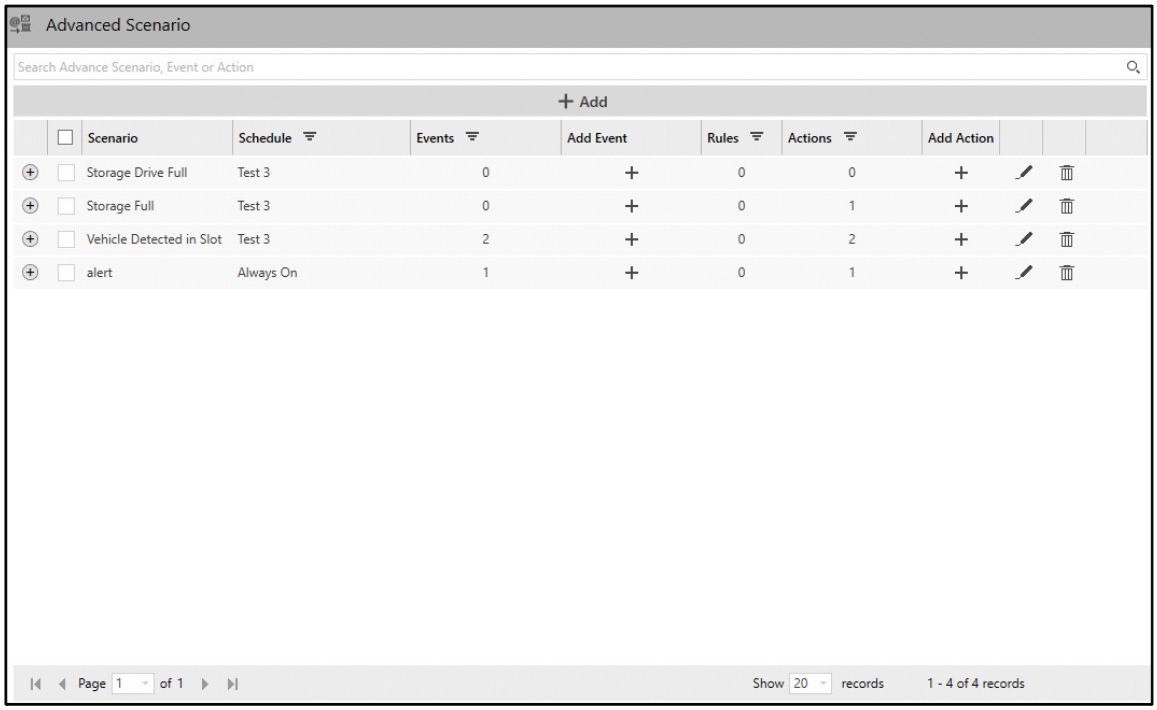


- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- Click **Save** to save the Scenario or click **Cancel** to discard.

The configured Scenario appears in a list.

You can either edit or delete a Scenario.



- Click **Edit** to edit the Scenario configurations.
- Click **Delete** to delete the Scenario.
- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

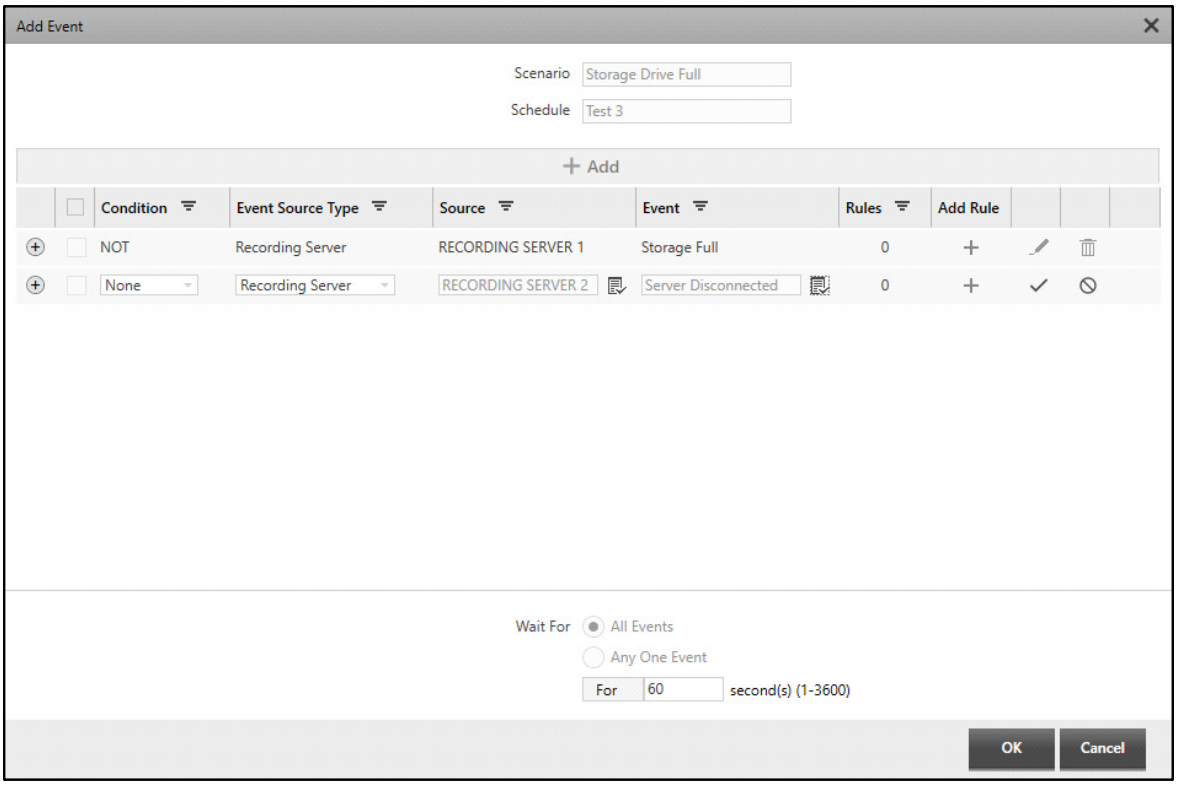
Once a Scenario is configured, you can add an Event and Action to the Scenario.

Add Event

This option allows you to add an Event to the configured Scenario. You can configure multiple Events for the same Scenario.

To add an Event,

- Click **Add Event** + . The **Add Event** pop-up appears.



- Click **Add** to add an Event.

  Configure the following parameters:

  - **Condition**: Select the desired Condition from the drop-down list — None, NOT.

    Select NOT, when you wish that a particular event is not required/should not occur. For example: You wish that the device should not be disconnected, then select NOT in Condition when the corresponding Event selected is Device Disconnected.

    Select None, when you wish that a particular event is required/should occur. For example: You wish that the device should be disconnected, then select None in Condition when the corresponding Event selected is Device Disconnected.

  - **Event Source Type**: Select the type of Event Source for which you wish to configure the Event from the drop-down list.

  - **Source**: Select the Source where the Scenario is to be initiated using the **Source** picklist. The Source depends on the selected Event Source Type. For example, if you select Camera as the Event

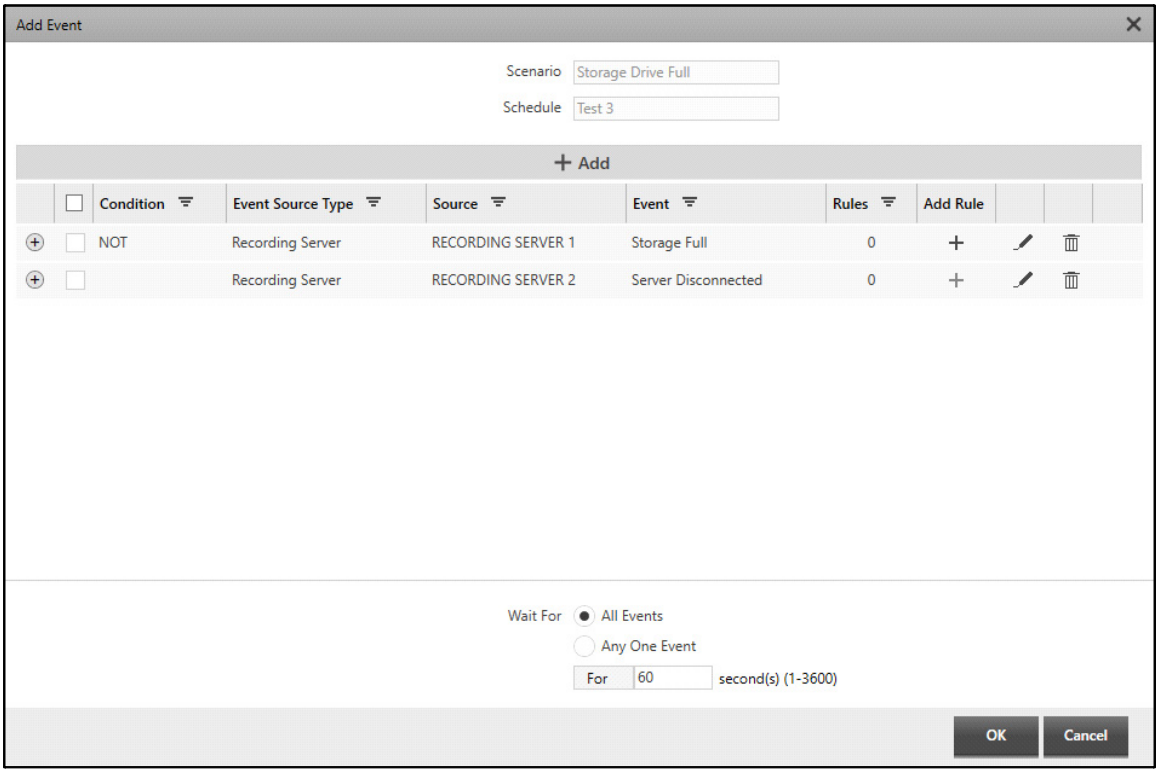
Source Type, a list of all the configured cameras appear in the Source picklist. Double-click to select the desired option.

- **Event**: Select the desired Event for which you wish to configure an Action using the **Event** picklist.The Event depends on the selected Event Source Type and Source. Double-click to select the desired option.
- **Add Rule**: Click **Add Rule** to add Rules. For details, refer to “Add Rule”.

- Click **Save** to save the Event or click **Cancel** to discard.

The configured Event appears in a list.

You can edit the Event parameters or delete the Event.



- Click **Edit** to edit the Event configurations.
- Click **Delete** to delete the Event.

Once you have added two or more Events, the **Wait For** parameter is enabled.

- **Wait For**: Select the desired condition from the options — All Events or Any One Event.

  Select **All Events**, if you wish that the system should wait for the specified time to generate all the Events.

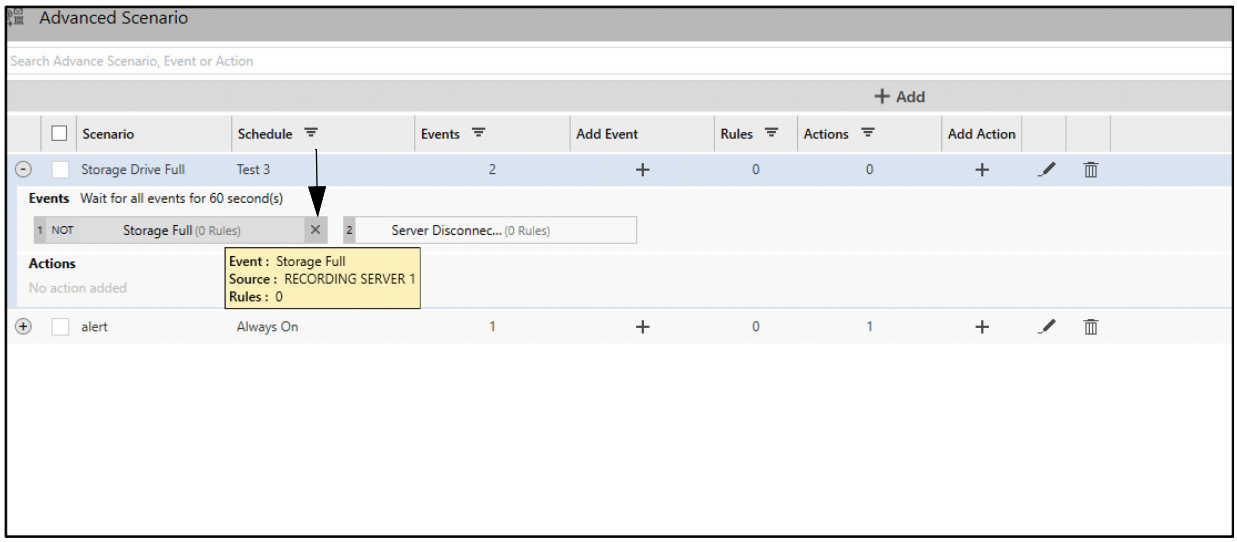
  Select **Any One Event**, if you wish that the system should wait for the specified time to generate any one Event.

After you select the desired condition, specify the time in seconds for which you wish the system to wait before generating the Events. Valid Range: 1 to 3600 seconds. Default: 60.

- Click **OK** to confirm or click **Cancel** to discard the changes.

The configured Event appears in the Scenario details. You can either edit the Event or delete it.

- Click **Show Events & Actions** . The Event details are displayed.
- Hover the cursor over the configured Event. The **Remove** option appears.



- Click **Remove** to remove the Event.

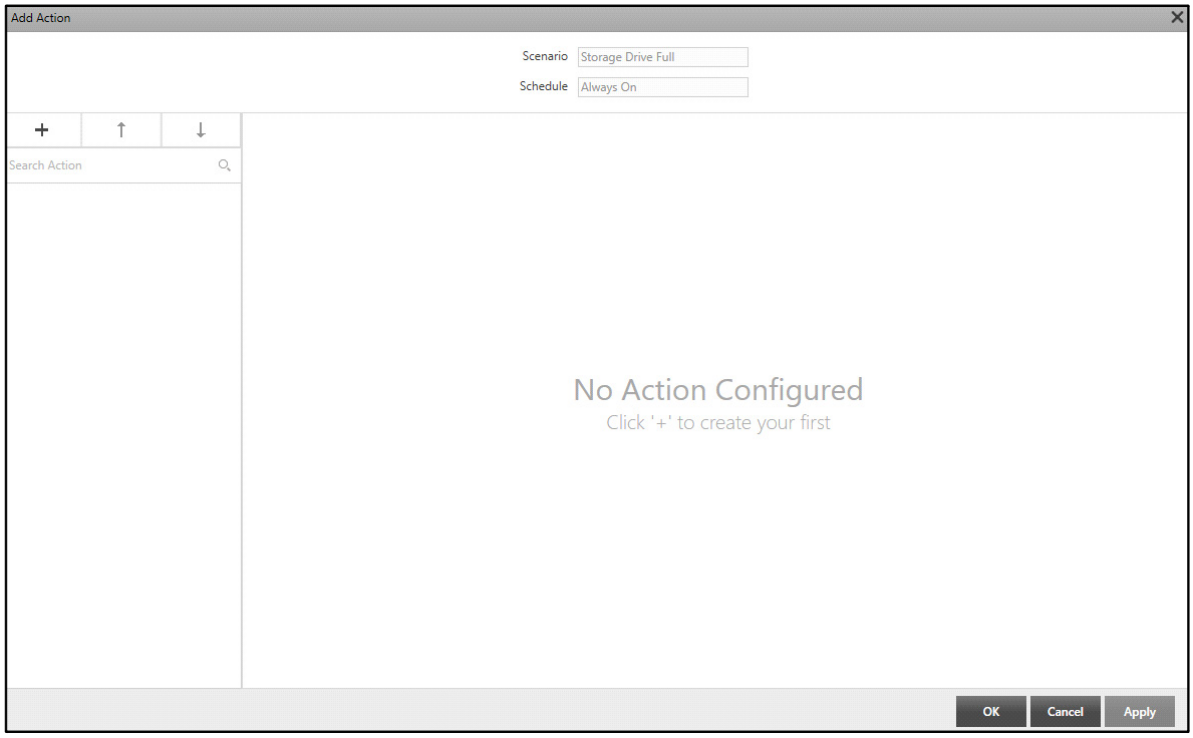
Add Action

This option allows you to add an action to the configured Scenario. You can configure multiple actions for the same Scenario.

The configurable Actions change as per the selected Event. Also, the configurable parameters differ from Action to Action.

To add an Action,

- Click **Add Action** . The **Add Action** pop-up appears.



All the Actions can be configured for Advanced Scenario from CREAM, whereas Module specific actions can be configured from their respective modules too. Refer to the respective module for the details.

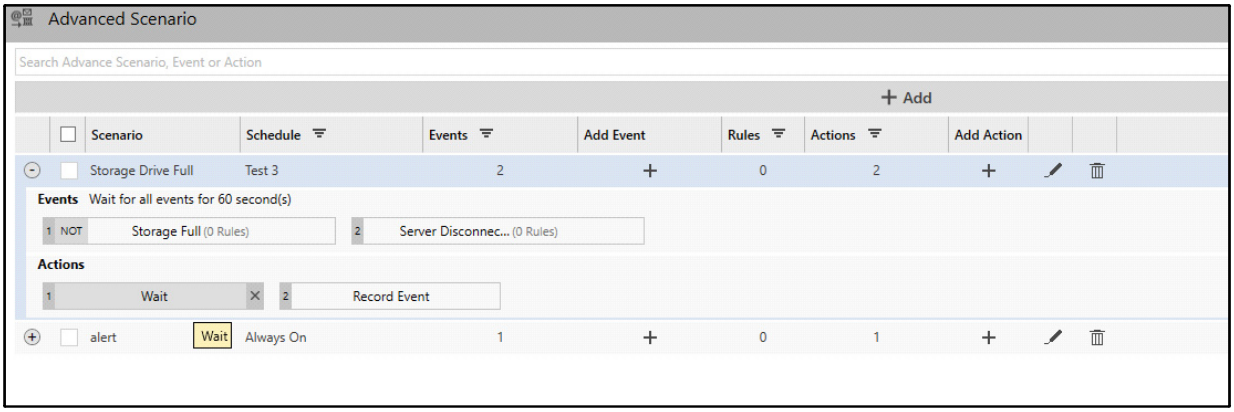
However, for Advanced Scenario you can also configure these additional actions — Import File, Trigger IVA Detection, Wait and Push Notification. For detailed configuration of all Actions, refer to “Configuring Actions for Events”.

*If you wish to add delay before the occurrence of any Event, make sure you select the Action as **Wait** and then select the Event Source Type as **None**.*

The configured Action appears in the Scenario details.

You can either edit the Action or delete it.

- Click **Show Events & Actions** . The Action details are displayed.
- Hover the cursor over the configured Action. The **Remove** option appears.

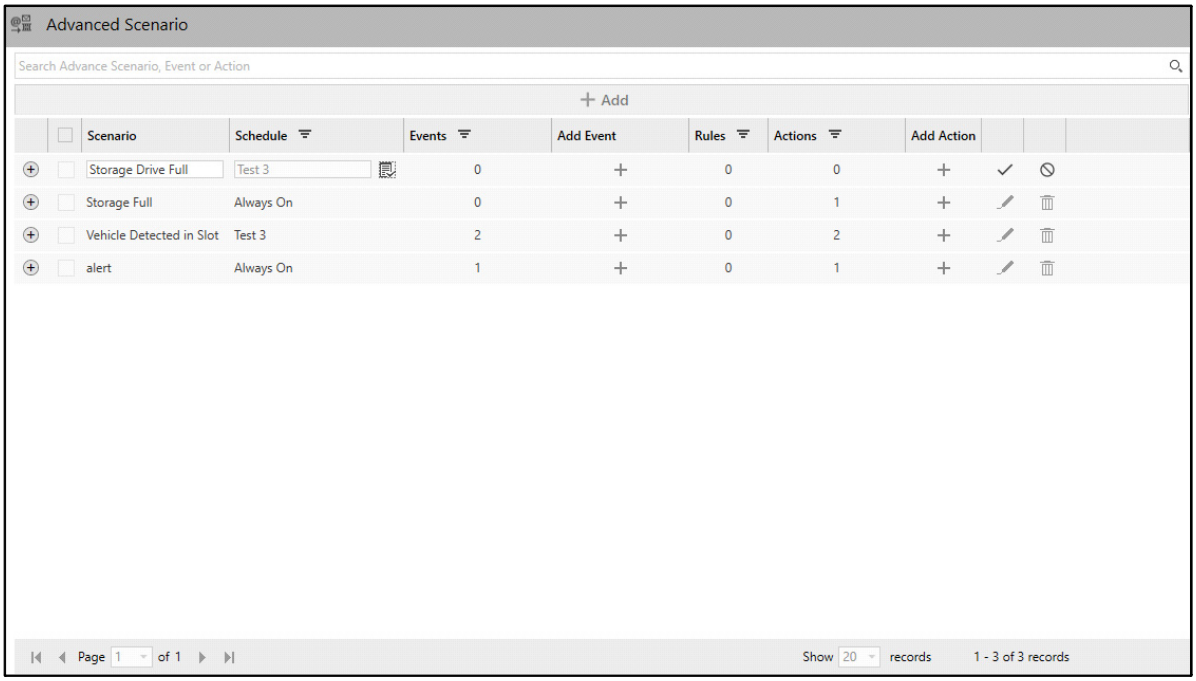


- Click **Remove** ✕ to remove the Action.

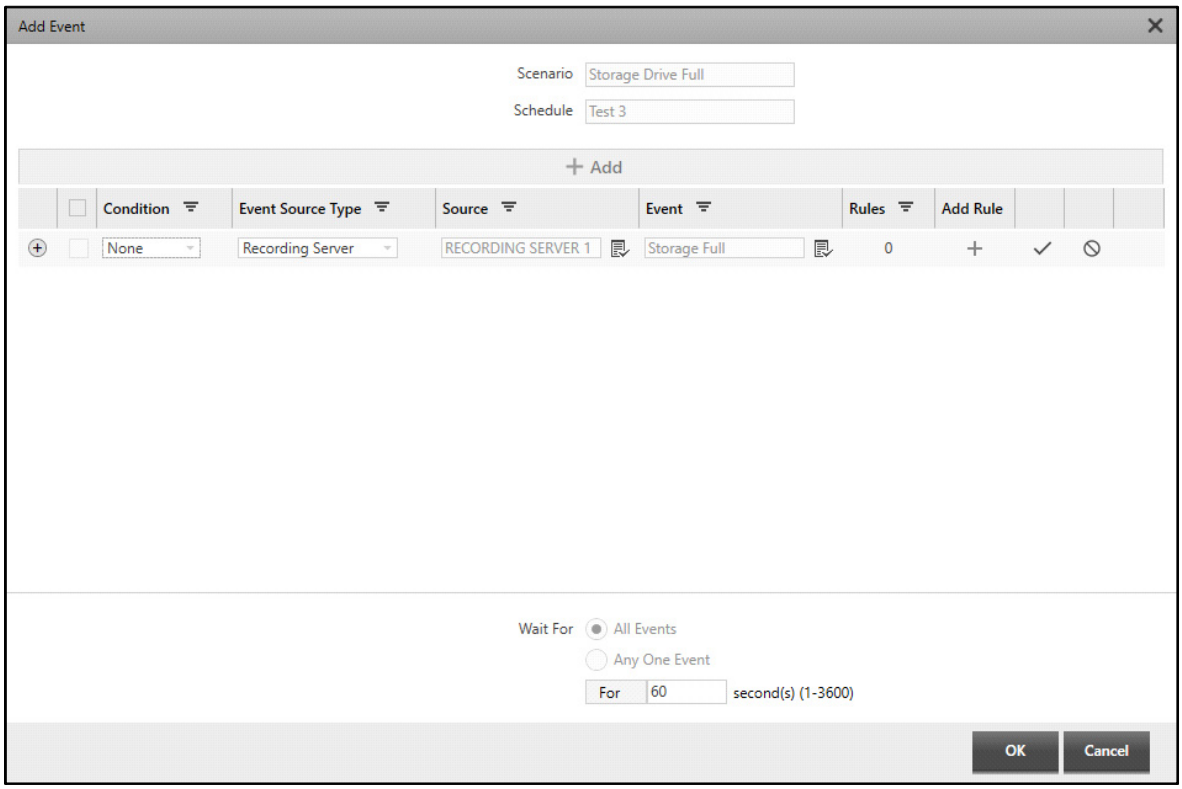
Consider the following examples for which you can configure different Events for the Advanced Scenario to be executed.

Example 1: On Storage Drive Full Event, wait for the Recording Server Storage to be normal, once it is normal, start recording.

- Configure the Scenario **Storage Drive Full**. For detailed Scenario configurations, refer to “Advanced Scenario”.



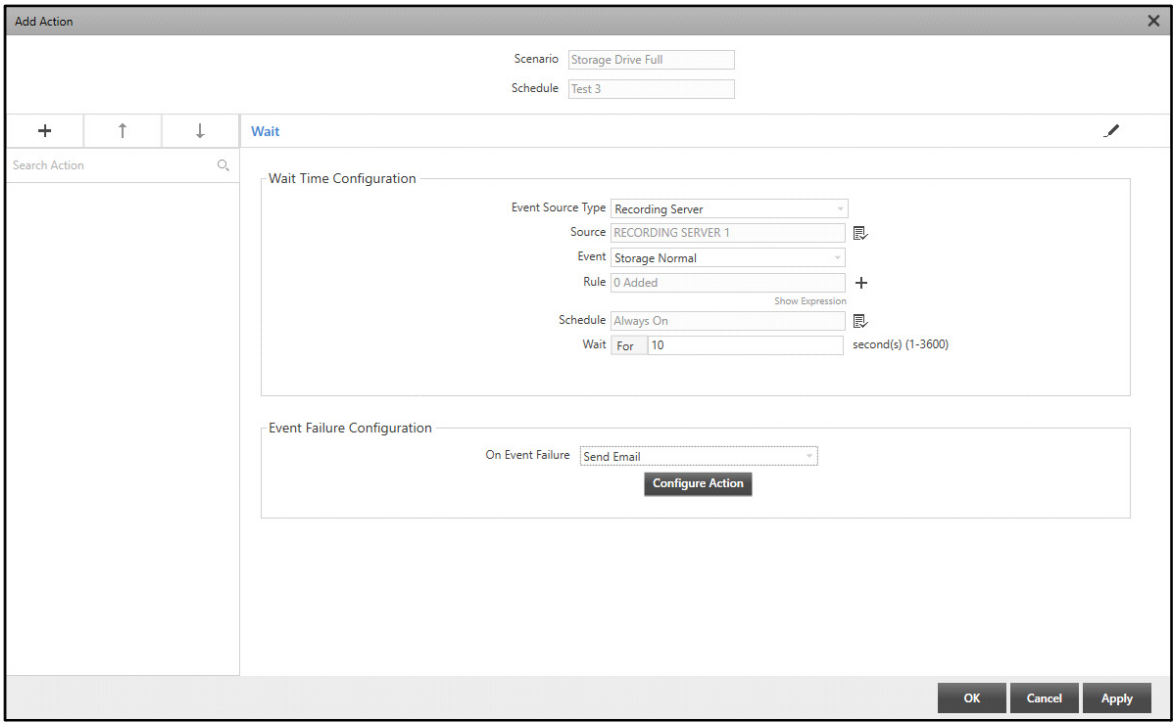
- Click **Save** ✓ to save the Scenario.
- Click **Add Event** ＋. Select the Event Source Type as **Recording Server** and Event as **Storage Full**. For detailed Event configurations, refer to “Add Event”.



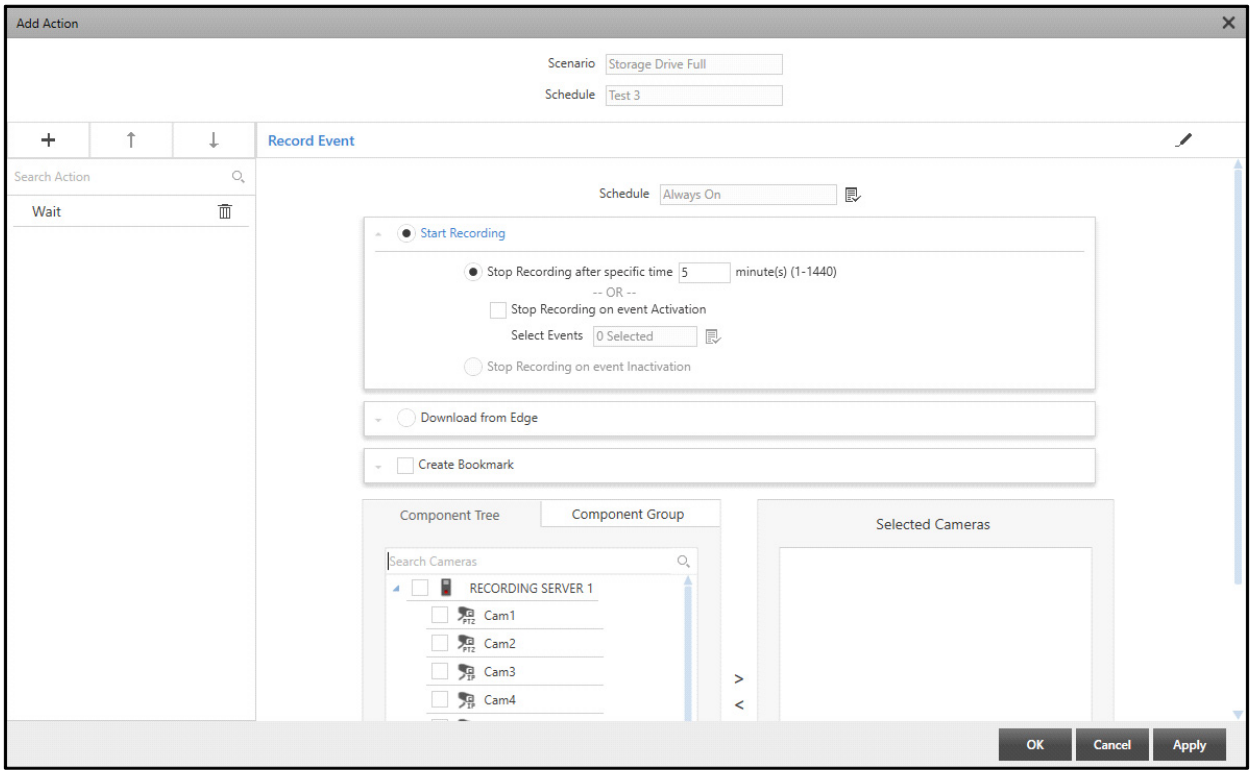
- Click **Save** ✓ to save the Event.

Once this Event is configured, you need to add two actions — **Wait** and **Record Event**.

- Click **Add Action** ＋. Select the **Wait** Action from the list. Select the Event Source Type as **Recording Server** and Event as **Storage Normal**. For detailed configurations of Action, refer to “Wait”.



- Click **Apply** and **OK** to save the settings.
- Click **Add Action** + . Select the **Record Event** Action from the list. For detailed configurations of Action, refer to “Record Event”.

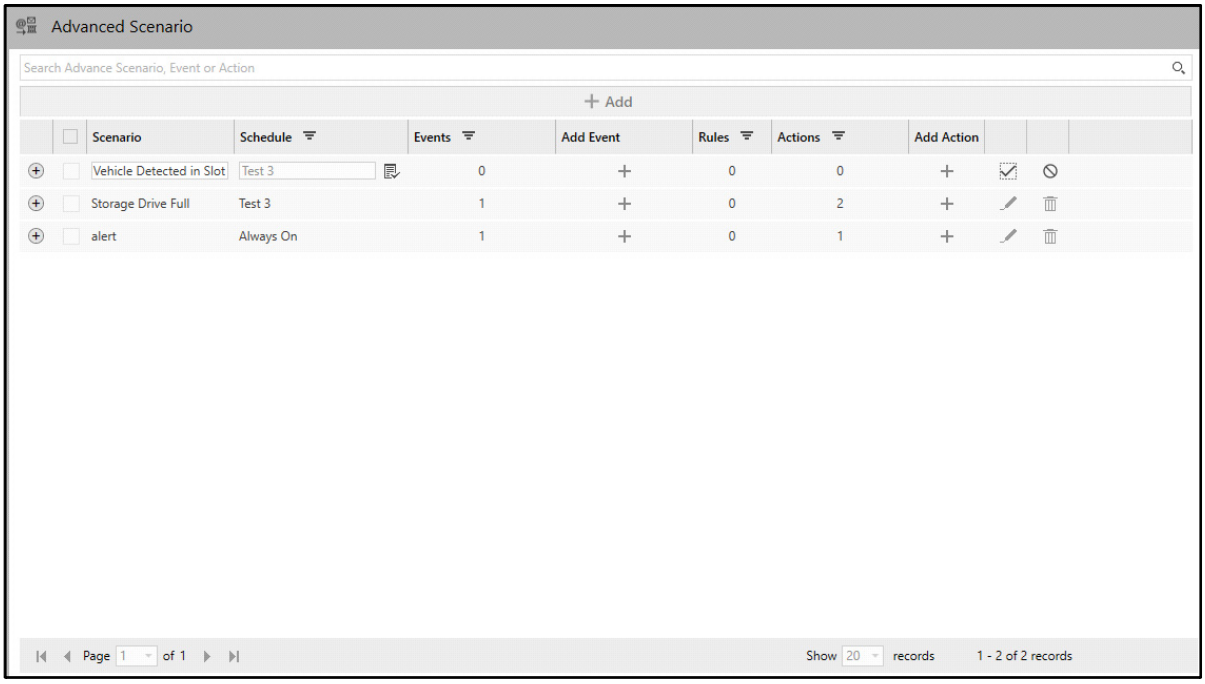


- Click **Apply** and **OK** to save the settings.

Now, whenever the storage of the configured Recording Server is full, the system will detect it. The system will wait for the Recording Server storage to be normal as per the **Wait** action. Once the Recording Server storage is normal, the **Record Event** action will be triggered.

Example 2: When the slot is occupied and Vehicle is detected, Capture Image and start Live View on Event.

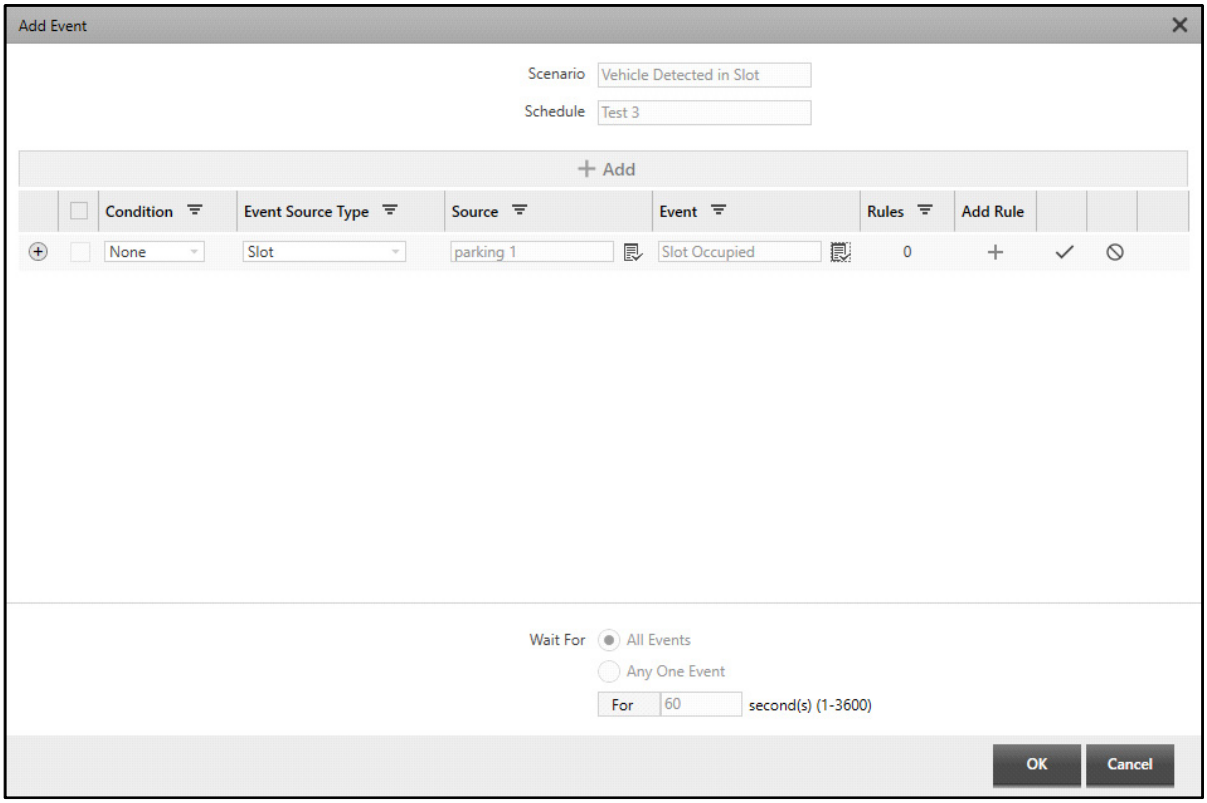
- Configure the Scenario **Vehicle Detected in Slot**. For detailed Scenario configurations, refer to “Advanced Scenario”.



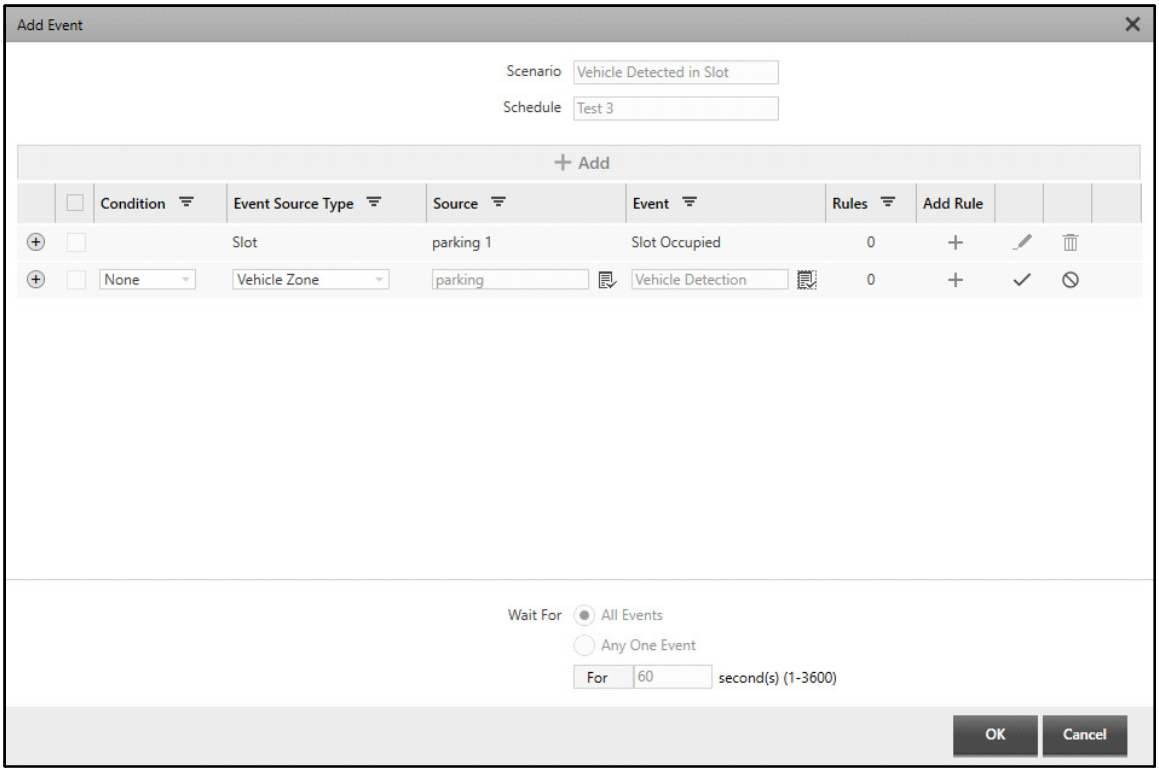
- Click **Save** ✓ to save the Scenario.

Once the Scenario is saved, you need to add two Events — **Slot Occupied** and **Vehicle Detection**.

- Click **Add Event** ＋. Select the Event Source Type as **Slot** and Event as **Slot Occupied**. For detailed Event configurations, refer to “Add Event”.



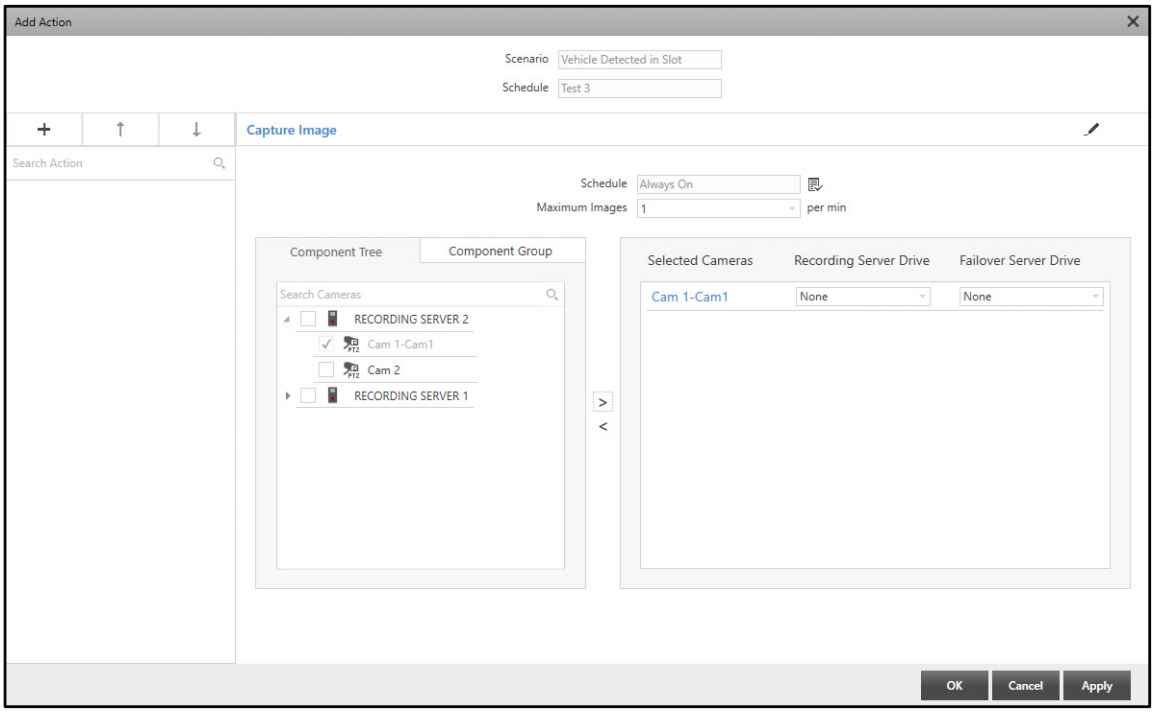
- Click **Save** ✓ to save the Event.
- Click **Add Event** + . Select the Event Source Type as **Vehicle Zone** and Event as **Vehicle Detection**. For detailed Event configurations, refer to “Add Event”.



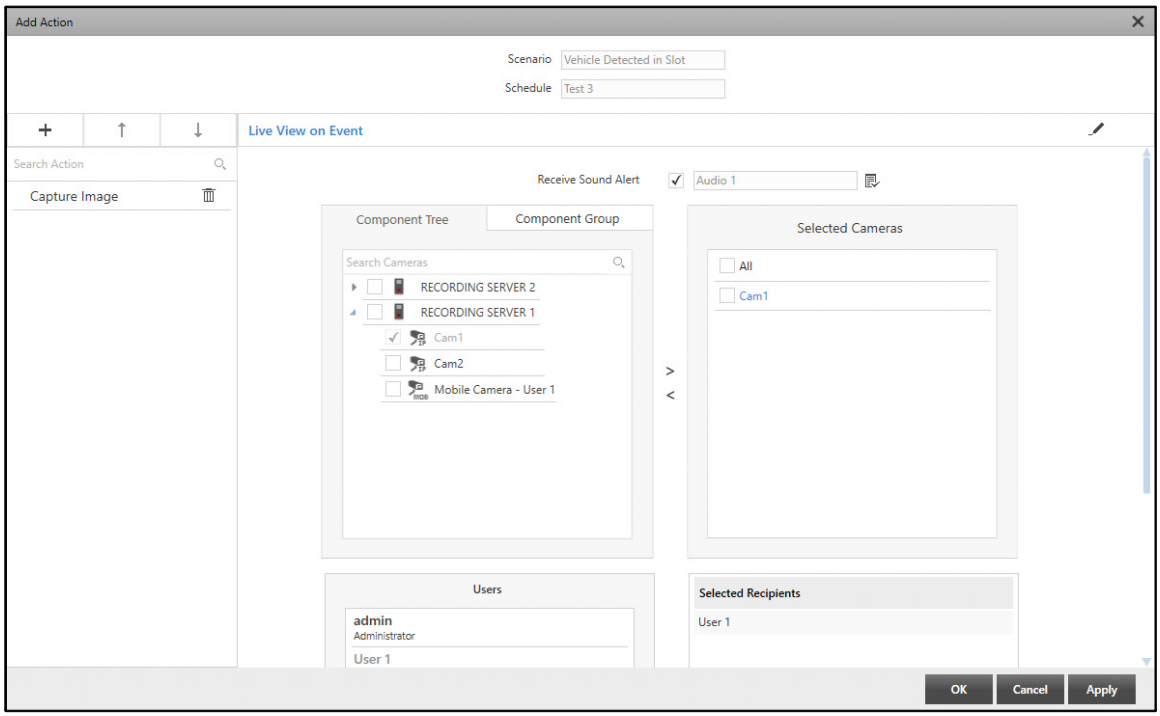
- Click **Save** ✓ to save the Event.

Once these Events are configured, you need to add two actions — **Capture Image** and **Live View on Event**.

- Click **Add Action** + . Select the **Capture Image** Action from the list. For detailed configurations of Action, refer to “Capture Image”.



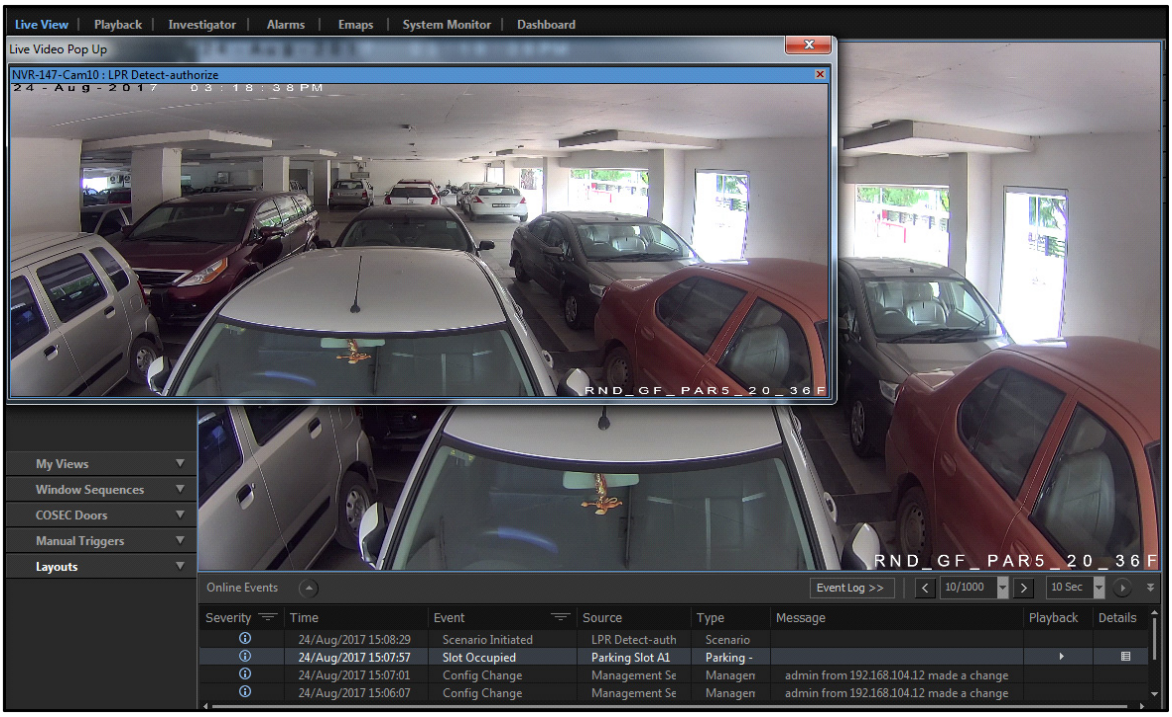
- Click **Apply** and **OK** to save the settings.
- Click **Add Action.** + . Select the **Live View on Event** Action from the list. For detailed configurations of Action, refer to “Live View on Event”.



- Click **Apply** and **OK** to save the settings.

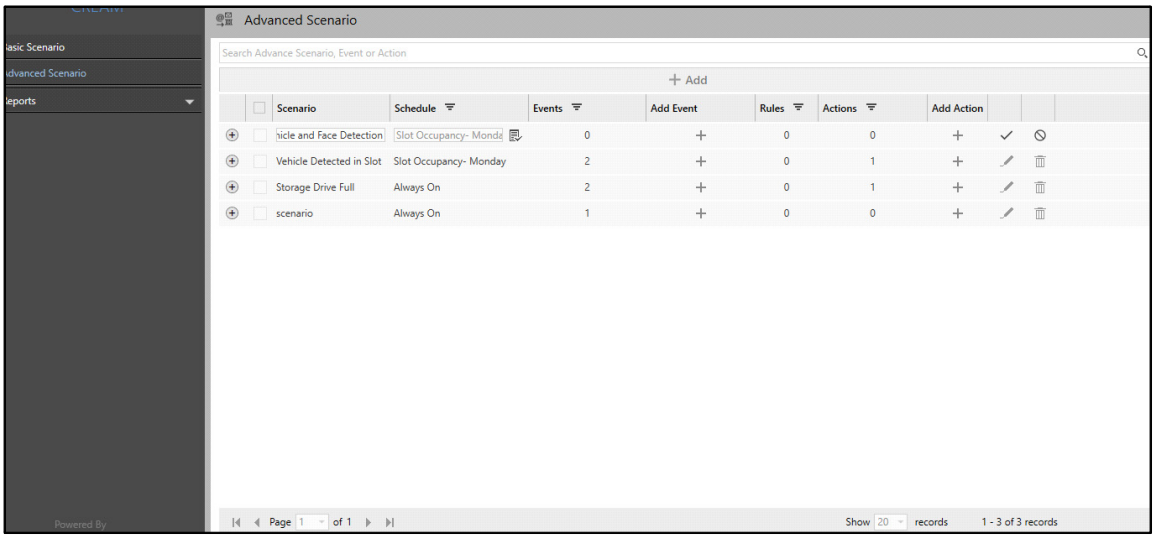
Now, whenever a vehicle is detected in the slot, the Scenario is executed. When two Events are configured for a Scenario, the system will either Wait for any one Event or for both the Events to occur for the specified time. Once the Events are generated, the actions, **Capture Image** and **Live View on Event** are triggered.

When the Scenario is executed, it is shown in Online Events in Smart Client as shown below:



Example 3: When a vehicle is detected, send SMS to the user, wait for 10 seconds for Face Detection and Open Door. If the face is not detected within 10 seconds, Trigger Device Alarm.

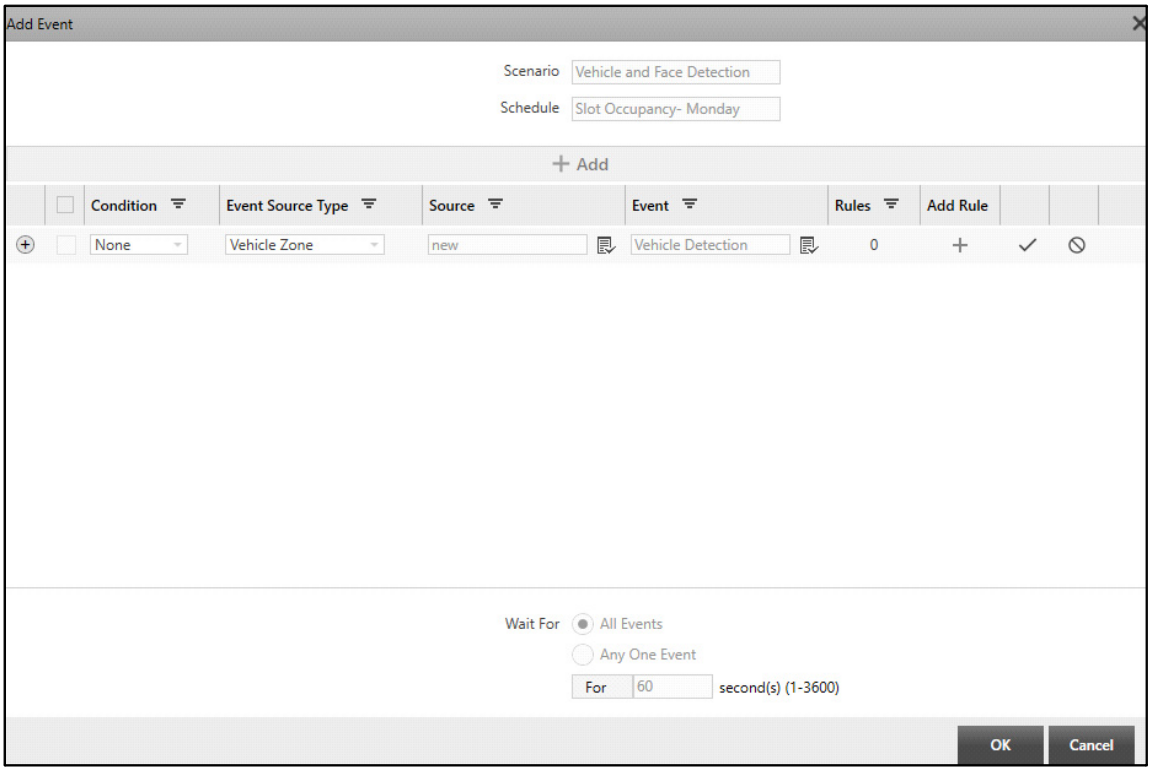
- Configure the Scenario **Vehicle and Face Detection**. For detailed Scenario configurations, refer to "Advanced Scenario".



- Click **Save** ✓ to save the Scenario.

Once the Scenario is saved, you need to add **Vehicle Detection** Event.

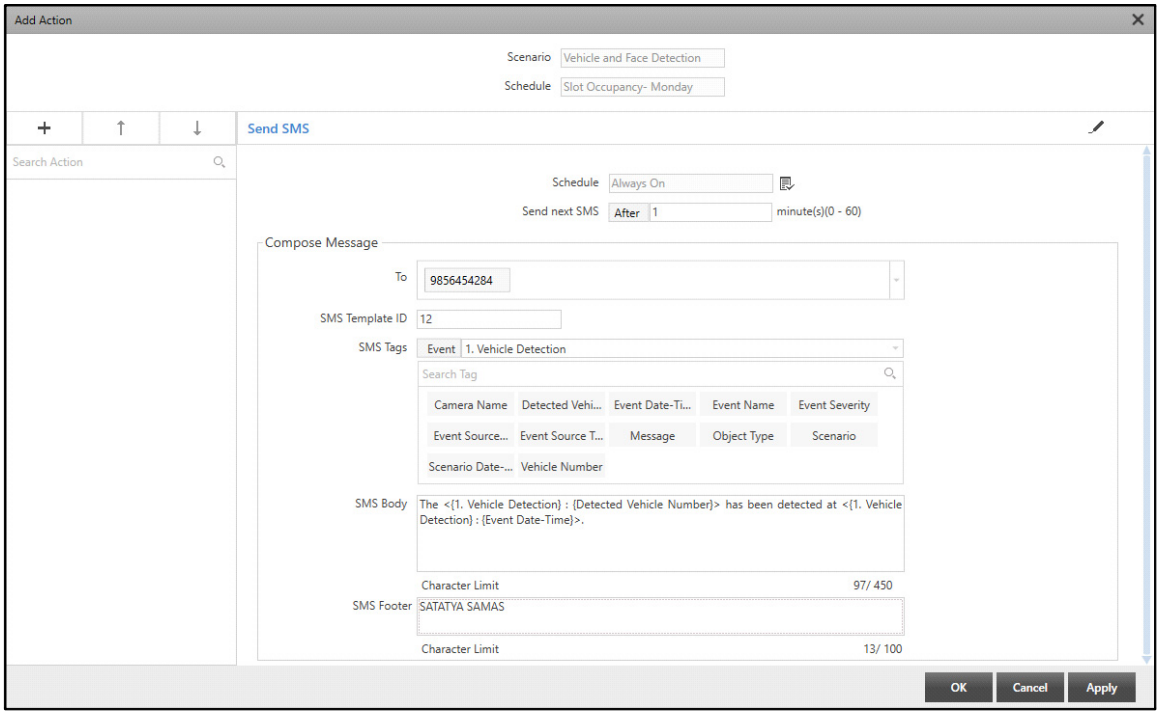
- Click **Add Event** + . Select the Event Source Type as **Vehicle Zone** and Event as **Vehicle Detection**. For detailed Event configurations, refer to “Add Event”.



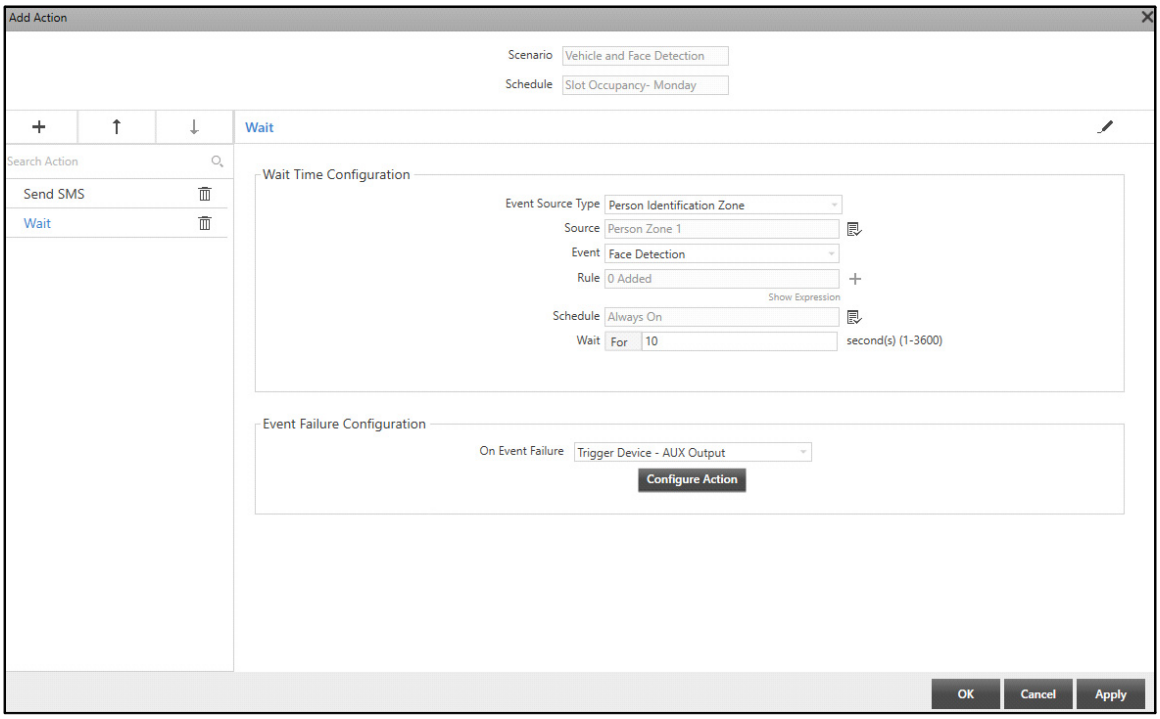
- Click **Save** ✓ to save the Event.

Once these Events are configured, you need to add two actions — **Send SMS** and **Wait**.

- Click **Add Action** + . Select the **Send SMS** Action from the list. For detailed configurations of Action, refer to “Send SMS”.



- Click **Apply** and **OK** to save the settings.
- Click **Add Action** . Select the **Wait** Action from the list. Select the Event Source Type as **Person Identification Zone** and Event as **Face Detection**. Select the Action as **Trigger Device- AUX Output** for On Event Failure. For detailed configurations of Action, refer to “Wait”.



- Click **Apply** and **OK** to save the settings.

Now, whenever a vehicle is detected in the Vehicle Zone, the Scenario is executed. The system will send SMS to the User you have selected as recipient in the Action. Then the system will trigger Wait Action, wherein the system will wait for Face Detection Event for the specified time period. If the Event is not detected within the specified time period, the system will Trigger Device Alarm.

Push Notification

Push Notification feature enables you to send Push Notifications on SATATYA VISION for the Scenarios for which the Push Notification action is configured.

Firebase Cloud Messaging (FCM)

Firebase Cloud Messaging (commonly referred to as FCM) is a platform notification service created by Google LLC that enables third party application developers to send notification data to their applications installed on Android/ iOS devices. Previously, applications needed to maintain a persistent connection in order to receive calls/ notifications. Keeping a connection open in the background, drains the battery as well as causes all kinds of problems when the application crashes or is terminated by users.

From Android 8.0 onwards, OS identifies an idle application, when the user is not actively using it and puts it in the App Standby mode. In this mode, OS prevents the application to access the network and limits its background execution. This is done to optimize battery usage by the application. Google has recommended using FCM in order to wake up the application on the end-user device in order to provide necessary notifications to it.

From iOS 8 onwards, Apple has removed the support of application functionalities that maintain a persistent connection with the Server in the background mode. The only way to reach to client is PUSH Notification through Apple PUSH Notification Service (APNS) or the Firebase Cloud Messaging (FCM) Server.

Firebase Cloud Messaging (FCM) is a cross-platform service that handles the sending, routing, and queuing of messages between Application Servers (SATATYA SAMAS) and Mobile Client Apps (SATATYA VISION).

It acts as an intermediary between message sender and clients. An android/iOS App is an FCM-enabled app that runs on a device. The Server is the FCM-enabled server that communicates with android/iOS app through FCM. Using FCM, Servers can send notifications to their apps running in background or exit modes on end-user devices.

SAMAS will use FCM token for Push Notifications. Push Notification action can be configured for any event by creating scenario for that event. When scenario will get executed then MS will send Push Notification to applicable client users.

Configuration for Push Notification

To Send Push Notifications to users, make sure you have:

- Persistent Internet Connectivity to receive Push Notifications on Mobile Client.
- Enabled the **Mobile Client** check box under “Application Rights” to assign Mobile Client rights to the selected User Group.
- Enabled the **Push Notification** check box under “Media Rights” to assign Push Notification rights and other required check boxes to assign the rights for parameters in Smart Client to the selected User Group.
- Enabled the required check boxes under “Configuration Rights”, “Entity Rights”, “Event Monitoring Rights” and “Report Rights” to assign the rights for desired modules, entities, Events and reports to the selected User Group.
- “Vision GUID Authorization” requests are approved for the selected Users.

- Configured the “Basic Scenario” or “Advanced Scenario” as required for the desired Events. For the Basic/ Advanced Scenario, you must configure the “Push Notification” action.

Push Video/Snapshot

Push Video/Snapshot feature enables you to send either live streaming or snapshots of a mobile camera from SATATYA VISION (Mobile Client) to the Recording Server at a time. This is useful in emergency situations, where security personnel, employees or other staff members can quickly share the live incident by capturing it on their mobile phone to SAMAS. In this manner, real-time information can be passed on to the surveillance system, which can also be stored as an evidence.

To use the Push Video/Snapshot feature, it is mandatory to grant the following permissions to the SATATYA VISION:

- Location Permission
- Storage Permission
- Camera Access Permission

When the user is capturing Video using SATATYA VISION, make sure the mobile screen is in Landscape mode, if you wish to configure IVA Events later from the Smart Client.

When the user is capturing Video/Snapshot using SATATYA VISION, it will be stored in the phone's local storage according to the Storage Permissions granted to SATATYA VISION. Thus, the user can either push live video/ snapshot instantly to the Recording Server. When the Mobile Client starts pushing data, the Recording Server starts storing the data in the configured Storage Drives. This is mapped according to the **Allow Push Data** configurations of the user.

You can configure all the IVA Events for Push Video received through Mobile Camera from the respective module or from the Investigator tab in Smart Client. To configure through Investigator tab in Smart Client, make sure the desired Events are enabled in "Detection Through Investigator".

Let us understand this with the help of an example.

Consider the following **Allow Push Data** configuration for User 1:

- **Camera Name**: Mobile Camera- User 1
- **Recording Server**: Recording Server 1
- **Failover Server**: Failover Server 1

The **Mobile Camera- User 1** will be added to the **Recording Server 1**. Also, the Recording Server 1 has one **Local Storage Drive** configured.

Now, when the video/snapshot is pushed from the Mobile Client by User 1, it will be stored in the Local Storage Drive configured in Recording Server 1 against the Mobile Camera- User 1. This video can be viewed from the Playback page in Smart Client whereas the Snapshot can be viewed from Alert pop-up, if configured. The Playback recording will be displayed with a yellow timeline to distinguish the Pushed Video from other recording. The Events will be visible in Event Log.

Configuration for Push Video/Snapshot

To be able to Push Video/Snapshot from Mobile Client, make sure you have:

- Make sure the connection between Mobile Client and Recording Server is persistent.
- **Mobile Camera Port** is configured in Recording Server Manager. For details, refer to **SATATYA SAMAS Installation Guide**.

- Enabled the **Mobile Client** check box under “Application Rights” to assign Mobile Client rights to the selected User Group.
- Enabled the required check boxes under “Configuration Rights”, “Entity Rights”, “Event Monitoring Rights” and “Report Rights” to assign the rights for desired modules, entities, Events and reports to the selected User Group.
- “Vision GUID Authorization” requests are approved for the selected Users.
- **Allow Push Video** is configured for the desired User. For details, refer to “Users”.
- Required “Recording” and “Backup” configurations are done for the **Mobile Camera**.
- Required “Detection Through Investigator” events are configured for the **Mobile Camera** to detect the events via Investigator in Smart Client.
- Configured the “Basic Scenario” or “Advanced Scenario” as required for the Events — Push Video Started, Push Video Stopped, Push Snapshot. Make sure you have assigned the “Event Monitoring Rights” for these Events. For the Basic/Advanced Scenario, you must configure the desired actions to be notified about the Push Video/Snapshot event. For details, refer to “Configuring Actions for Events”.

  If you wish to notify Mobile Client users, you must configure the “Push Notification” action for the configured Basic/Advanced Scenario.

CREAM - Report

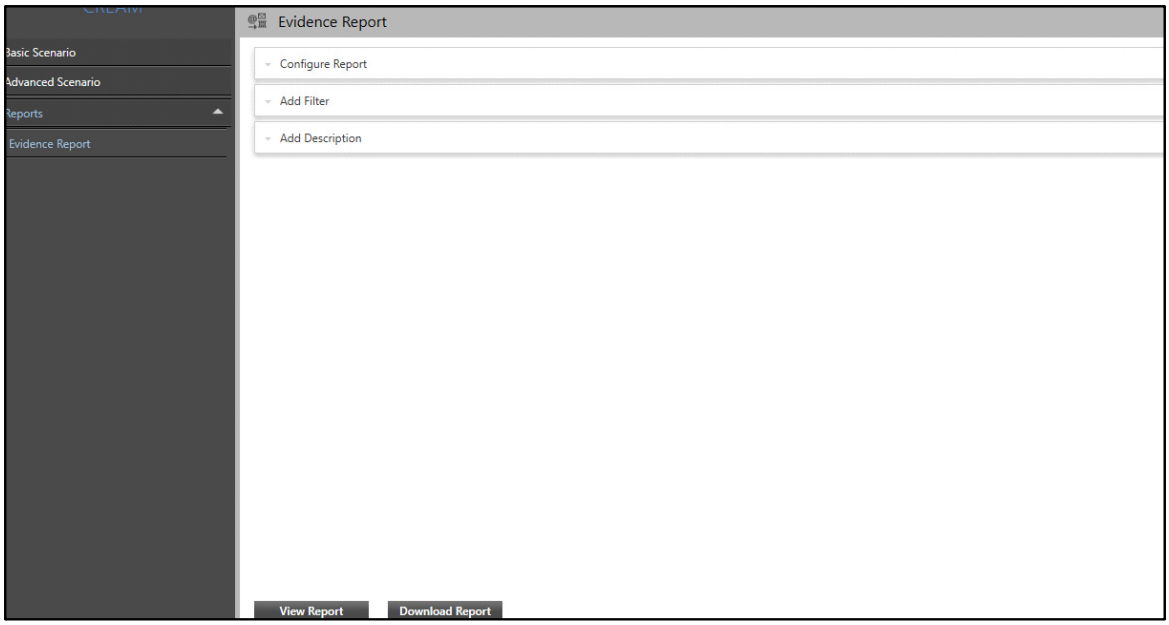
Evidence Report

The Evidence report contains data that is imported from third party application and linked with the Admin Client data. These reports can be presented to the higher authorities as proof whenever required. For example, a third party application data is imported in Admin Client custom database and **Capture Snapshot** action is triggered at the time of the Event. Now, an Admin Client user can link the captured snapshots from assigned cameras and input data in custom table and generate the report.

The Evidence Report page enables you to configure parameters for Evidence Reports. You can view and configure **Daily** or **Hourly** reports with captured images.

To configure Evidence Reports,

- Click **CREAM > Reports > Evidence Report**.



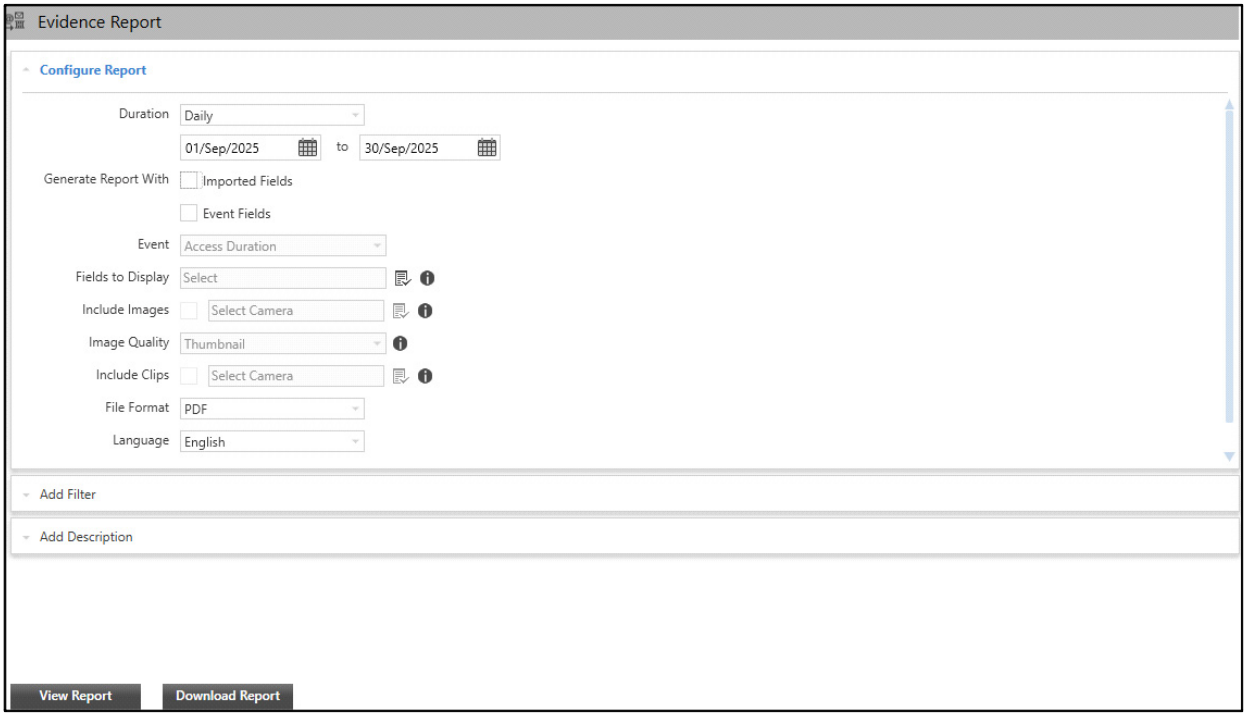
The Evidence Report page contains three collapsible panels — “Configure Report”, “Add Filter” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Evidence Report from this collapsible panel.

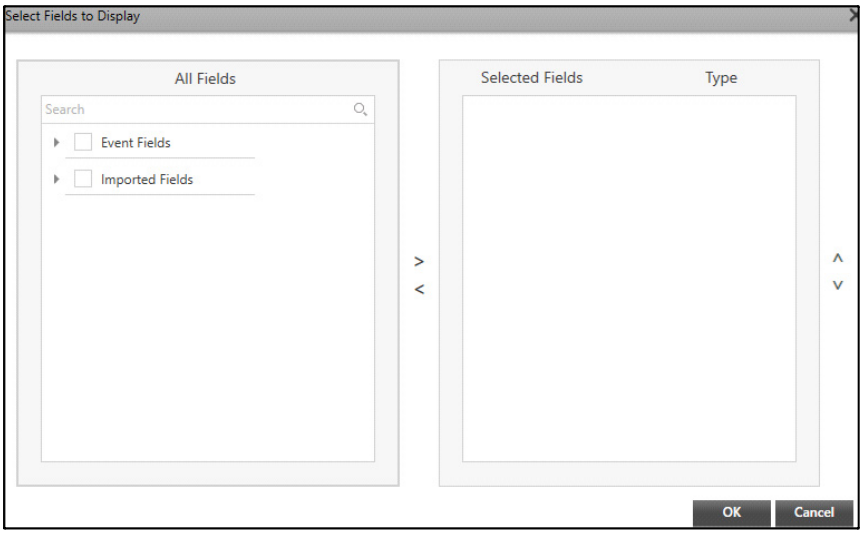
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

- **Duration**: Select the Duration from the drop-down list — Daily or Hourly.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To dates from the calendar and specify the time.
- **Generate Report With**: Select the option to generate the report with either **Imported Fields** or **Event Fields** or both.
- **Event**: If you have selected **Event Fields** as the **Generate Report With** option, select the desired Event for which you wish to generate the report from the drop-down list.
- **Fields to Display**: Select the desired fields that you wish to display in the report using the **Fields to Display** picklist.
    - Click the **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.

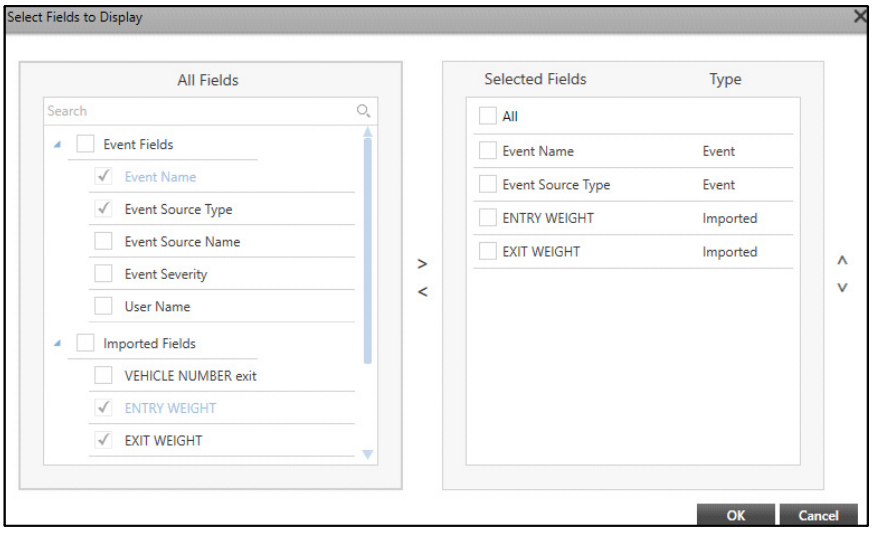


The fields that you have selected under **Generate Report With** are enabled for selection in the pop-up. Select the check boxes of the desired fields you wish to include in the report from the **Event Fields** or **Imported Fields**.

Click the right arrow button to move these fields in the **Selected Fields** list. The **Type** of field is indicated along with the fields you select in Selected Fields. You can also search for the desired fields using the search bar.

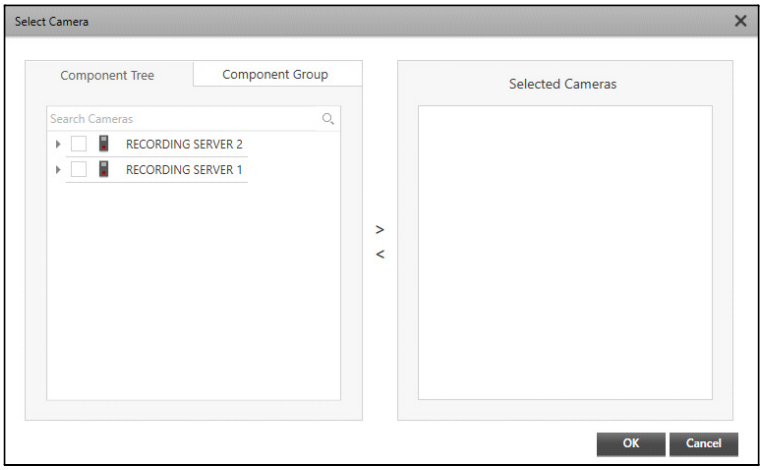
To remove fields, select the check boxes of the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields.

You can also change the sequence of the fields in Selected Fields list using the up and down arrow buttons. To do so, select the check box of the desired field, click the up/down arrow button as per your requirement.



- Click **OK** to confirm or click **Cancel** to discard.
- **Include Images**: Select the check box to include images in the report. Select the desired cameras from which you wish to select the images for the report using the **Include Images** picklist.

- Click the **Include Images** picklist. The **Select Camera** pop-up appears.

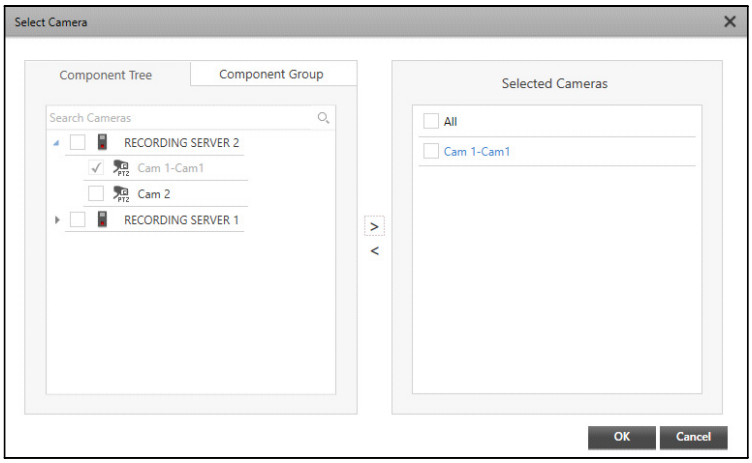


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”.

  Select the check boxes of the desired cameras from which you wish to include images in the report from the Component Tree or Component Group tabs.

  Click the right arrow button to add these cameras in the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button.



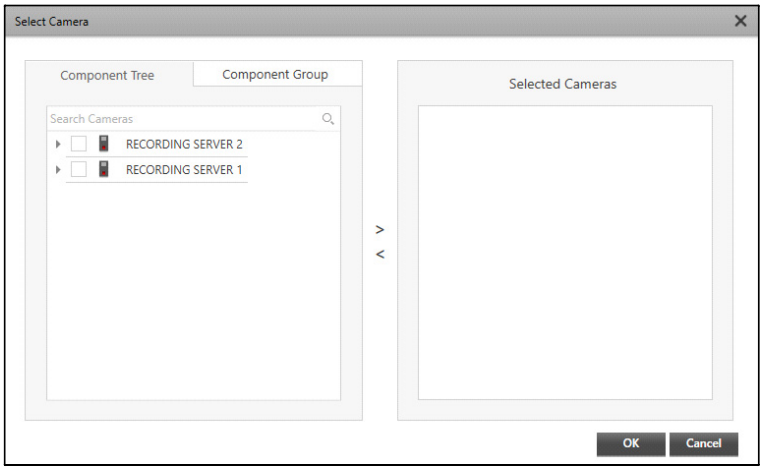
- Click **OK** to confirm or click **Cancel** to discard.
- **Image Quality**: If you have selected **Include Images**, select the desired quality of images to be included in the report from the drop-down list options — Thumbnail, Original.

  If you select **Thumbnail**, the thumbnails of the images from the selected cameras will be included.

  If you select **Original**, the full-resolution images from the selected cameras will be included.

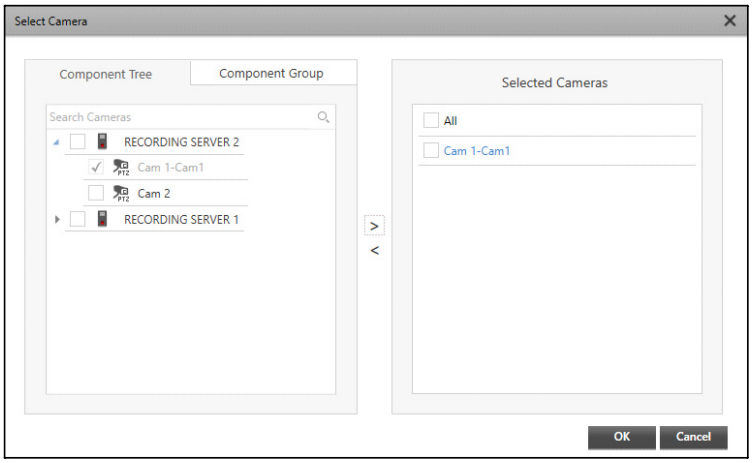
If no images are available in the configured Backup Drive, then images will not be included in the report irrespective of the selected Image Quality.

- **Include Clips**: Select the check box to include clips in the report. Select the desired cameras from which you wish to select clips for the report using the **Include Clips** picklist.
    - Click the **Include Clips** picklist. The **Select Camera** pop-up appears.



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to "Component Group". Select the check boxes of the desired cameras from which you wish to include clips in the report from the Component Tree or Component Group tabs. Click the right arrow button to add these cameras in the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list.



- Click **OK** to confirm or click **Cancel** to discard.
- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.

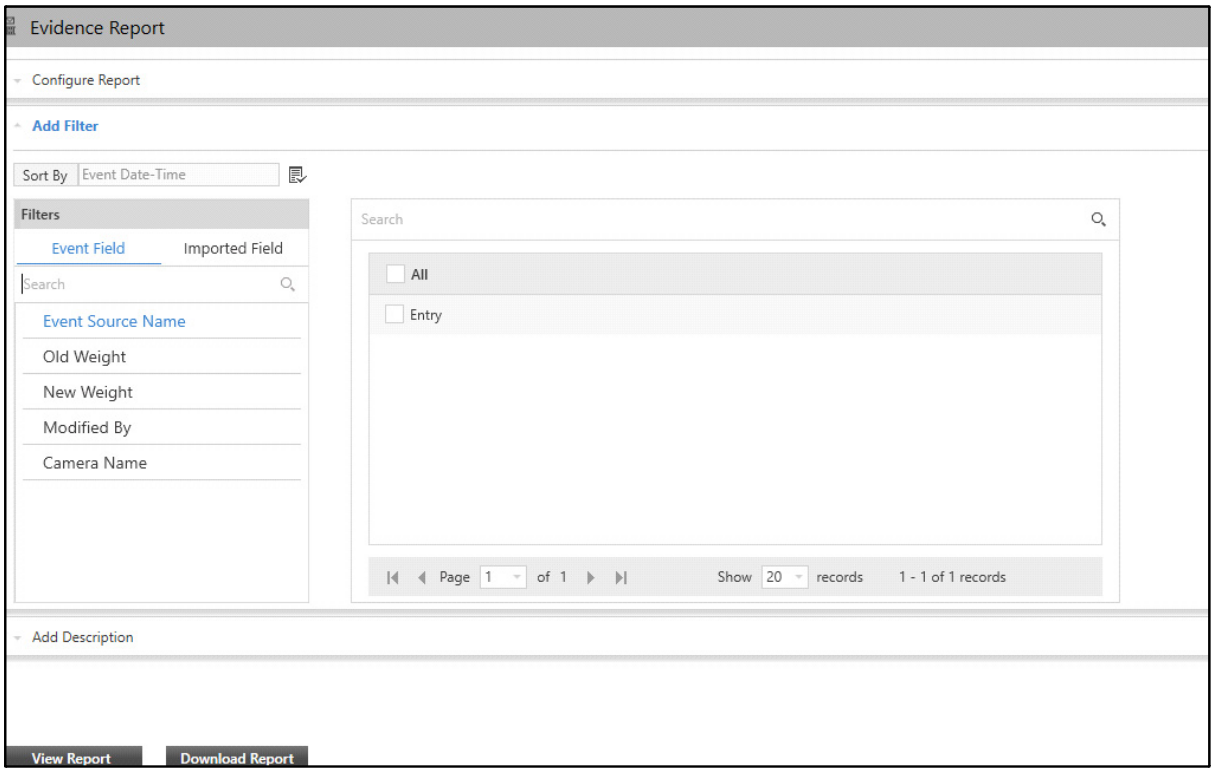
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Filter

This panel allows you to add filters for the Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters. You can view and edit the filters from this collapsible panel.

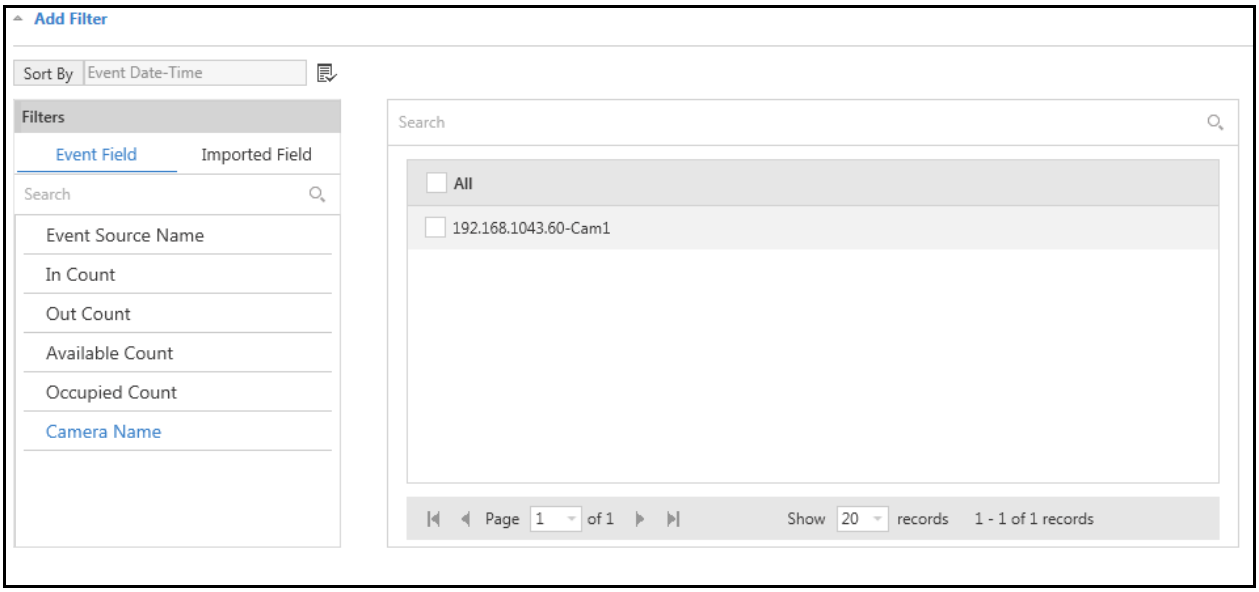
To set the filters,

- Click the **Add Filter** collapsible panel.



Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data from Event Fields or Imported Fields in the report using the **Sort By** picklist. Double-click to select the desired option. By default, the sorting is done as per the Date and Time of Event Occurrence.
- **Filters**: You can get the desired data for the report using Filters. The Filters section contains two tabs — Event Field and Imported Field. Select the tab to view the associated parameters.
    - Click the desired parameter to view the associated entities with the selected Event. For example, if you select Camera, all the cameras associated with the selected Event are displayed on the right hand side. Select the desired entities to include in the report.

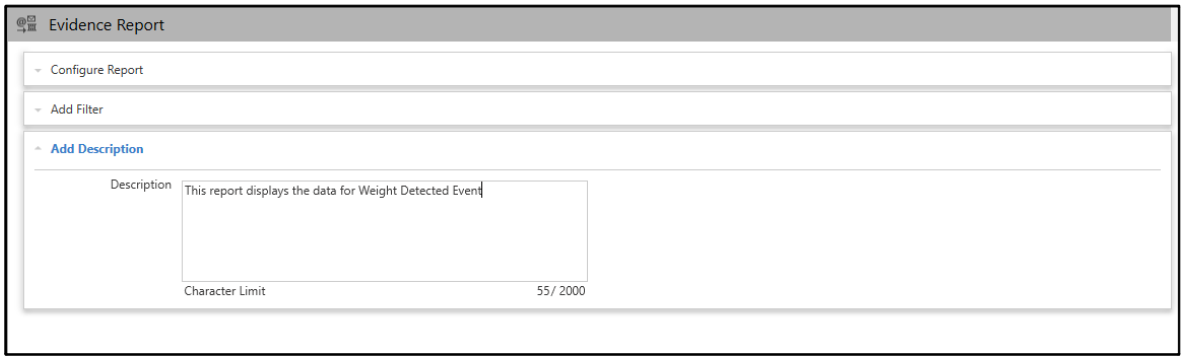


Add Description

This panel allows you to add a description for the Evidence Report once the report configurations are done. This description is visible in the generated report.

To view and edit the description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. The Description can be of upto 2000 characters only and it is displayed on the second page of the report.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

CHAPTER 9

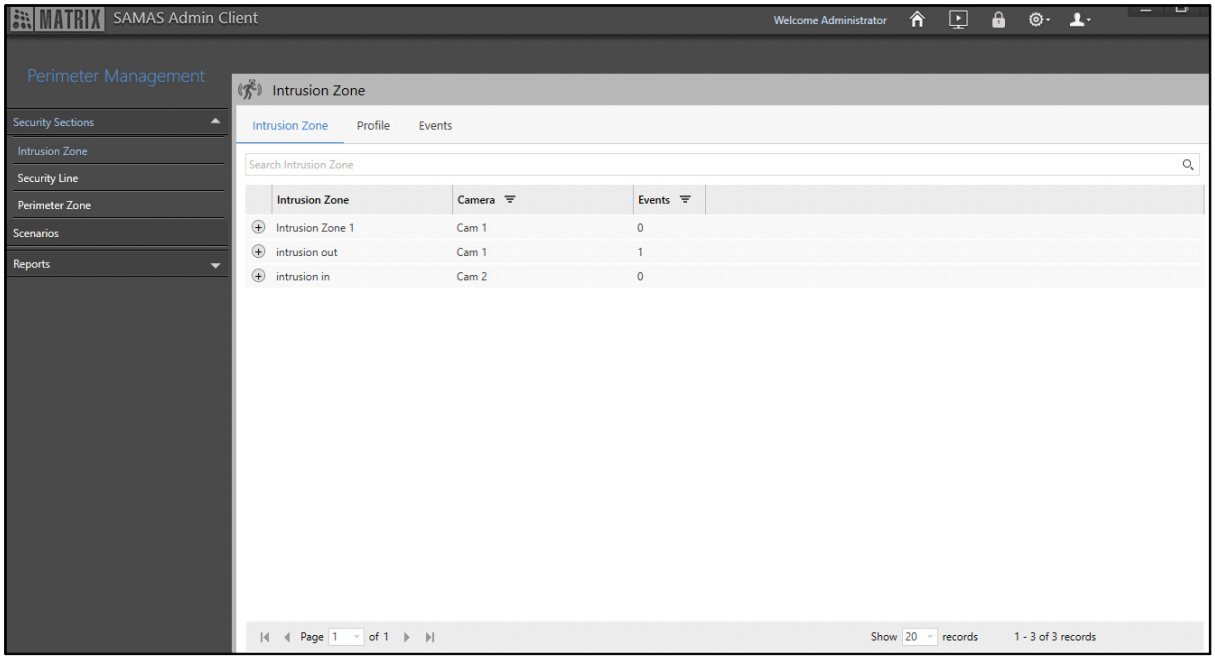
Perimeter Management

The Perimeter Management module enables you to configure various zones and Events for them. Perimeter Management uses video content analysis which is effective in detecting Events such as Intrusion Detection, Trip-Wire Detection, Tailgating, Motion Detection, No Motion Detection, Camera Tampering, Missing Object, Loitering Detection, Object Detection based on live stream of a camera. It also enables you to configure Scenarios based on Events.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure Perimeter Management,

- Click **Perimeter Management**.



The Perimeter Management module contains these pages — "Intrusion Zone", "Security Line", "Perimeter Zone", "Perimeter Management-Scenarios", "Perimeter Management - Report".

Intrusion Zone

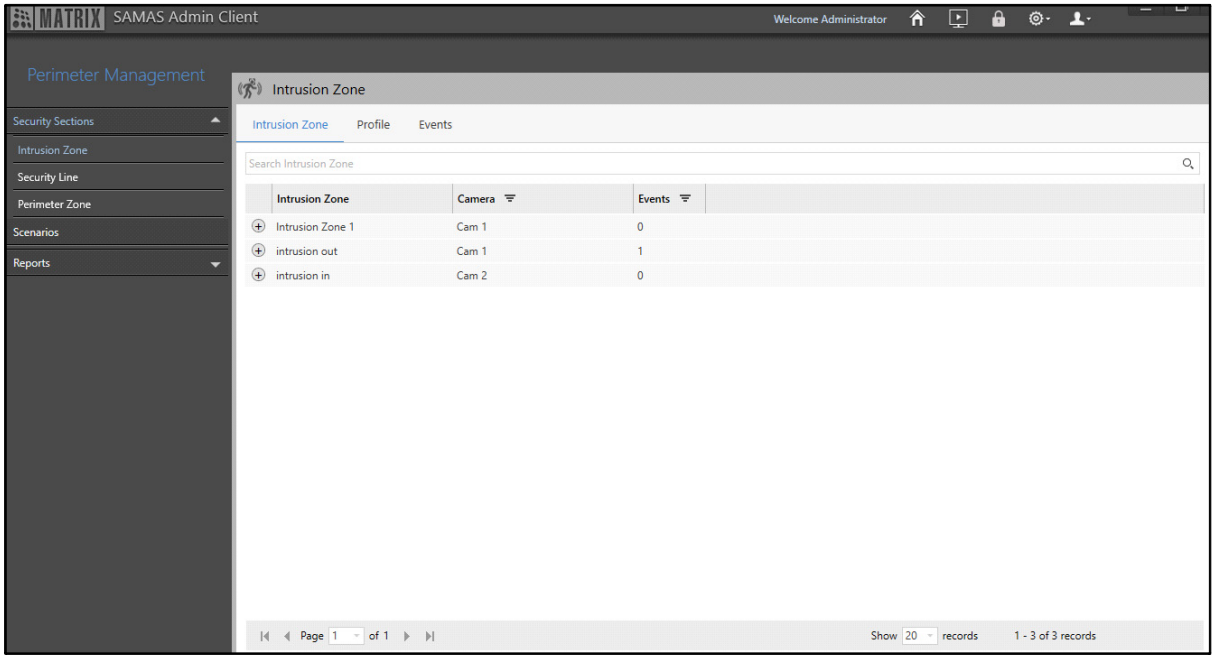
The Perimeter Management module allows you to configure the intrusion zones in the perimeter of an organization. This helps to detect any new object or person (such as people, vehicle) entering or leaving the defined area.

Event that can be configured against the configured intrusion zones is Intrusion Detection. This Event can then be used to create Scenarios which can alert the security person or management through the actions on the occurrence of any intrusion in the defined perimeter.

The Intrusion Zone page displays all the configured zones. You can view and configure the Intrusion Zones from this page.

To configure Intrusion Zones,

- Click **Perimeter Management > Security Sections**. The **Intrusion Zone** page appears by default.



The Intrusion Zone page consists of the following tabs.

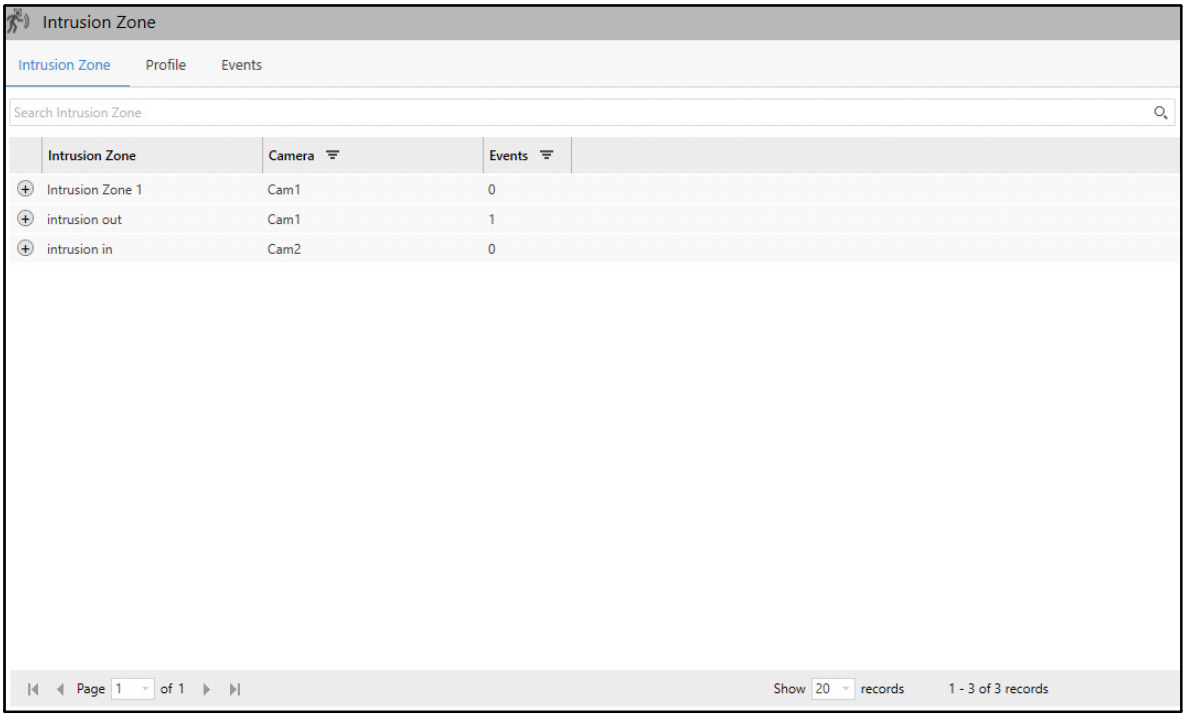
- "Intrusion Zone"
- "Profile"
- "Events"

Intrusion Zone

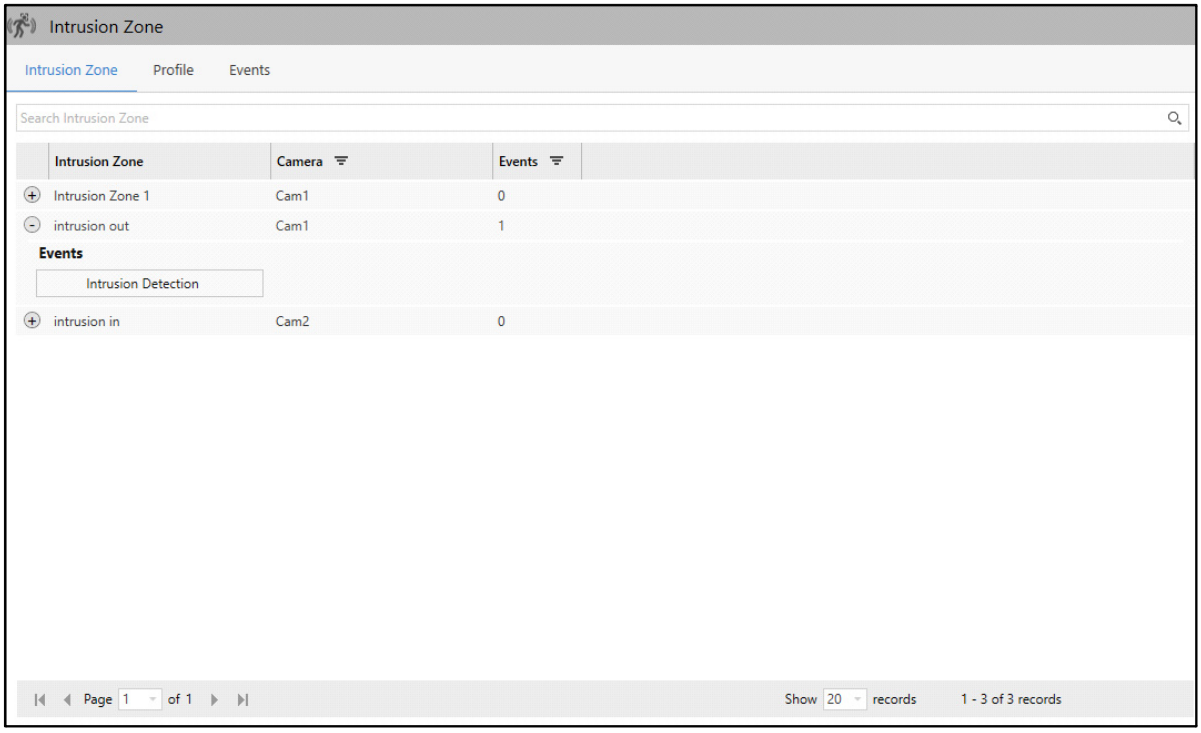
This tab enables you to view Intrusion Zones. You can configure the Intrusion Zones from "Profile". All the Intrusion Zones and the Events configured for them appear under this tab. The following Intrusion Zone details are displayed — Intrusion Zone, Camera and Events.

To view Intrusion Zones,

- Click the **Intrusion Zone** tab.



- Click **Show Events** to view the Events configured for the Intrusion Zone.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR FILTER**.

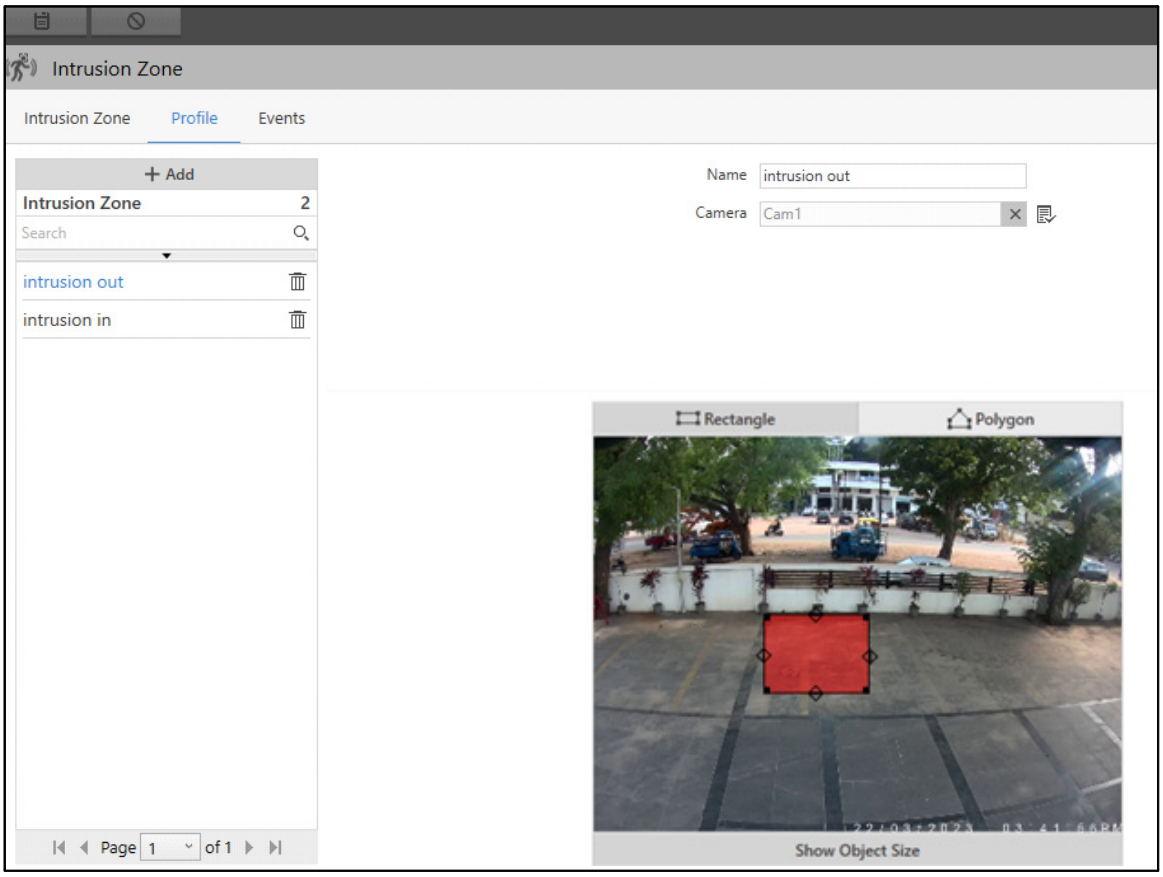
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

This tab enables you to configure Intrusion Zones. All the Intrusion Zones configured here appear under the **Intrusion Zone** tab.

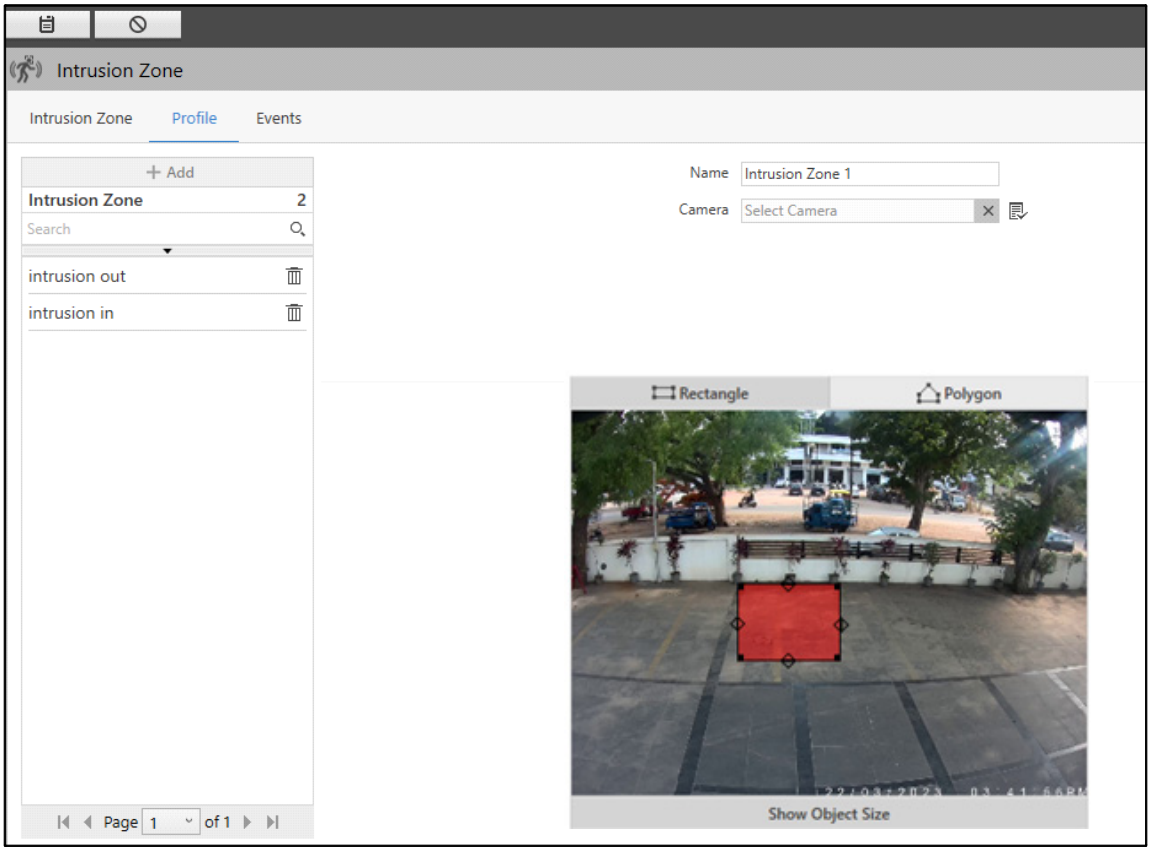
To configure Intrusion Zones,

- Click the **Profile** tab.



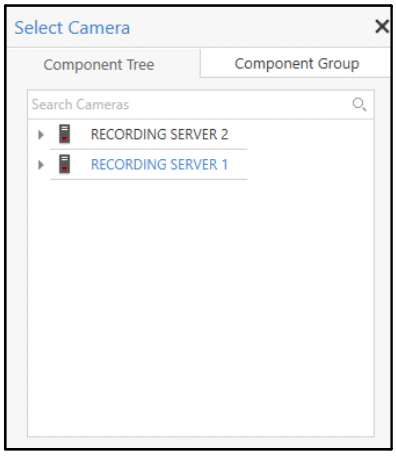
*The **Add** button is disabled when you are configuring Intrusion Zone for the first time. You can directly configure the parameters and save the Intrusion Zone.*

- Click **Add**.



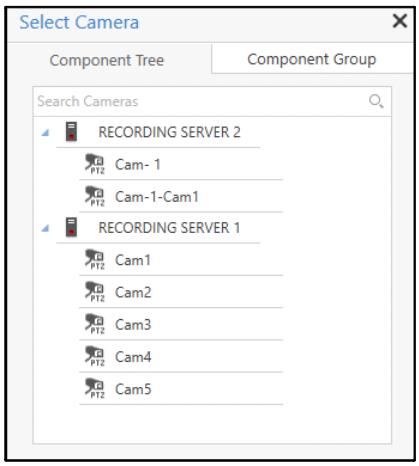
Configure the following parameters:

- **Name**: Specify a suitable name for the Intrusion Zone. In Name, you can enter upto 50 characters. Default: Blank.
- **Camera**: Select the desired camera which you wish to assign to the Intrusion Zone using the **Camera** picklist.
  - Click **Camera** picklist. The **Select Camera** pop-up appears.



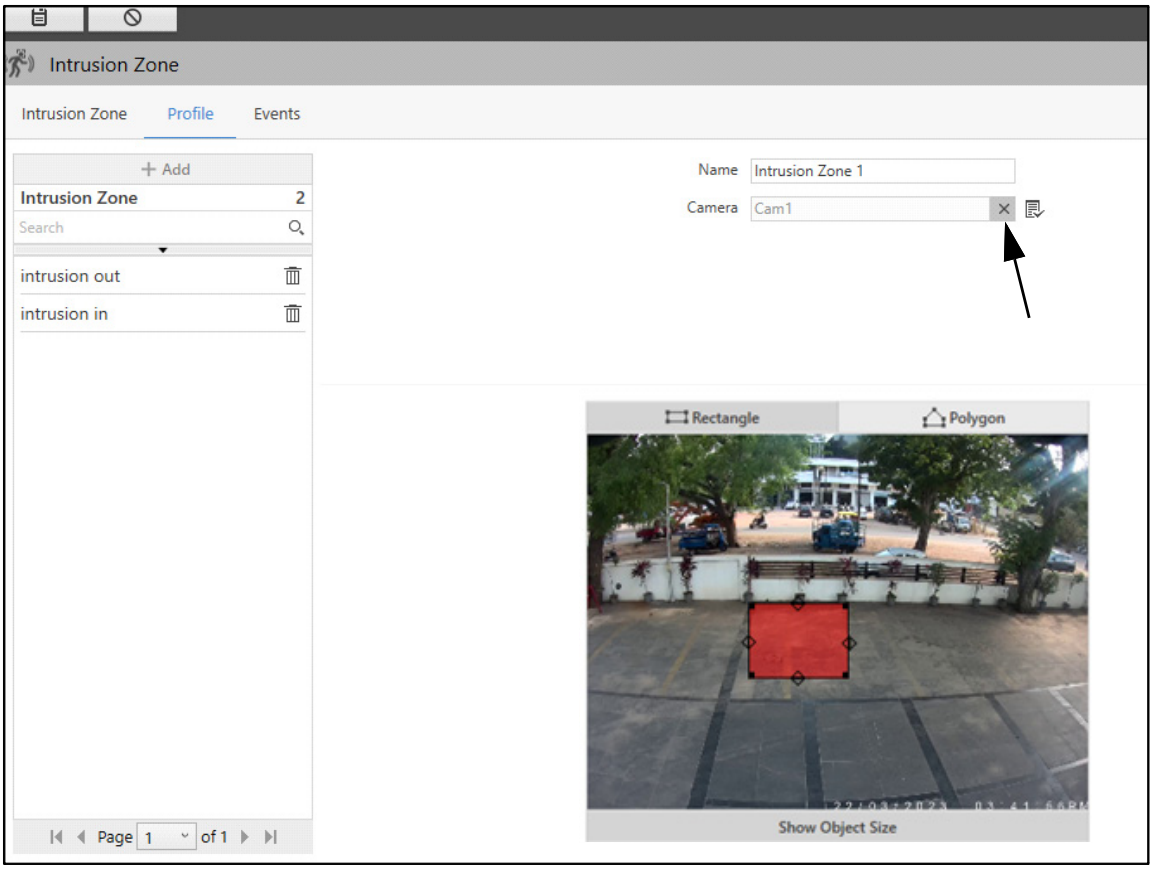
- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”.

  Double-click the desired camera to assign it to the Intrusion Zone. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

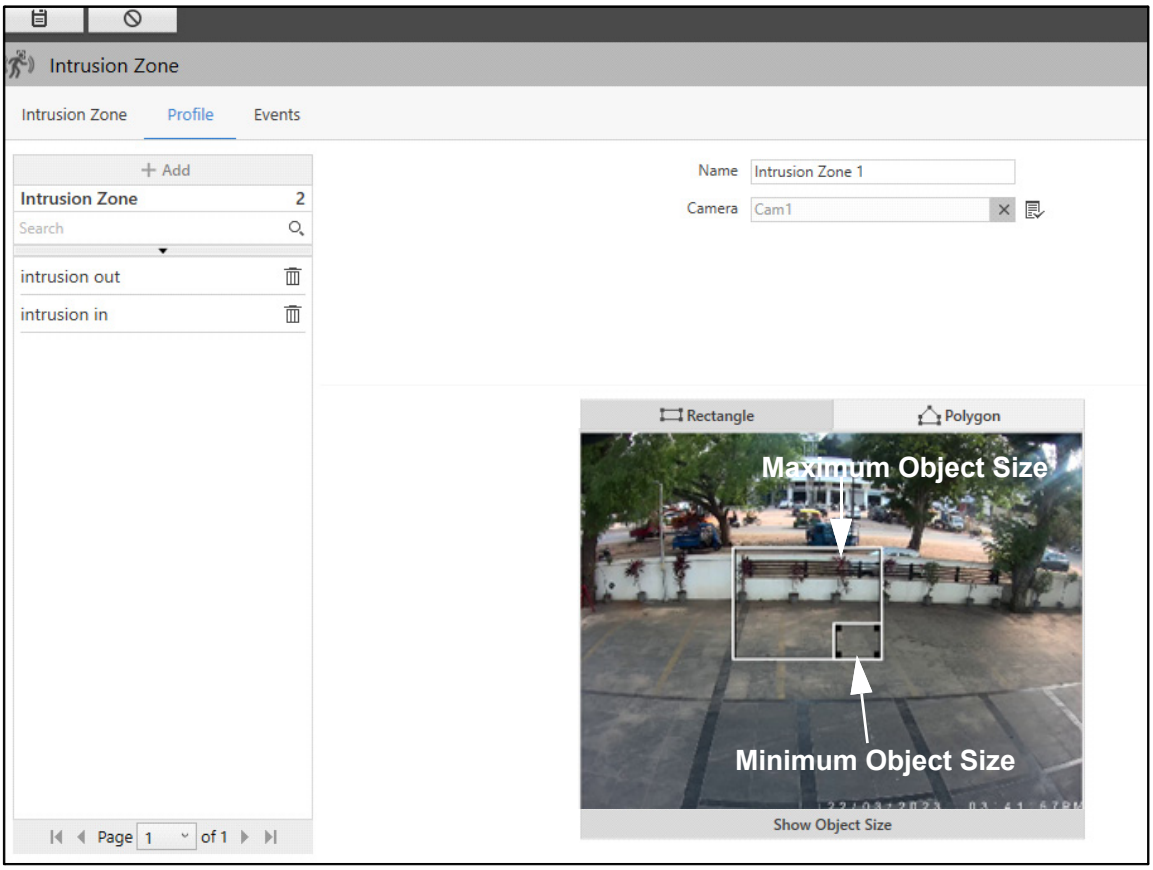
- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click to select the desired option.
  - Click **Go to selected position** , to move the camera as per the selected preset position.
- To remove the camera, click **Remove** .



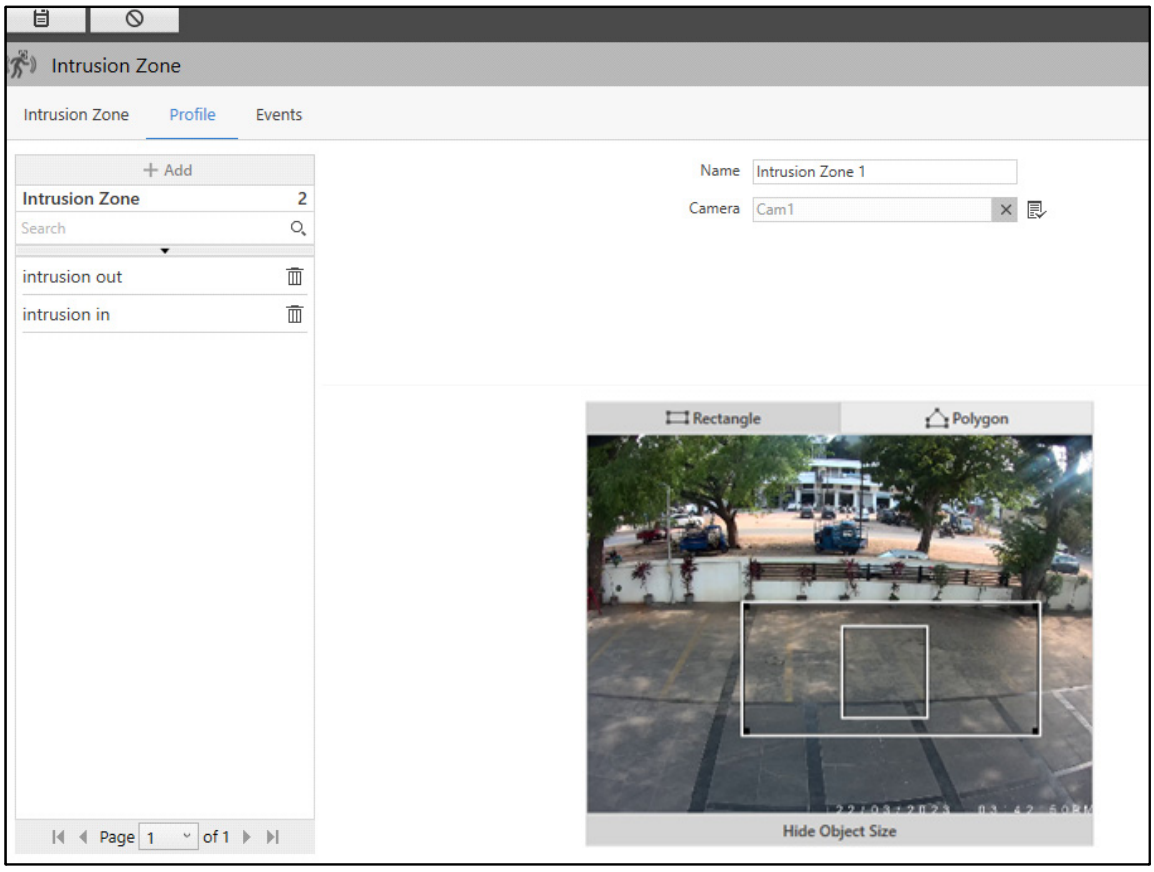
Once a camera is assigned, you can draw an Intrusion Zone on the live view of the camera. You can also define the **Minimum** and **Maximum Object Size**. You can either draw a **Rectangle** or **Polygon** to define the Intrusion Zone.

Object Size will not be applicable if you select Object Type in any Event. For details, refer to "Events".

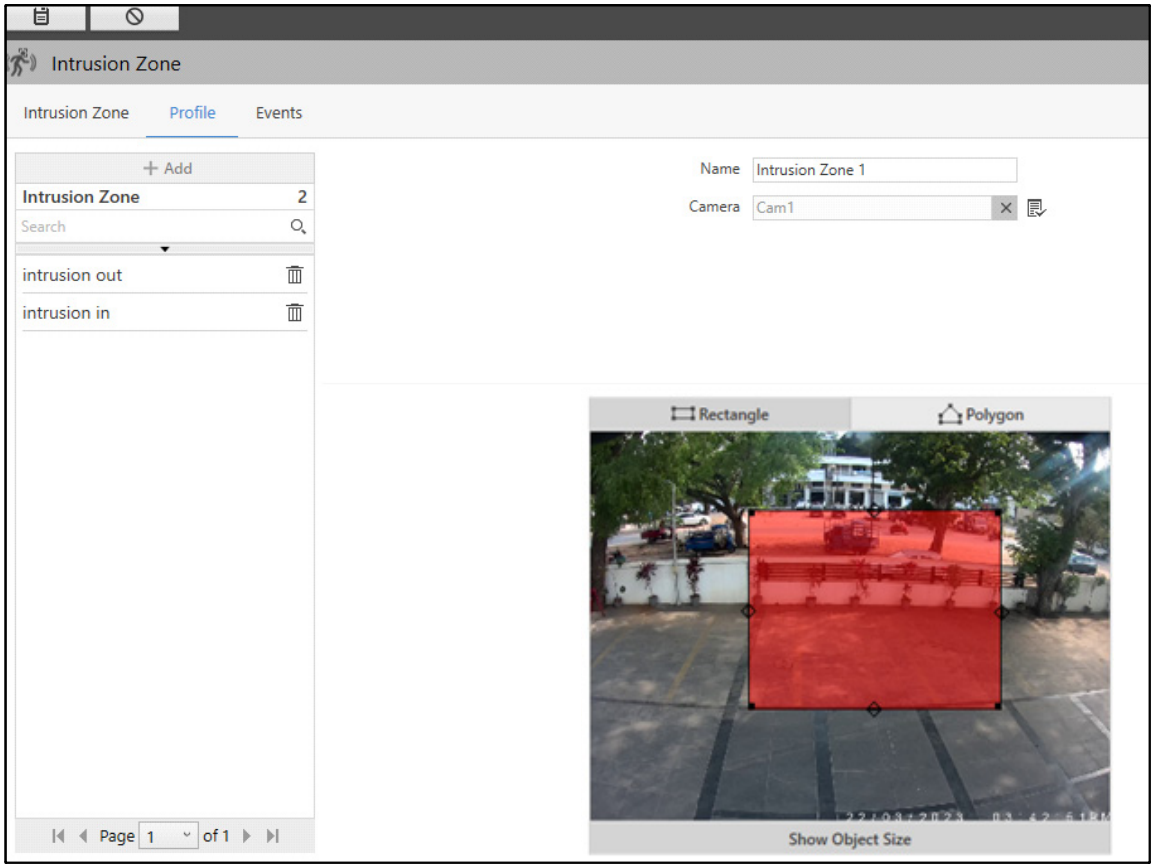
- Click **Show Object Size**. The default **Minimum** and **Maximum Object Size** appear.



- Drag the corners of the rectangles to configure the Minimum and Maximum Object Size to be detected in the Event, if required. When the object size meant to be detected in the Event does not fit in the default Minimum and Maximum Object Size, you can configure it to match the desired object size.

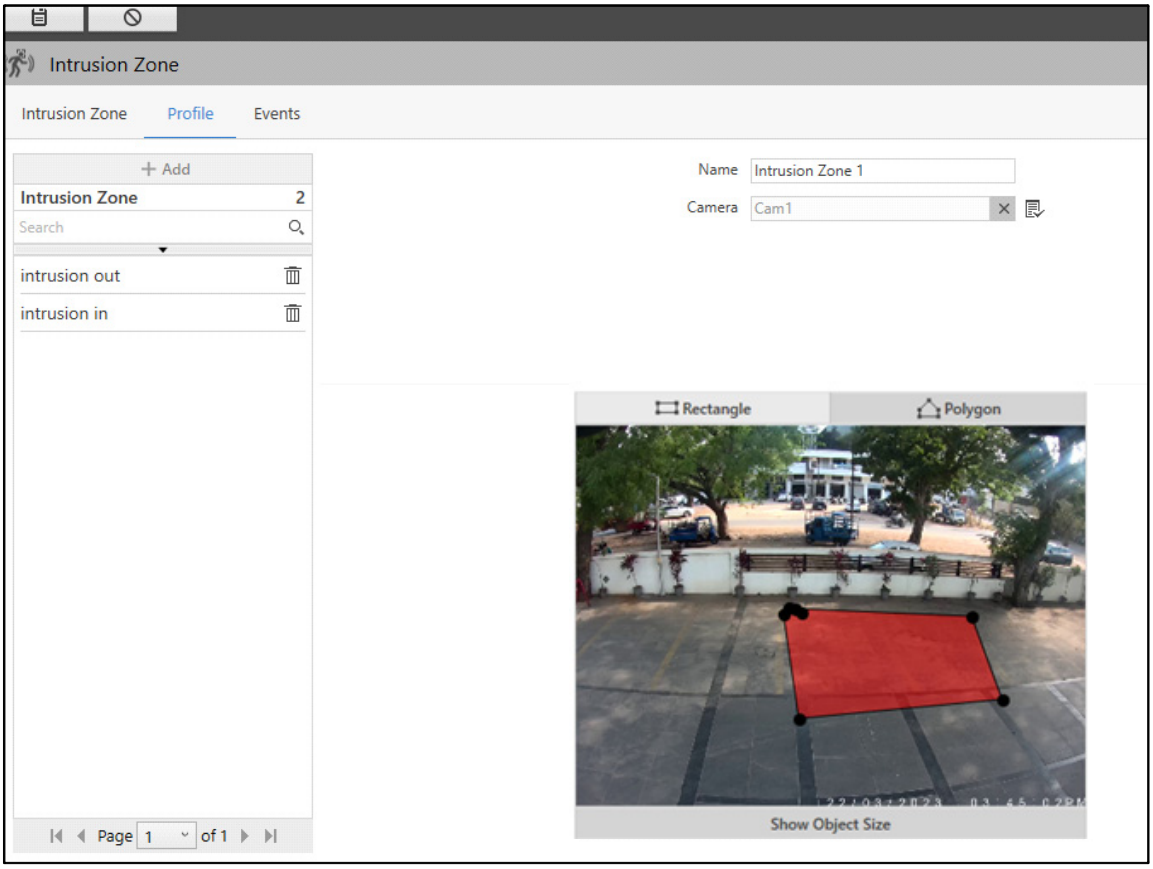


- Click **Save** to save the settings or **Cancel** to discard.
- Click **Hide Object Size** to hide the size and draw the perimeter.
  - Select either **Rectangle** or **Polygon** to draw the perimeter.
  - If you select **Rectangle**, drag the corners and sides of the rectangle to configure the perimeter.



- If you select **Polygon**, click on the live view to place the vertex of the polygon. Click again on the desired place to join the previous vertex with a new vertex. Continue this process to complete the polygon.

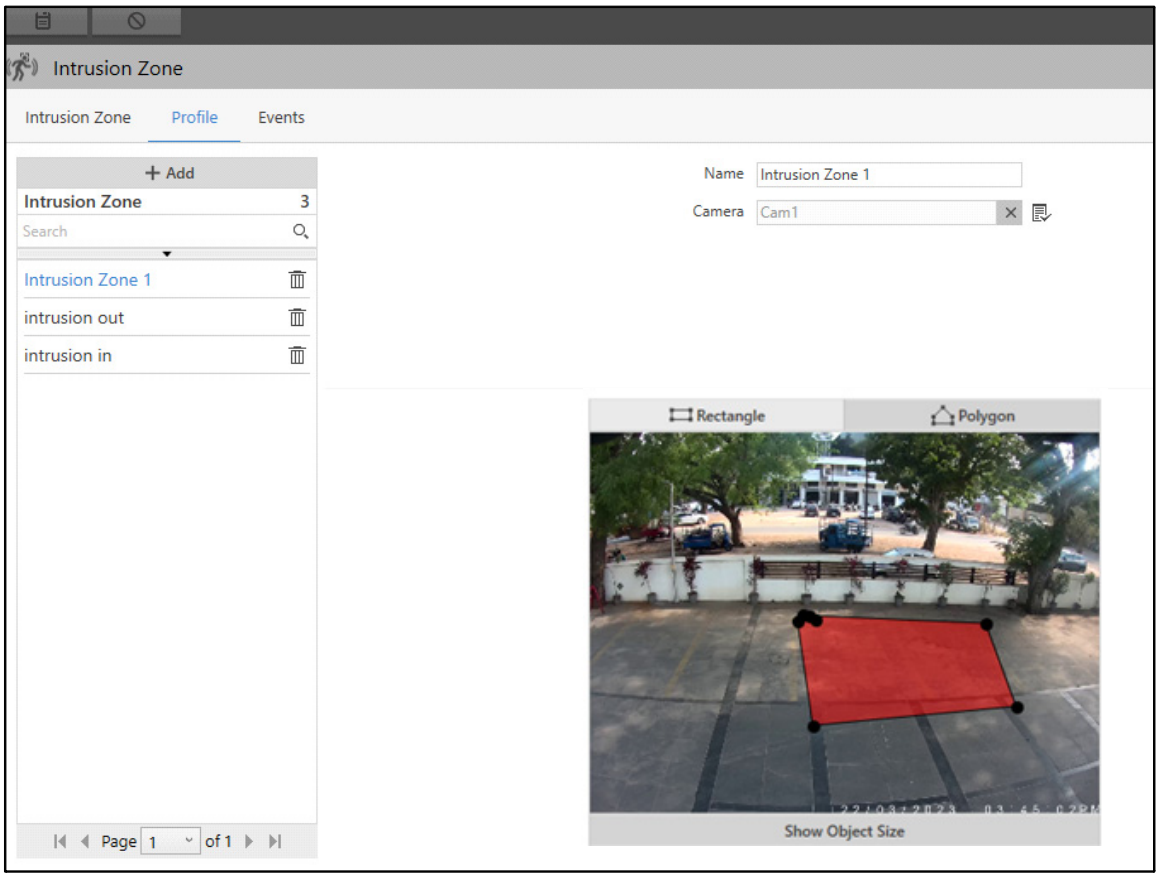
  The arrows pointing inwards within the zone represent **Intrusion In**, whereas, the arrows pointing outwards represent **Intrusion Out**.



- Click **Save** to save the settings or **Cancel** to discard.

The new Intrusion Zone will appear in the list on the left hand side. Similarly, you can create the other Profiles—intrusion out, intrusion in.

You can edit the configurations of the Intrusion Zone or delete it.



- Select the desired Intrusion Zone from the list and edit the details on the right hand side.
  - Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired zone.

Similarly, you can configure the other Intrusion Zones.

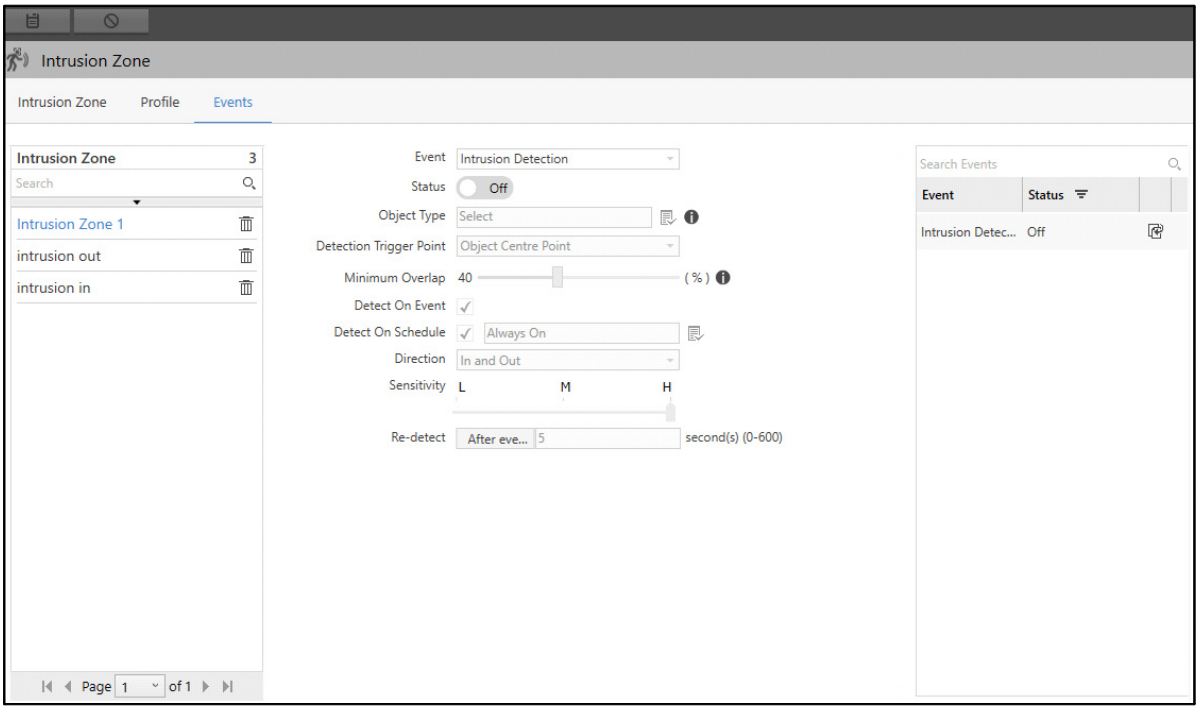
Events

This tab enables you to configure the Intrusion Detection Event for the Intrusion Zones. All the configured Events appear under the **Intrusion Zone** tab.

Object Size configured in any "Profile" will not be applicable if you select Object Type in any Event.

To configure Intrusion Detection Event,

- Click the **Events** tab.
- Select the desired Profile from the list on the left hand side for which you wish to configure the Event.

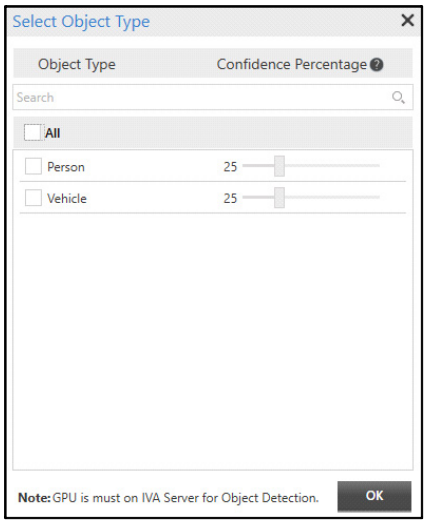


Configure the following parameters:

- **Event**: Select the desired Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



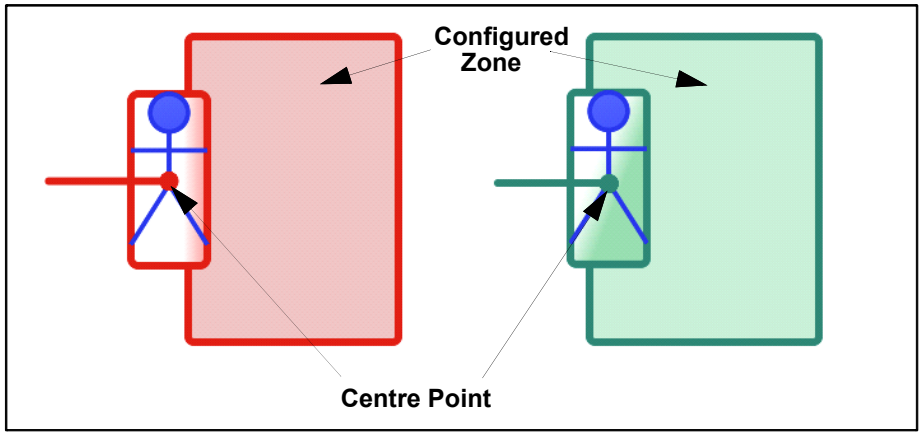
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point, Minimum Overlap. Based on the selected option, the IVA engine will detect the selected Object Type.

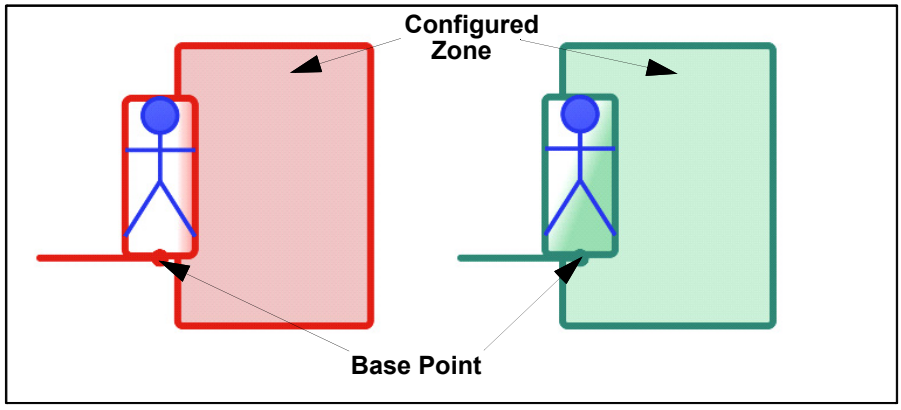
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured zone.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point of the object crosses the configured zone, an event will be generated.



  If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured zone.

  In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured zone, an event will be generated.

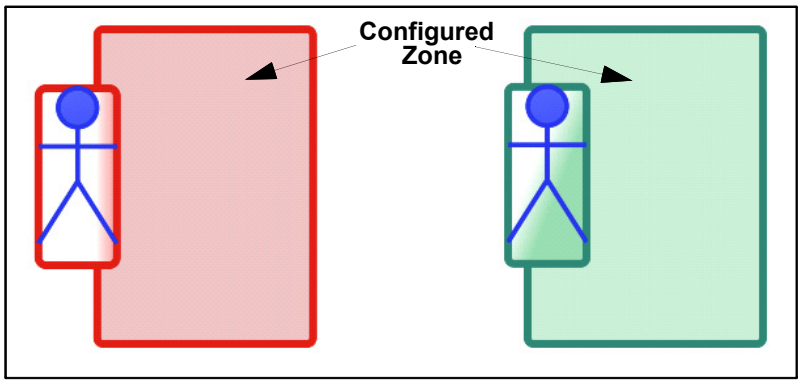


  If you select **Minimum Overlap**, the IVA engine will detect the event based on the minimum percentage of overlap of detected object across the configured zone.

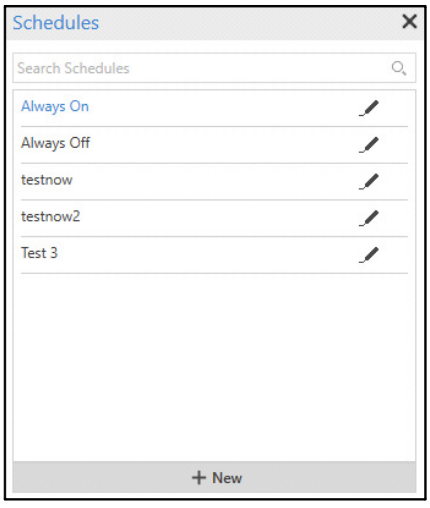
- **Minimum Overlap**: If you have selected **Detection Trigger Point** as **Minimum Overlap**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the zone to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the zone will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the zone will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Zone, the event will be triggered when 30% of the object is overlapping the configured zone. Whereas, in the Red Zone, the event will not be triggered as only 10% of the object is overlapping the configured zone.



- **Detect on Event**: Select the check box to detect Intrusion only on the occurrence of the Event.
- **Detect on Schedule**: Select the check box to detect Intrusion as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Direction**: Select the direction from the drop-down list — In and Out, In, Out.

  If you select **In**, the Event will occur when an object/person enters inside the configured zone represented by arrows pointing inwards.

  If you select **Out**, the Event will occur when an object/person exits the configured zone represented by arrows pointing outwards.

  If you select **In and Out**, the Event will occur either when an object/person enters or exits the zone.

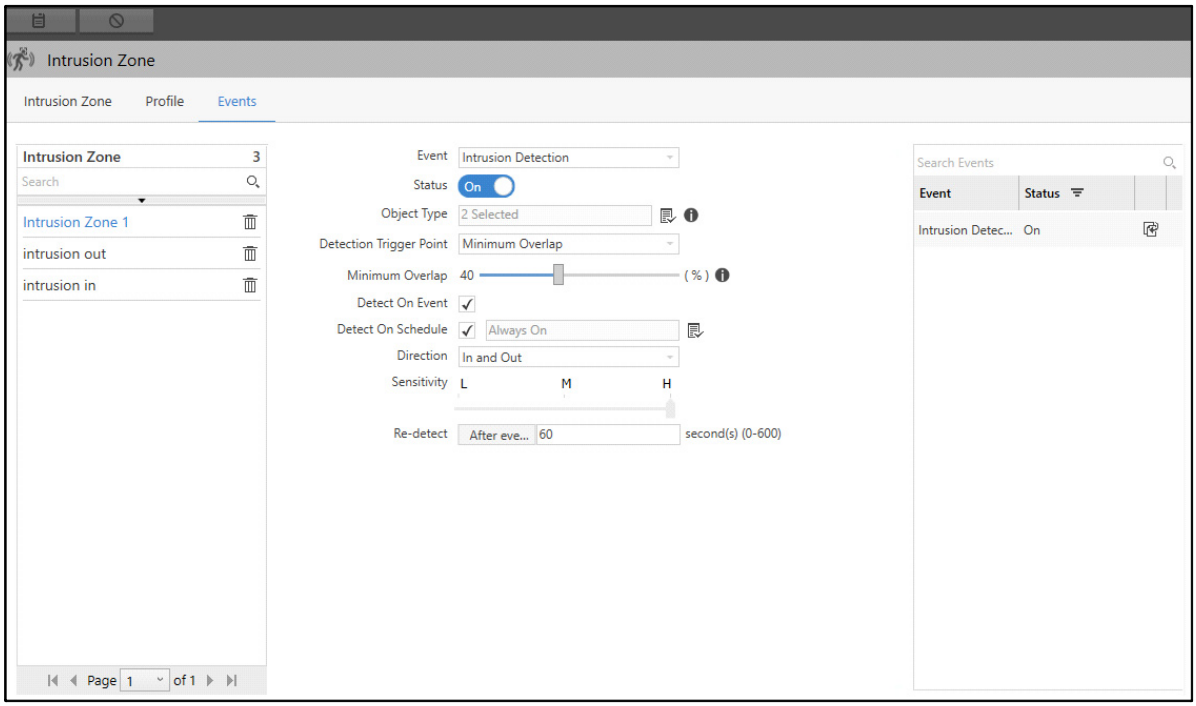
- **Sensitivity**: Drag the slider to set the desired sensitivity for the Intrusion Detection Event — Low, Medium or High.

If you have selected Object Type, then Sensitivity will be disabled.

- **Re-detect After every**: Specify the Re-detect time after which the Intrusion Detection Event should be detected again after the previous detection. Valid Range: 0-600 seconds. Default:5.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

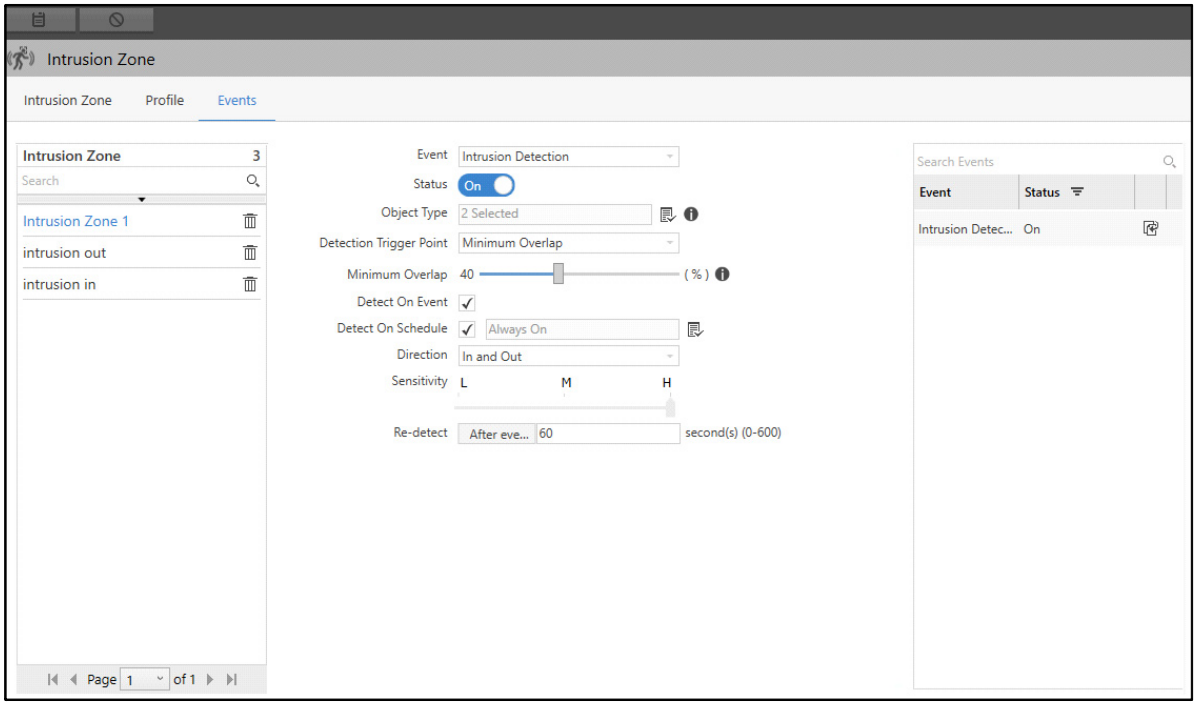


- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

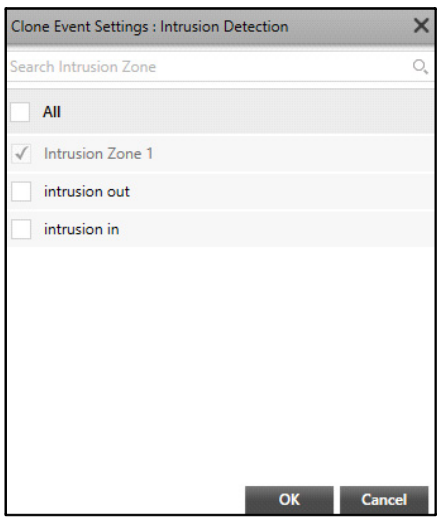
Once the Event is configured, you can also copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Intrusion Detection is created, the **Clone Event Settings** option gets enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Intrusion Detection** pop-up appears.



- Select the desired zones to which you wish to copy these configurations.

- Click **OK** to confirm or click **Cancel** to discard.

Security Line

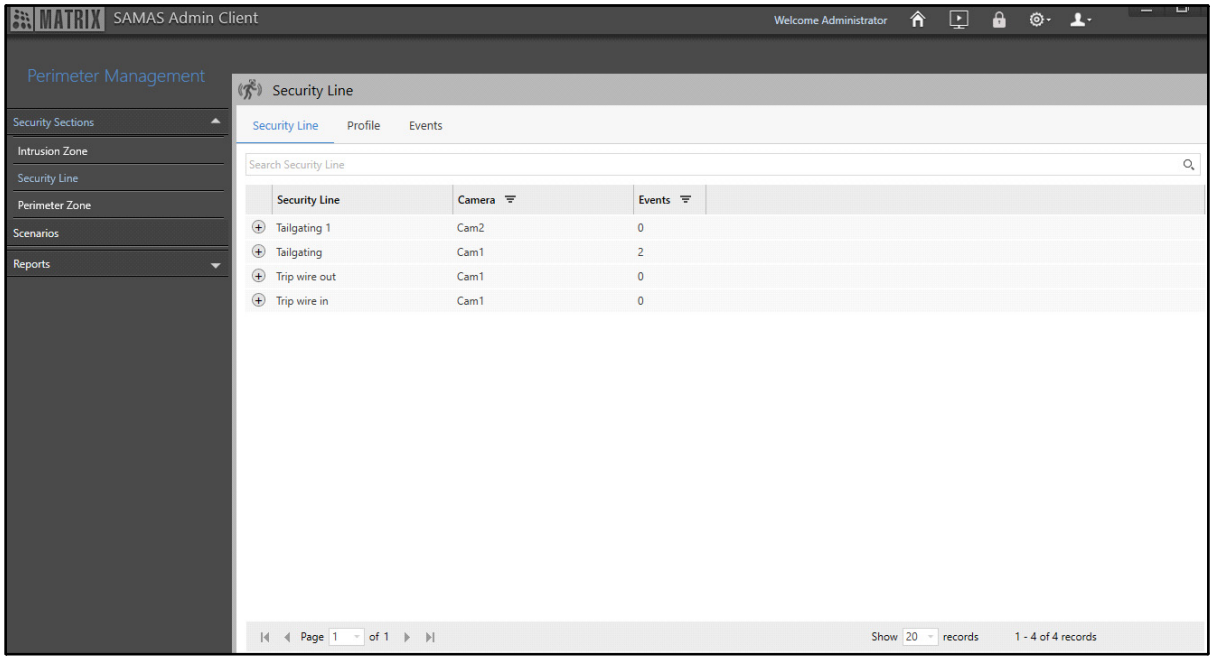
The Perimeter Management module allows you to configure the Security Lines in the perimeter of an organization. This helps to detect any unwanted object or person (such as people or vehicle) passing through the configured Security Line in the area.

Let us understand this with the help of an example: In an organization, the security guard wants to restrict the entry of people in a danger zone. A Security Line at the entrance of that area can be configured, passing it will trigger the Event. The security person can be notified about the Event by configuring Scenarios and actions.

The Security Line page displays all the configured Security Lines. You can view and configure the Security Lines from this page.

To configure Security Line,

- Click **Perimeter Management > Security Sections > Security Line**.



The Security Line page consists of the following tabs.

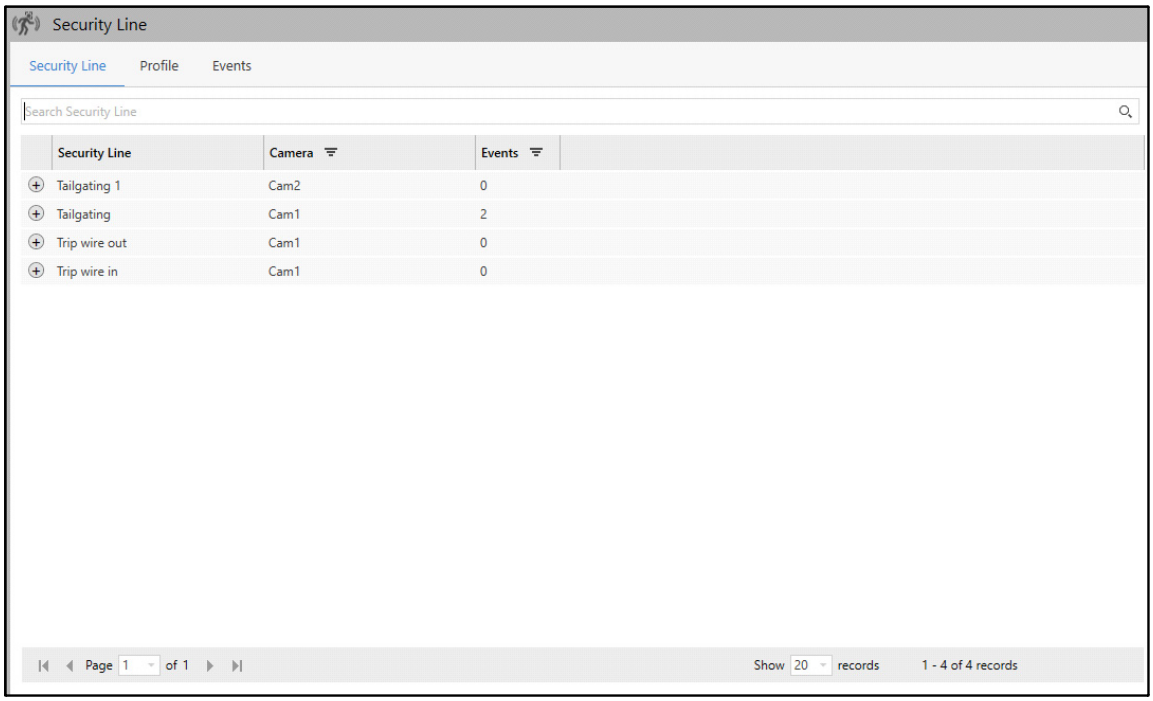
- “Security Line”
- “Profile”
- “Events”

Security Line

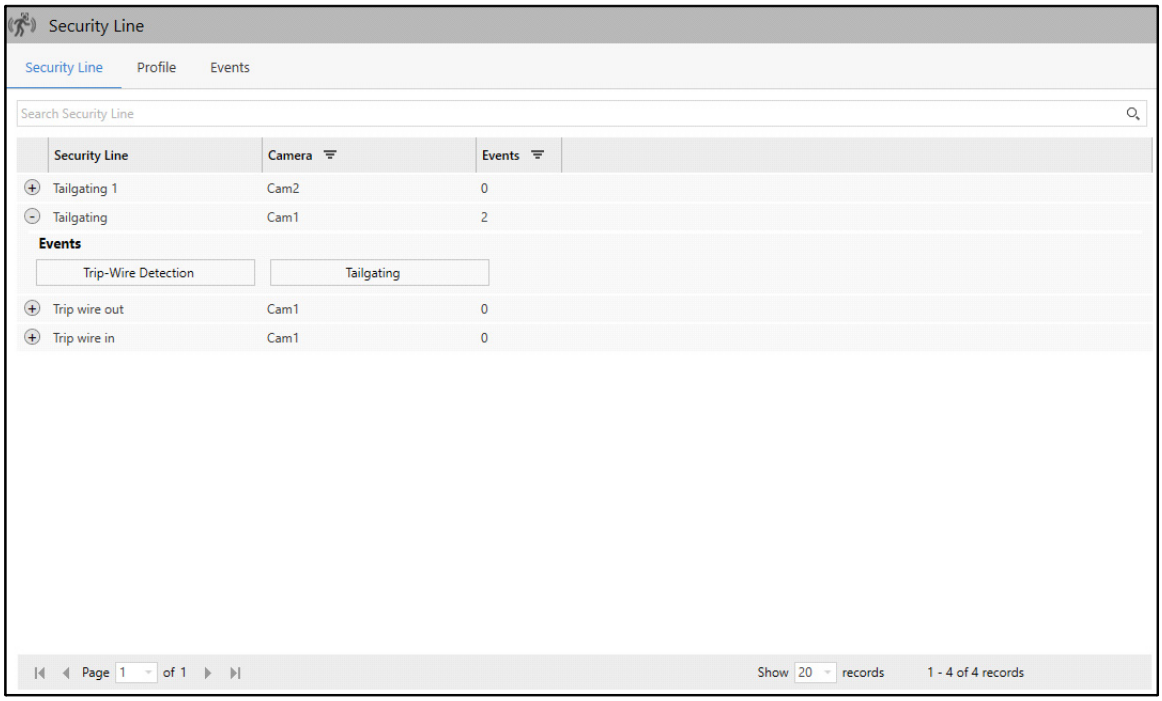
This tab enables you to view Security Lines. You can configure the Zones from “Profile”. All the Security Lines and the Events configured for them appear under this tab. The following Security Line details are displayed — Security Line, Camera and Events.

To view Security Line,

- Click the **Security Line** tab.



- Click **Show Events** to view the Events configured for the Security Line.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR FILTER**.

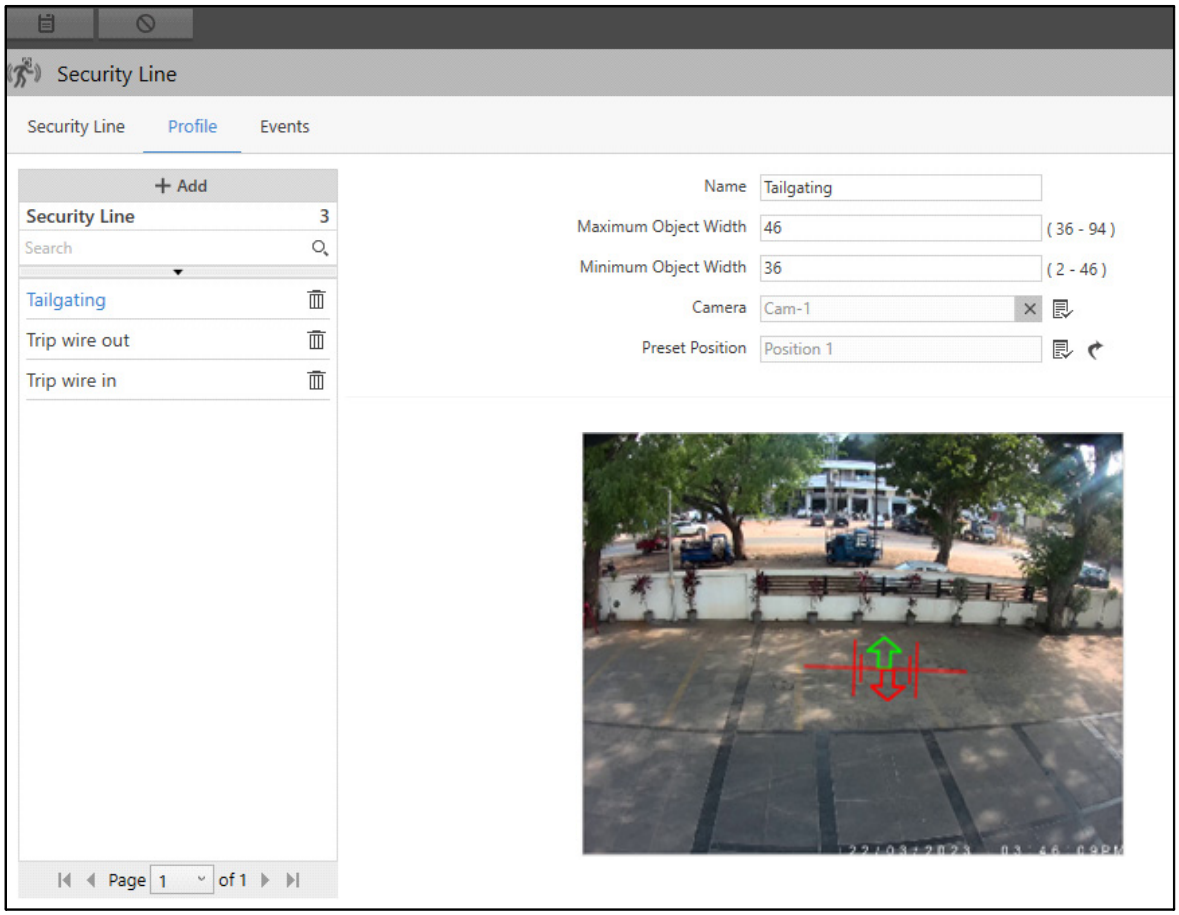
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

This tab enables you to configure Security Lines. All the Security Lines configured here appear under the **Security Line** tab.

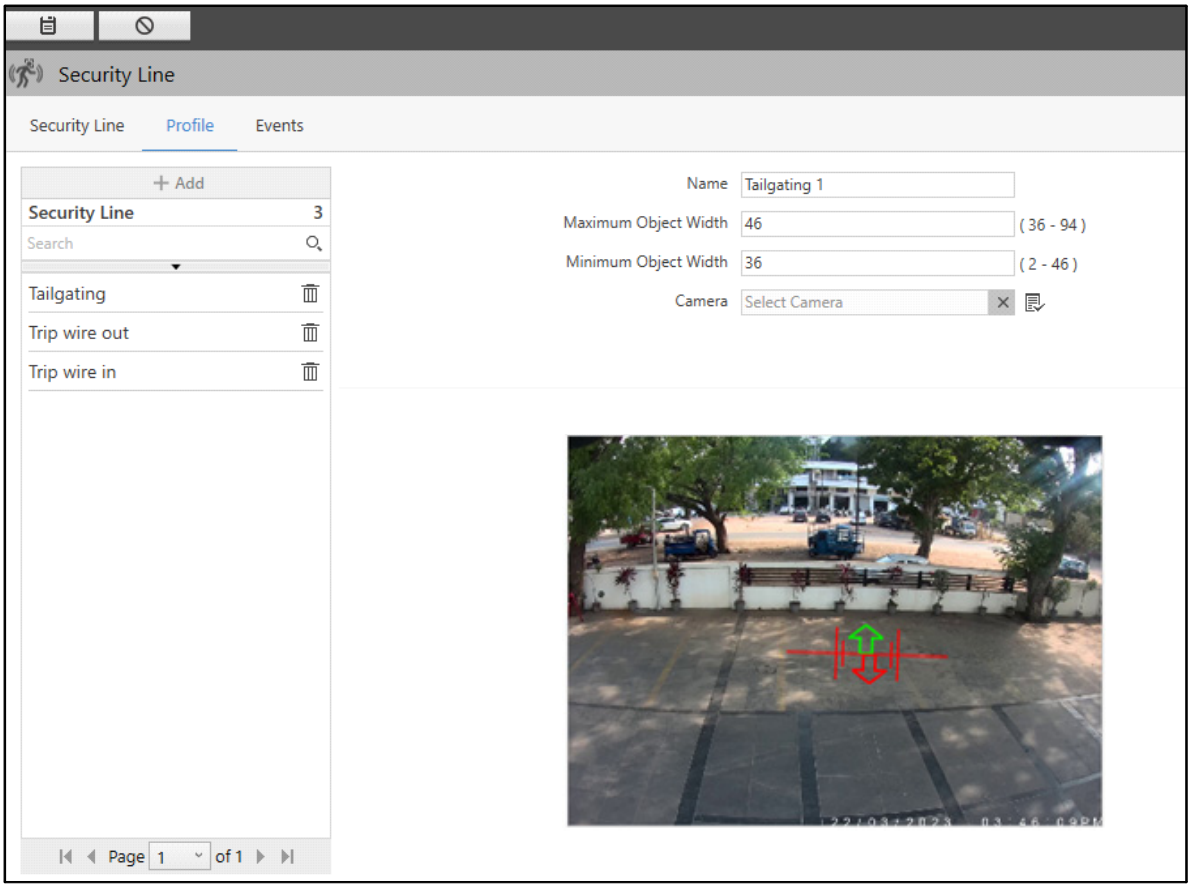
To configure Security Lines,

- Click the **Profile** tab.



*The **Add** button is disabled when you are configuring Security Line for the first time. You can directly configure the parameters and save the Security Line.*

- Click **Add**.



Configure the following parameters:

- **Name**: Specify a suitable name for the Security Line. In Name, you can enter upto 50 characters. Default: Blank.

Maximum and Minimum Object Width will not be applicable if you select Object Type in any Event. For details, refer to "Events".

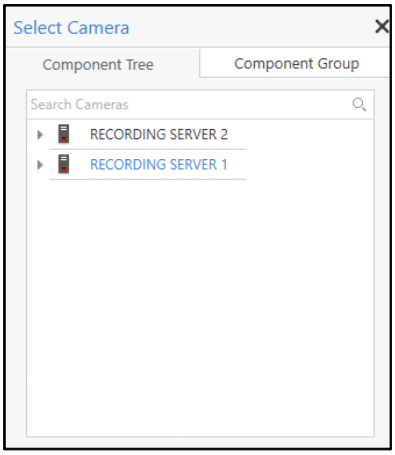
- **Maximum Object Width**: Specify the maximum width of the object which is meant to be detected in the Event using the live view. Default Range: 36 to 492. Maximum Width will vary as per the line configured by you. Default:46.

- **Minimum Object Width**: Specify the minimum width of the object which is meant to be detected in the Event using the live view. Default Minimum Object Width: 2 (Lower limit). The Upper limit of Minimum Object Width will vary as per the Maximum Object Width configured by you. Default:36.

- **Camera**: Select the desired camera which you wish to assign to the Security Line using the

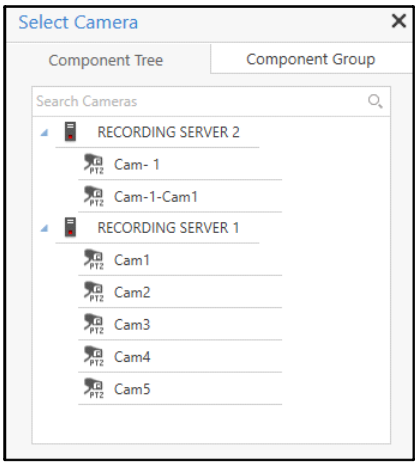
  Camera picklist.

  - Click **Camera** picklist. The **Select Camera** pop-up appears.



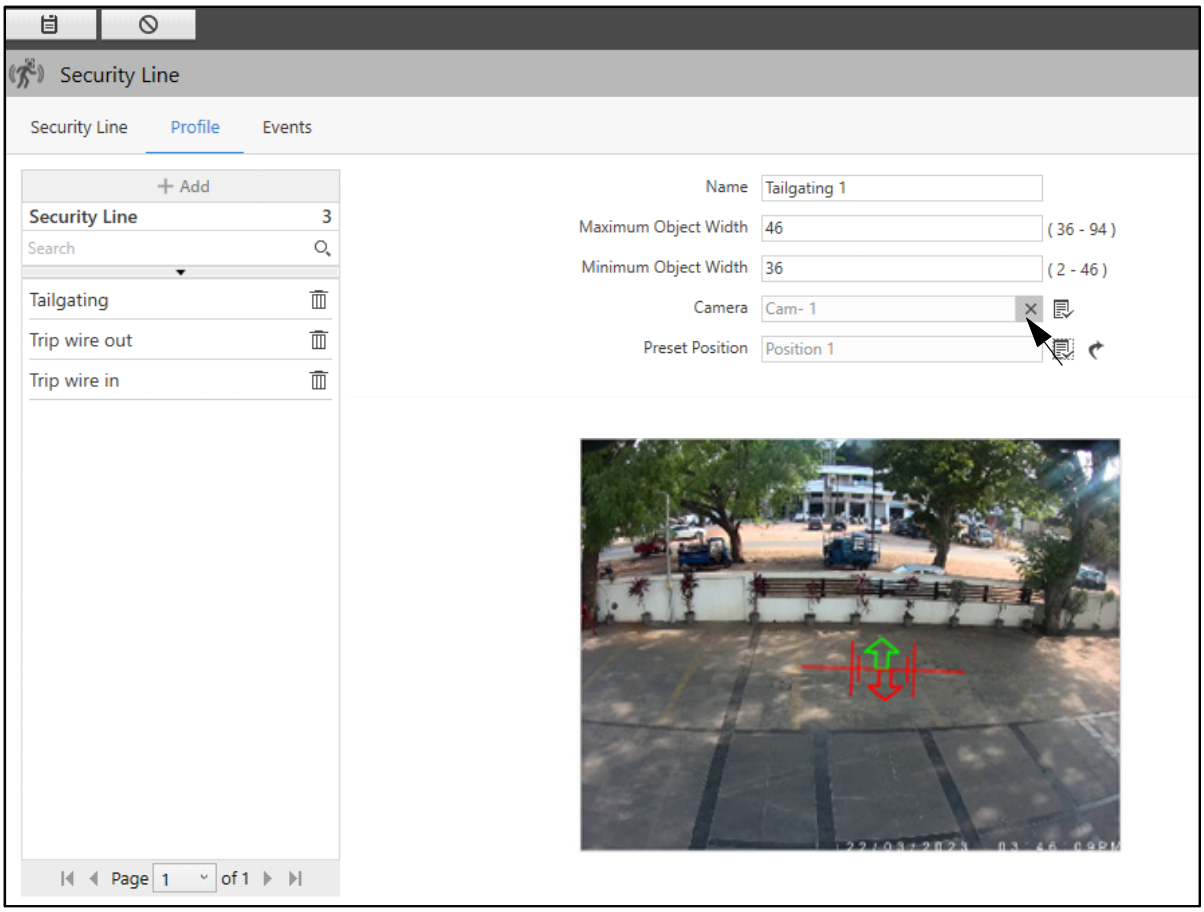
- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”.

  Double-click the desired camera to assign it to the Security Line. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click to select the desired option.
  - Click **Go to selected position** , to move the camera as per the selected preset position.
- To remove the camera, click **Remove** .



Once a camera is assigned, you can draw a Security Line on the live view of the camera.

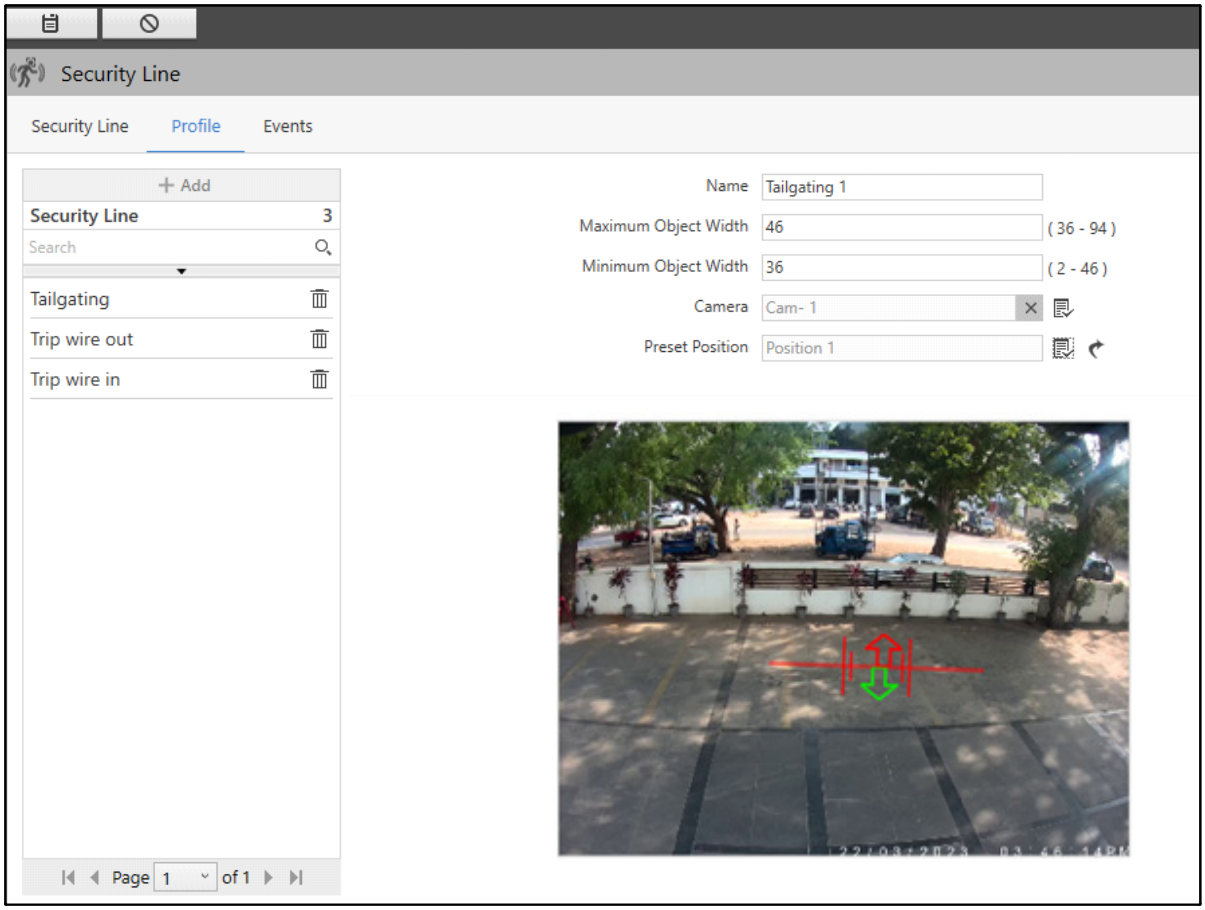
- Drag the line to increase or decrease the length of the Security Line and set it as required.

  You can also drag it to change the Entry (Green arrow) and Exit (Red arrow) direction. To do so,

  Move the mouse pointer to any one end of the line, a four direction arrow appears.

  Now, drag it in the desired direction.

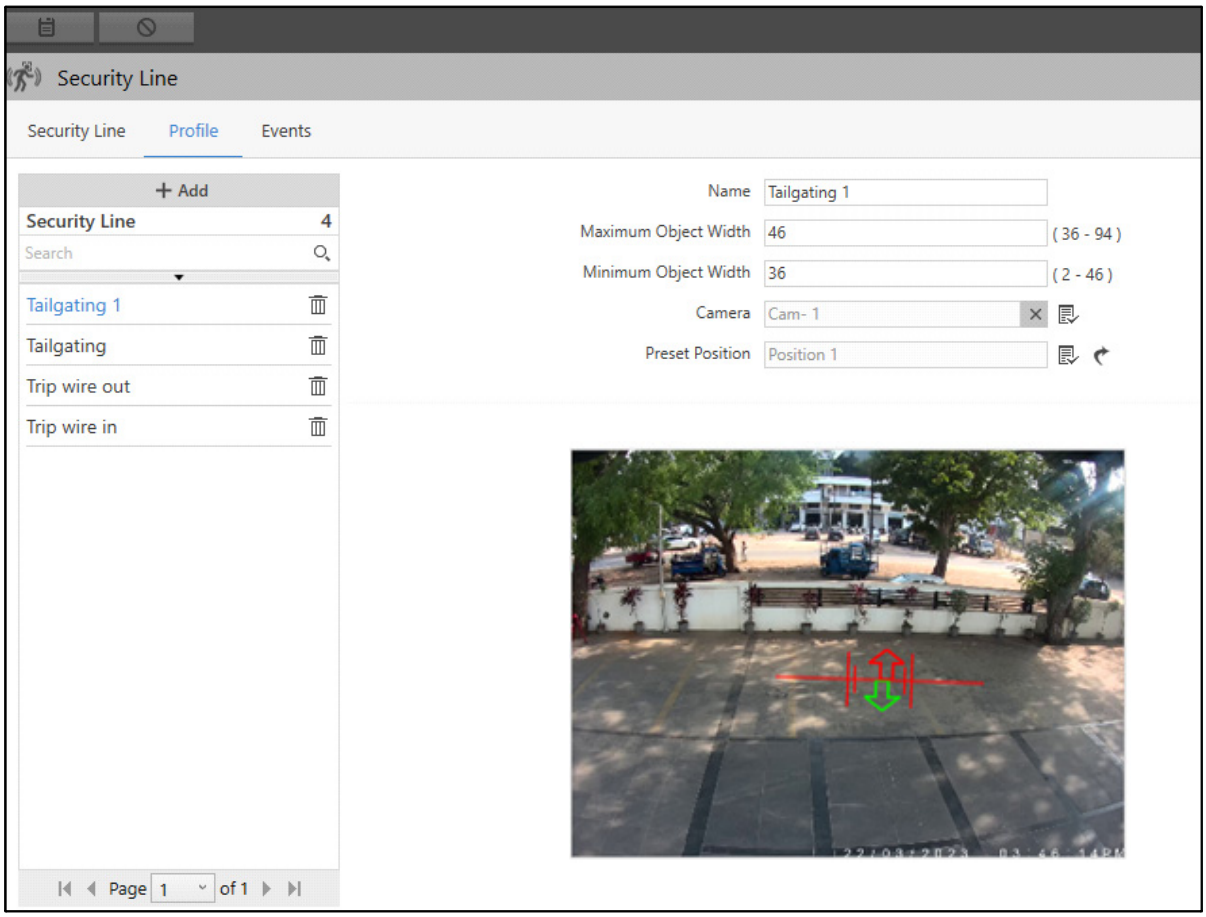
In case of Tailgating, the event will be generated only when any object moves in the Entry (Green arrow) direction. Hence, configure the Security Line accordingly.



- Click **Save** to save the settings or **Cancel** to discard.

The new Security Line will appear in the list on the left hand side.

You can edit the configurations of the Security Line or delete it.



- Select the desired Security Line from the list and edit the details on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the Security Line.

Similarly, you can configure the other Security Lines.

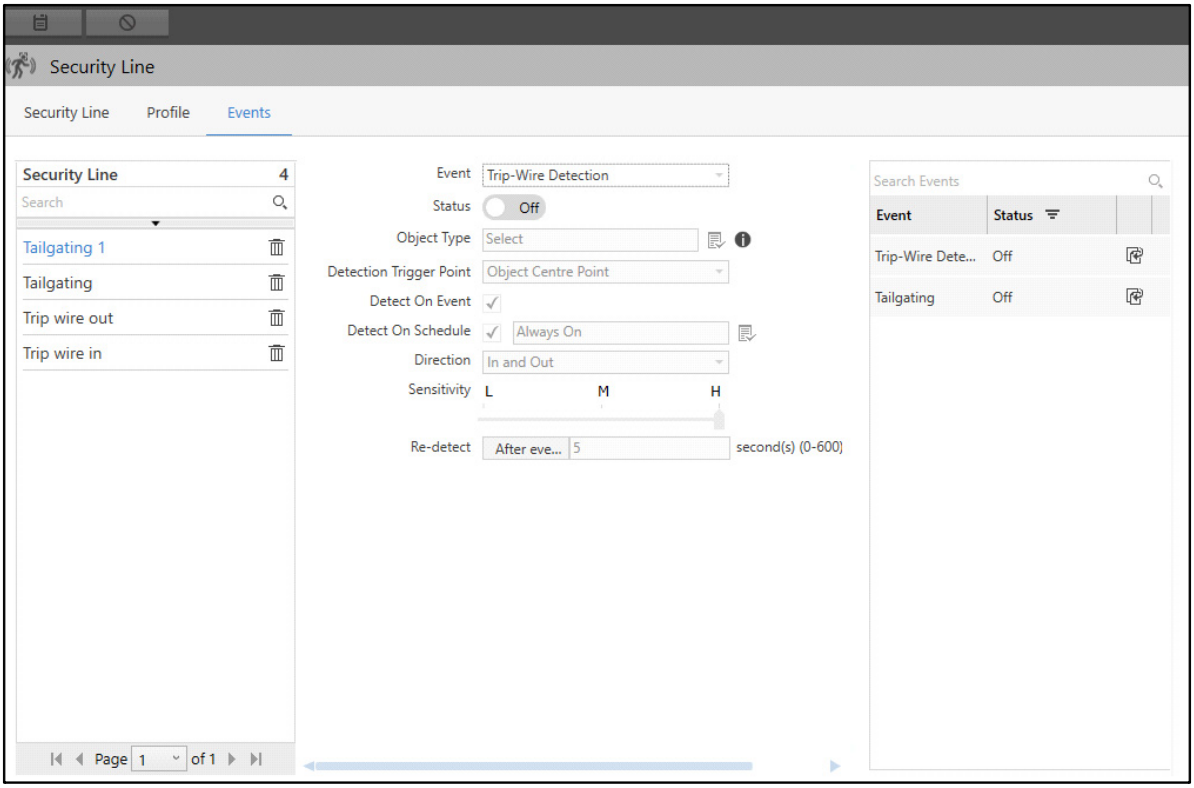
Events

This tab enables you to configure Events for the Security Lines. All the configured Events appear under the **Security Lines** tab.

Maximum and Minimum Object Width configured in any "Profile" will not be applicable if you select Object Type in any Event.

To configure Events,

- Click the **Events** tab.



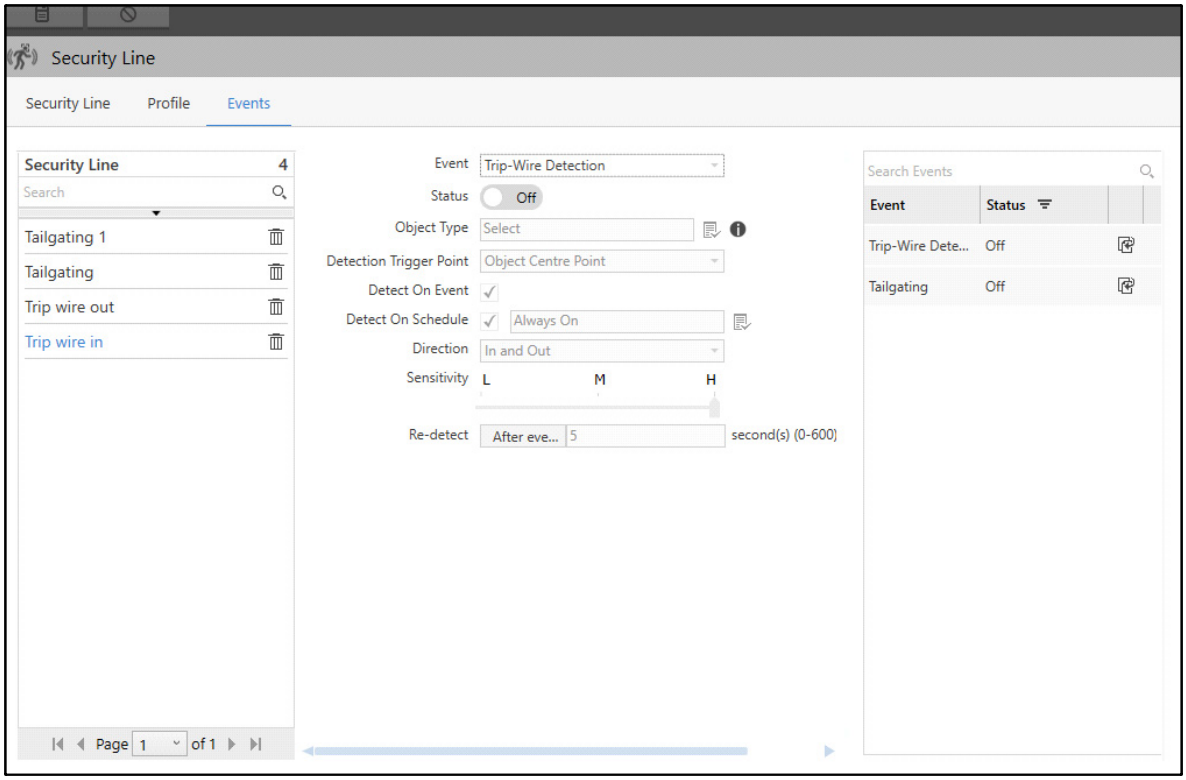
For Security Lines, you can configure two types of Events — “Trip-Wire Detection” and “Tailgating”.

Trip-Wire Detection

The Trip-Wire feature restricts a trespasser from crossing the line. A line can be drawn across the camera live view. Any object or person crossing the drawn line will generate an Event depending on the direction of movement.

To configure Trip-Wire Event for Security Lines,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

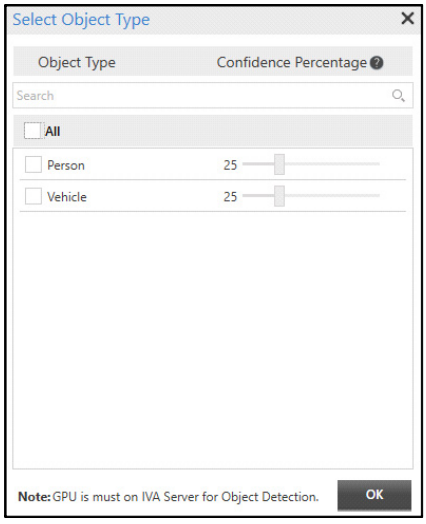


Configure the following parameters:

- **Event**: Select the Trip-Wire Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



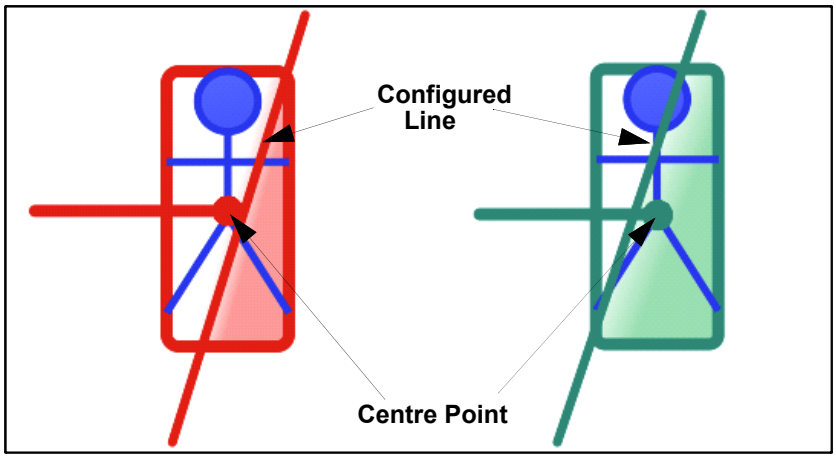
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point. Based on the selected option, the IVA engine will detect the selected Object Type.

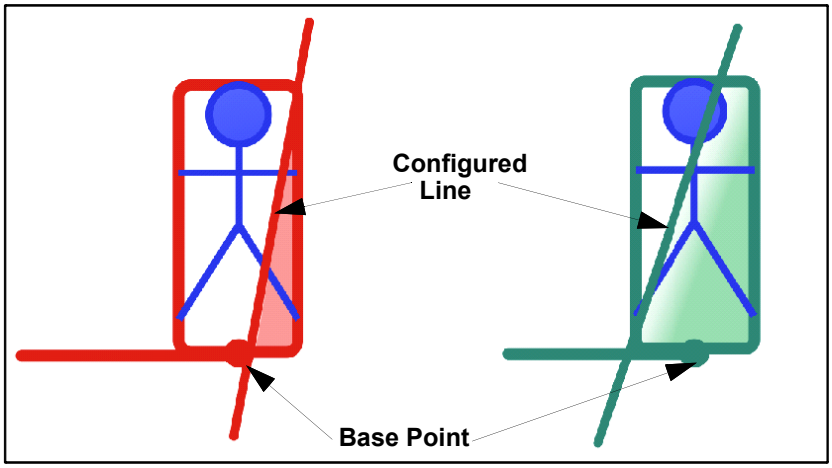
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured line.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point of the object crosses the configured line, an event will be generated.



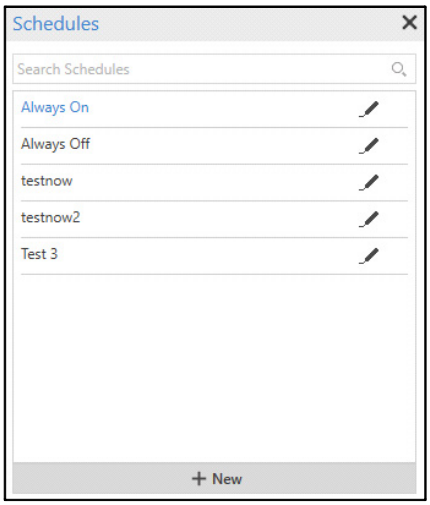
  If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured line.

  In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured line, an event will be generated.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.

- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



    - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.
- **Direction**: Select the direction from the drop-down list options — In and Out, Out, In.

  If you select **In**, the Event will occur when an object/person crosses the line in the direction of green color.

  If you select **Out**, the Event will occur when an object/person crosses the line in the direction of red color.

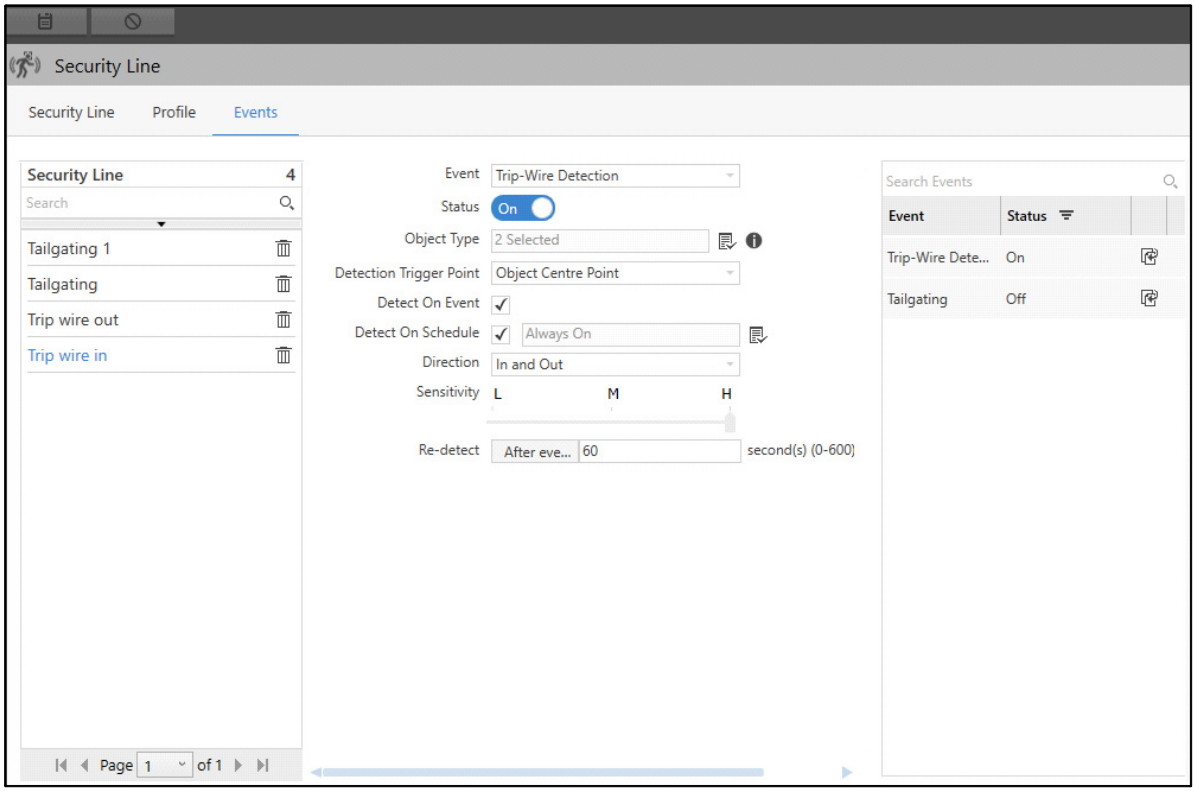
  If you select **In and Out**, the Event will occur either when an object/person crosses the line either in the direction of green or red color.
- **Sensitivity**: Drag the slider to set the desired sensitivity for the Trip-Wire Detection Event — Low, Medium or High.

If you have selected Object Type, then Sensitivity will be disabled.

- **Re-detect**: Specify the Re-detect time after which the Trip-Wire Detection Event should detect again after the previous detection. Valid Range: 0-600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

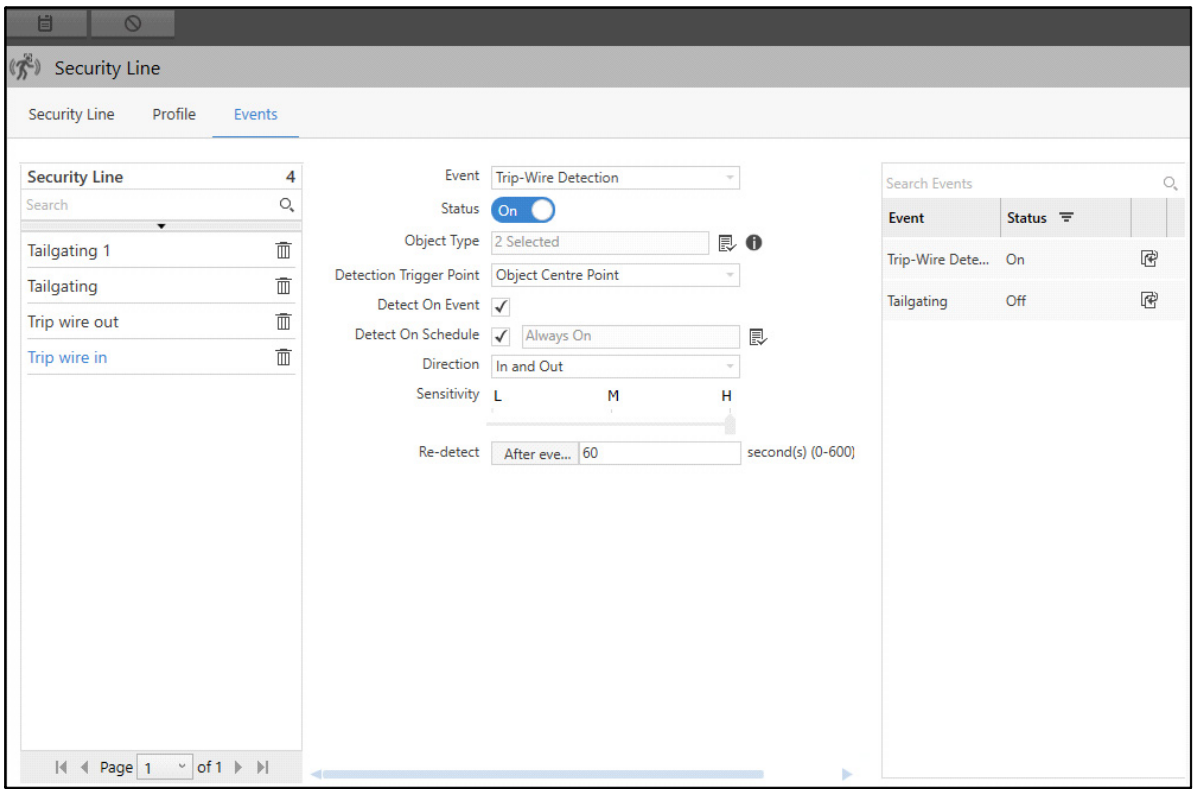


- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

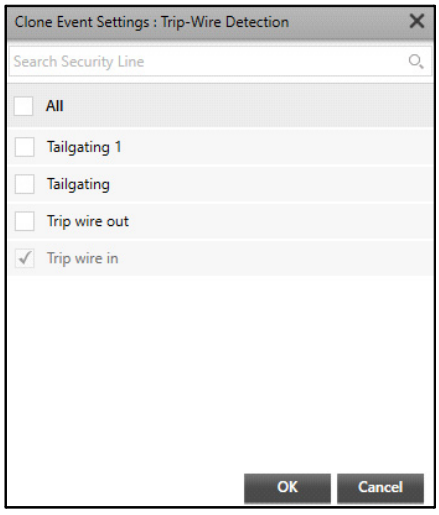
Once the Event is configured, you can also copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Security Line is created, the **Clone Event Settings** option gets enabled.*

Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Trip-Wire Detection** pop-up appears.



- Select the desired security lines to which you wish to copy these configurations.

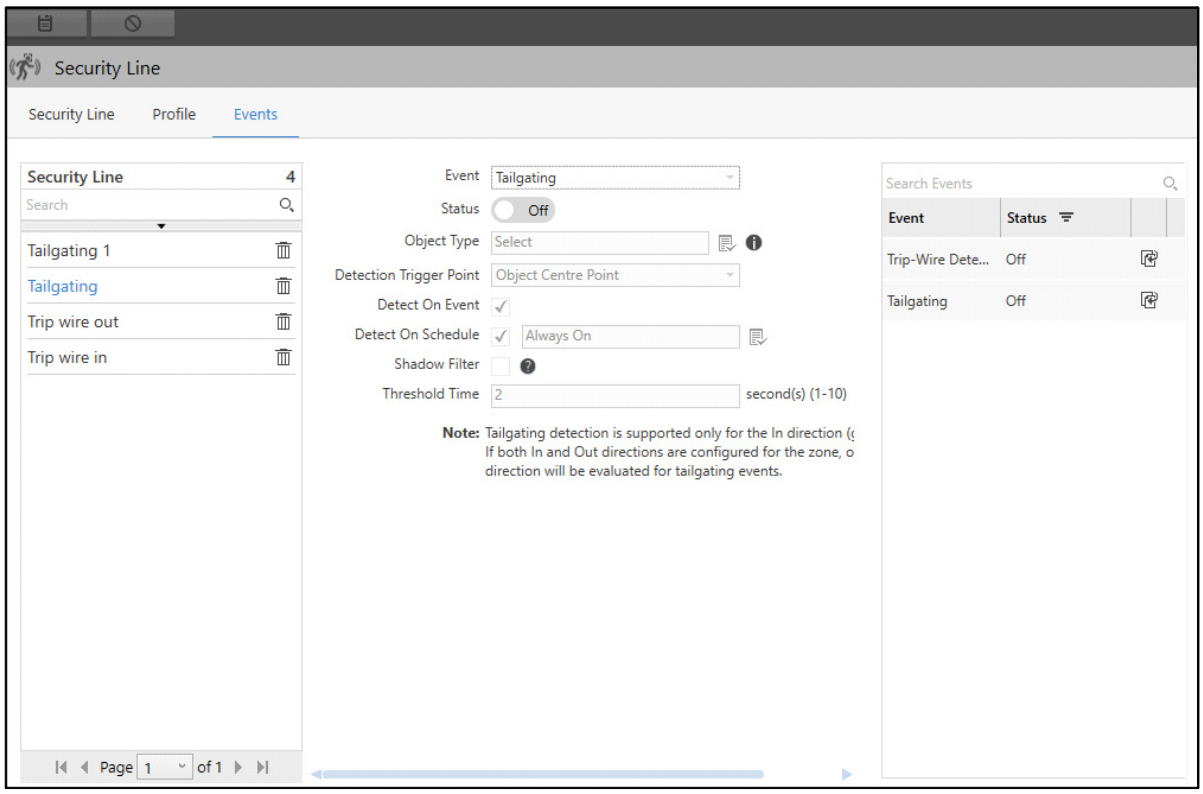
- Click **OK** to confirm or click **Cancel** to discard.

Tailgating

Tailgating feature is used in offices or access control areas where valid entry of only one person with proper access is allowed. If another person is entering forcibly without having proper authorization of entering then such entering can be triggered as event.

To configure Tailgating Event for Security Lines,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

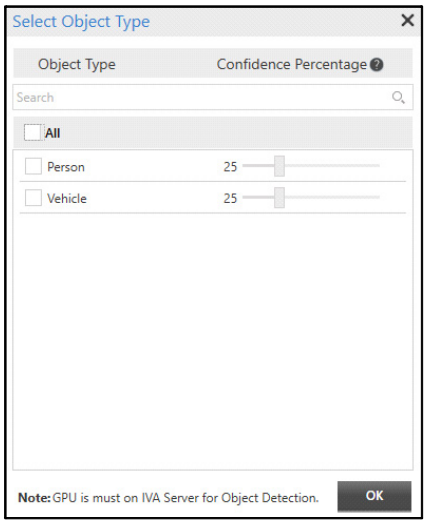


Configure the following parameters:

- **Event**: Select the Tailgating event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



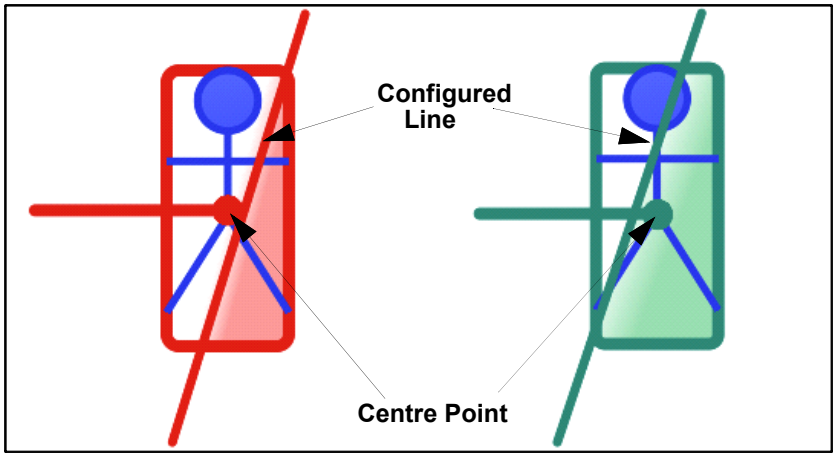
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point. Based on the selected option, the IVA engine will detect the selected Object Type.

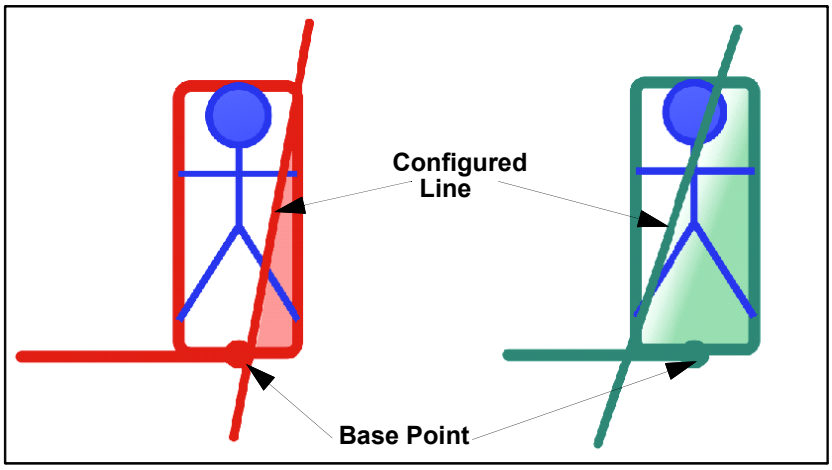
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured line.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point of the object crosses the configured line, an event will be generated.

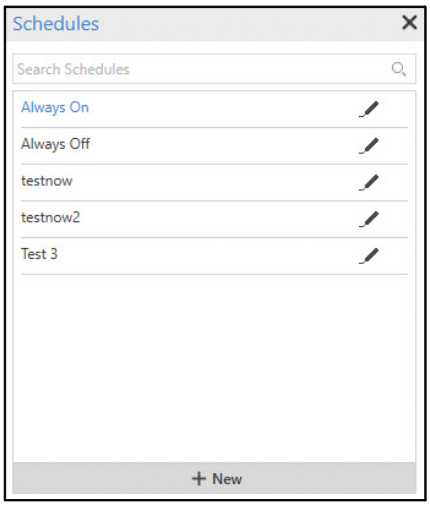


If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured line.

In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured line, an event will be generated.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



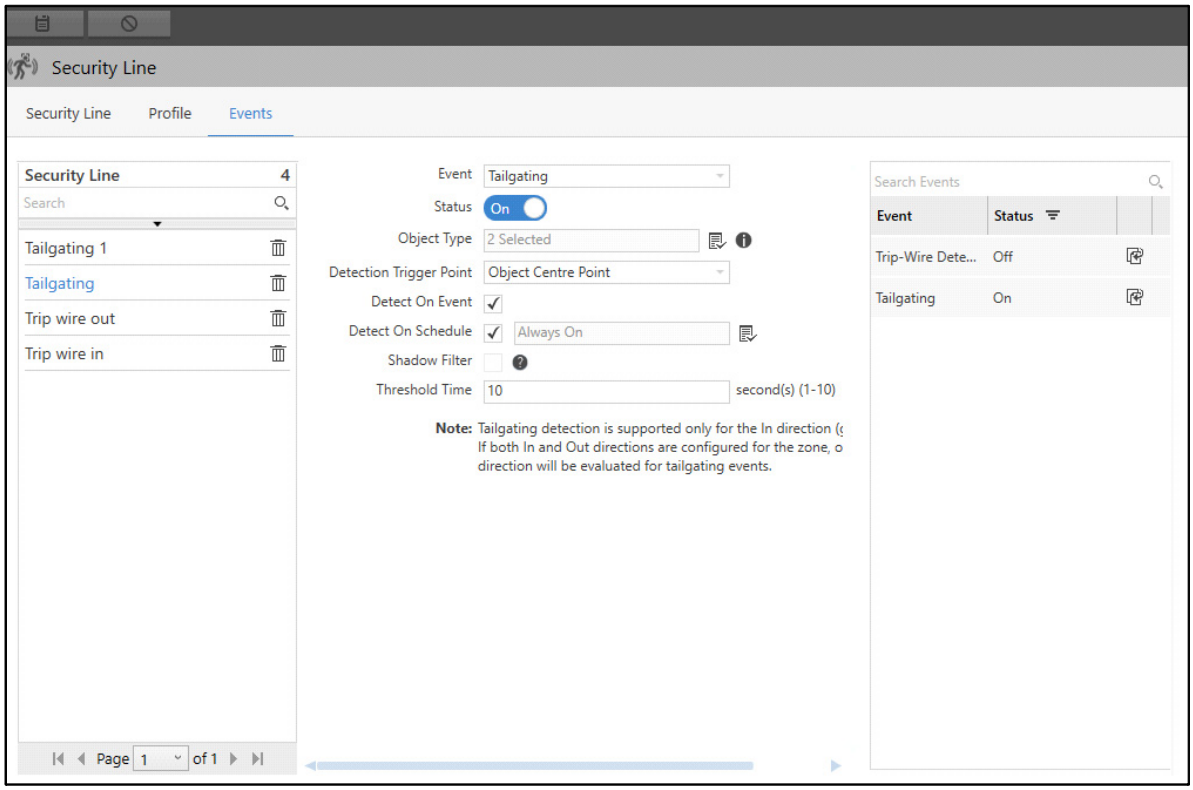
  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.
- **Shadow Filter**: Select the check box to ignore the shadow of people crossing the line and reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Threshold Time**: Specify the Threshold time. This is the time between two events crossing the Tailgating Line. If 2nd person crosses the line before the threshold time then it is considered as Tailgating. Valid Range: 1-10 seconds. Default: 2.

- Click **Save** to save the settings or **Cancel** to discard.

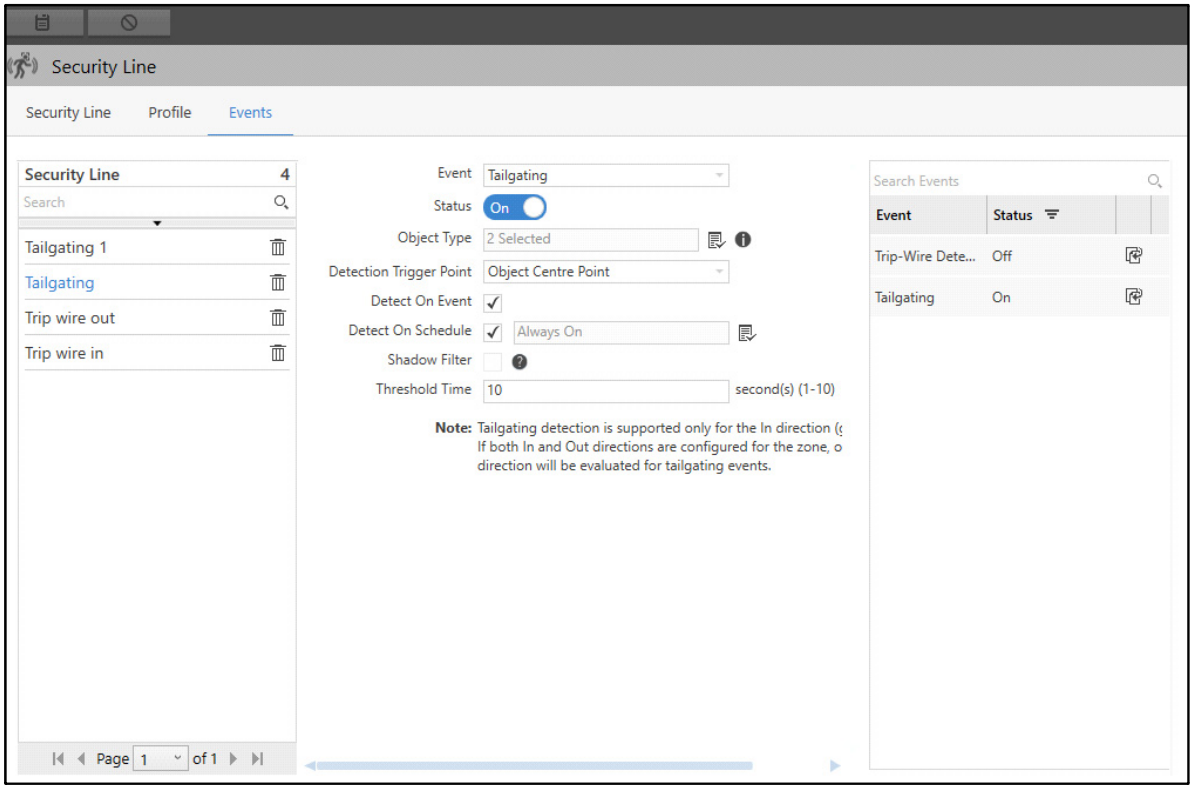
Once you have configured the Event, you can edit its configurations or disable it.



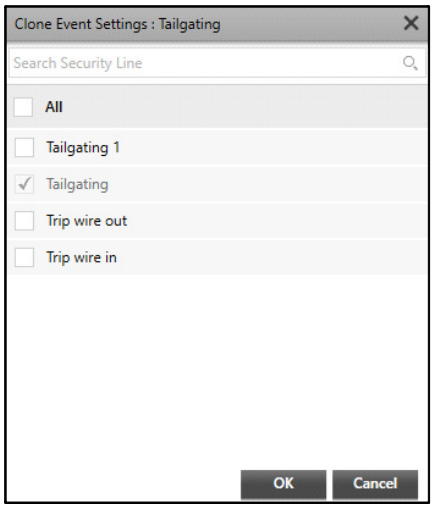
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Tailgating** pop-up appears.



- Select the desired security lines to which you wish to copy these configurations.

- Click **OK** to confirm or click **Cancel** to discard.

Perimeter Zone

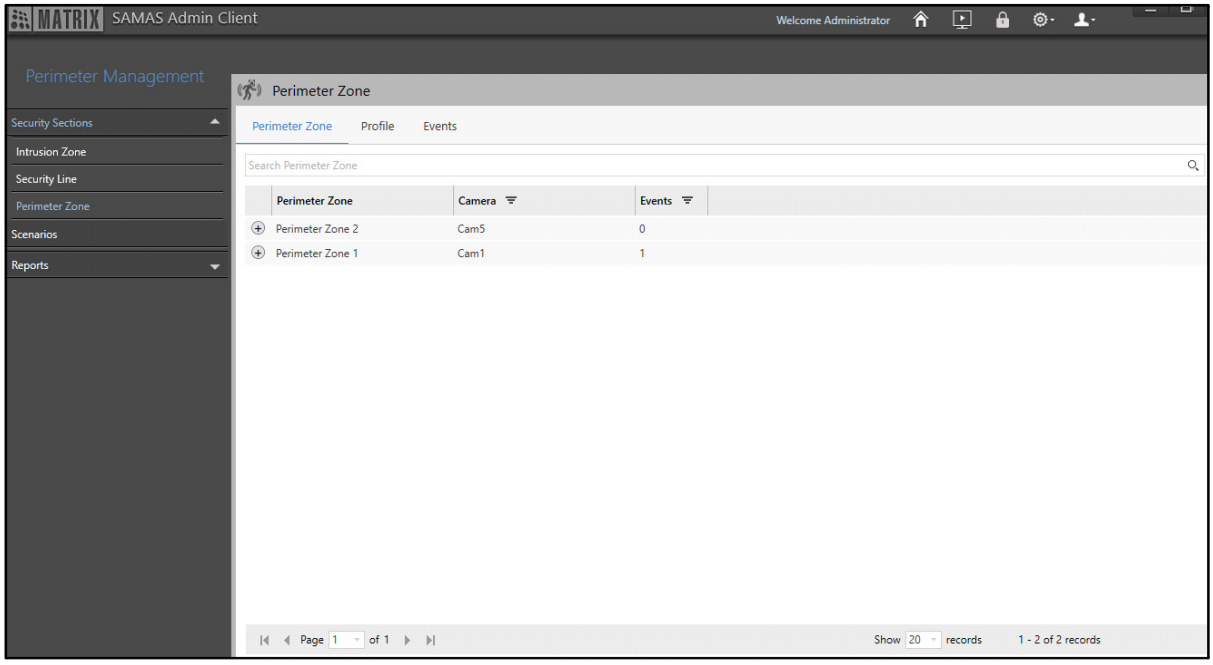
The Perimeter Management module allows you to configure the Perimeter Zones in the perimeter of an organization. This helps to detect any unwanted object/person (such as people or vehicle) passing through the configured zone in the area.

Perimeter Zone allows the configuration of an Event detection area on the perimeter of an organization and configure Motion Detection, No Motion Detection, Camera Tampering, Missing Object, Loitering Detection and Object Detection Event. These Events can then be used to create the scenarios which can alert the security person or management through the actions.

The Perimeter Zone page displays all the configured zones. You can view and configure the Perimeter Zones from this page.

To configure Perimeter Zone,

- Click **Perimeter Management > Security Sections > Perimeter Zone**.



The Perimeter Zone page consists of the following tabs.

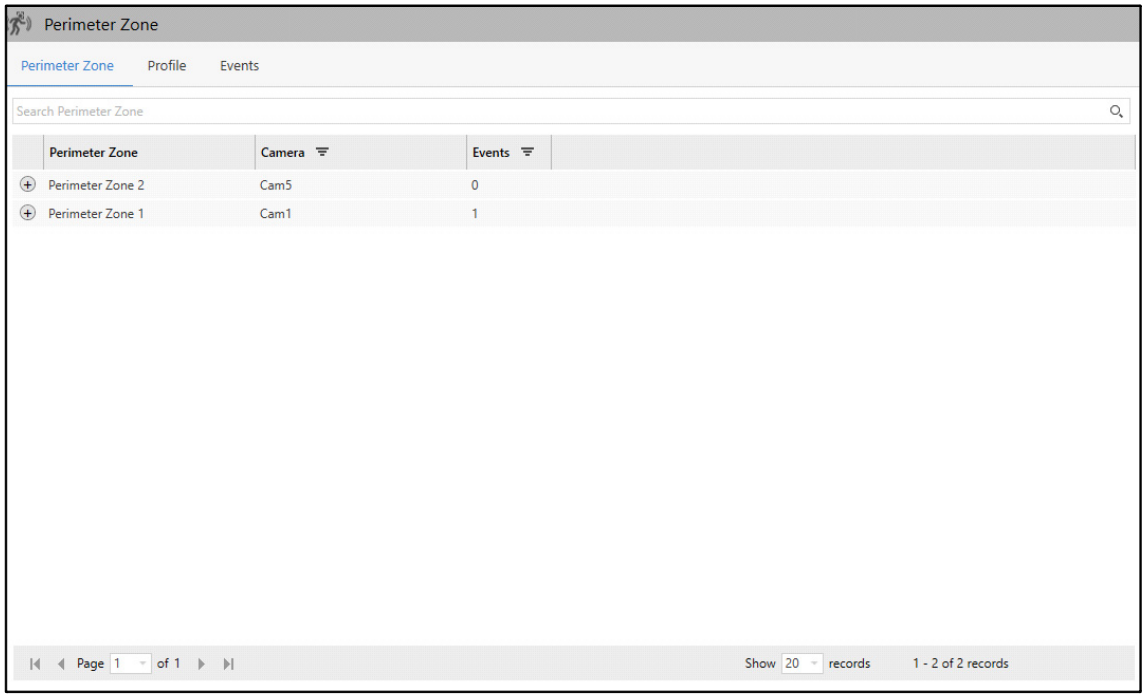
- “Perimeter Zone”
- “Profile”
- “Events”

Perimeter Zone

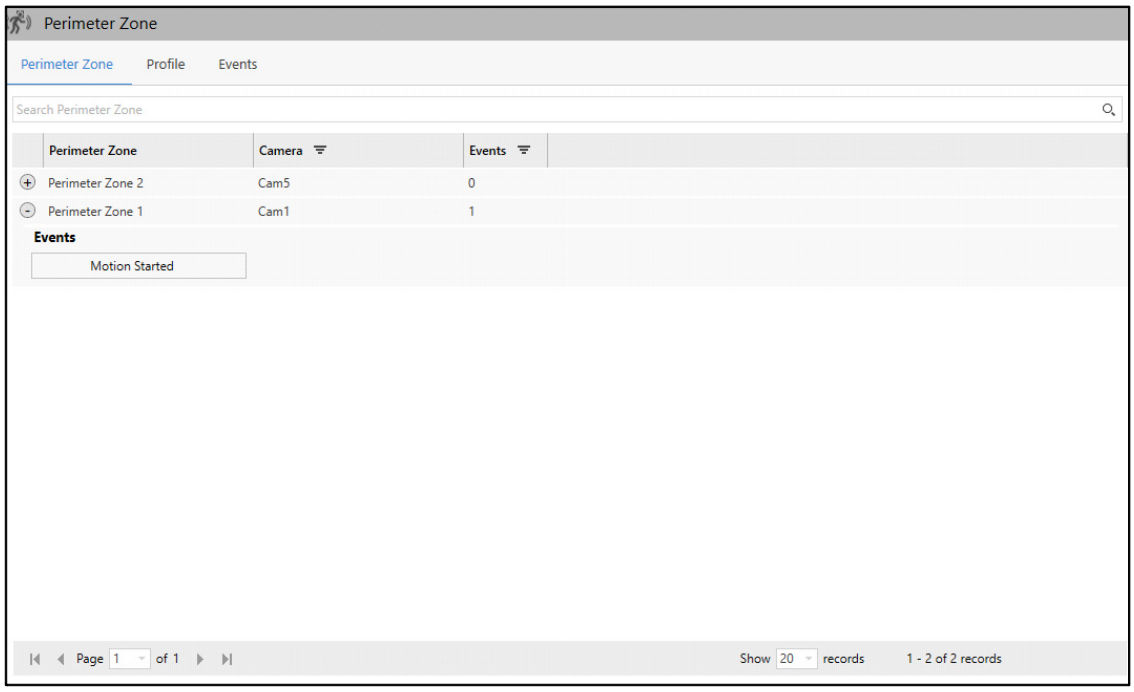
This tab enables you to view Perimeter Zones. You can configure the Perimeter Zones from “Profile”. All the Perimeter Zones and the Events configured for them appear under this tab. The following Perimeter Zone details are displayed — Perimeter Zone, Camera and Events.

To view Perimeter Zones,

- Click the **Perimeter Zone** tab.



- Click **Show Events** to view the Events configured for the Perimeter Zone.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

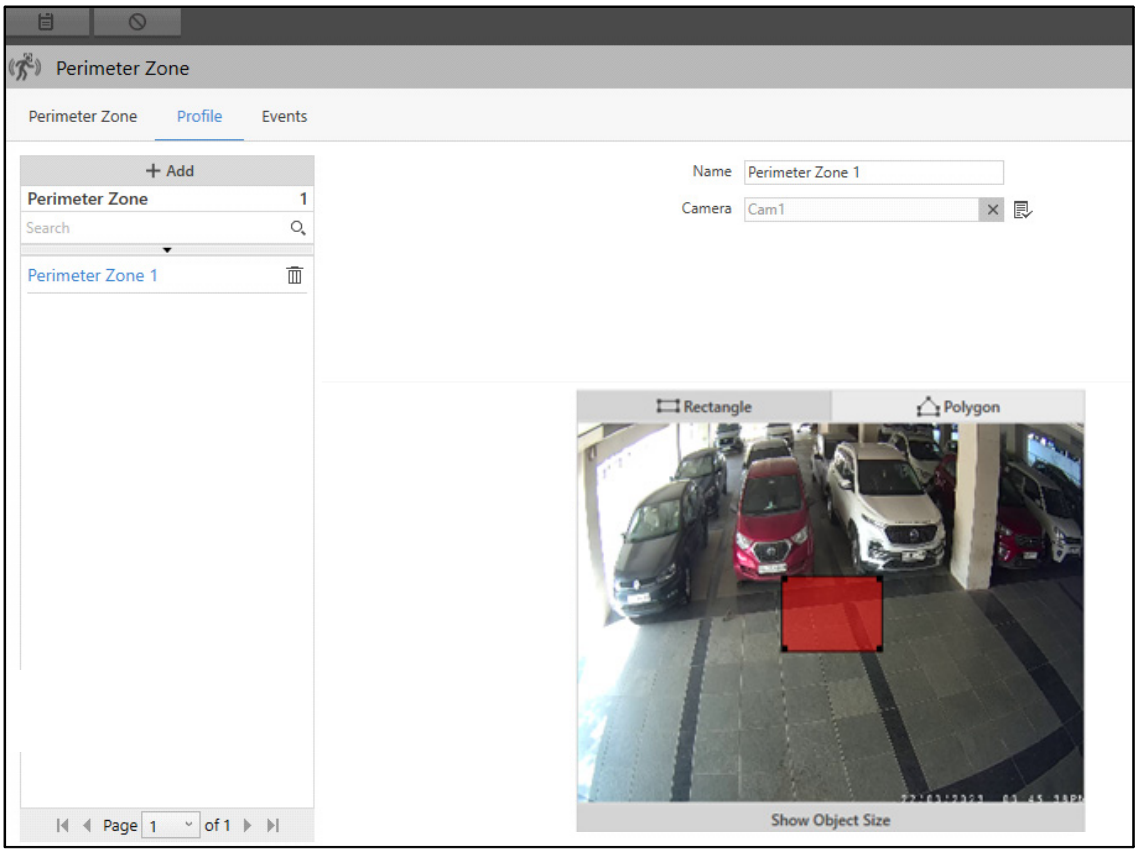
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

This tab enables you to configure Perimeter Zones. All the Perimeter Zones configured here appear under the **Perimeter Zone** tab.

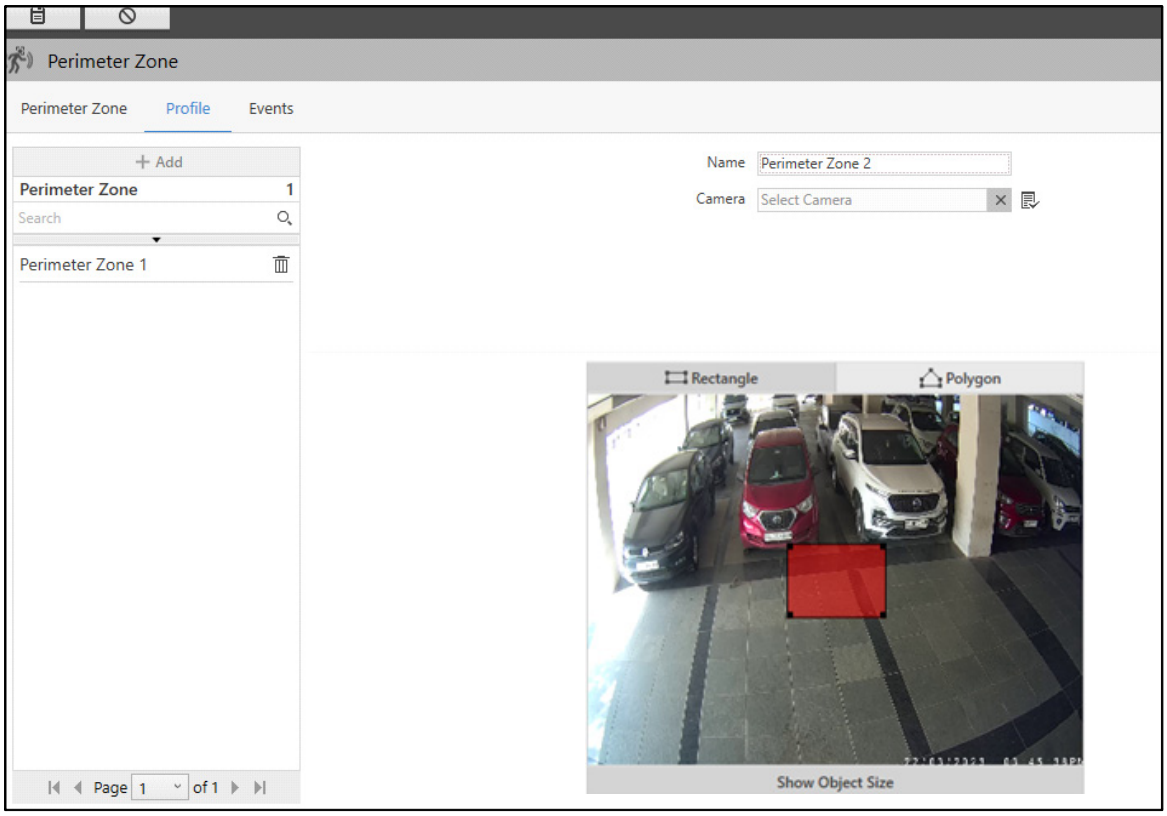
To configure Perimeter Zones,

- Click the **Profile** tab.



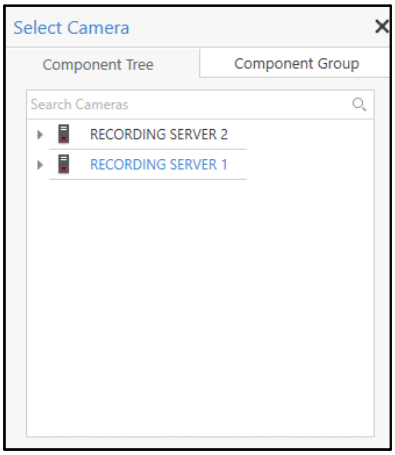
*The **Add** button is disabled when you are configuring Perimeter Zone for the first time. You can directly configure the parameters and save the Perimeter Zone.*

- Click **Add**.



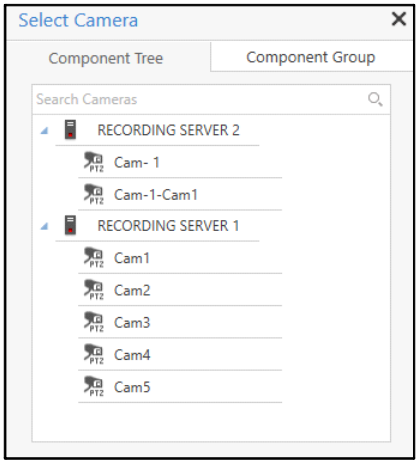
Configure the following parameters:

- **Name**: Specify a suitable name for the Perimeter Zone. In Name, you can enter upto 50 characters. Default: Blank.
- **Camera**: Select the desired camera which you wish to assign to the Perimeter Zone using the **Camera** picklist.
  - Click **Camera** picklist. The **Select Camera** pop-up appears.



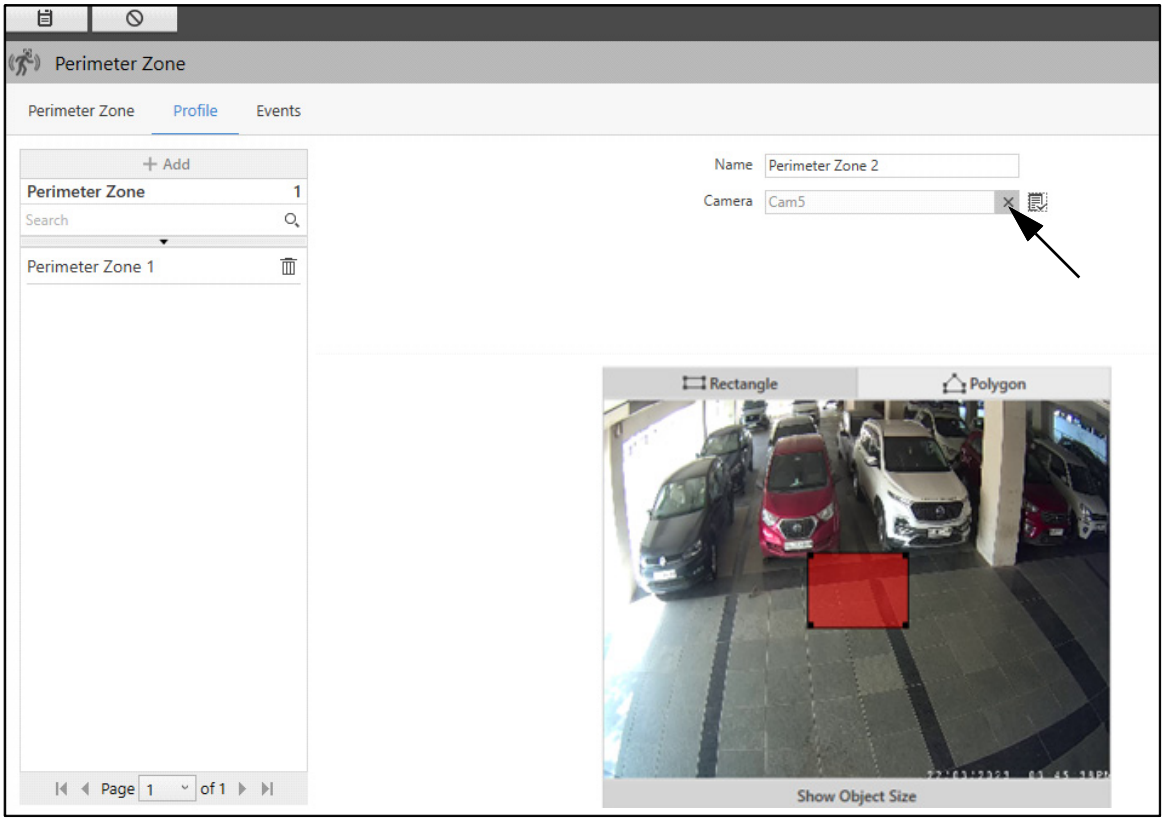
  - The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”.

Double-click the desired camera to assign it to the Perimeter Zone. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

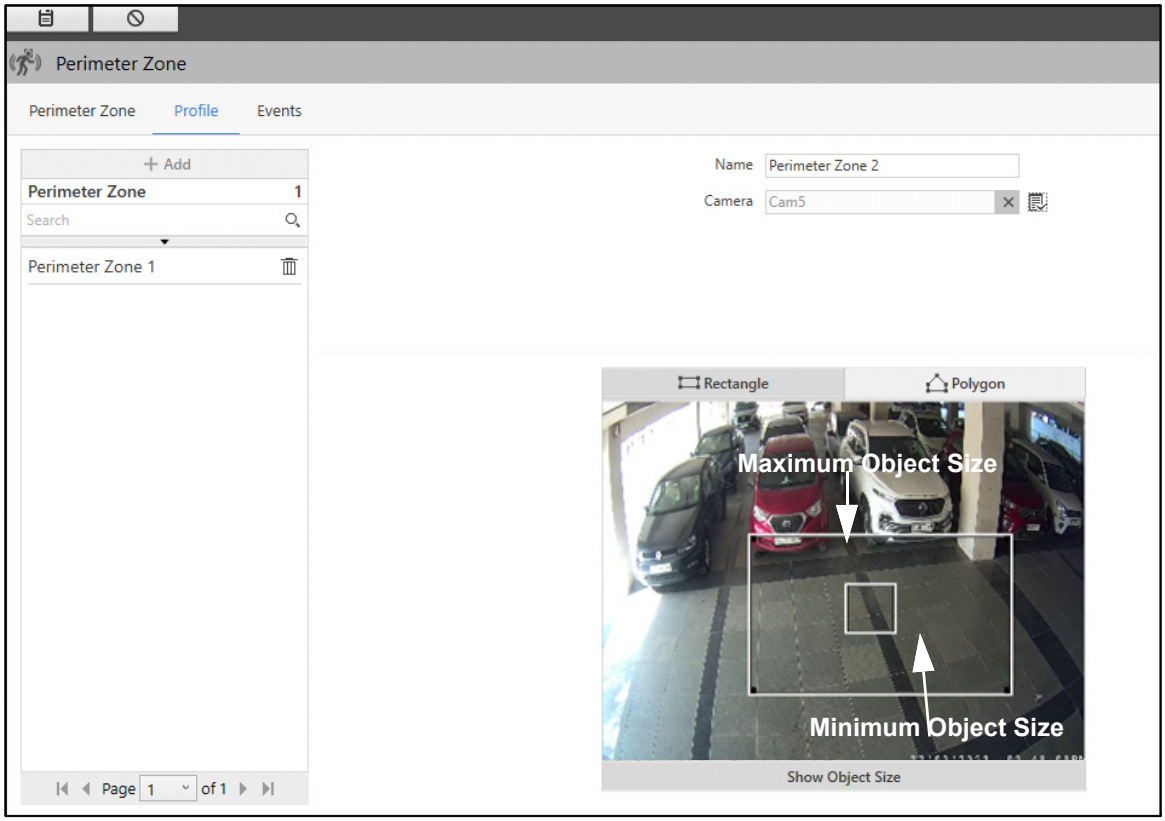
- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click to select the desired option.
  - Click **Go to selected position** , to move the camera to the selected preset position.
- To remove the camera, click **Remove** .



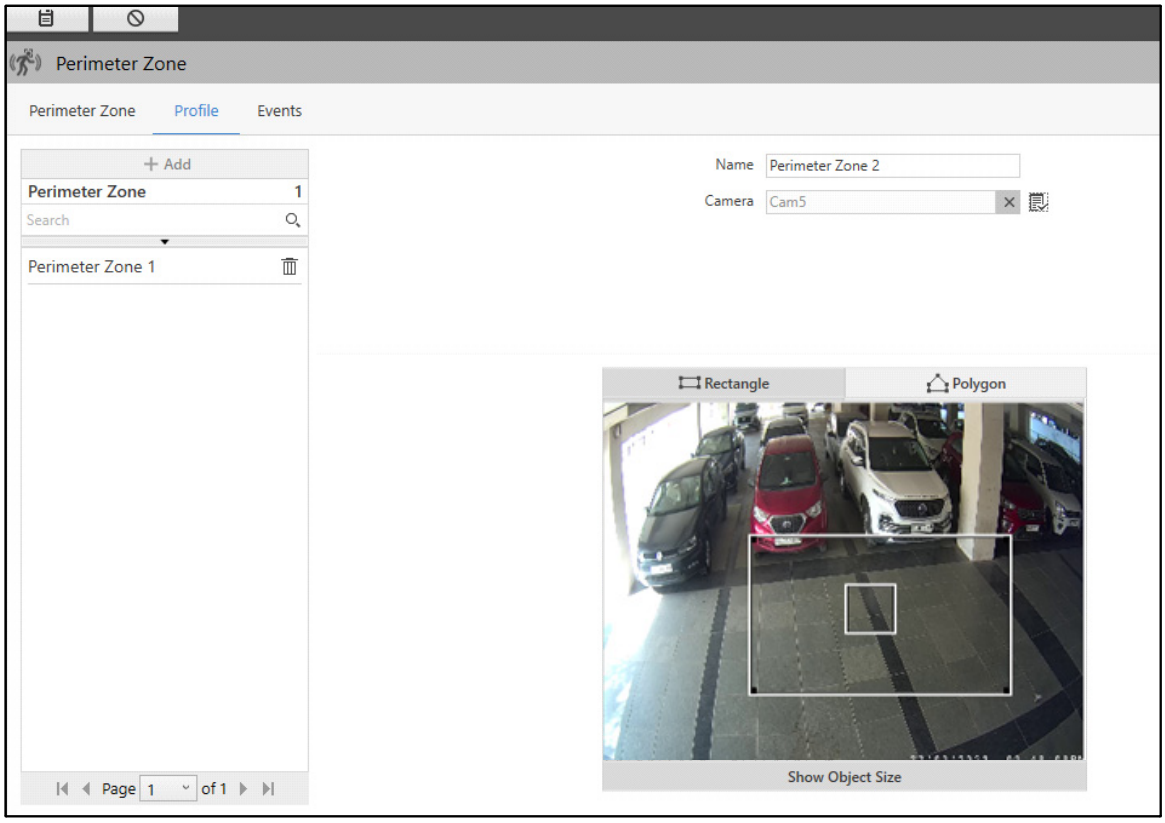
Once a camera is assigned, you can draw a Perimeter Zone on the live view of the camera. You can also define the Minimum and Maximum Object Size. You can either draw a Rectangle or Polygon to define the Perimeter Zone.

Object Size will not be applicable if you select Object Type in any Event. For details, refer to "Events".

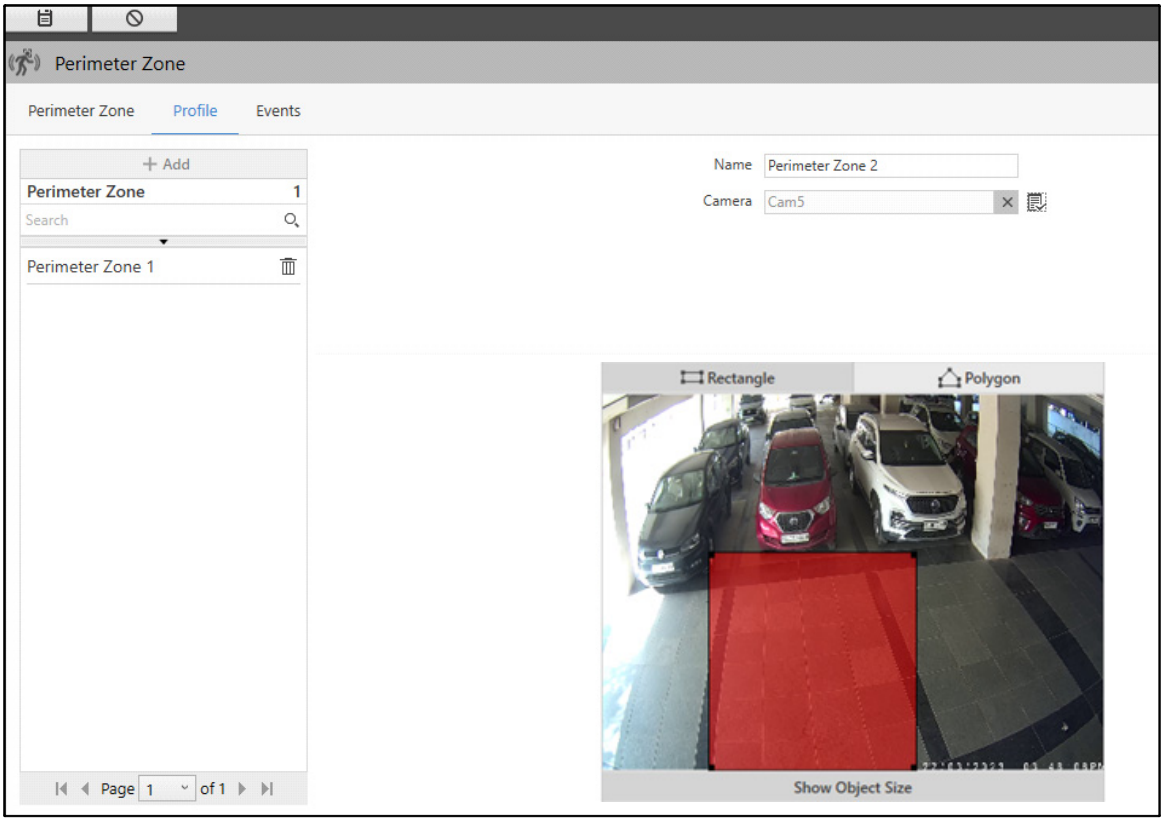
- Click **Show Object Size**. The default **Minimum** and **Maximum Object Size** appear.



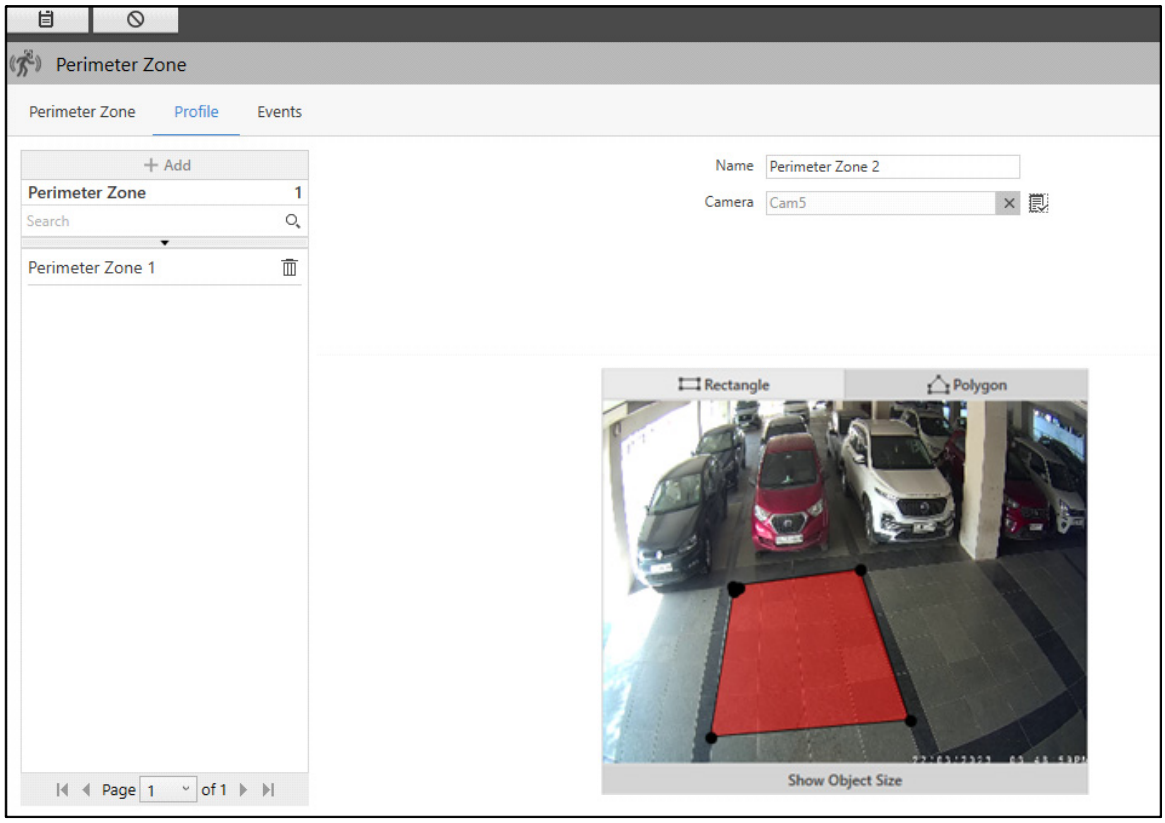
- Drag the corners of the rectangles to configure the Minimum and Maximum Object size to be detected in the Event, if required. When the object size meant to be detected in the Event does not fit in the default Minimum and Maximum Object Size, you can configure it to match the desired object size.



- Click **Save** to save the settings or **Cancel** to discard.
- Click **Hide Object Size** to hide the size and draw the perimeter.
  - Select either **Rectangle** or **Polygon** to draw the perimeter.
  - If you select **Rectangle**, drag the corners and sides of the rectangle to configure the perimeter.



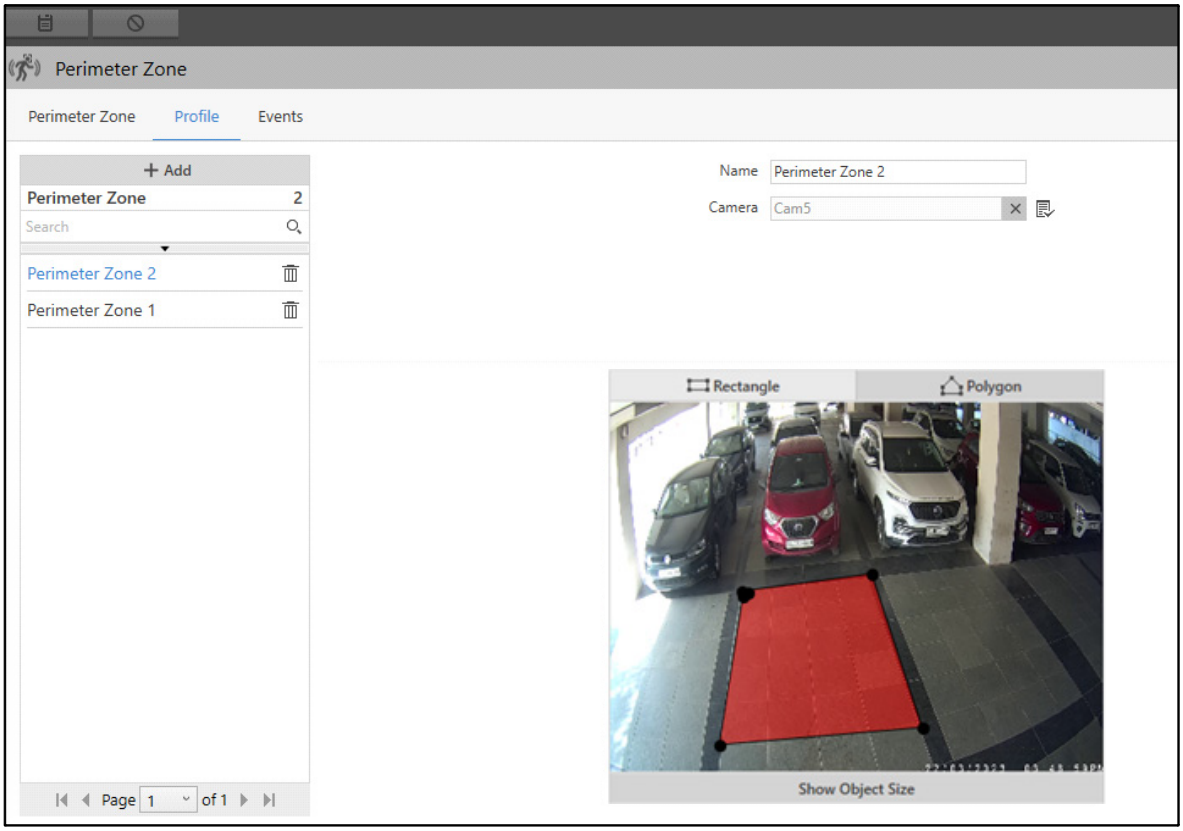
- If you select **Polygon**, click on the live view to place the vertex/node of the polygon. Click again on the desired place to join the previous vertex/node with the new vertex/node. Continue this process to complete the polygon.



- Click **Save** to save the settings or **Cancel** to discard.

The new Perimeter Zone will appear in the list on the left hand side.

You can edit the configurations of the Perimeter Zone or delete it.



- Select the desired Perimeter Zone from the list and edit the details on the right hand side.
  - Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired zone.

Similarly, you can configure the other Perimeter Zones.

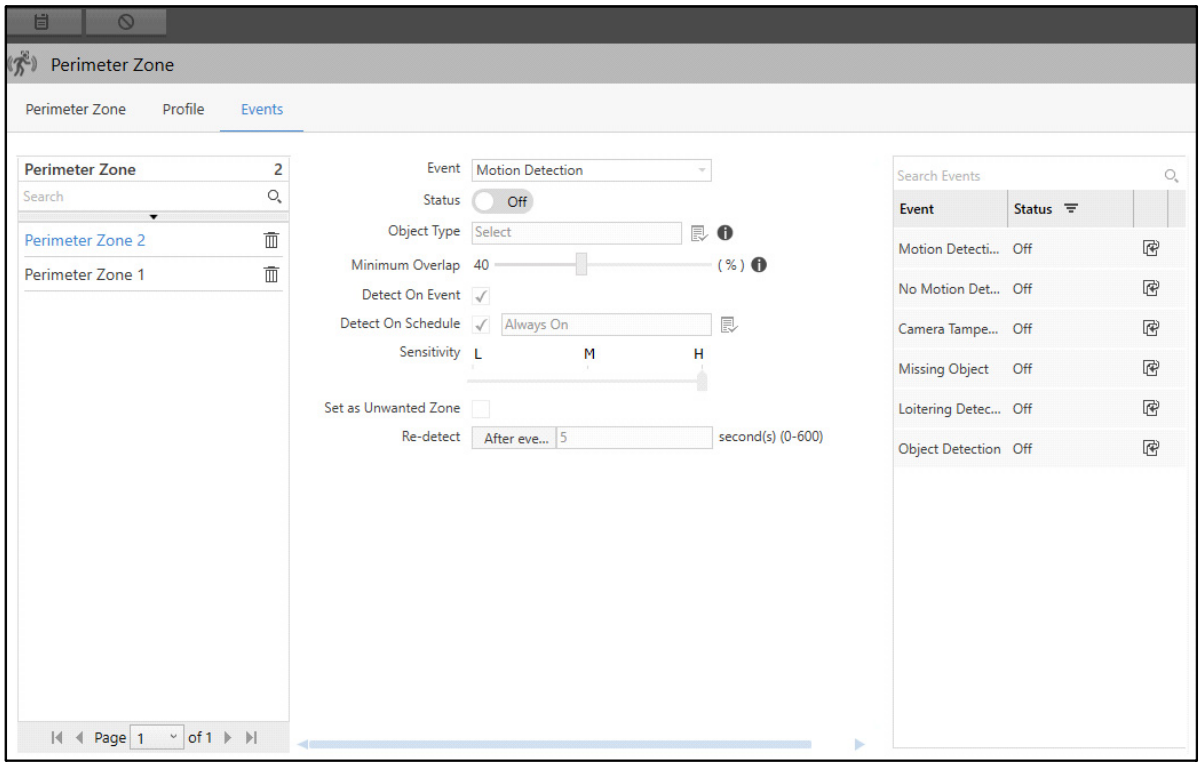
Events

This tab enables you to configure Events for the Perimeter Zones. All the configured Events appear under the **Perimeter Zone** tab.

Object Size configured in any "Profile" will not be applicable if you select Object Type in any Event.

To configure Events,

- Click the **Events** tab.



For Perimeter Zones, you can configure the following Events:

- "Motion Detection"
- "No Motion Detection"
- "Camera Tampering"
- "Missing Object"
- "Loitering Detection"
- "Object Detection"

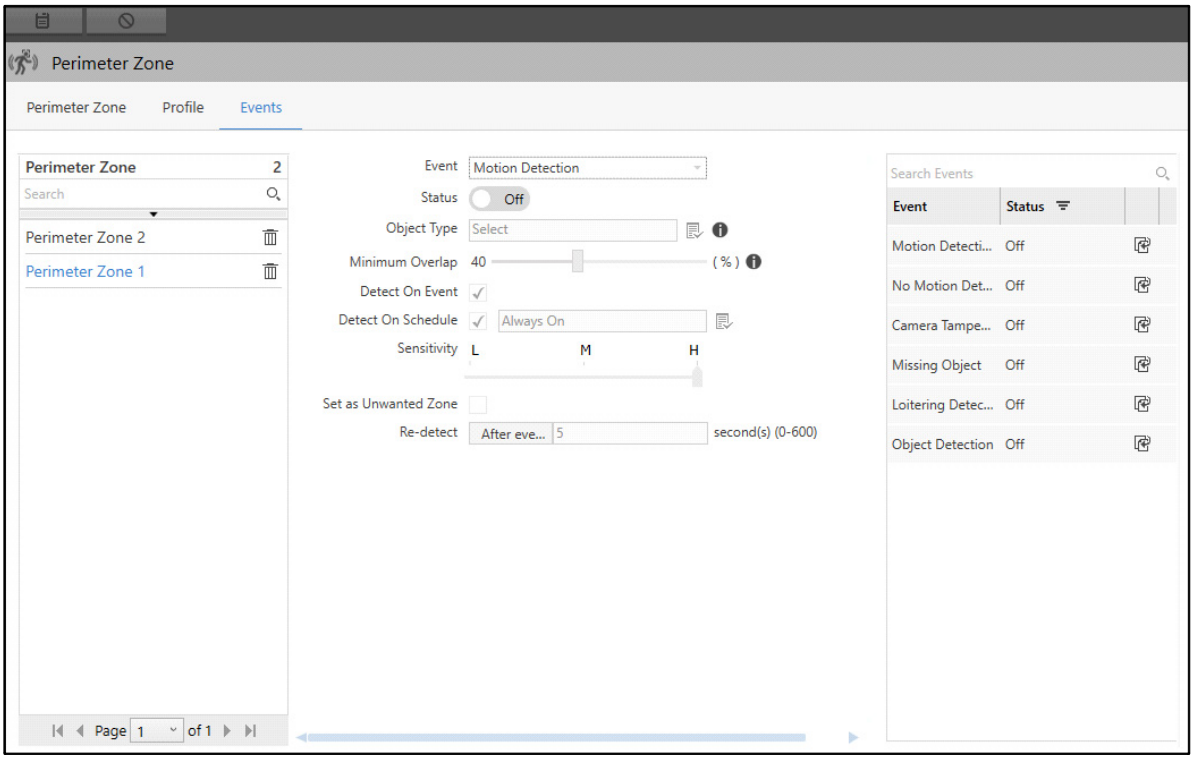
Make sure you select Object Type in the desired Event as per your application scenario.

Motion Detection

The Motion Detection feature enables you to configure Motion Detection Event for a Perimeter Zone. Such an event is required where no motion is expected to occur in the area of vision of the configured camera. For example, at a location such as Server Room, where entry is restricted. If any motion takes place at this location, the Motion Detection Event will occur.

To configure Motion Detection Event for Perimeter Zones,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

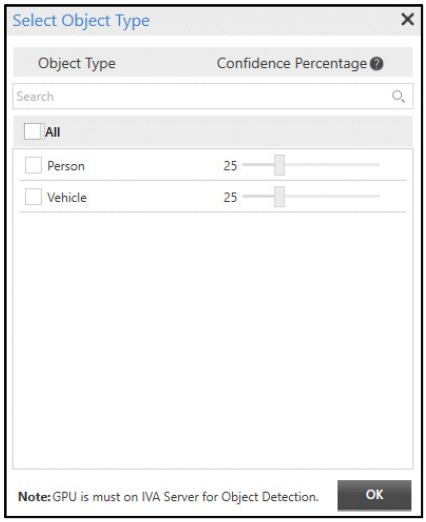


Configure the following parameters:

- **Event:** Select the Motion Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



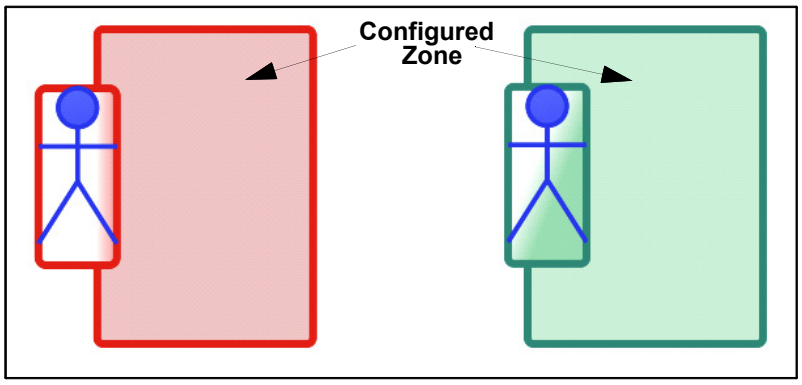
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

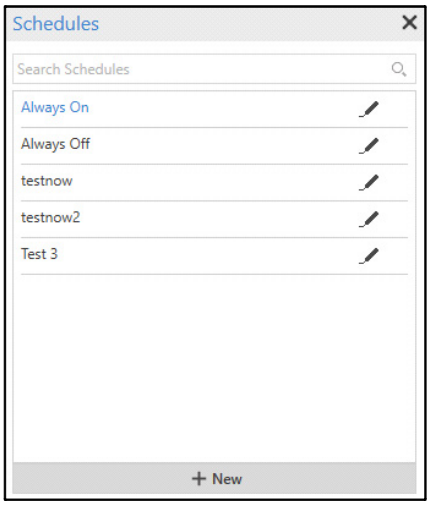
- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the zone to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the zone will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the zone will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Zone, the event will be triggered when the object is moving and 30% of the object is overlapping the configured zone. Whereas, in the Red Zone, the event will not be triggered as, the object is moving but only 10% of the object is overlapping the configured zone.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Sensitivity**: Drag the slider to set the desired sensitivity for the Motion Detection Event — Low, Medium or High.

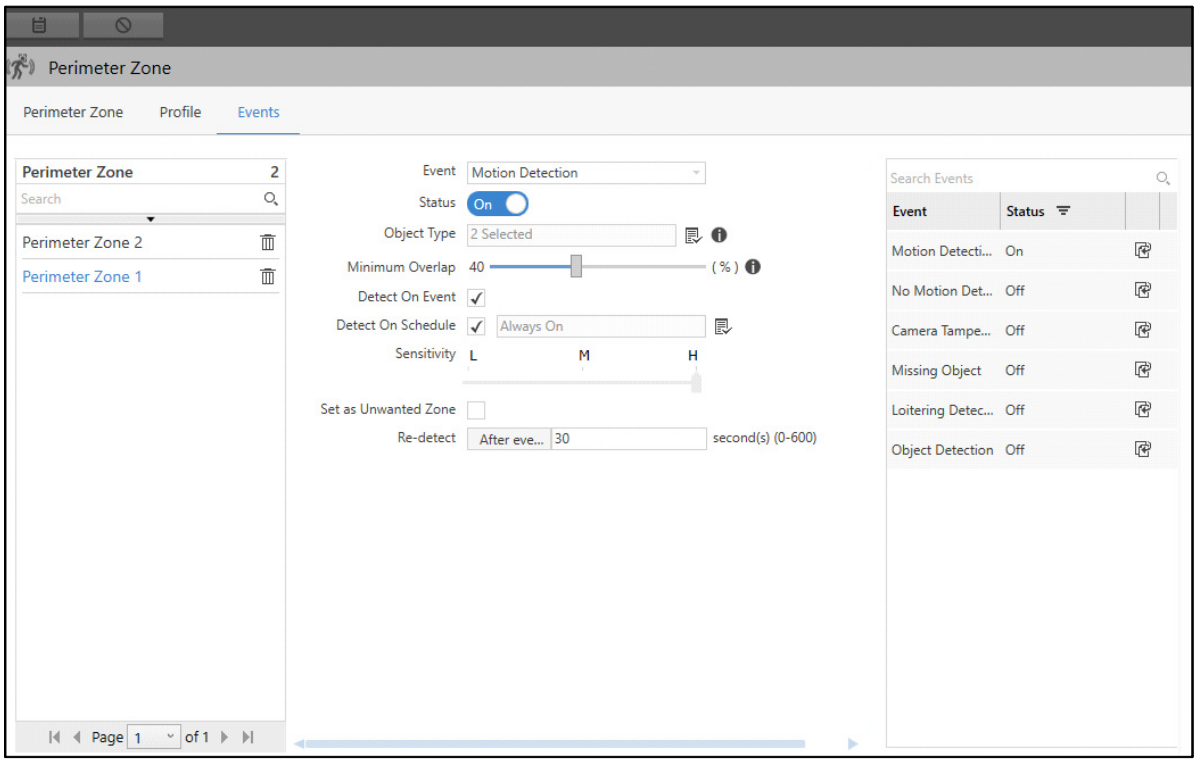
If you have selected Object Type, then Sensitivity will be disabled.

- **Set as Unwanted Zone**: Select the check box to ignore all the motion detected in the selected zone. This is useful in eliminating the detection of false Events due to unwanted motion in certain regions of the live view. For example, moving trees, flickering lights, etc.

- **Re-detect After every**: Specify the Re-detect time after which the Motion Detection Event should be detected again after the previous detection. Valid Range:0-600 seconds. Default:5.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

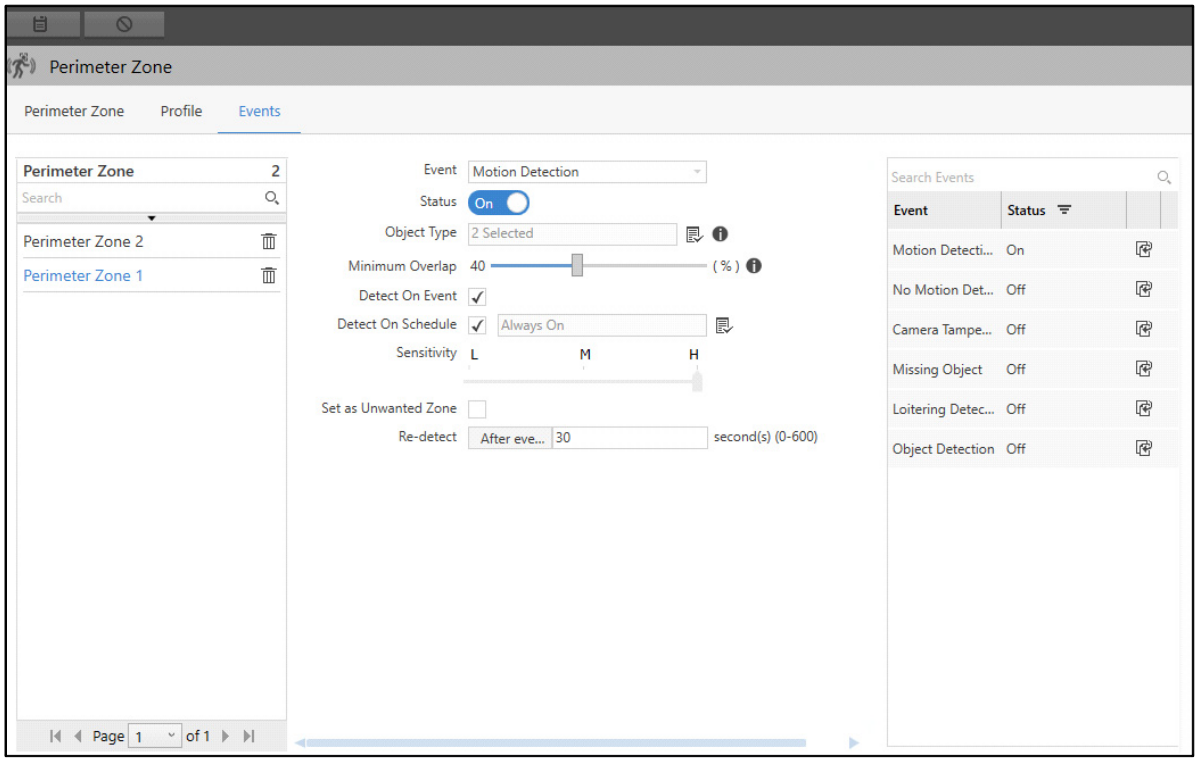


- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

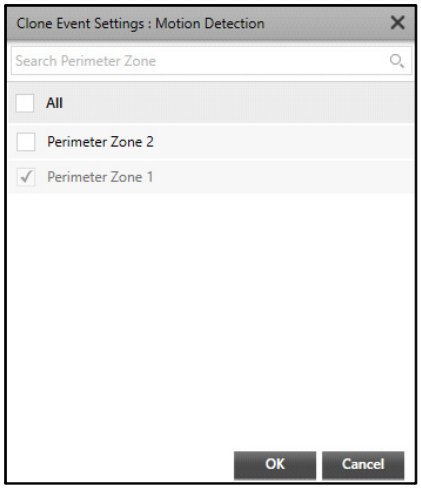
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Perimeter Zone is created, the **Clone Event Settings** option gets enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Motion Detection** pop-up appears.



- Select the desired zones to which you wish to copy these configurations.

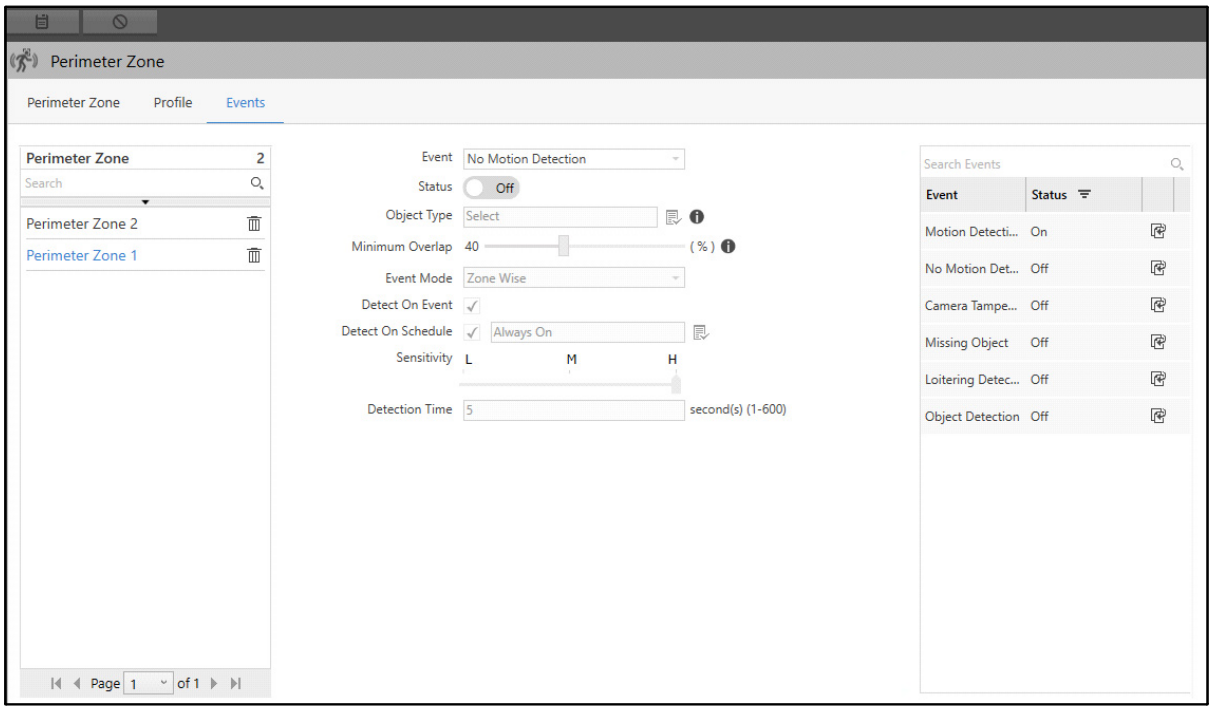
- Click **OK** to confirm or click **Cancel** to discard.

No Motion Detection

The No Motion Detection feature enables you to configure No Motion Detection Event for a Perimeter Zone. Such an event is required where continuous motion is expected to occur in the area of vision of the configured camera. For example, at locations such as factories, security check-posts etc. If continuous motion does not take place at this location, the No Motion Detection Event will occur.

To configure No Motion Detection Event for Perimeter Zones,

- Select the desired profile from the left hand side for which you wish to configure the Event.

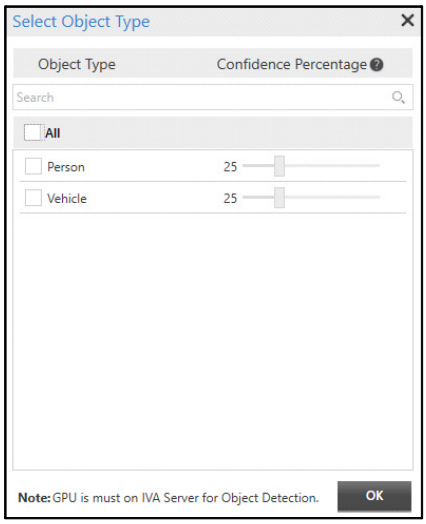


Configure the following parameters:

- **Event:** Select the No Motion Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



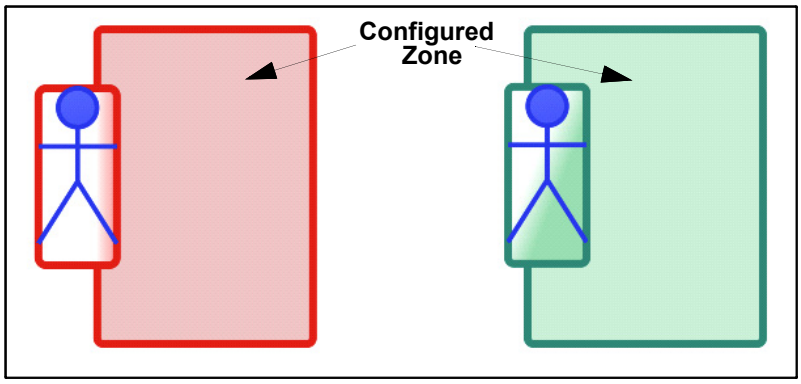
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the zone to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the zone will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the zone will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Zone, the event will be triggered as the object is static and 30% of the object is overlapping the configured zone. Whereas, in the Red Zone, the event will not be triggered as the object is static but only 10% of the object is overlapping the configured zone.

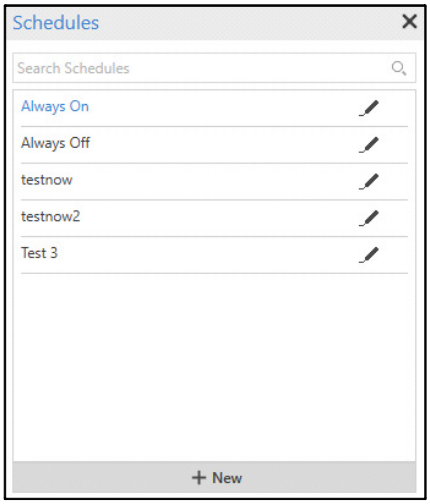


- **Event Mode**: It is un-editable and displays **Zone Wise**. This indicates the mode through which the IVA engine will trigger the event.

Under **Zone Wise** Event Mode, the event will be triggered only when all the objects in the configured zone are not moving.

For example, the selected Object Type is Person for a zone configured as Zone 1. Now, two persons are detected in this zone, say Person A and B. Under Zone Wise Event Mode, the No Motion event will be triggered only when both Person A and B are not moving.

- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".
- **Sensitivity**: Drag the slider to set the desired sensitivity for the No Motion Detection Event — Low, Medium or High.

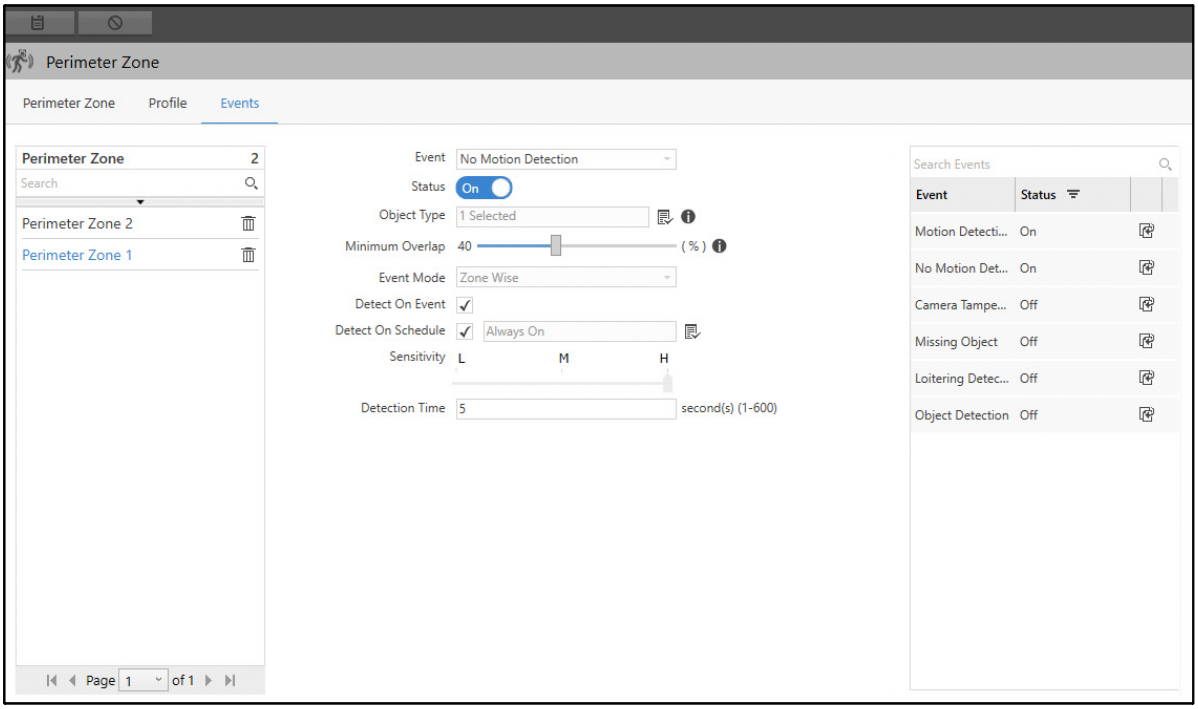
If you have selected Object Type, then Sensitivity will be disabled.

The term Sensitivity refers to the amount of change required in image for no motion to be detected in a no motion block between two consecutive frames. While at high sensitivity, the slightest variation in a no motion block would trigger a No Motion Started Event from the IVA Server, lowering the sensitivity would reduce the number of no motion blocks to be detected in the video, hence no motion will be detected only after a considerable change.

- **Detection Time**: Specify the Detection Time in seconds. If no motion is detected in the configured zones during this time, a No Motion Event is generated. Valid Range: 1-600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

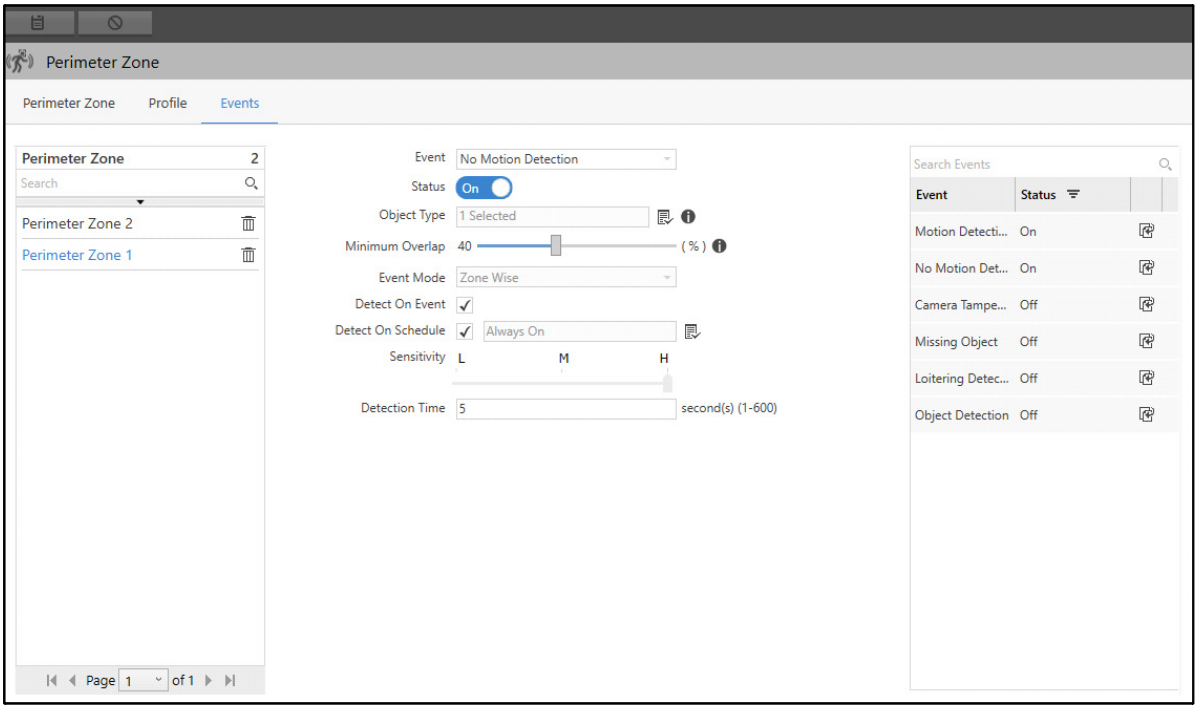
Once you have configured the Event, you can edit its configurations or disable it.



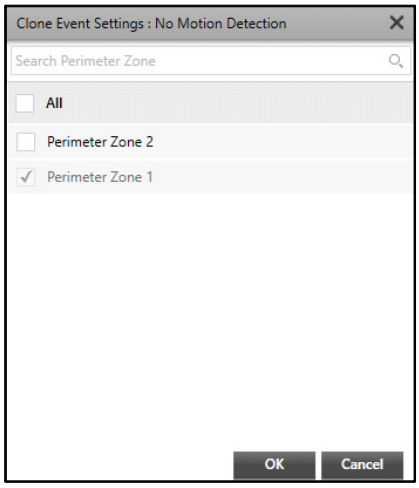
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: No Motion Detection** pop-up appears.



- Select the desired zones to which you wish to copy these configurations.

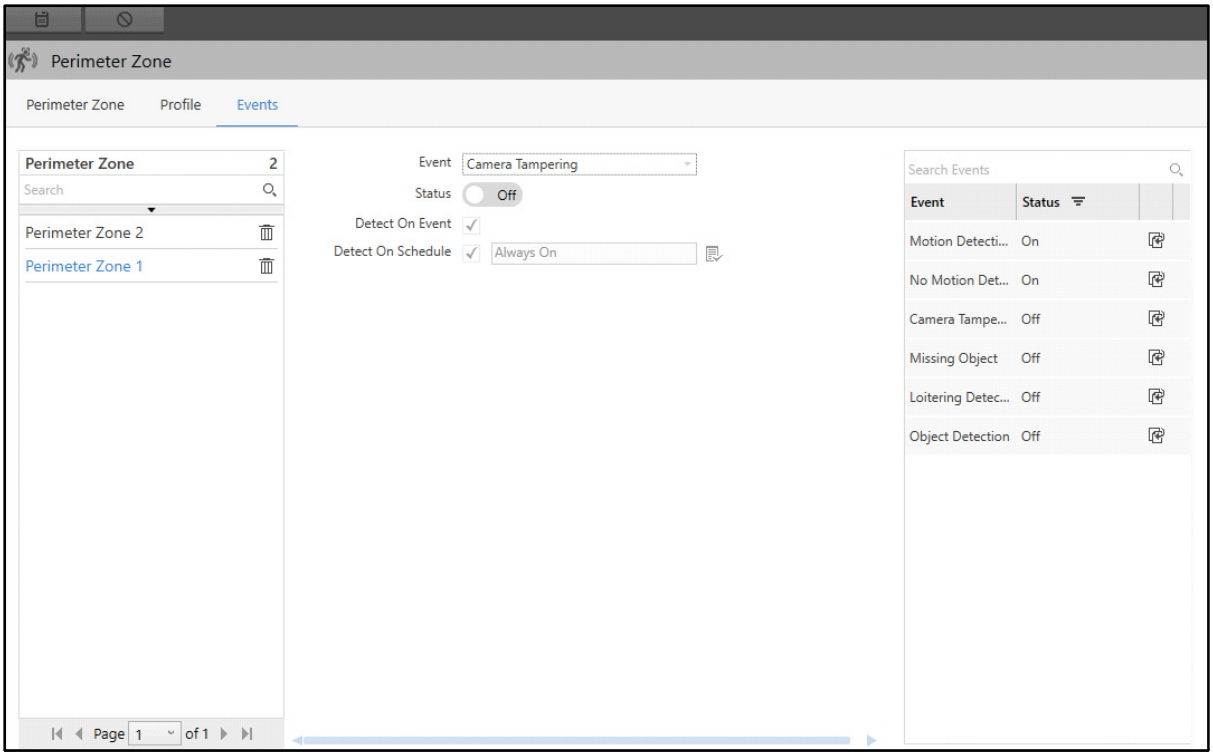
- Click **OK** to confirm or click **Cancel** to discard.

Camera Tampering

The Camera Tampering feature monitors the live streaming of a camera and detects any attempts to impair the normal camera functioning. This may involve sabotaging actions such as partially or fully blocking the lens or field of view of the camera, drastically changing the camera angle or other similar actions leading to camera failure.

To configure Camera Tampering Event for Perimeter Zones,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

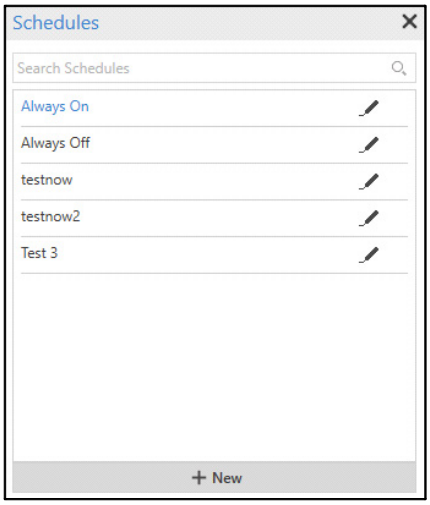


Configure the following parameters:

- **Event:** Select the Camera Tampering Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

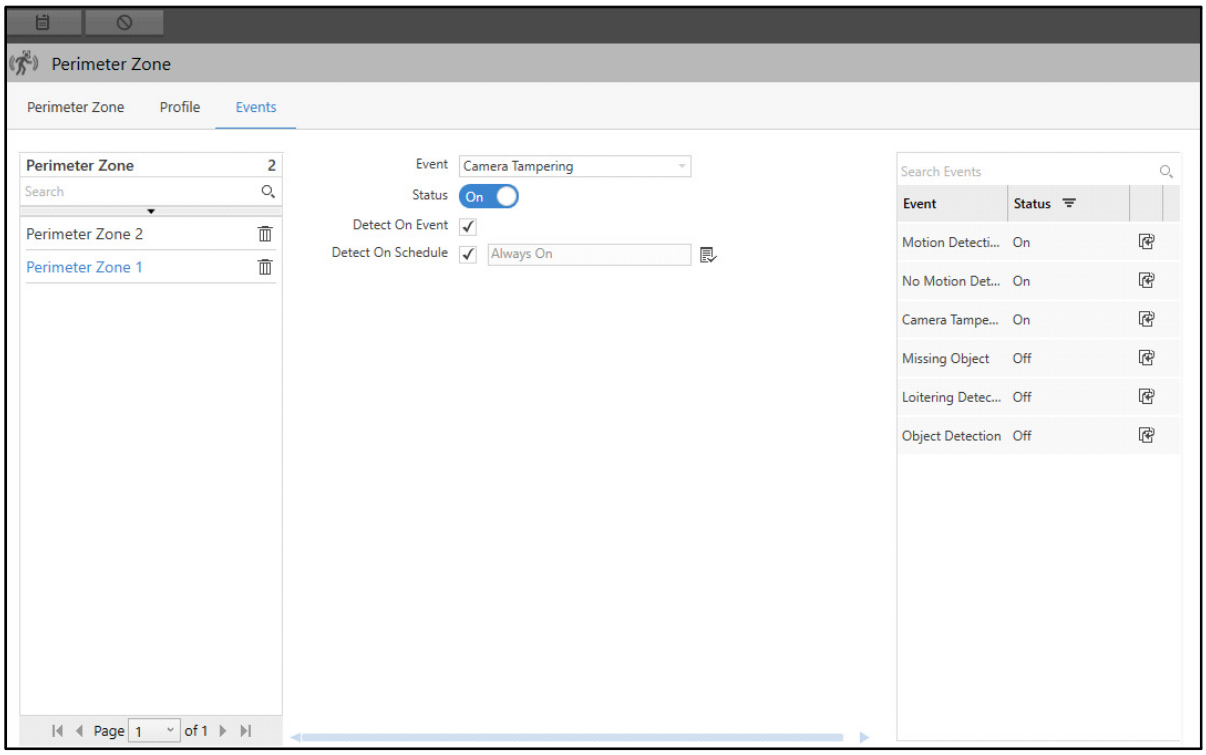
- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.



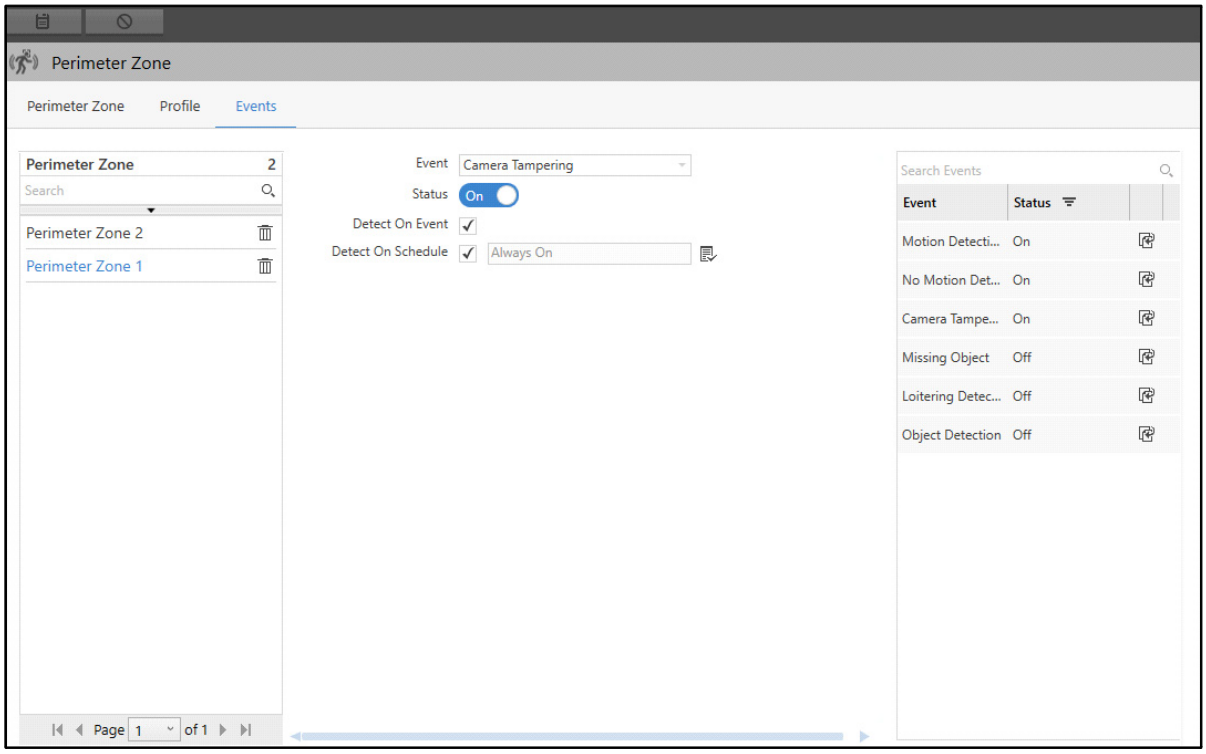
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.

- Click **Save** to save the settings or **Cancel** to discard.

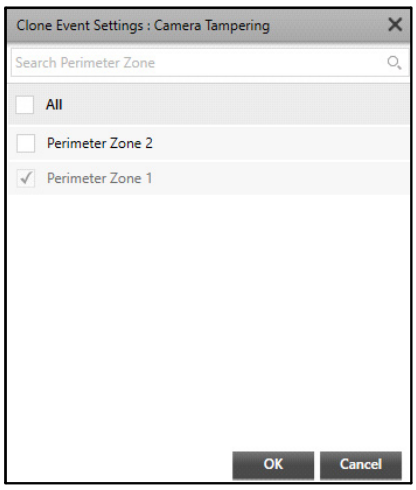
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Camera Tampering** pop-up appears.



- Select the desired zones to which you wish to copy the configurations.

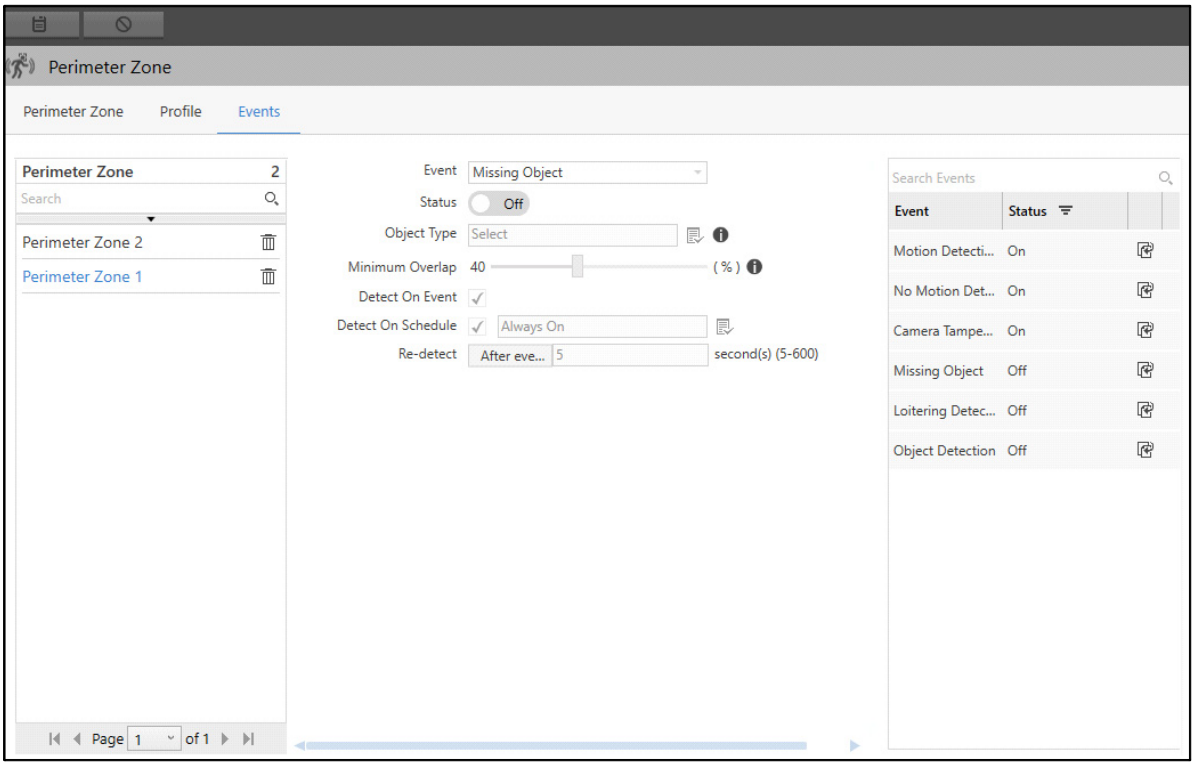
- Click **OK** to confirm or click **Cancel** to discard.

Missing Object

The Missing Object feature monitors the live streaming of a camera and detects any objects that go missing from the Perimeter Zone.

To configure Missing Object Event for Perimeter Zones,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

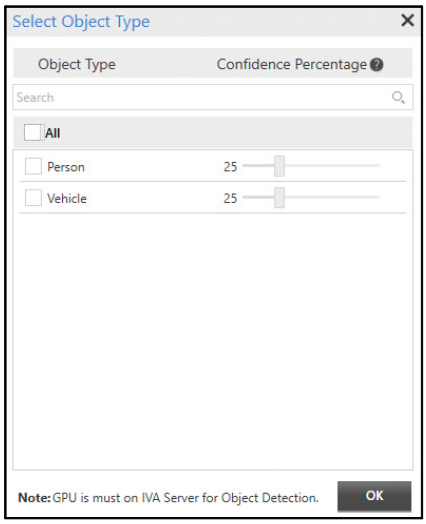


Configure the following parameters:

- **Event:** Select the Missing Object Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



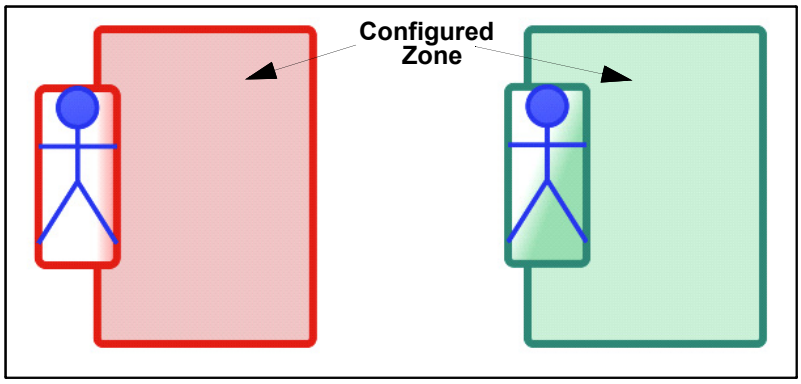
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the zone to trigger the event.

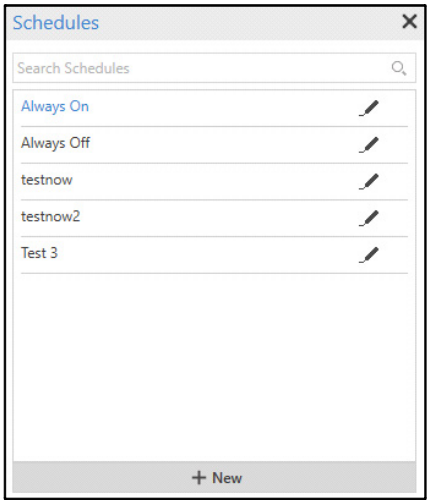
  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the zone will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the zone will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 10%, then as per the Red Zone, the event will be triggered as the object will be considered as Missing because 10% of the object is overlapping the configured zone. Whereas, in the Green Zone, the event will not be triggered as the object will not be considered as missing because 30% of the object is overlapping the configured zone.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.

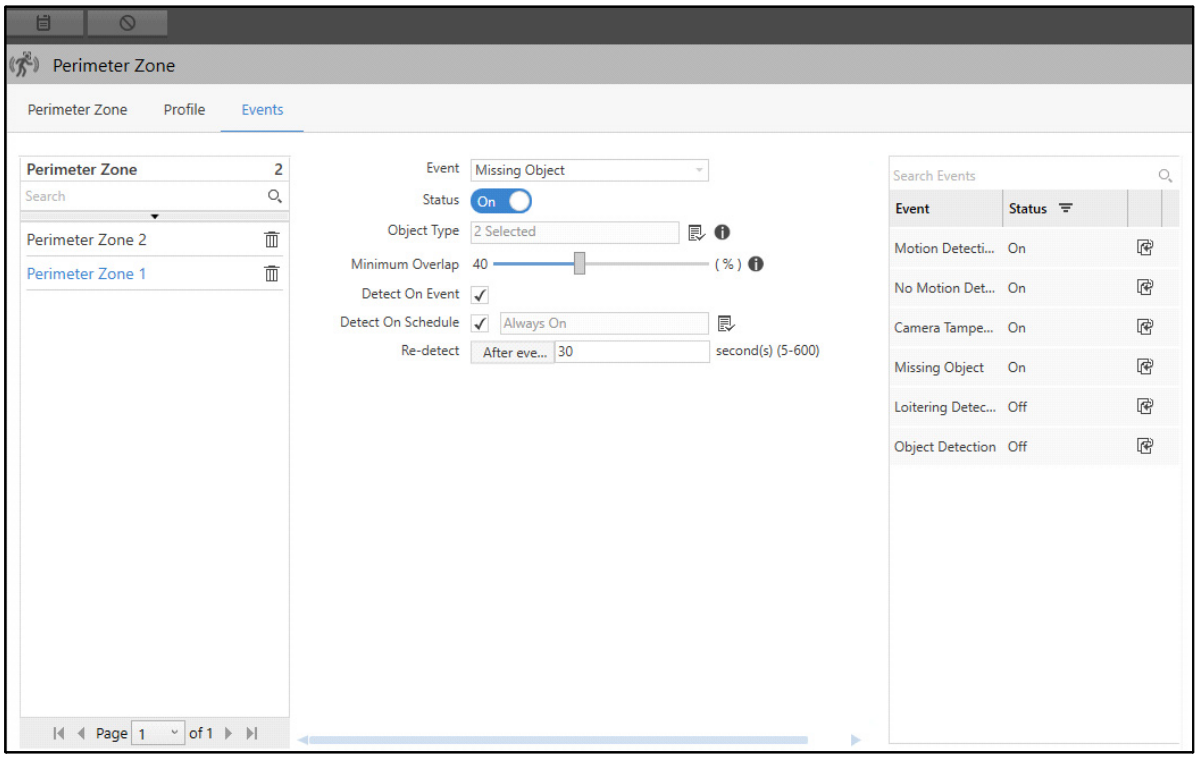
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



    - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.
- **Re-detect**: Specify the Re-detect time after which the Missing Object Event will be detected again after the previous detection. Valid Range: 5-600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

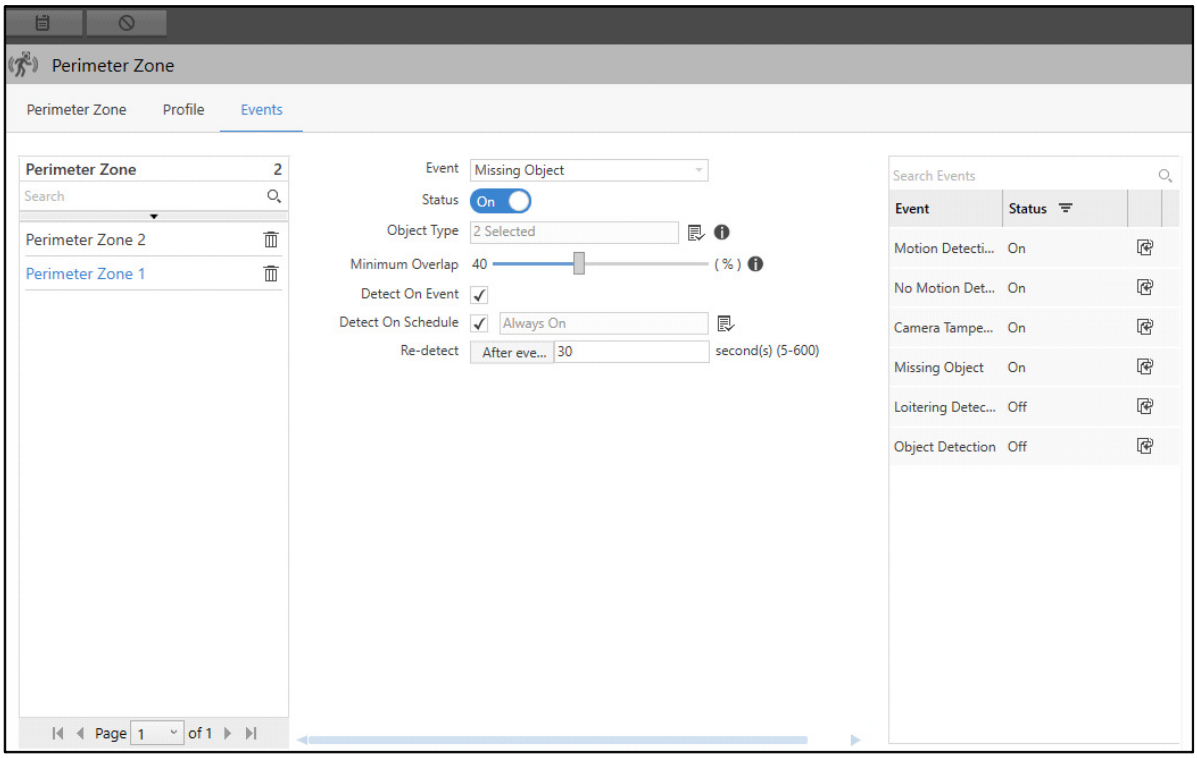
Once you have configured the Event, you can edit its configurations or disable it.



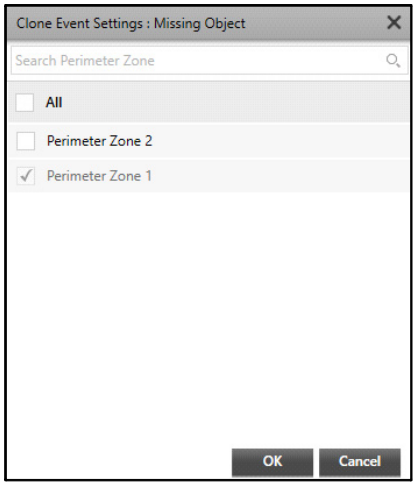
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Missing Object** pop-up appears.



- Select the desired zones to which you wish to copy the configurations.

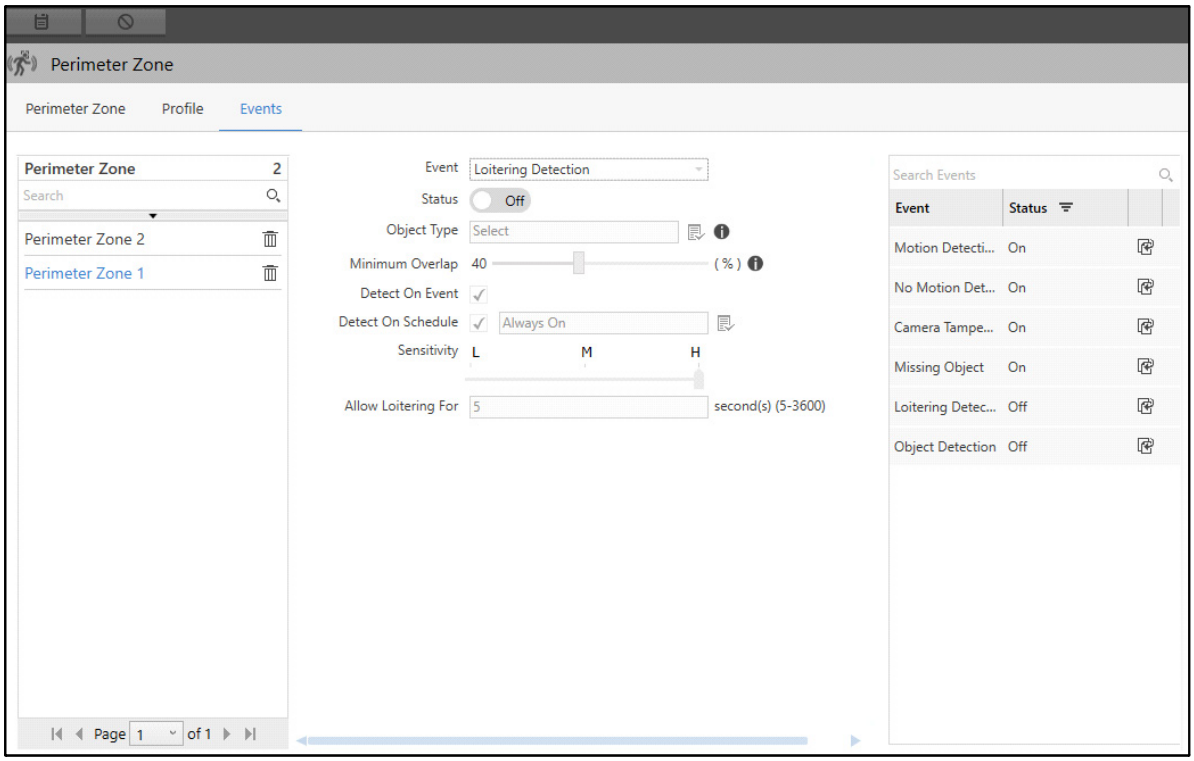
- Click **OK** to confirm or click **Cancel** to discard.

Loitering Detection

Loitering is an act of remaining in a particular public place for a prolonged time without an apparent purpose. Loitering is often indicative of suspicious activity and some imminent act of violation. The Loitering Detection feature monitors the live streaming of a camera and detects individuals that remain at a place for a prolonged time.

To configure Loitering Detection Event for Perimeter Zones,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

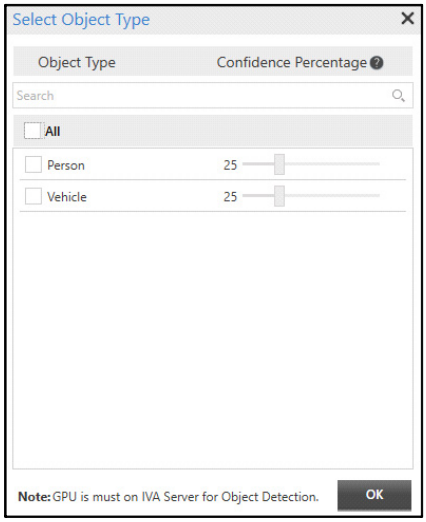


Configure the following parameters:

- **Event:** Select the Loitering Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



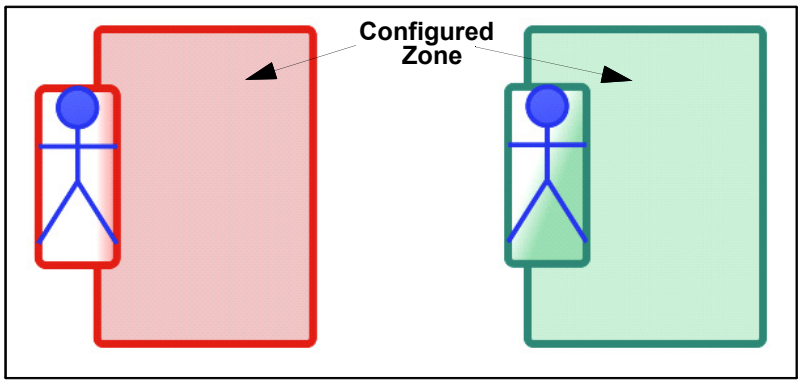
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

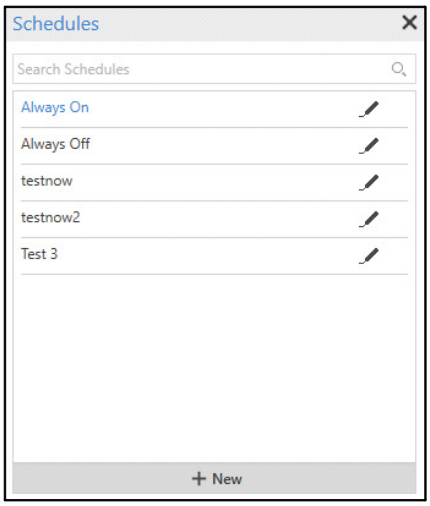
- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the zone to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the zone will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the zone will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Zone, the event will be triggered as the object is moving and 30% of the object is overlapping the configured zone. Whereas, in the Red Zone, the event will not be triggered as the object is moving but only 10% of the object is overlapping the configured zone.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

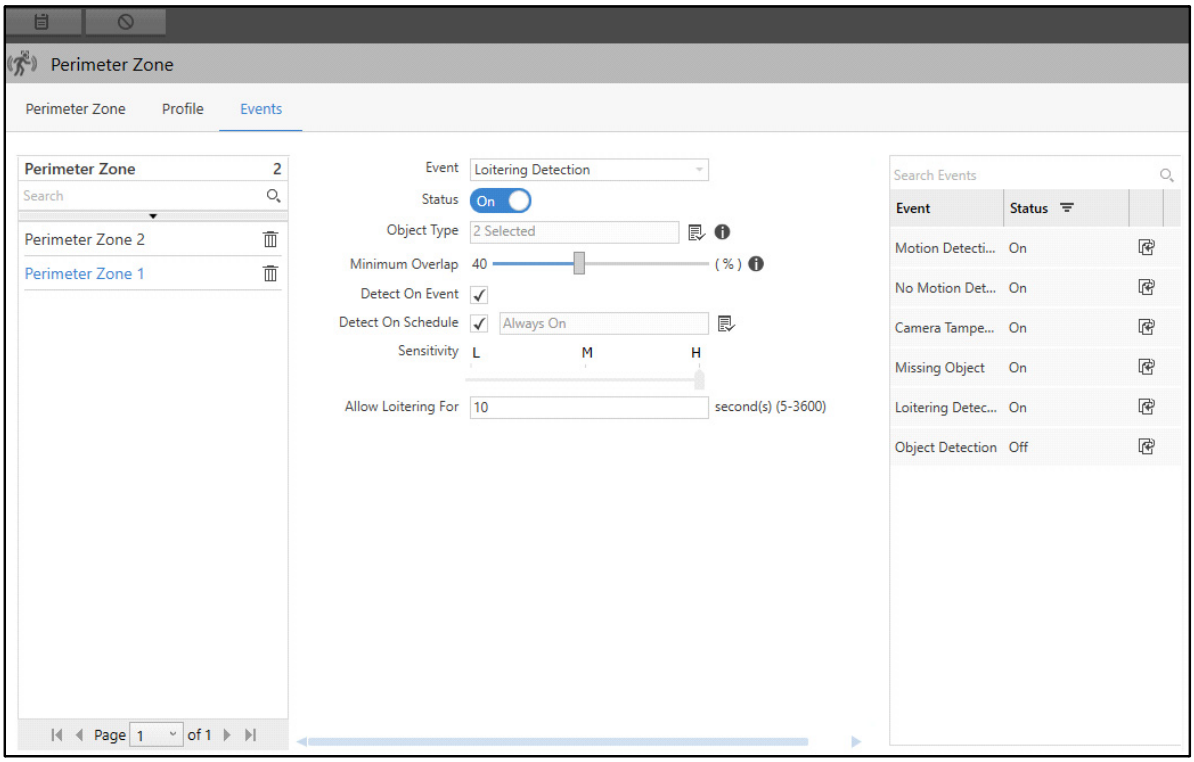
- **Sensitivity**: Drag the slider to set the desired sensitivity for the Loitering Detection Event — Low, Medium or High.

If you have selected Object Type, then Sensitivity will be disabled.

- **Allow Loitering For**: Specify the time till which loitering is permitted after which a Loitering Event is detected and it triggers the necessary action (For example, an alarm). Valid Range: 5-3600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

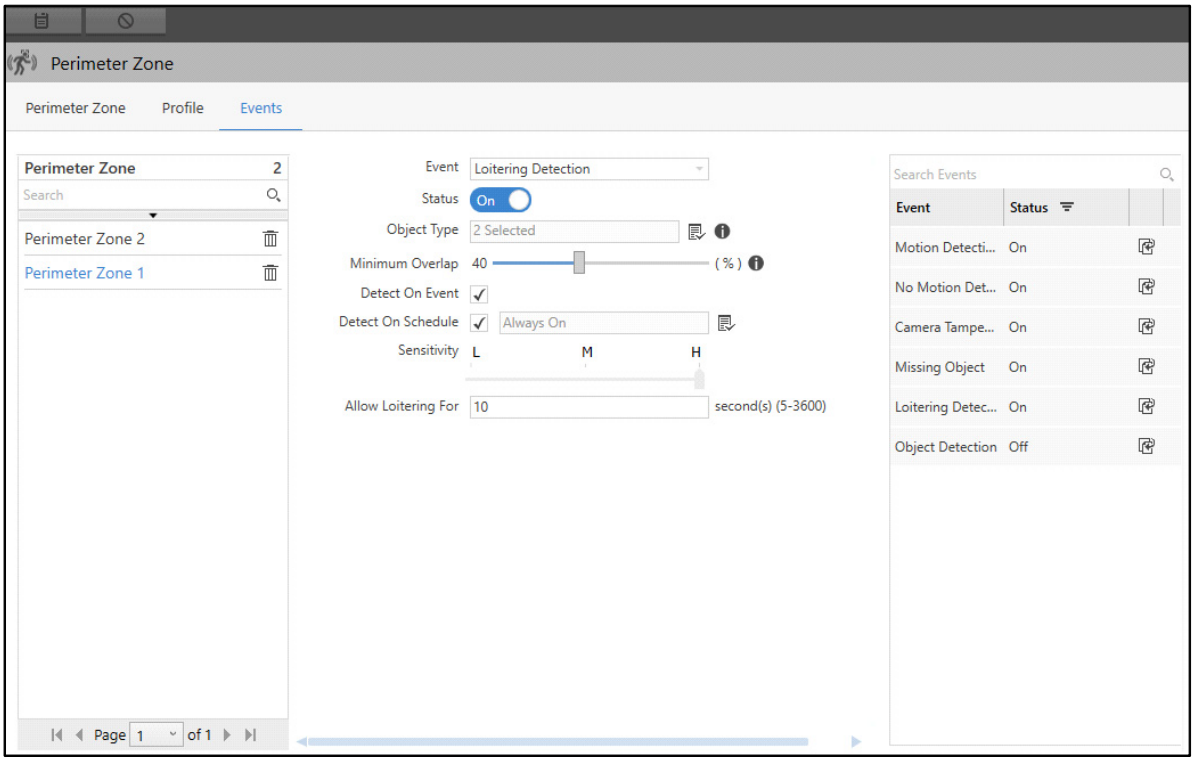
Once you have configured the Event, you can edit its configurations or disable it.



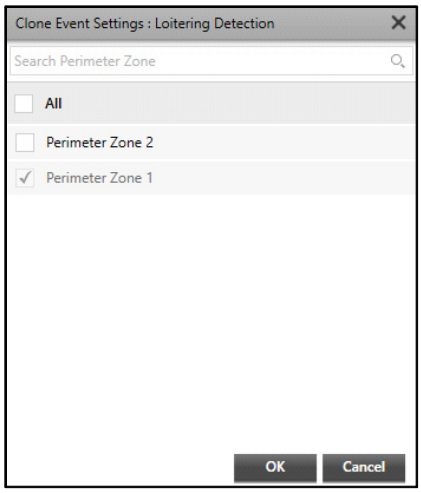
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Loitering Detection** pop-up appears.



- Select the desired zones to which you wish to copy these configurations.

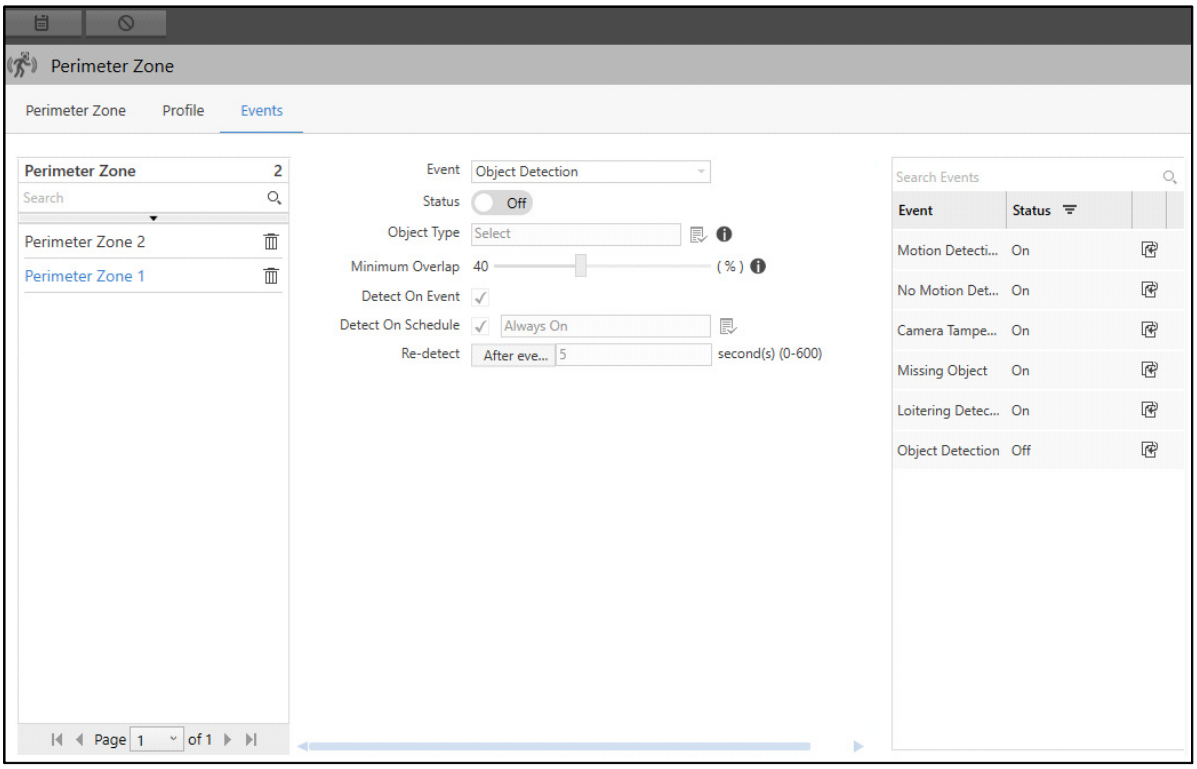
- Click **OK** to confirm or click **Cancel** to discard.

Object Detection

The Object Detection feature monitors the live streaming of a camera and detects the selected objects based on the confidence percentage.

To configure Object Detection Event for Perimeter Zones,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

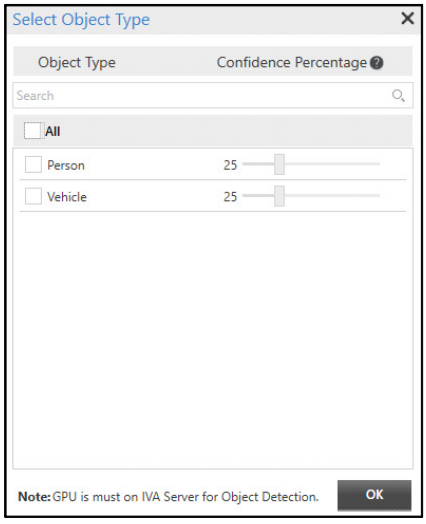


Configure the following parameters:

- **Event:** Select the Object Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



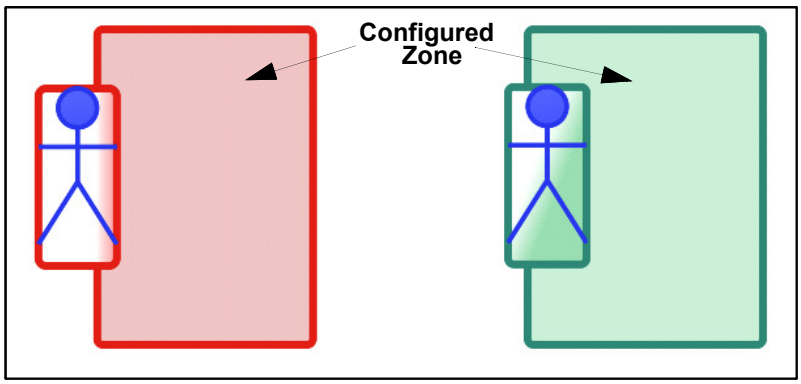
- Select the check boxes for the desired Object Types from the list or select the **All** check box to select all the Object Types. You can also search for the desired Object Types using the search bar.

  Set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

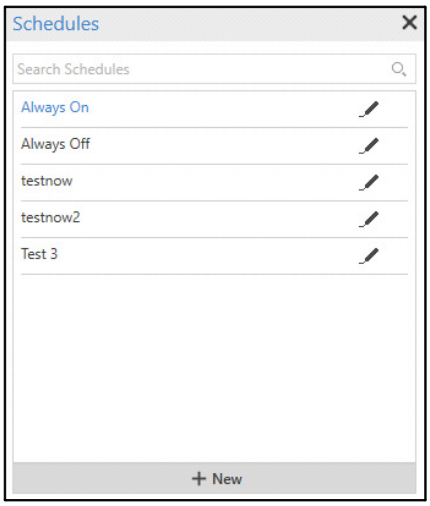
- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the zone to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the zone will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the zone will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Zone, the event will be triggered as 30% of the object is overlapping the configured zone. Whereas, in the Red Zone, the event will not be triggered as only 10% of the object is overlapping the configured zone.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.

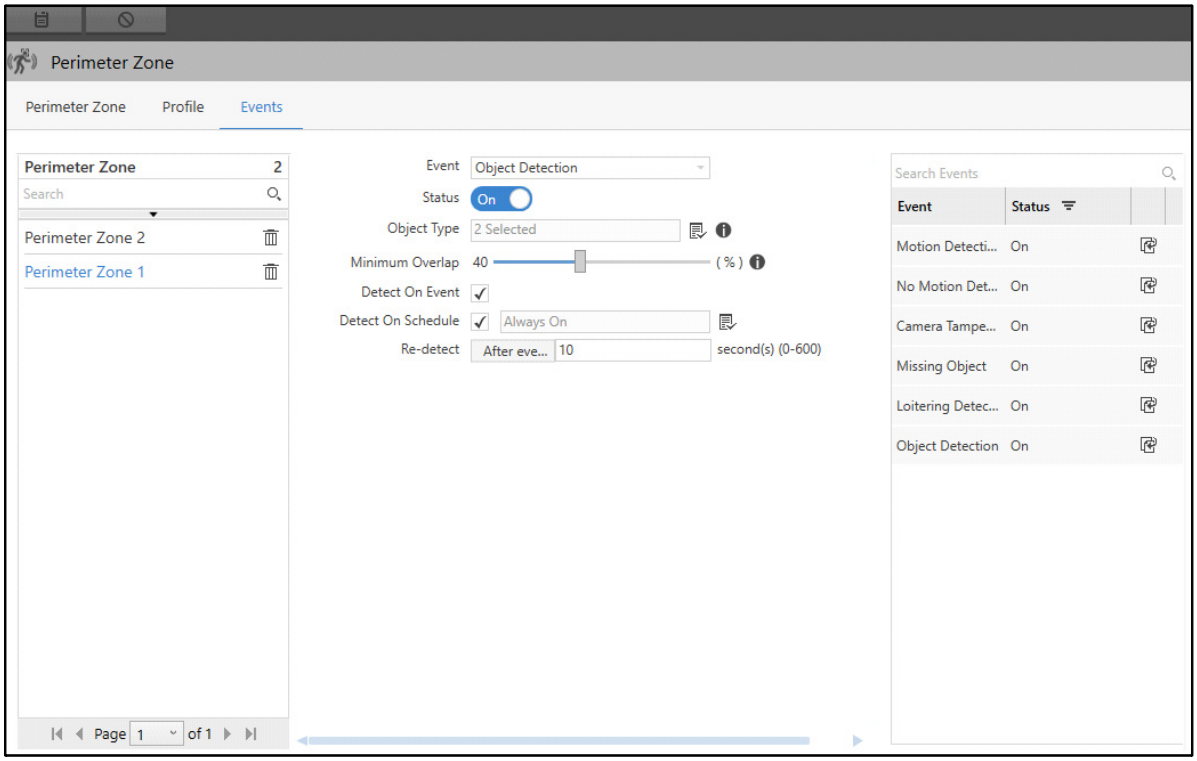


- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Re-detect After every**: Specify the Re-detect time after which the Object Detection Event will be detected again after the previous detection. Valid Range: 0-600 seconds. Default: 10.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.



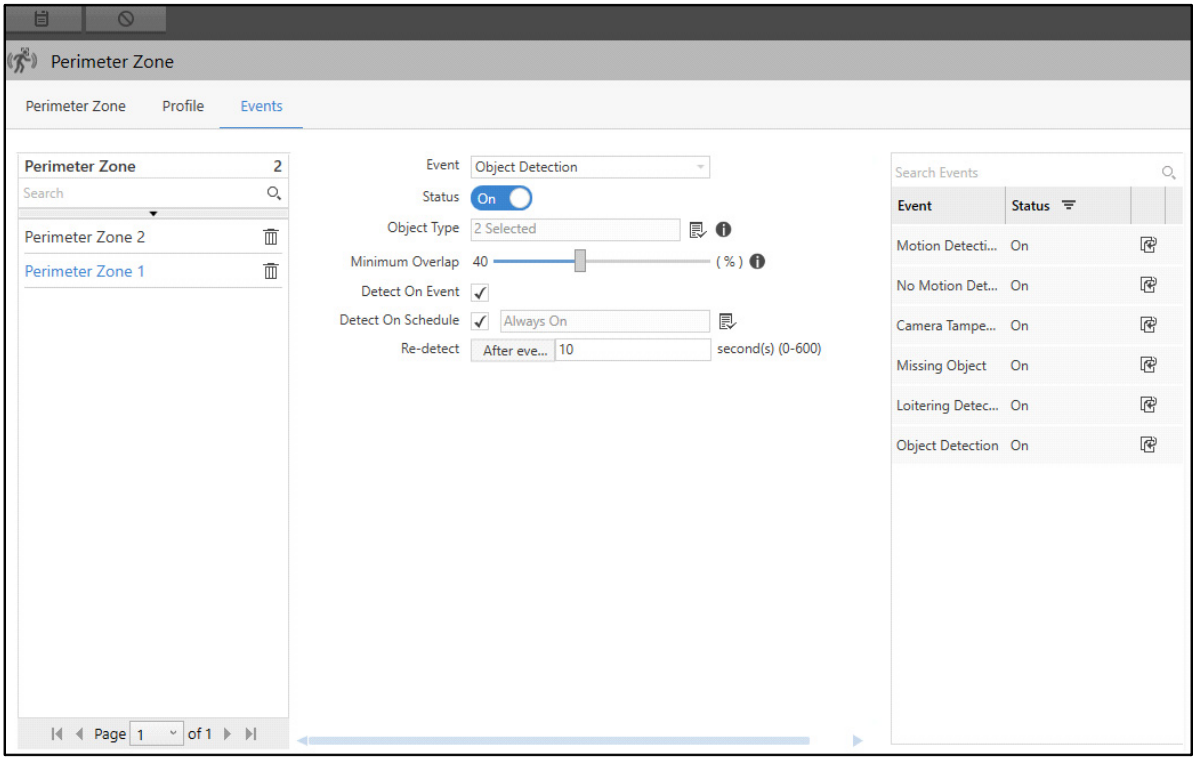
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.

- Click **Save** to save the settings or **Cancel** to discard.

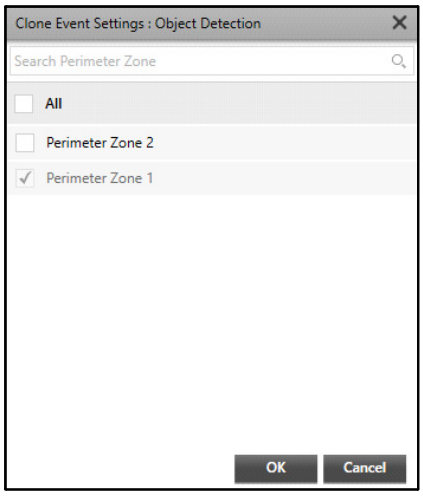
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Object Detection** pop-up appears.



- Select the desired zones to which you wish to copy the configurations.

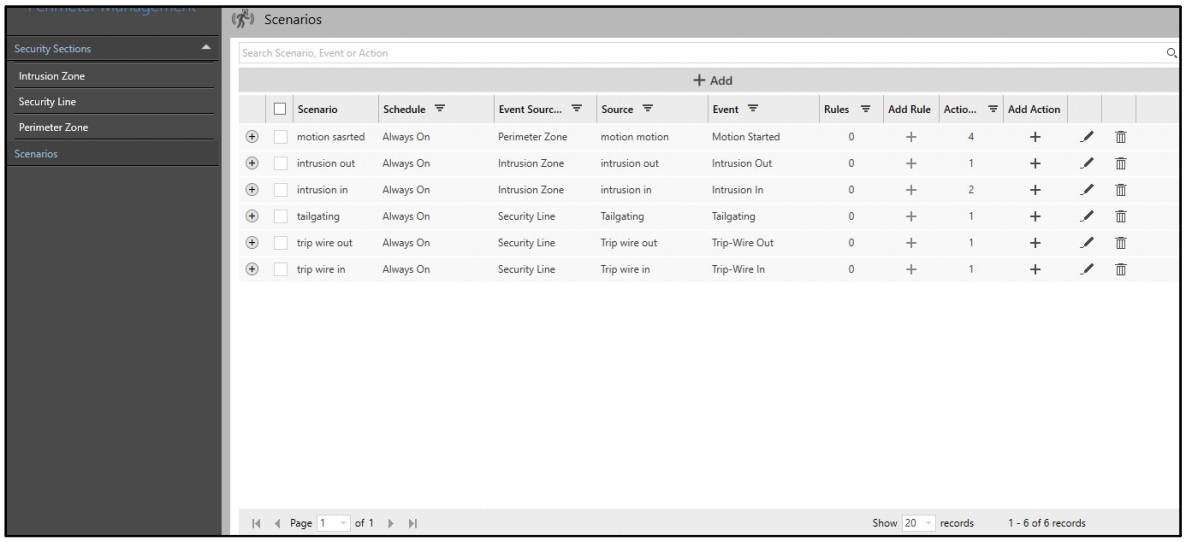
- Click **OK** to confirm or click **Cancel** to discard.

Perimeter Management-Scenarios

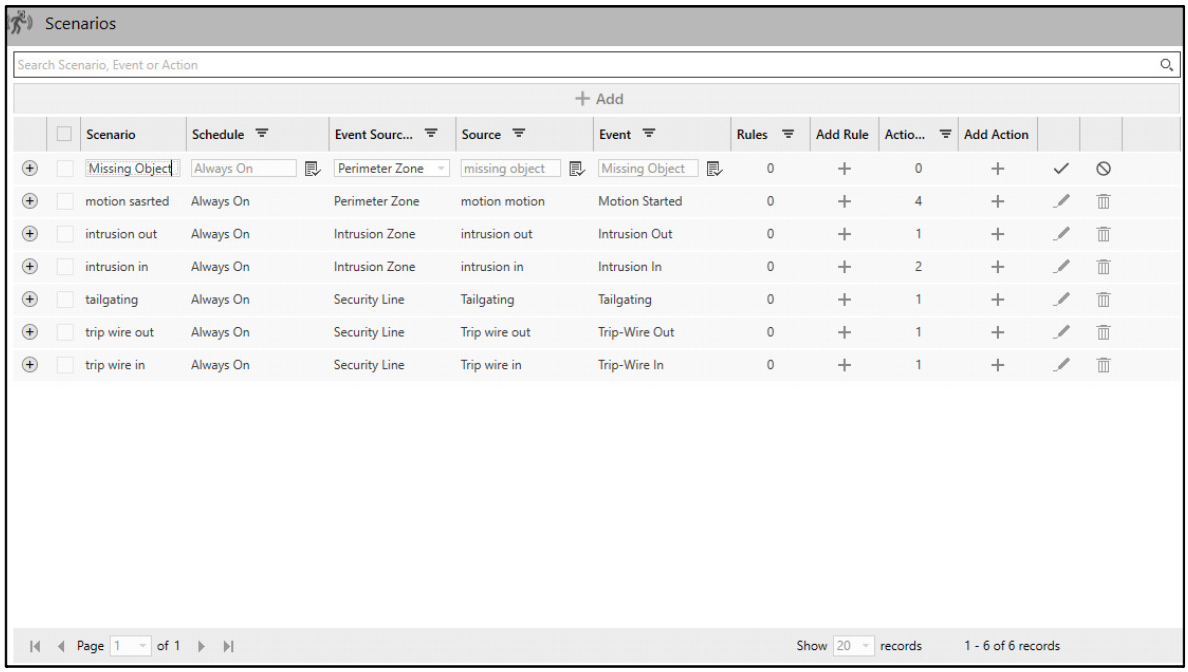
In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send SMS) on Events occurring at certain sources (For example, Storage Memory Low). The Scenarios page displays all the Scenarios configured for Perimeter Management. You can view and configure the Scenarios for all the configured Intrusion Zones, Security Lines and Perimeter Zones.

To configure Scenarios,

- Click **Perimeter Management > Scenarios**.



- Click **Add**.



The configurations of Scenarios for Perimeter Management are similar to the Basic Scenario. For details, refer to “Basic Scenario”.

Perimeter Management - Report

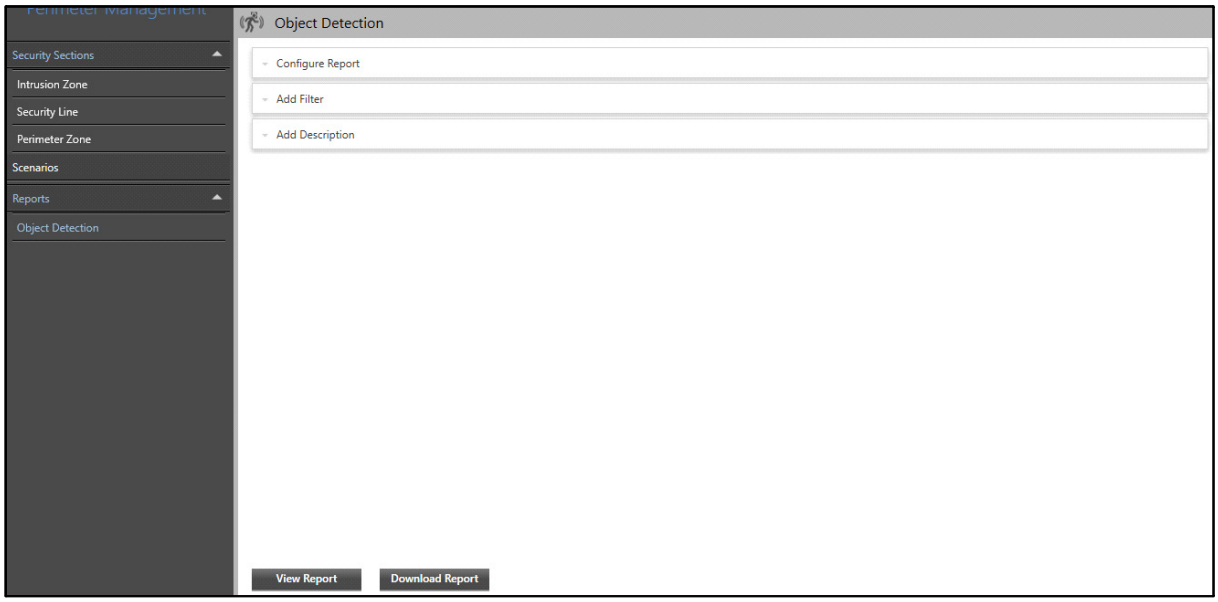
Object Detection Report

The Object Detection report contains data of all the events in which different objects are detected. The Object Detection report is useful to keep a track of objects detected in various events such as Loitering Detection, Missing Object and so on. For example, the Object Detection report can be useful to track number of people detected in the perimeter of an office. Based on this report, objects can be identified under different events which will help in effective monitoring of perimeter.

The Object Detection page enables you to configure parameters for Object Detection Reports. You can view and configure **Daily** or **Hourly** reports with captured images.

To configure Object Detection Reports,

- Click **Perimeter Management > Reports > Object Detection**.



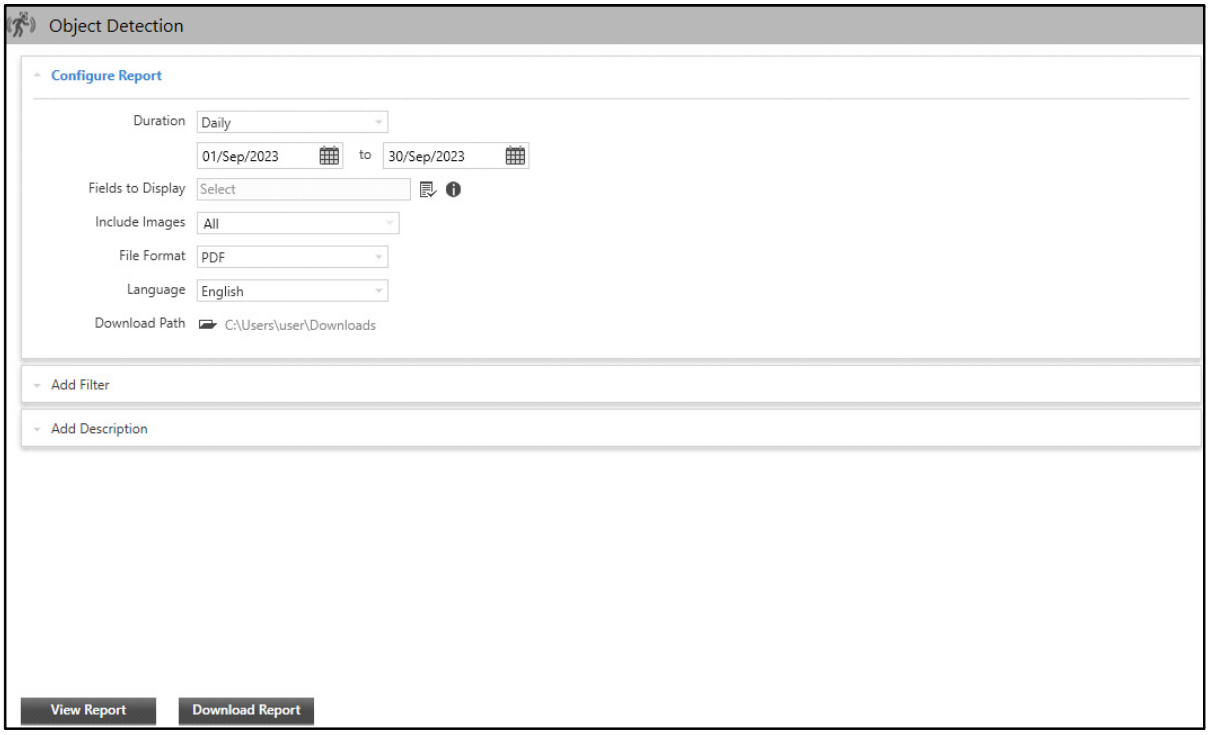
The Object Detection page contains three collapsible panels — “Configure Report”, “Add Filter” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Object Detection Report from this collapsible panel.

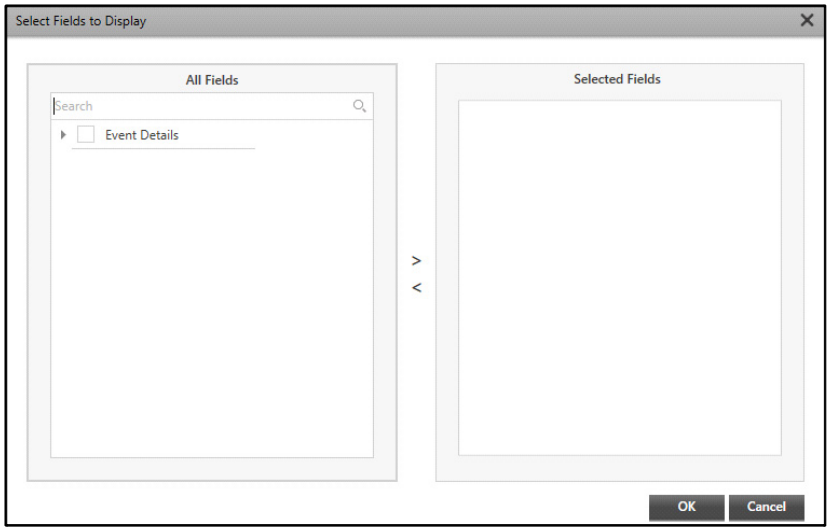
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

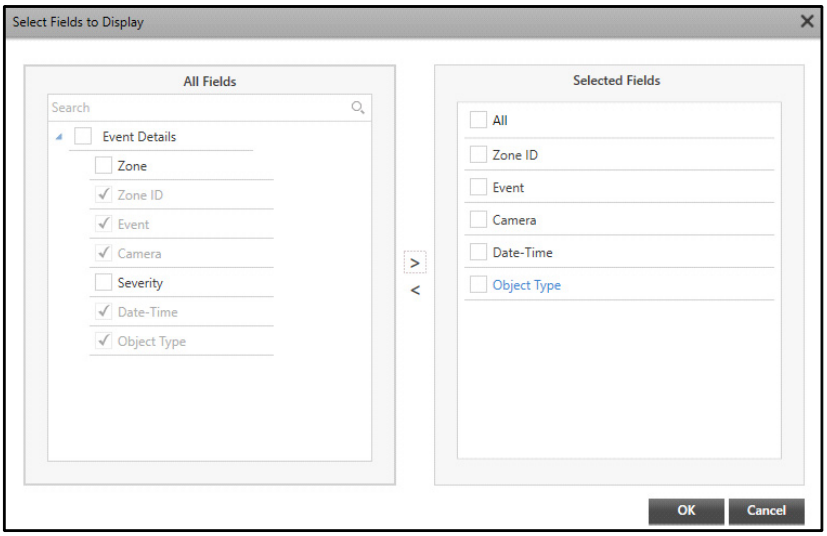
- **Duration**: Select the Duration from the drop-down list — Daily or Hourly.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To dates from the calendar and specify the time.
- **Fields to Display**: Select the desired fields that you wish to display in the report using the **Fields to Display** picklist.
    - Click the **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



Double-click **Event Details** to view the options. Select the check boxes of the desired fields you wish to include in the report from the **Event Details**.

Click the right arrow button to move these fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

To remove fields, select the check boxes of the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields.



- Click **OK** to confirm or click **Cancel** to discard.
- **Include Images**: Select the check boxes for the type of images you wish to include in the report from the drop-down list options— All, Source Image or Object Image.
- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.

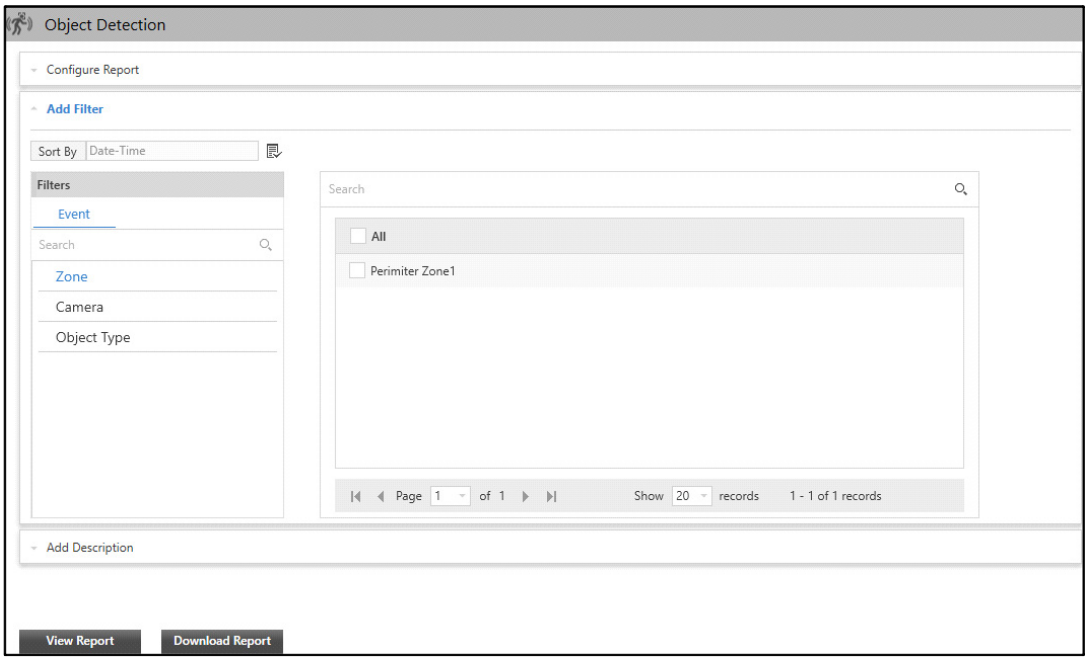
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Filter

This panel allows you to add filters for the Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters. You can view and edit the filters from this collapsible panel.

To set the filters,

- Click the **Add Filter** collapsible panel.

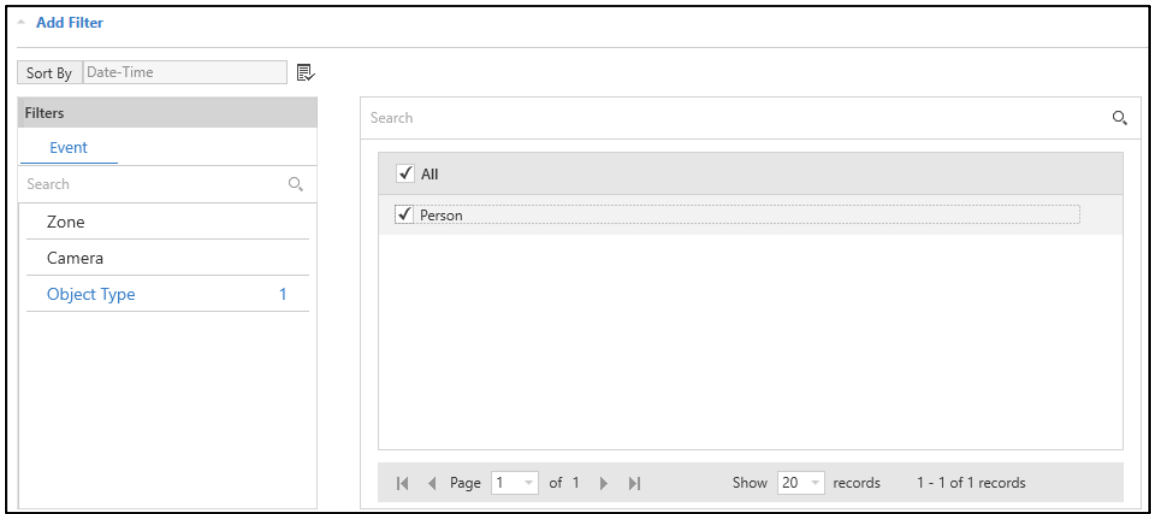


Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data from Event Fields in the report using the **Sort By** picklist. Double-click to select the desired option. By default, the sorting is done as per the Date and Time of Event Occurrence.

- **Filters**: You can get the desired data for the report using Filters. The Filters section contains only one tab — Event. Select the tab to view the associated parameters.

  - Click the desired parameter to view the associated entities with the selected Event. For example, if you select Object Type, all the object types associated with the selected Event are displayed on the right hand side. Select the desired entities to include in the report.

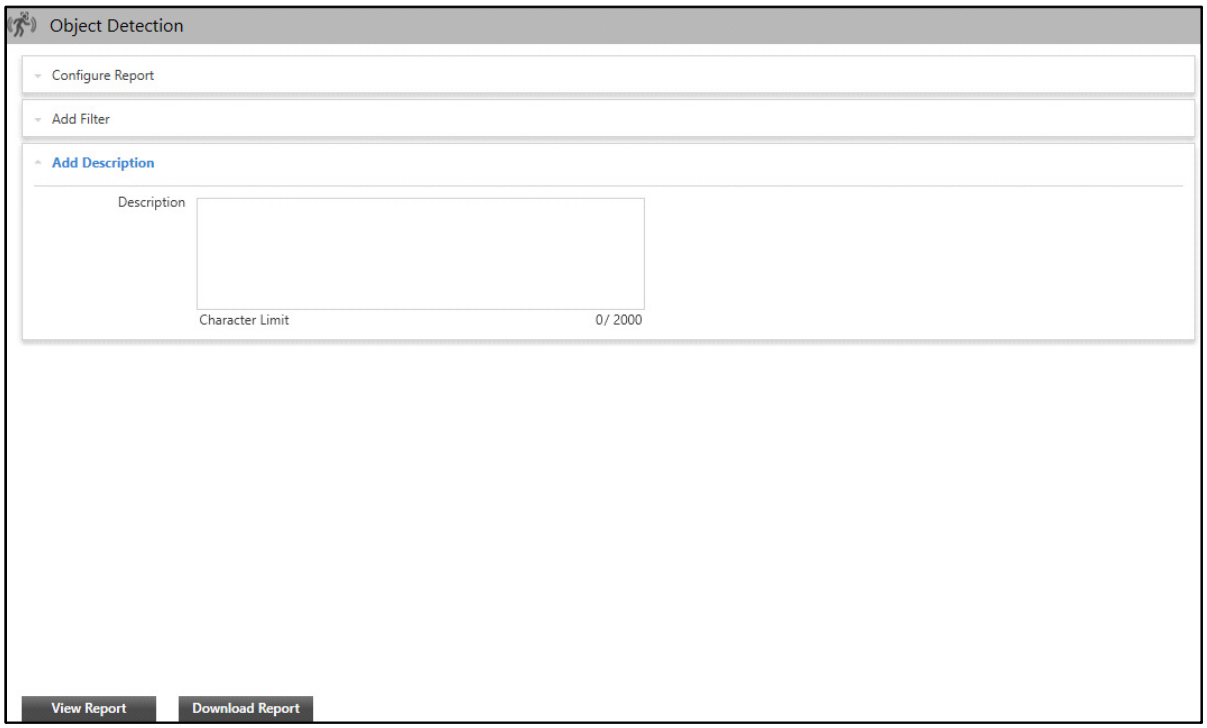


Add Description

This panel allows you to add a description for the Object Detection Report once the report configurations are done. This description is visible in the generated report.

To view and edit the description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

CHAPTER 10

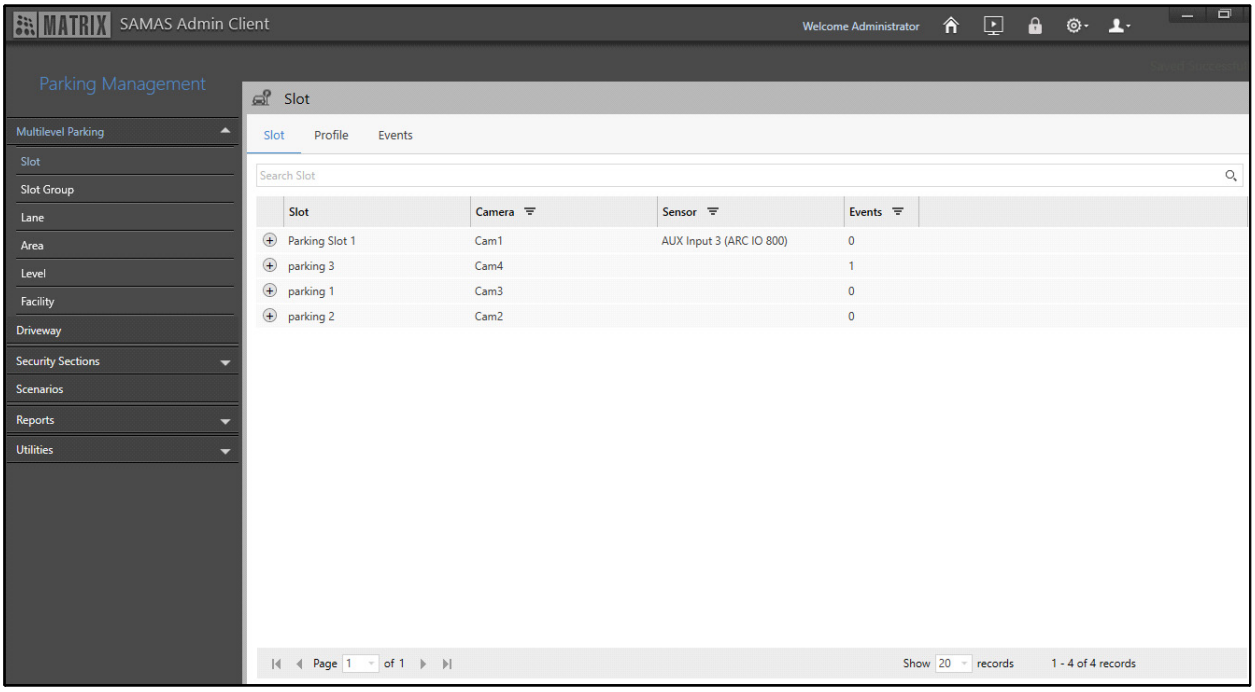
Parking Management

The Parking Management module enables you to configure various parking zones and events for them. Parking Management uses video content analysis which is effective in detecting events such as Vehicle Counting, Unauthorized Parking, Premises Availability based on live stream of a camera. It also enables you to configure Scenarios based on Events.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure Parking Management,

- Click **Parking Management**.

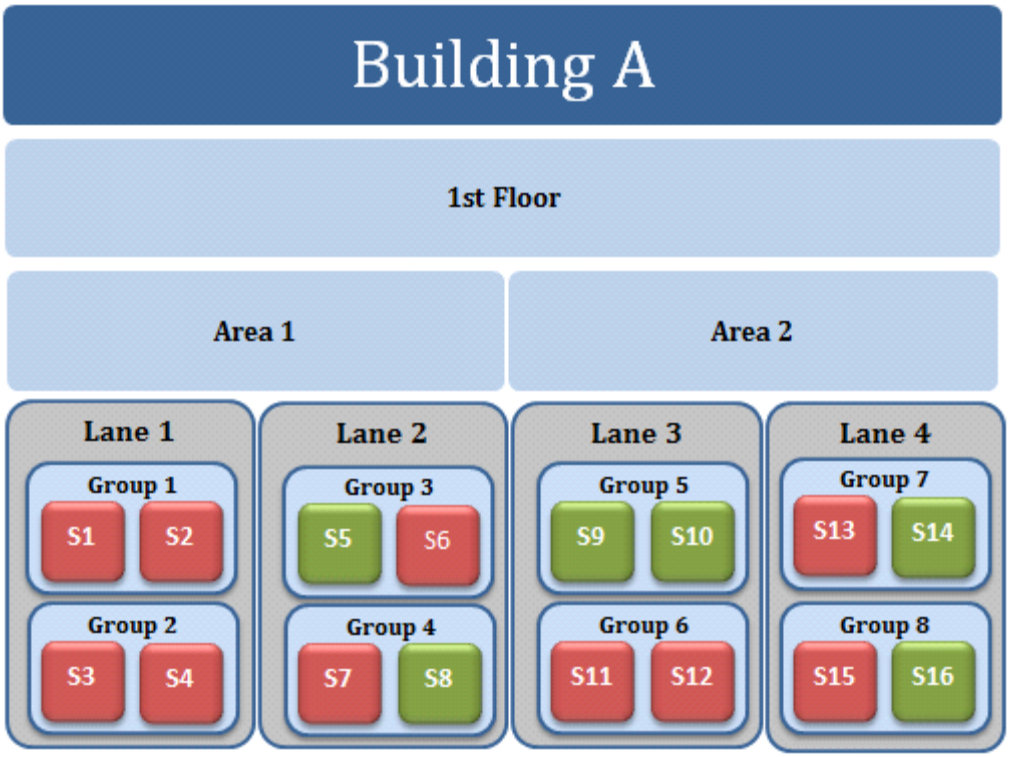


The Parking Management module contains these pages — Multilevel Parking, Driveway, Security Sections, Scenarios, Reports and Utilities.

Multilevel Parking

The Parking Management module allows the configuration of various zones for parking premises. The Multilevel Parking feature provides a solution to the Multilevel Parking System. This solution enables the Admin Client user to direct a person with the detailed path of the available or unavailable parking slots.

This is a depiction of Multilevel Parking.



The figure depicts the availability of the parking entities such as - Slots, Groups, Lanes, Areas, Level and Facility. These entities can be configured from the Parking Management module.

Now, consider a Parking facility, which consists of several **Slots** such as S1, S2, S3, S4 etc. Various slots can be combined to form various **Groups** such as G1, G2, G3 etc. Further, the Groups can be combined to form **Lanes** such as L1, L2, L3 etc. These Lanes can further be combined to form **Areas** such as Area 1, Area 2, Area 3, etc. Furthermore, the Areas can be combined to form **Levels** such as 1st floor, 2nd floor, etc. All the Levels are finally combined together to form a **Facility** like a Multilevel Parking Building.

In the above figure, red colored boxes depict engaged parking slots while the green ones depict available parking slots.

When a person arrives at that parking facility and wants to park his car in the S5 Vacant slot, he can be directed along the path of the available slot verbally or digitally. The path can be represented as:
Building A -> 1st Floor -> Area 1 -> Lane 2 -> Group 3 -> S5 is vacant.

The Parking Management module allows you to manage a complex parking facility like a Multilevel Parking facility easily by configuring different **Scenarios**. It also allows you to configure Scenarios such as availability/ unavailability of the parking slots and **Actions** such as LED indication or Alarm indication for the Scenario. For example, an available parking slot can be indicated by a green LED.

Slot

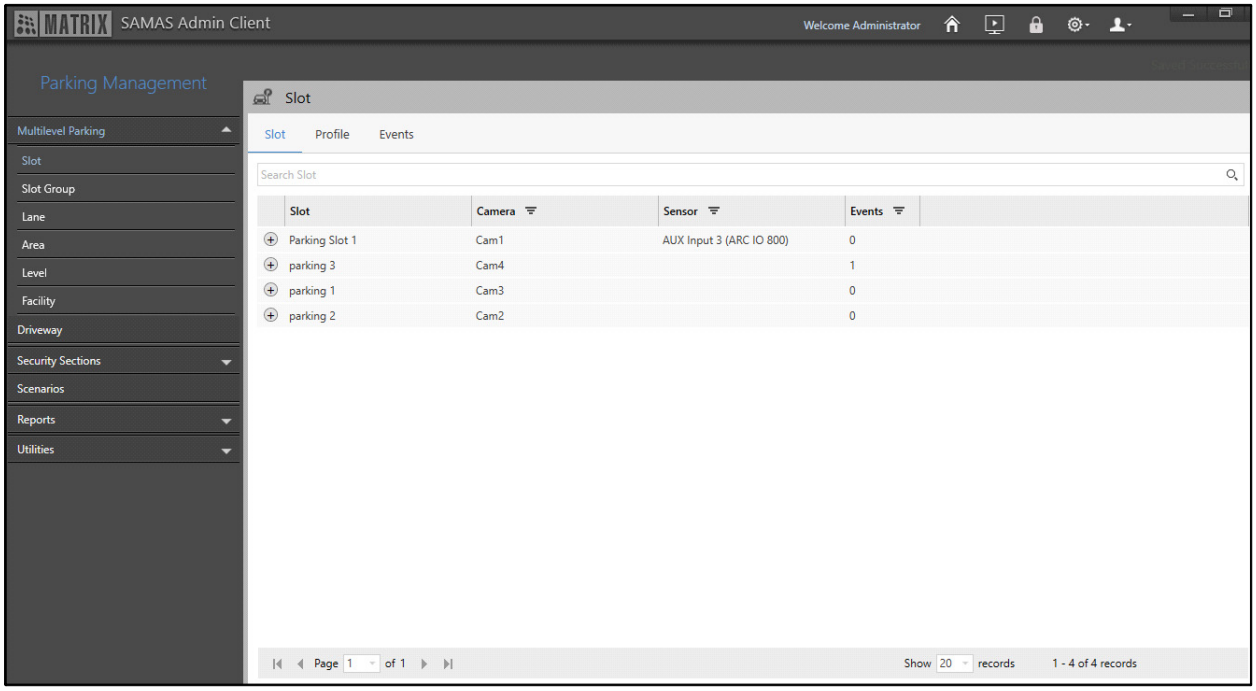
In Admin Client, a **Slot** refers to the parking lot where a person can park his vehicle. The Parking Management module allows you to configure slots in the parking premises of an organization. This helps in efficient management of the parking facility and detect any events (For example, Prohibited Parking) in the premises. The slot can be configured for various parking types, such as Reserved Parking, Visitor Parking, etc. and for different types of vehicles, such as 2-wheelers and 4-wheelers.

Events that can be configured against the configured slots are: Unauthorized Parking, Prohibited Parking, Improper Parking, Slot Occupancy, Vehicle Overstay and Parking After Closing Hours. These Events can then be used to create Scenarios which can alert the security person or management through the actions on the occurrence of any parking related circumstances in the defined zone.

The Slot page displays all the configured slots. You can view and configure the Slots from this page.

To configure Slots,

- Click **Parking Management > Multilevel Parking**. The **Slot** page appears by default.



The entity name (Slot) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities" The reflection will be seen everywhere in the Admin Client.

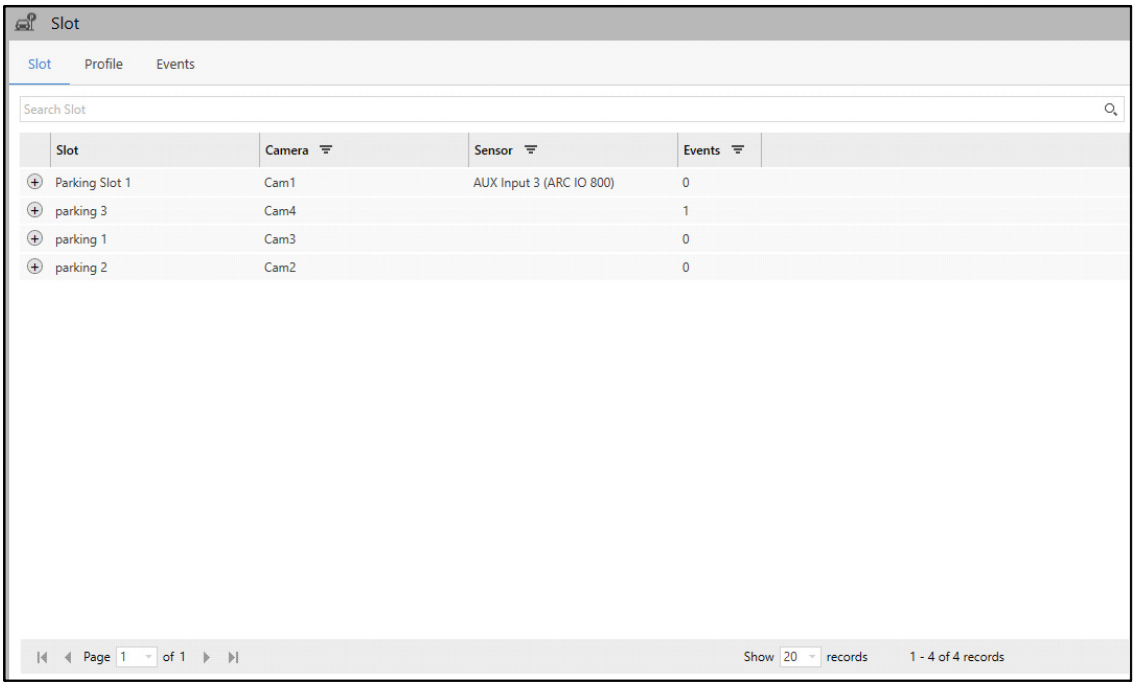
The Slot page consists of the following tabs.

- "Slot"
- "Profile"
- "Events"

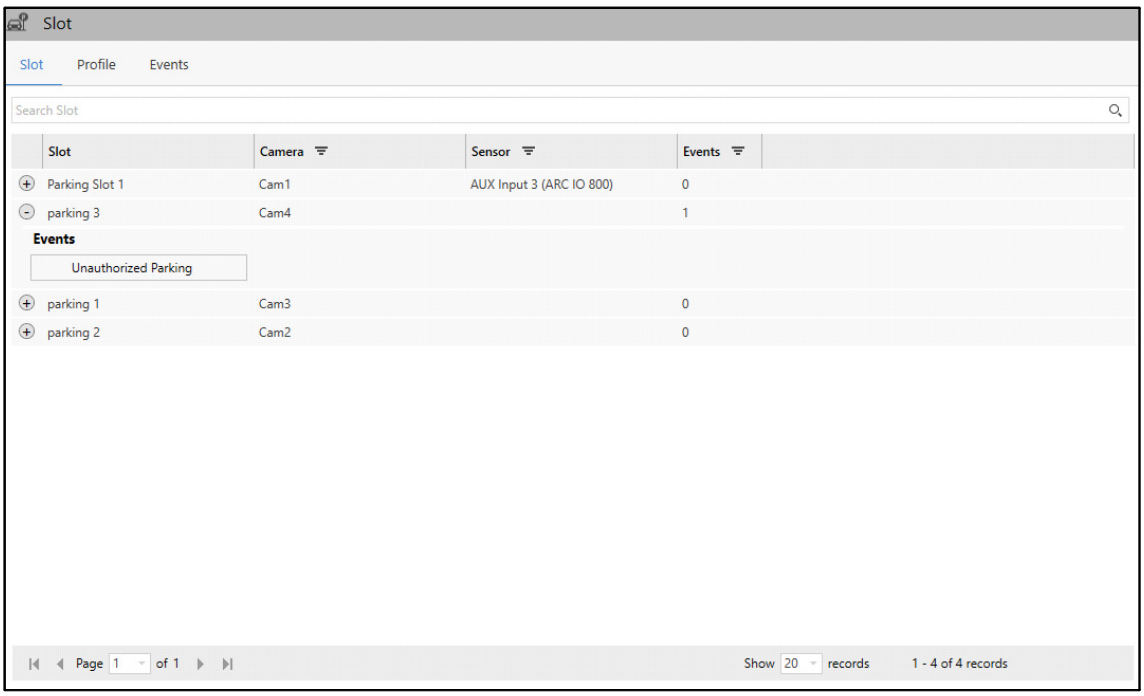
Slot

This tab enables you to view slots. You can configure the slots from “Profile”. All the slots and the Events configured for them appear under this tab. The following details are displayed — Slots, Camera, Sensor and Events.
To view Slots,

- Click the **Slot** tab.



- Click **Show Events** to view the Events configured for the slot.



- Click **Filter** of the respective parameter in the header row.

Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR FILTER**.

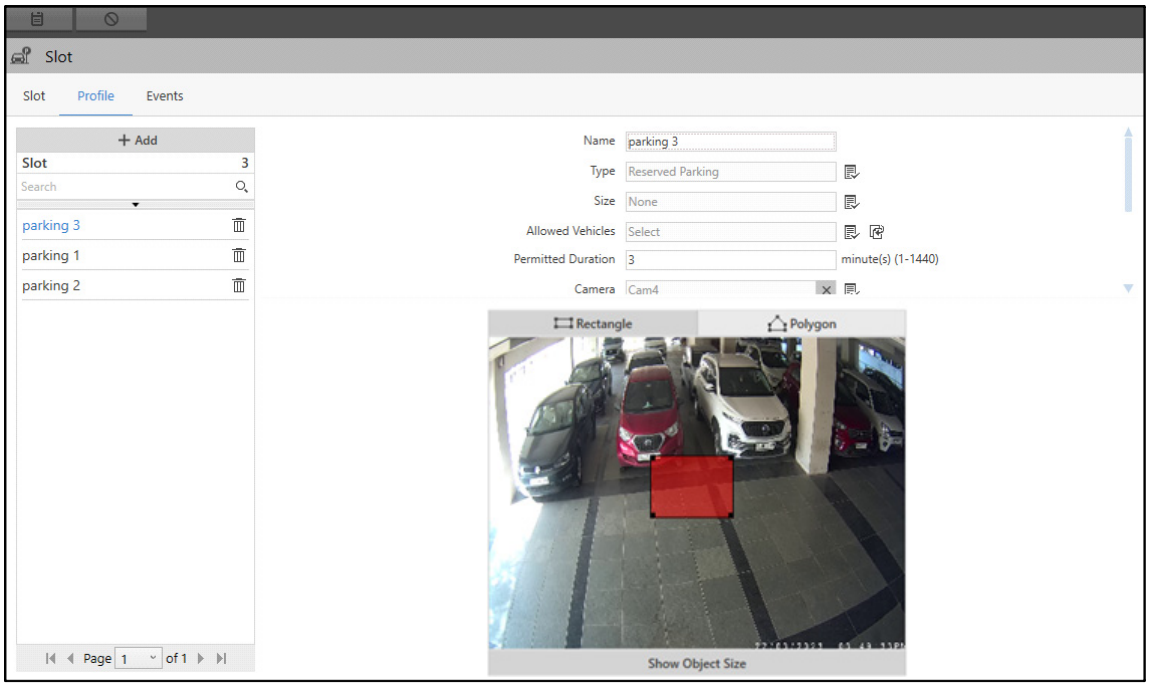
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

This tab enables you to configure slots. All the slots configured here appear under the **Slot** tab.

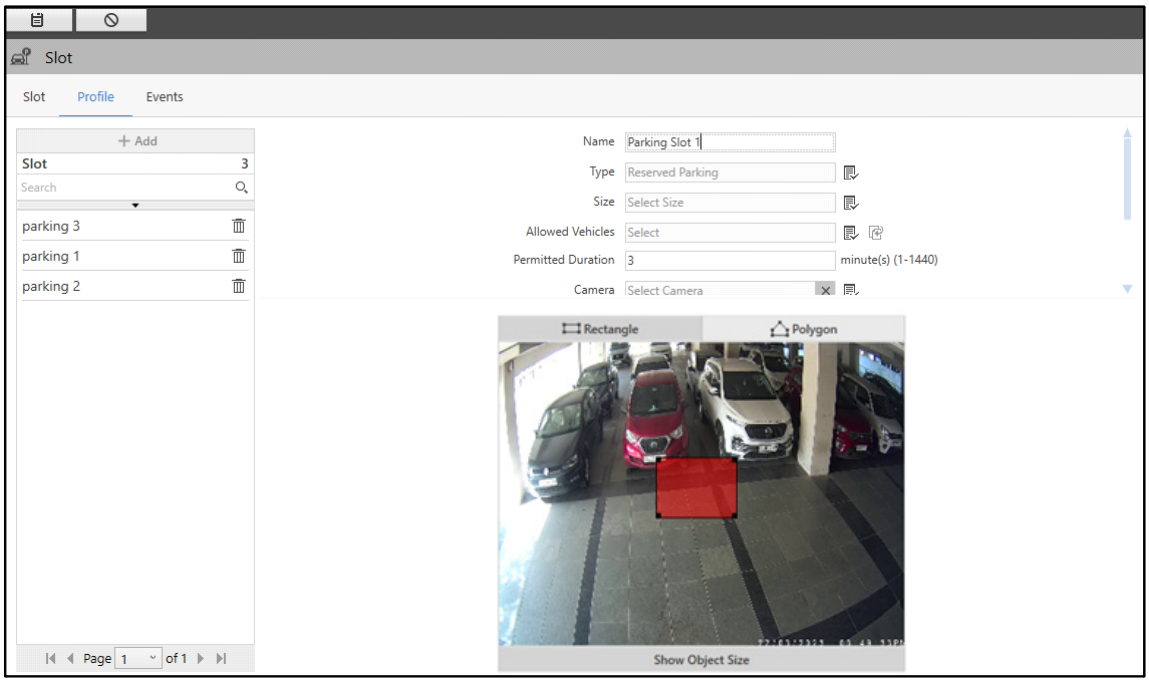
To configure Slots,

- Click the **Profile** tab.



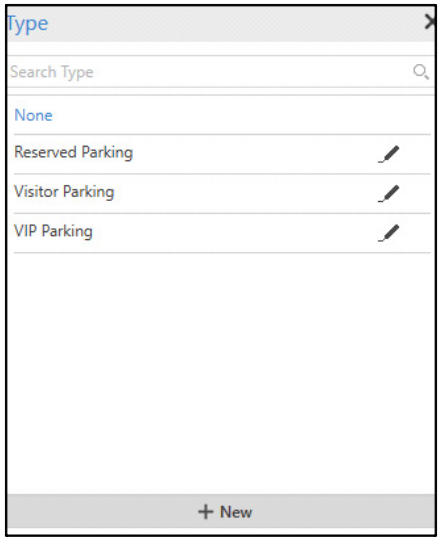
*The **Add** button is disabled when you are configuring slot profile for the first time. You can directly configure the parameters and save the slot.*

- Click **Add**.



Configure the following parameters:

- **Name**: Specify a suitable name for the parking slot. In Name, you can enter upto 50 characters. Default: Blank.
- **Type**: Select the desired type which you wish to assign to the slot using the **Type** picklist.
  - Click **Type** picklist. The **Type** pop-up appears.

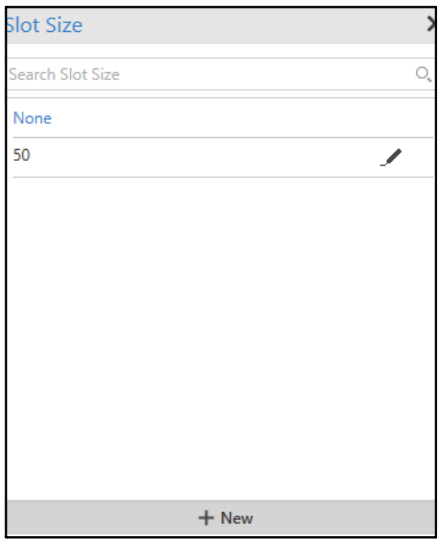


*By default two slot Types are configured — **Reserved Parking** and **Visitor Parking**.*

*By default, **Assign Vehicle** is enabled for **Reserved Parking** type of slot, while it is disabled for **Visitor Parking** type of slot. For more details, refer to "Utilities".*

- Double-click to select the desired type from the list. You can edit an existing type by clicking on **Edit** . You can also configure a new type by clicking **New**. For more details, refer to "Utilities".

- **Size**: Select the desired size which you wish to assign to the slot using the **Size** picklist.
  - Click **Size** picklist. The **Slot Size** pop-up appears.

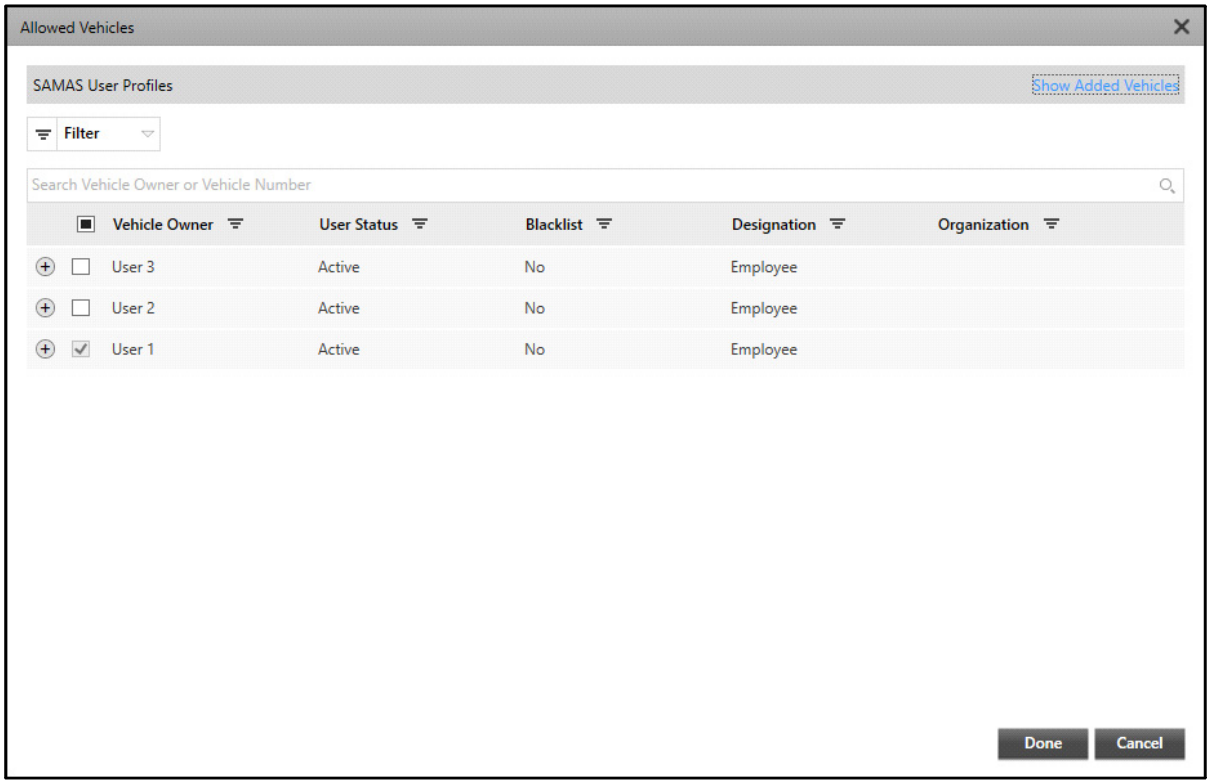


  - Double-click to select the desired size from the list. You can edit an existing size by clicking on **Edit** . You can also configure a new size by clicking **New**. For more details, refer to "Utilities".

- **Allowed Vehicles**: This feature allows you to add all the authorized vehicle numbers. This list can be used in the generation of Unauthorized Parking Event, that is, any vehicle whose number is not listed in the allowed vehicle list will not be allowed to park their vehicle and hence, Unauthorized Parking Event will be generated. Select the desired vehicles using the **Allowed Vehicles** picklist.

*Allowed Vehicles will be enabled only when **Assign Vehicles** is enabled for the selected slot **Type**. For more details, refer to "Utilities".*

  - Click **Allowed Vehicles** picklist. The **Allowed Vehicles** pop-up appears.



By default, this is the **Choose Vehicle Number** window and the details are displayed for the same.

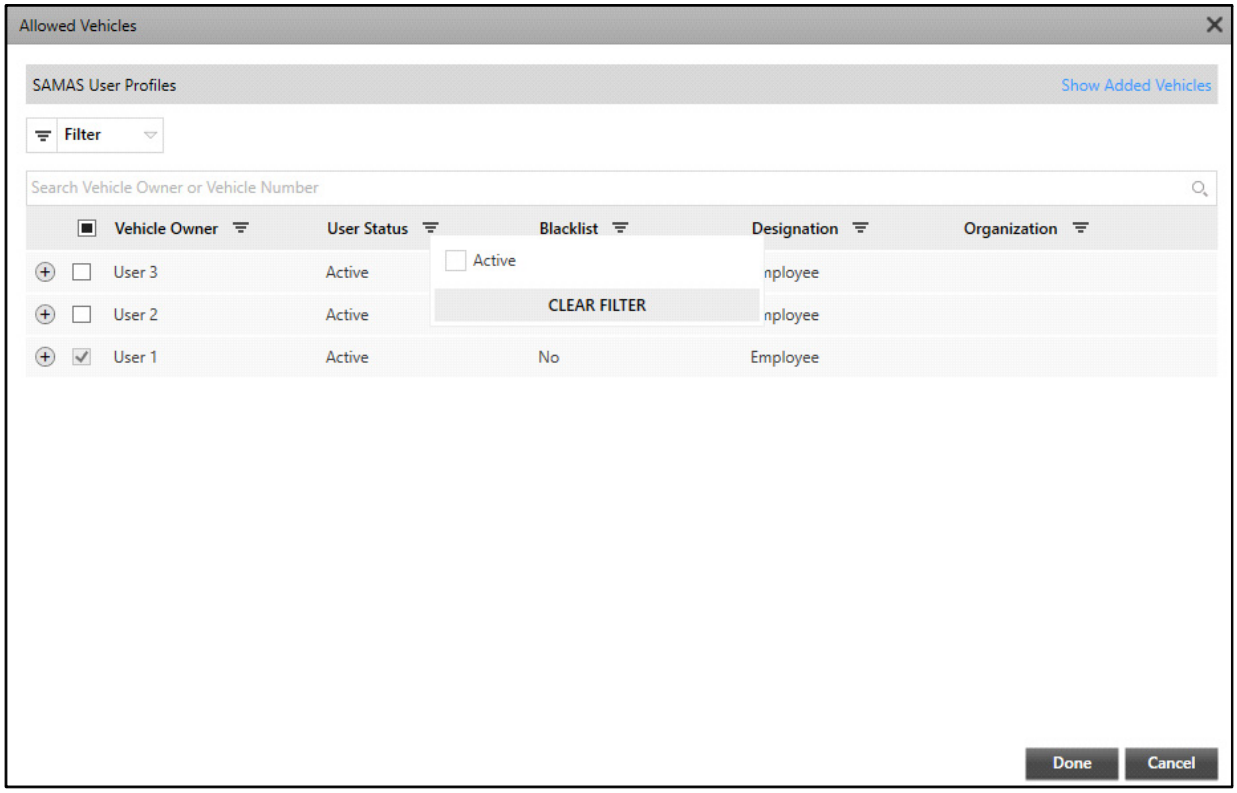
- Select the desired Vehicles from the list. You can select vehicles from either COSEC database or SAMAS User Profiles.

  If you wish to configure allowed vehicles from **Cosec database**, select **Cosec** as the Database Type from **General Settings > User Profiles** and click **Save** .

  If you wish to configure allowed vehicles from **SAMAS User Profiles**, select **Custom** as the Database Type from **General Settings > User Profiles** and click **Save** .

- You can filter records in two ways:

  Click **Filter** of the respective parameter — Vehicle Owner, User Status, Blacklist, Designation, Organization.

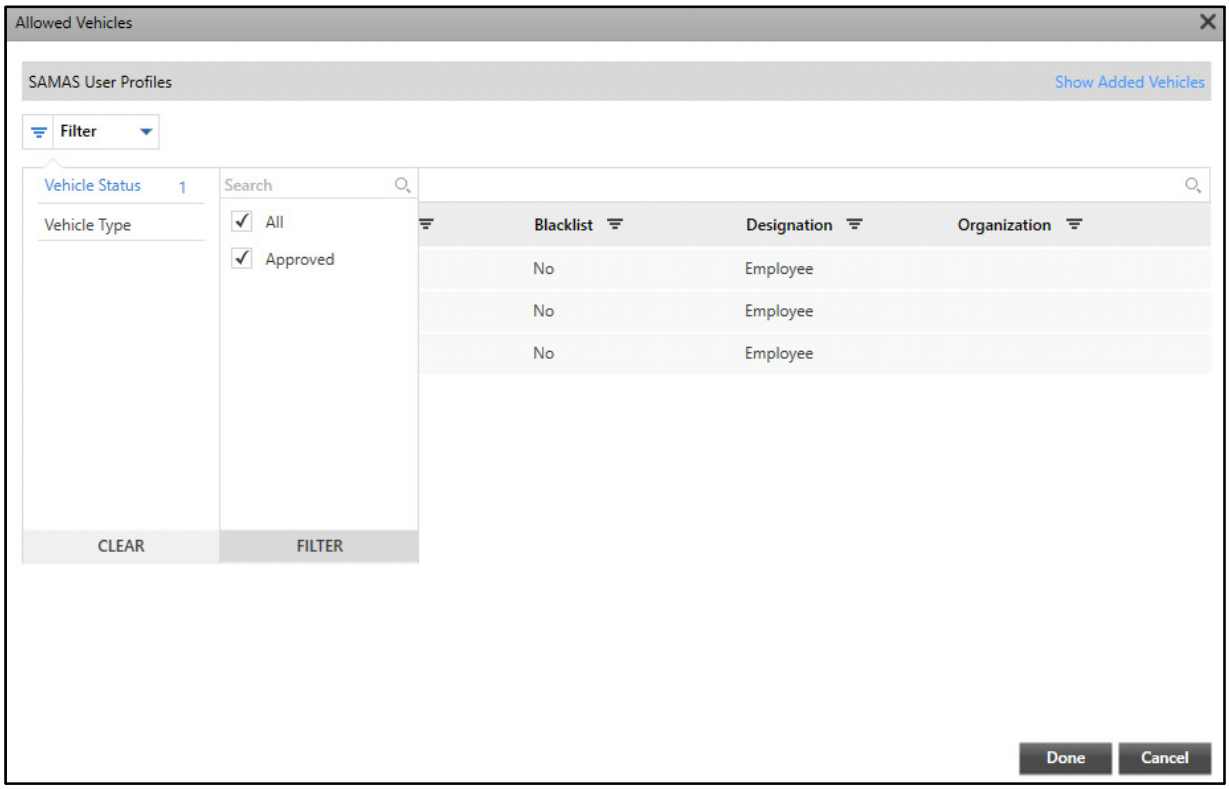


Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR FILTER**.

OR

Click **Filter** on the top left of the window. The records can be filtered according to the **Vehicle Status** and **Vehicle Type**.

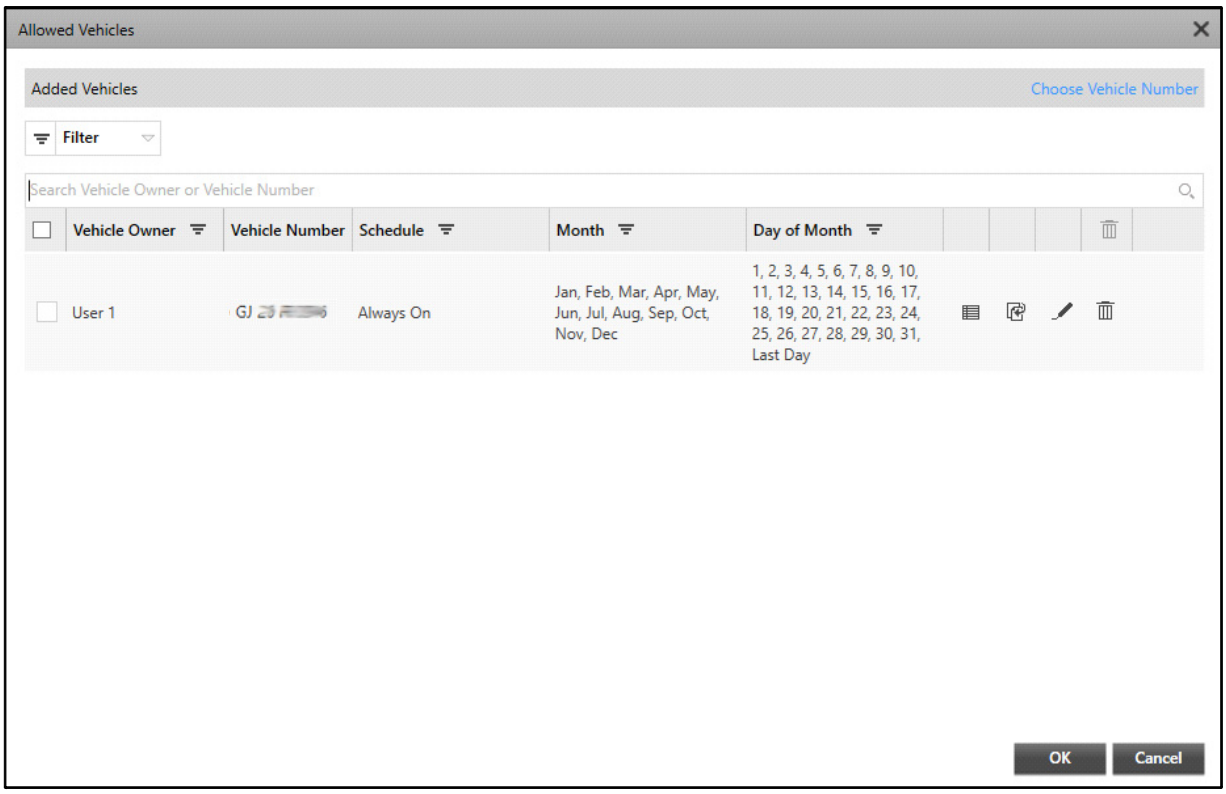


Select the check box of the desired options and click **FILTER**. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR**.

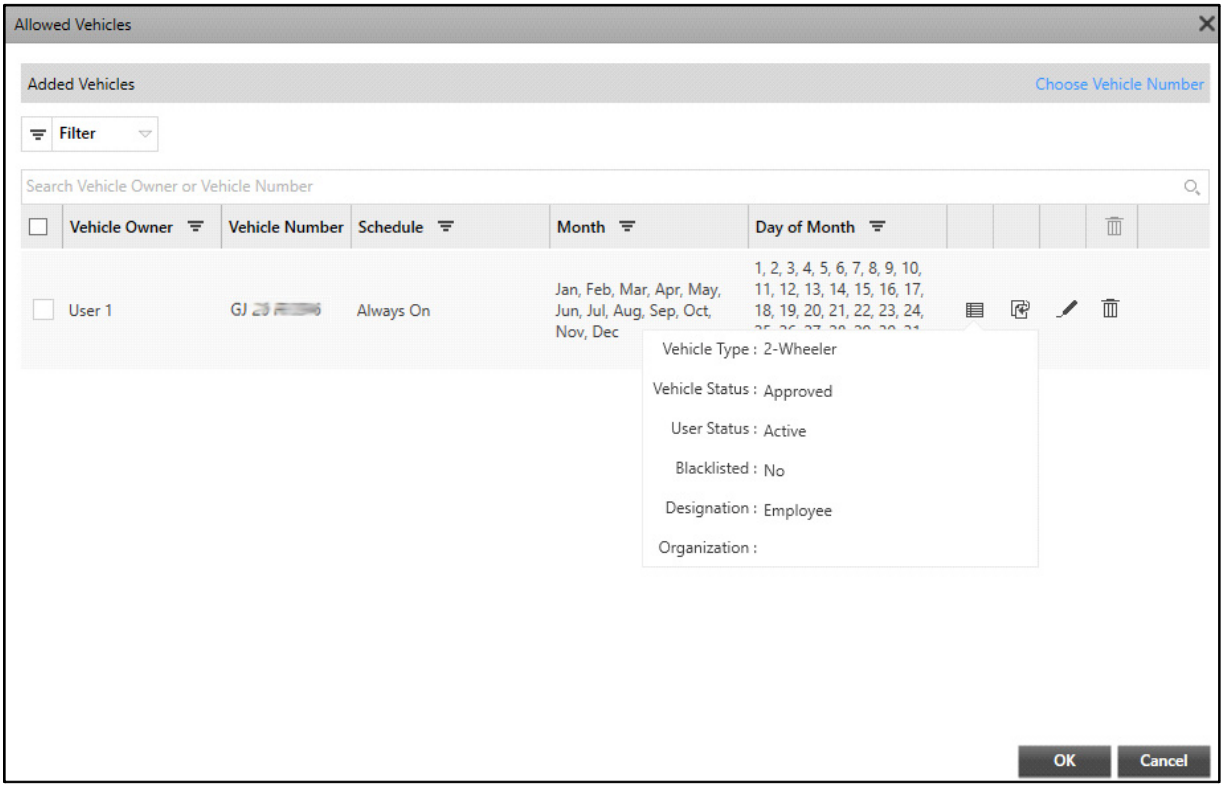
- You can also **Sort** records. To do so, click on the desired option — Vehicle Owner, User Status, Blacklist, Designation, Organization in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.
- Click **Done** to add the selected vehicle or click **Cancel** to discard.

The added vehicles automatically appear under **Show Added Vehicles**.

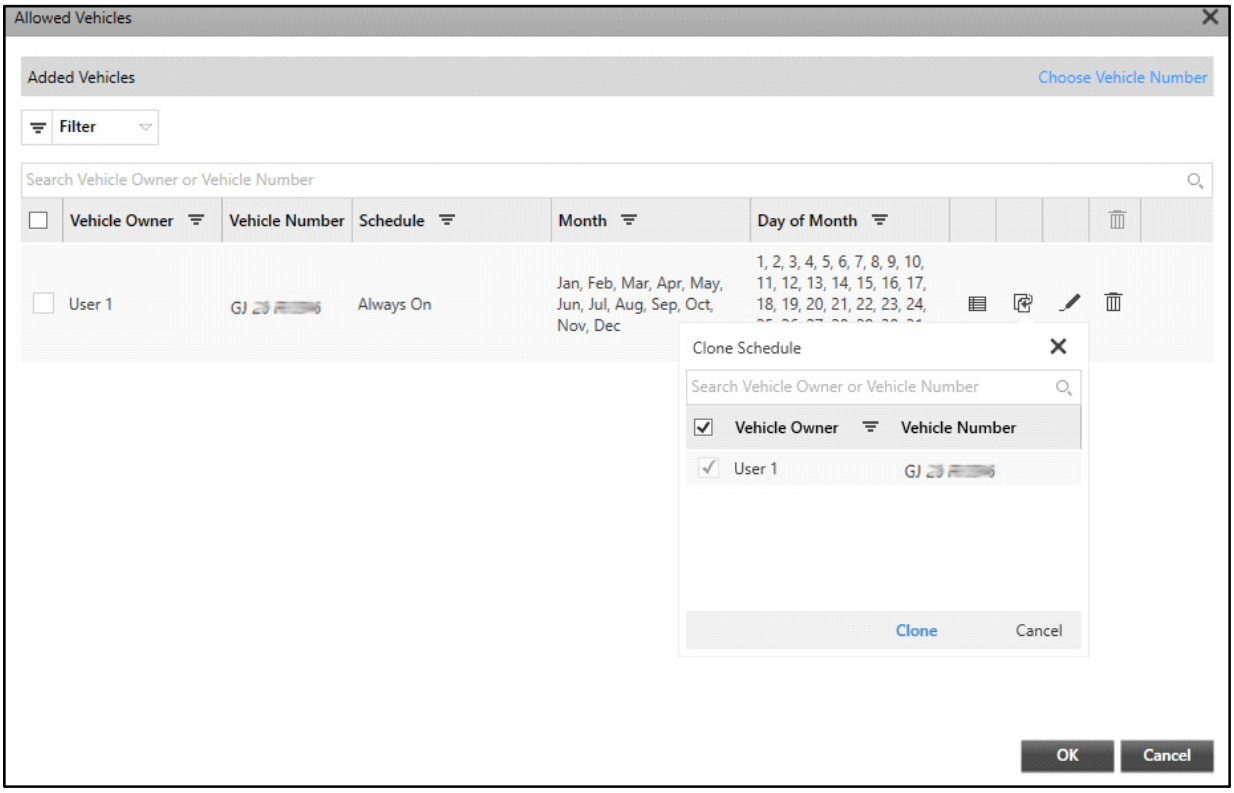


All the added vehicles appear in a list. You can view the Details, Clone, Edit and Delete the records.

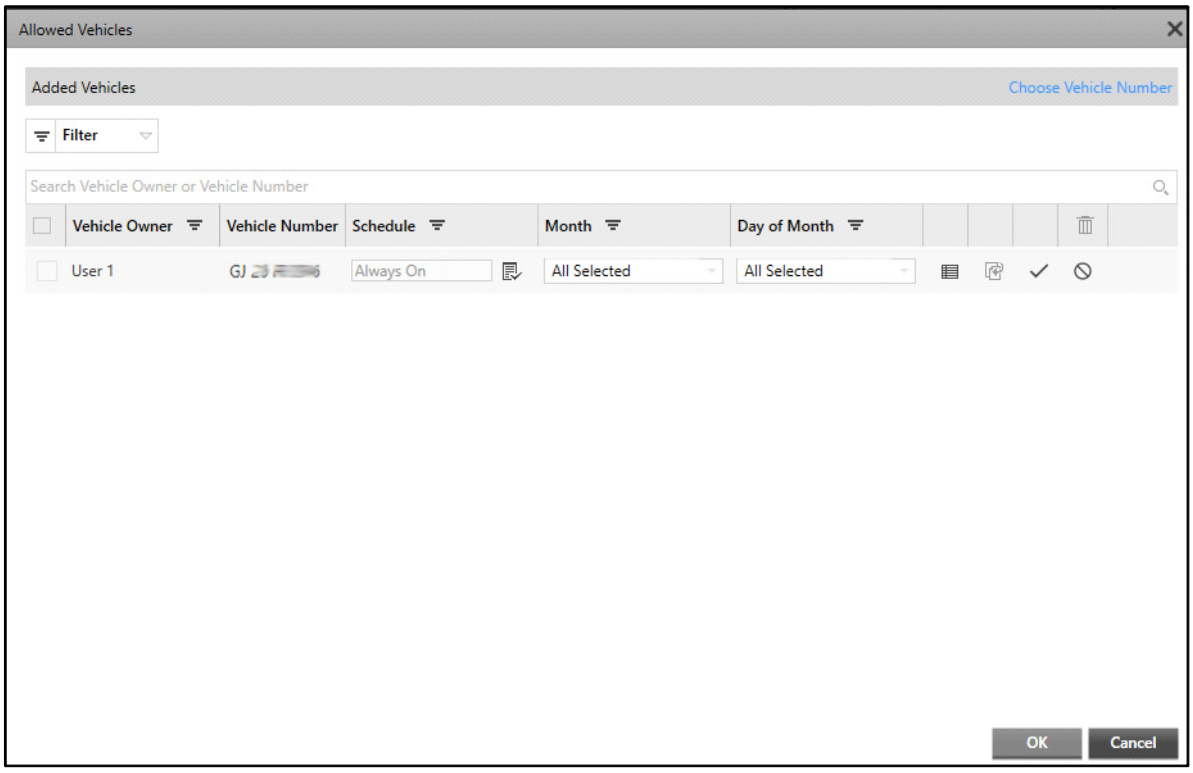
- **Details**: Click **Details** to view the additional details of the added vehicle. A pop-up appears with the additional details.



- **Clone**: Click **Clone** to copy the schedule of the selected vehicle to other added vehicles. The **Clone Schedule** pop-up appears.



- Select the vehicles to which you wish to copy the schedule.
- Click **Clone** to copy schedule or click **Cancel** to discard.
- **Edit**: Click **Edit** to edit the vehicle details.

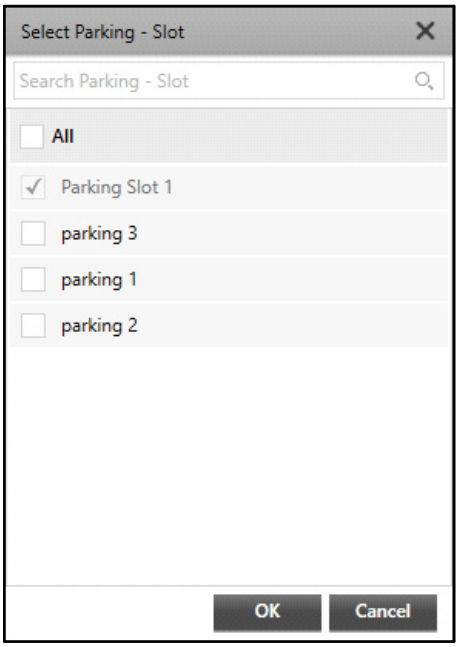


- Edit the desired details. Click **Save** to save the details or click **Cancel** to discard.
- **Delete**: Click **Delete** to delete the added vehicle.

- Click **OK** to confirm or click **Cancel** to discard.

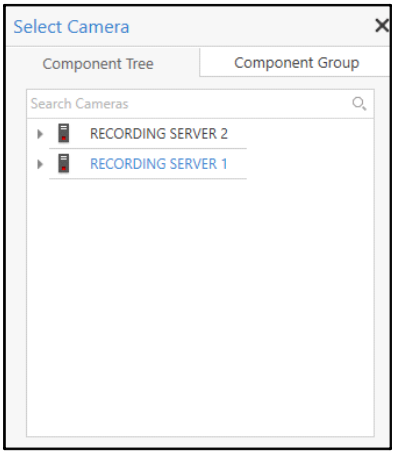
  All the added vehicles appear in **Allowed Vehicles**. You can clone the allowed vehicles configuration to other slots.

  - Click **Clone Allowed Vehicle** . The **Select Parking Slots** pop-up appears.

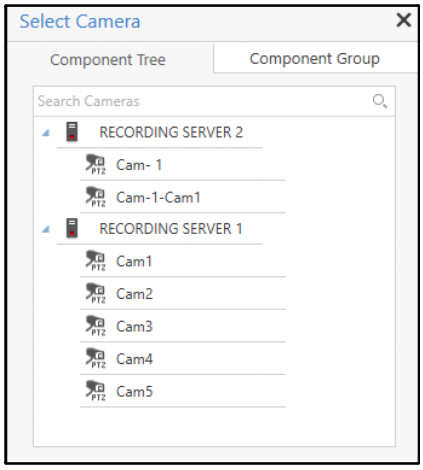


- Select the desired slots. Click **OK** to confirm or click **Cancel** to discard.

- **Permitted Duration**: Specify the permitted duration in seconds. If the vehicle is found to be parked for more than the specified permitted duration, then an alert will be send to the user regarding the same. Valid Range: 1 to 1440 minutes. Default: 3.
- **Camera**: Select the desired camera which you wish to assign to the slot using the **Camera** picklist.
  - Click **Camera** picklist. The **Select Camera** pop-up appears.

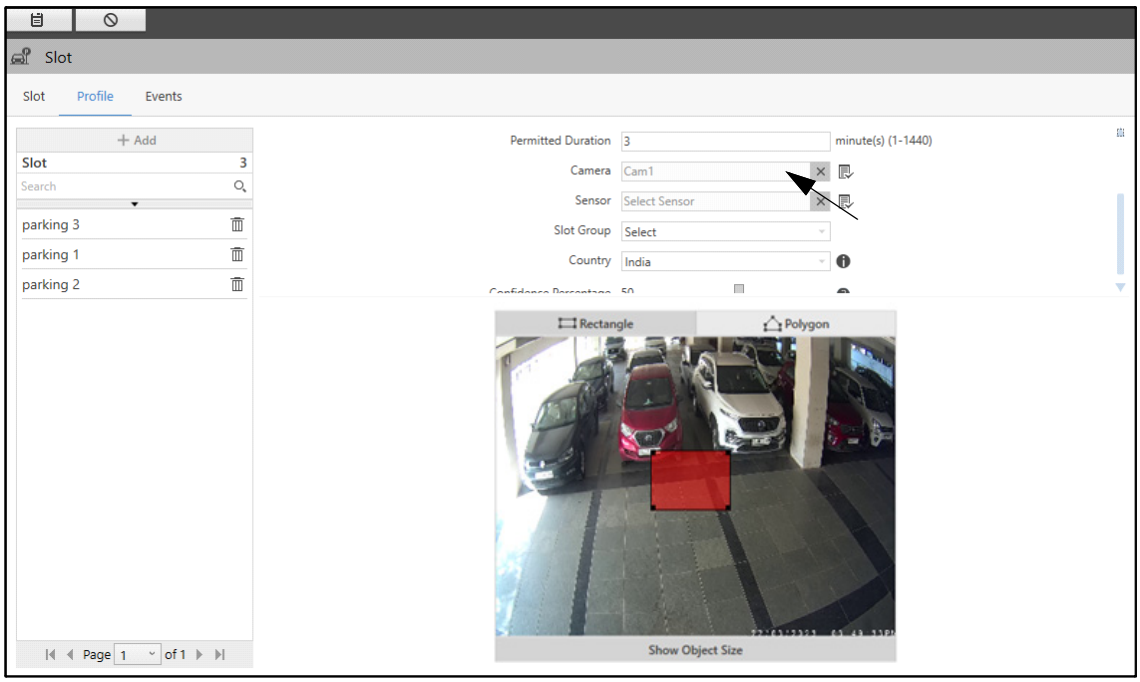


  - The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Double-click the desired camera to assign it to the slot. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

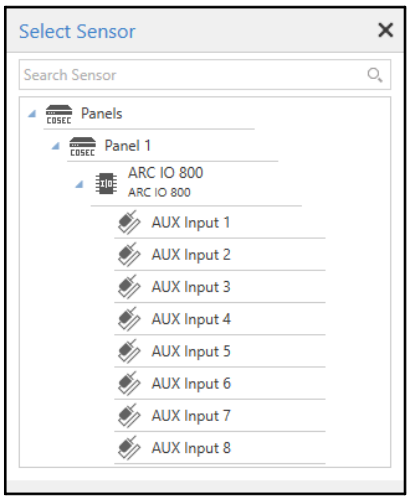
- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click to select the desired option.
  - Click **Go to selected position** , to move the camera to the selected preset position.
- To remove the camera, click **Remove** .



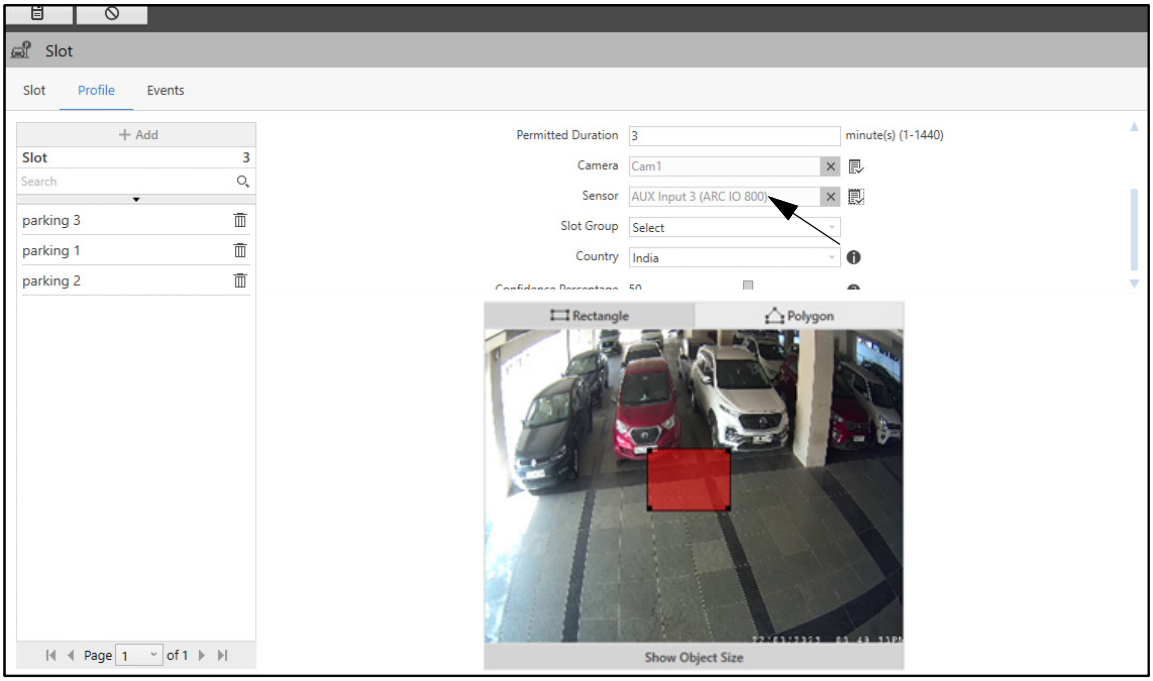
- **Sensor**: Select the desired sensor for the slot using the **Sensor** picklist. The 8 AUX Inputs of each IO controller appear in the list. You can assign an AUX input to a particular slot.

You need to add the COSEC Standalone Panel and the IO Controller from the Access Control Module prior to configuring sensors. To know more about Panel configuration, refer to "Standalone Panel".

- Click **Sensor** picklist. The **Select Sensor** pop-up appears.



- Double-click to select the desired sensor from the list.
- To remove the sensor, click **Remove** .



- **Slot Group**: Select the desired slot group from the drop-down list. All the configured slot groups appear in this list. To know about configuring slot groups, refer to "Slot Group".
- **Country**: Select the country from the drop-down list where the camera is installed. This increases the efficiency of vehicle recognition.

*The **Country** option will be applicable only when Number Plate Detection is done using Native ANPR.*

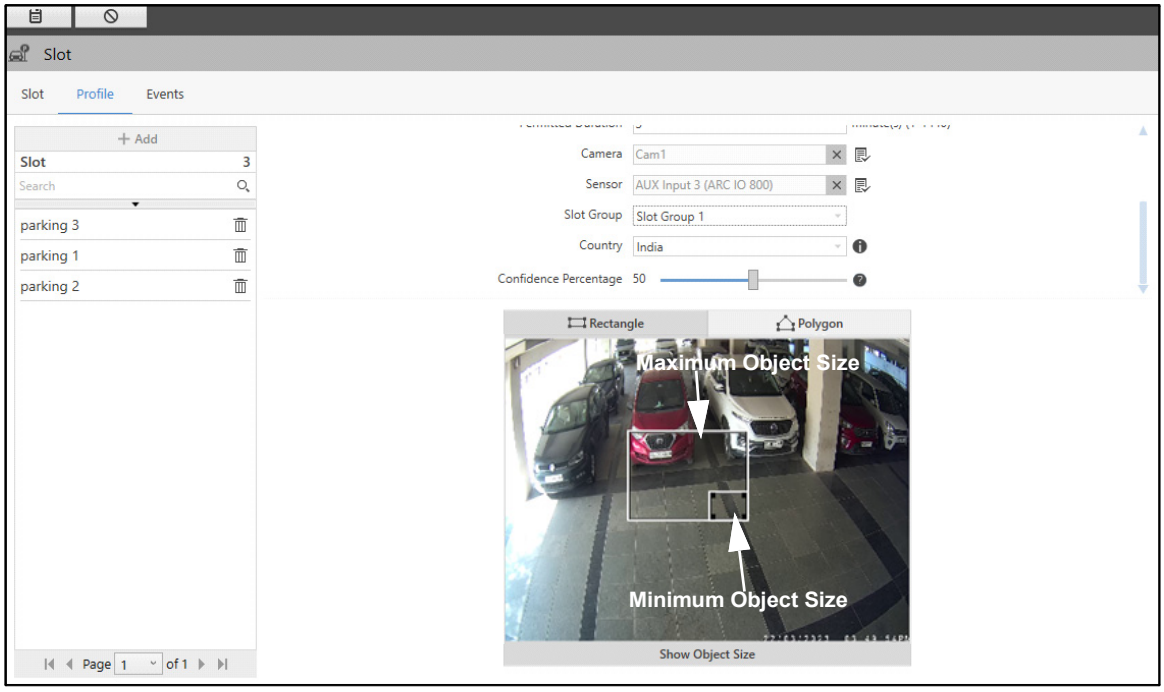
- **Confidence Percentage**: Set the Confidence Percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the percentage of success between image plate recognized and the text which is recognized from the image plate. This is the minimal percentage allowed for successful vehicle detection. Valid Range: 0 to 100%. Default: 50.

- Click **Save** to save the settings or **Cancel** to discard.

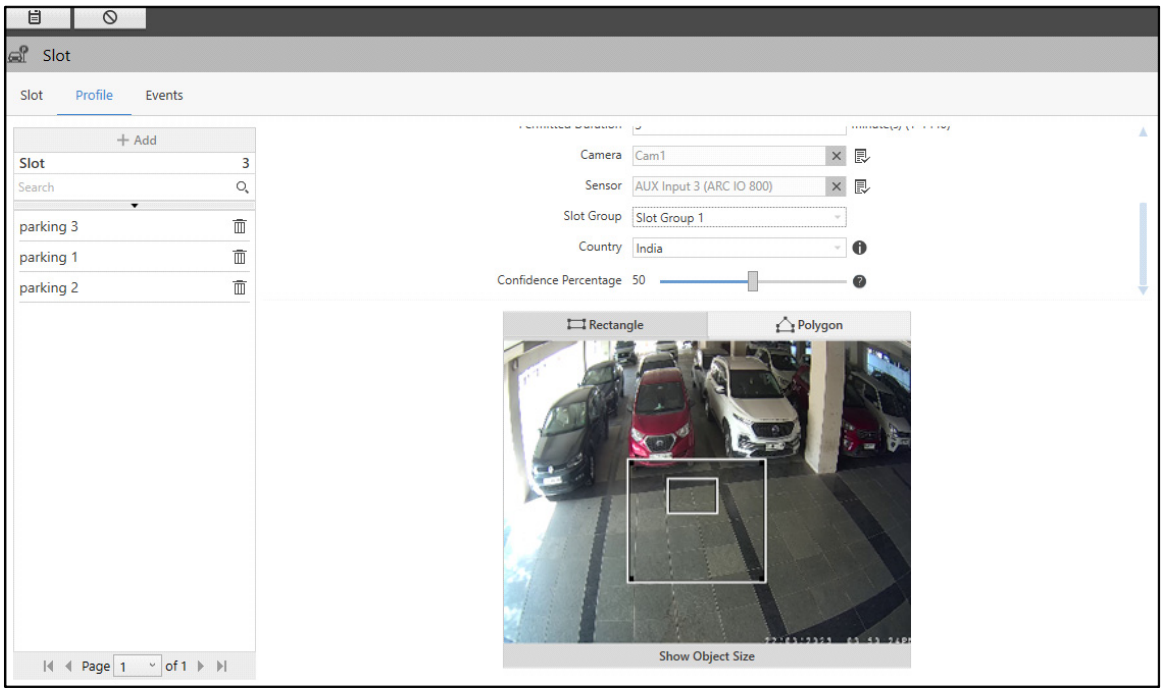
Once a camera is assigned, you can draw a slot on the live view of the camera. You can also define the **Minimum** and **Maximum Object Size**. You can either draw a **Rectangle** or **Polygon** to define the slot.

Object Size will not be applicable if you select Object Type in any Event. For details, refer to "Events".

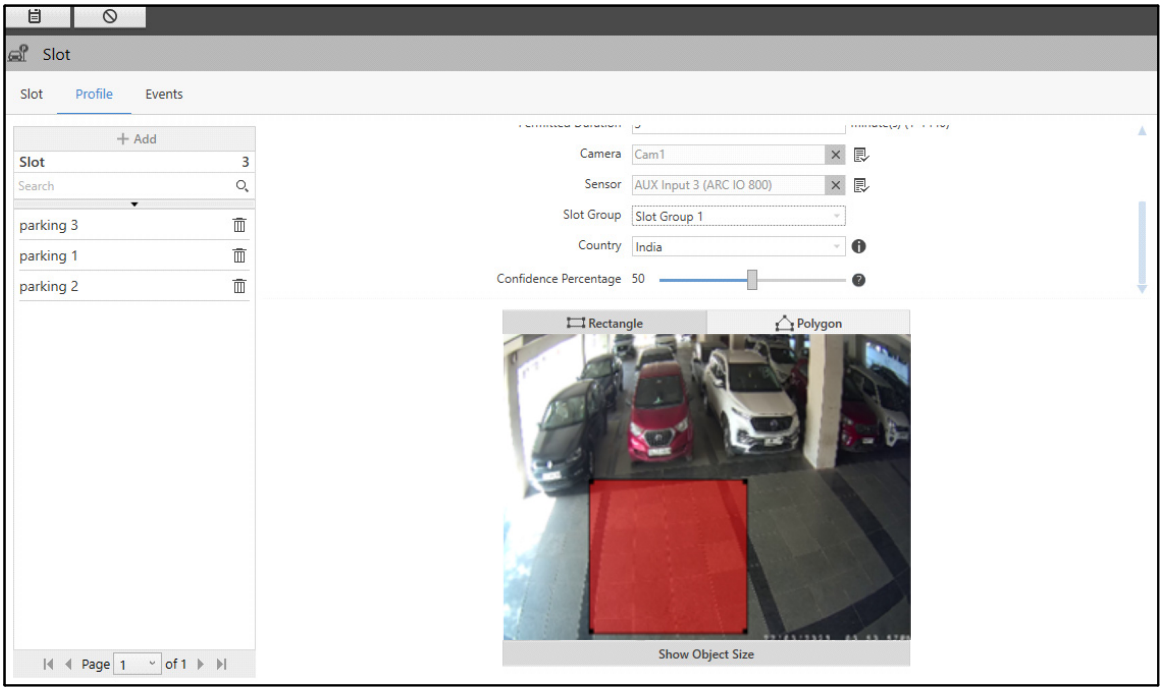
- Click **Show Object Size**. The default **Minimum** and **Maximum Object Size** appear.



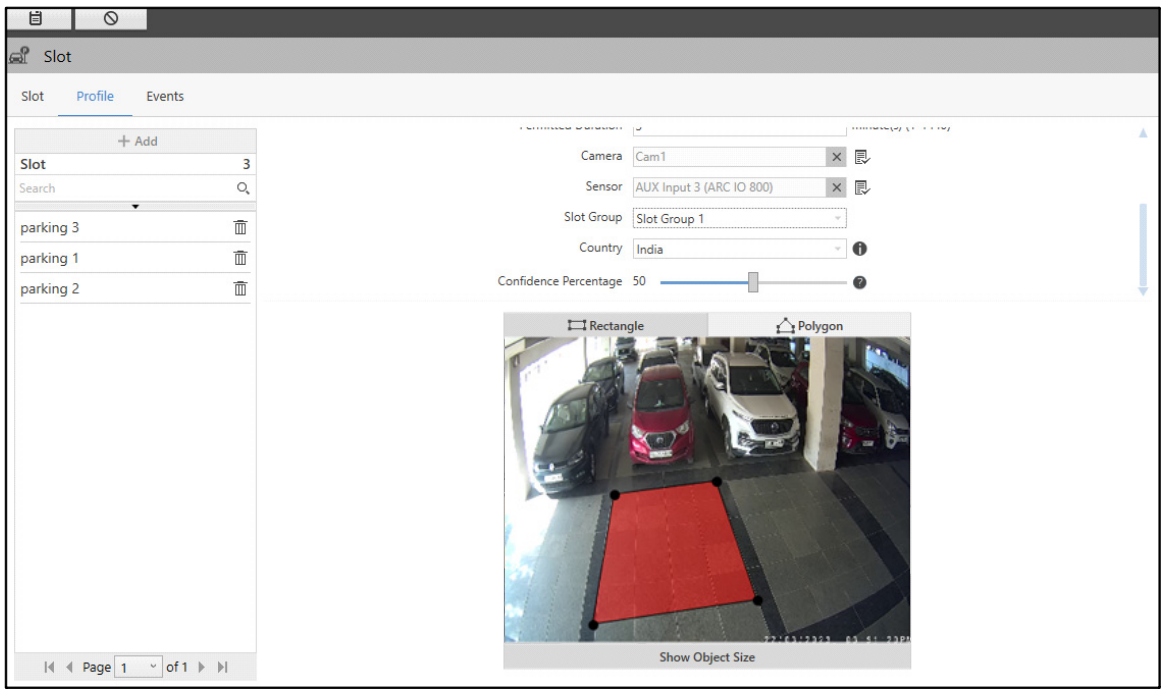
- Drag the corners of the rectangles to configure the minimum and maximum object size to be detected in the Event, if required. When the object size meant to be detected in the Event does not fit in the default Minimum and Maximum Object Size, you can configure it to match the desired object size.



- Click **Save** to save the settings or **Cancel** to discard.
- Click **Hide Object Size** to hide the size and draw the slot.
  - Select either **Rectangle** or **Polygon** to draw the slot.
  - If you select **Rectangle**, drag the corners and sides of the rectangle to configure the slot.



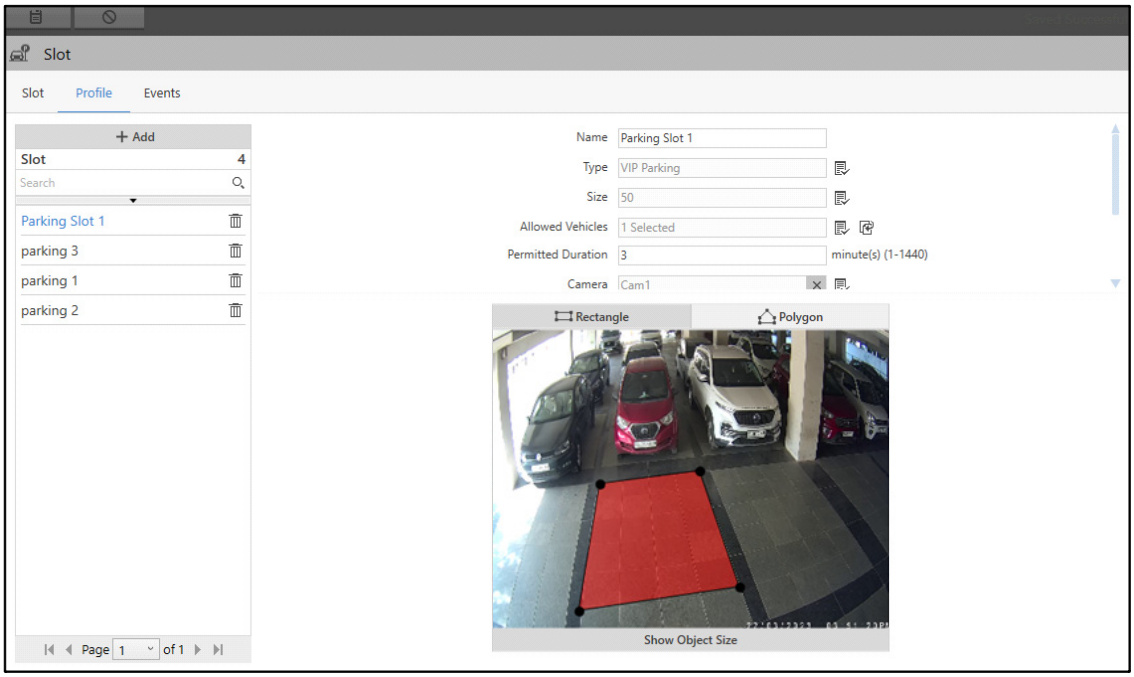
- If you select **Polygon**, click on the live view to place the vertex of the polygon. Click again on the desired place to join the previous vertex with a new vertex. Continue this process to complete the polygon.



- Click **Save** to save the settings or **Cancel** to discard.

The new slot will appear in the list on the left hand side.

You can edit the configurations of the slot or delete it.



- Select the desired slot from the list and edit the configurations on the right hand side.

- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired slot.

Similarly, you can configure the other Slots.

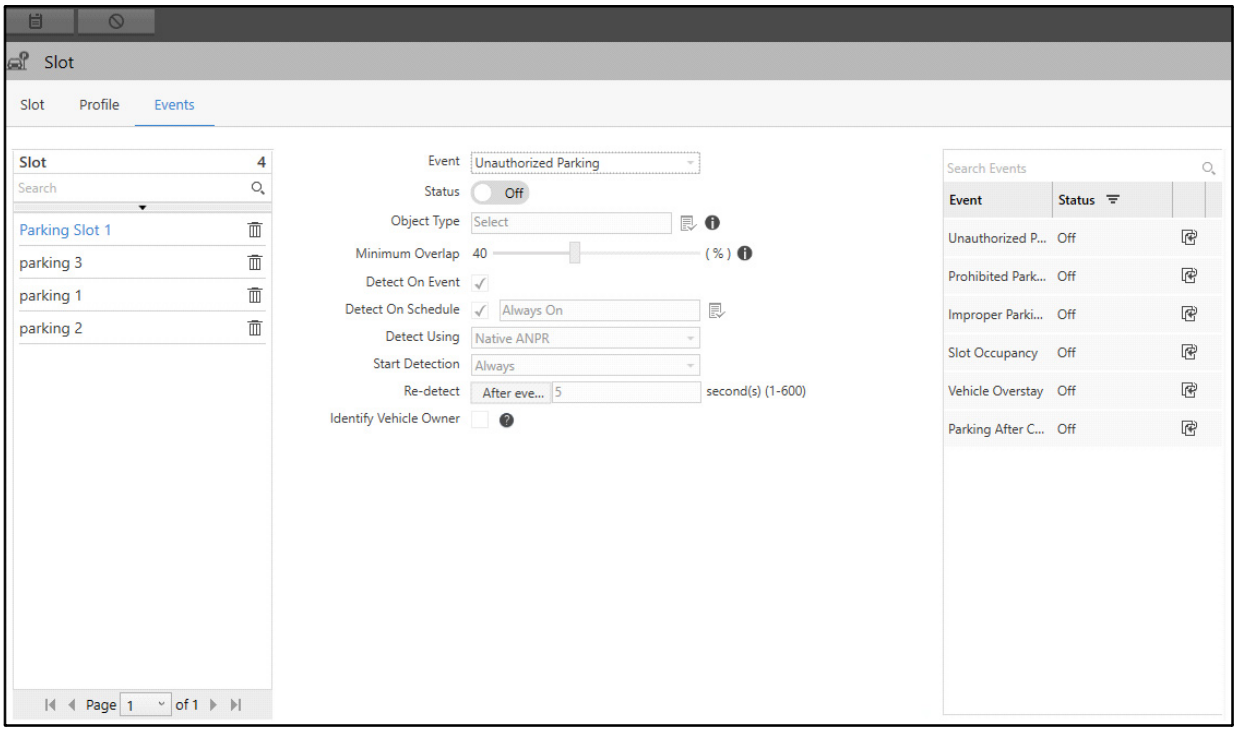
Events

This tab enables you to configure Events for the Slots. All the configured Events appear under the **Slot** tab.

Object Size configured in any "Profile" will not be applicable if you select Object Type in any Event.

To configure Events,

- Click the **Events** tab.



For slots, you can configure the following Events:

- "Unauthorized Parking"
- "Prohibited Parking"
- "Improper Parking"
- "Slot Occupancy"
- "Vehicle Overstay"
- "Parking After Closing Hours"

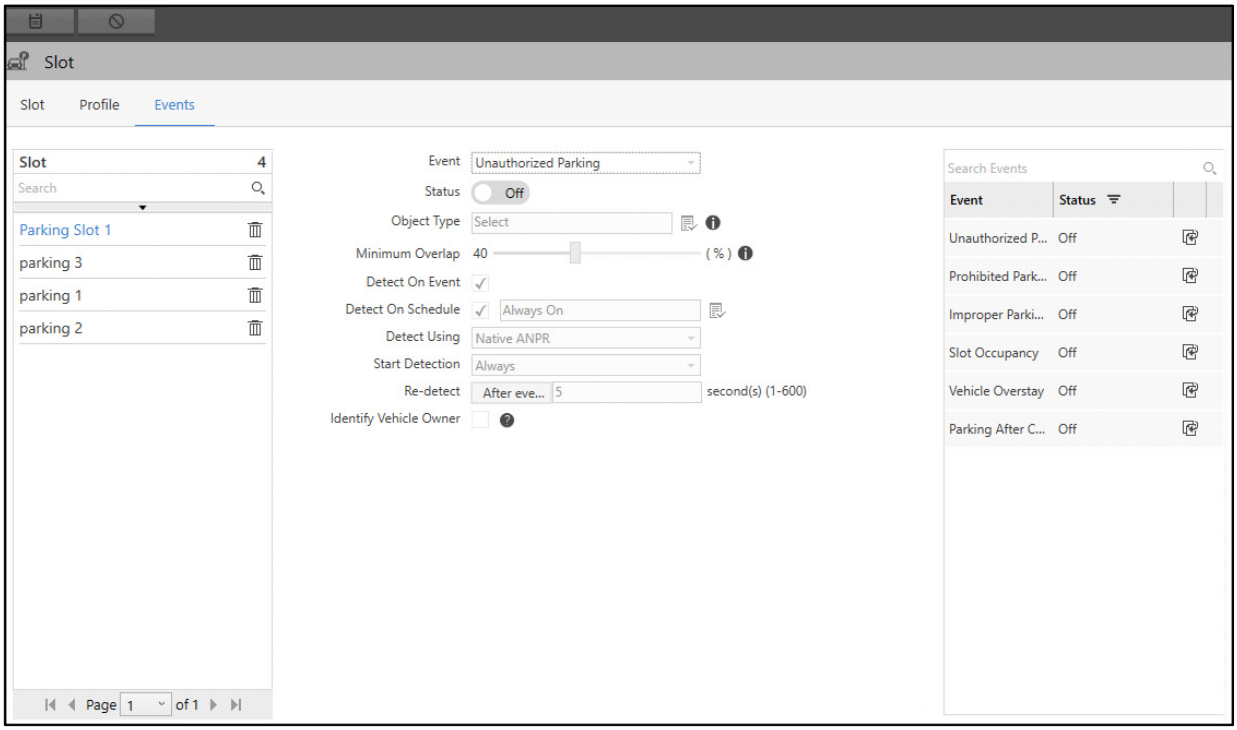
Unauthorized Parking

The Unauthorized Parking feature enables you to allot a particular zone on the basis of an unique vehicle number. Thus, you get an alert if someone else is parking in a parking area allotted to someone else. Allowed vehicles can be defined from the slot Profile. This feature enables you to add all the authorized vehicle numbers. This list can be used to generate Unauthorized Parking Event, that is, any vehicle whose number is not listed in the allowed vehicle list will not be allowed to park their vehicle and hence, Unauthorized Parking Event will be generated.

For example, in apartments or regional offices, people have allotted parking or authorized parking. When some other person or visitor park their vehicle in someone else's allotted parking, this creates a problem. As a result, Unauthorized Parking Event is useful to manage such situations.

To configure Unauthorized Parking Event for slots,

- Select the desired Profile from the list on the left hand side for which you wish to configure the Event.

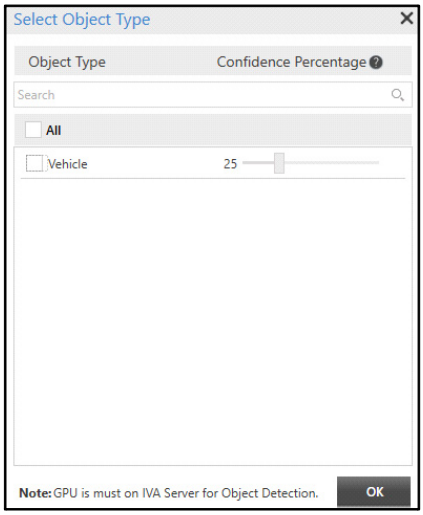


Configure the following parameters:

- **Event:** Select the Unauthorized Parking Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

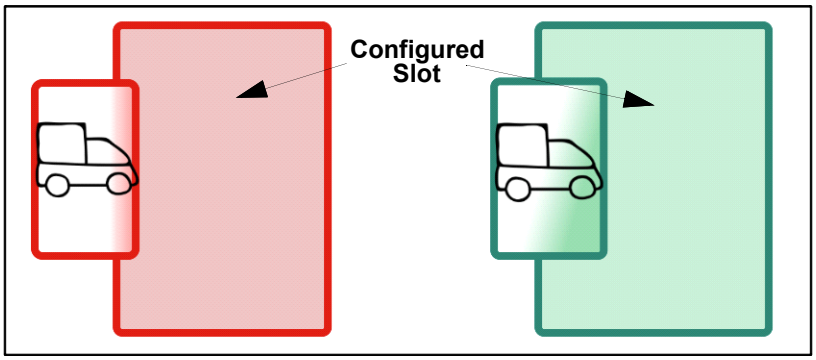


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection.Valid Range: 0 to 100%. Default: 25. Click **OK**.

- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the slot to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the slot will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the slot will trigger the event. Valid Range: 0-100%. Default: 40.

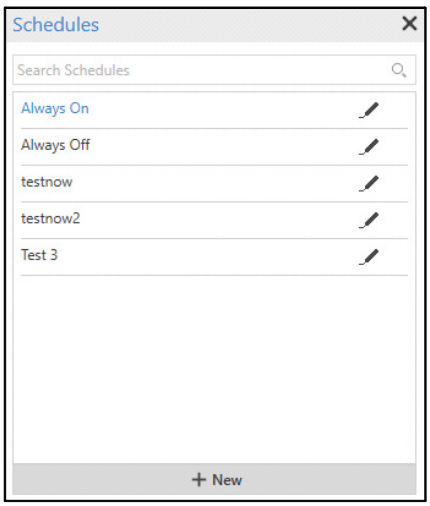
  For example, if you have configured Minimum Overlap as 30%, then as per the Green Slot, the event will be triggered when 30% of the unauthorized vehicle is overlapping the configured slot. Whereas, in the Red Slot, the event will not be triggered as, only 10% of the unauthorized vehicle is overlapping the configured slot.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.

- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.

- Click **Schedule** picklist. The **Schedules** pop-up appears.



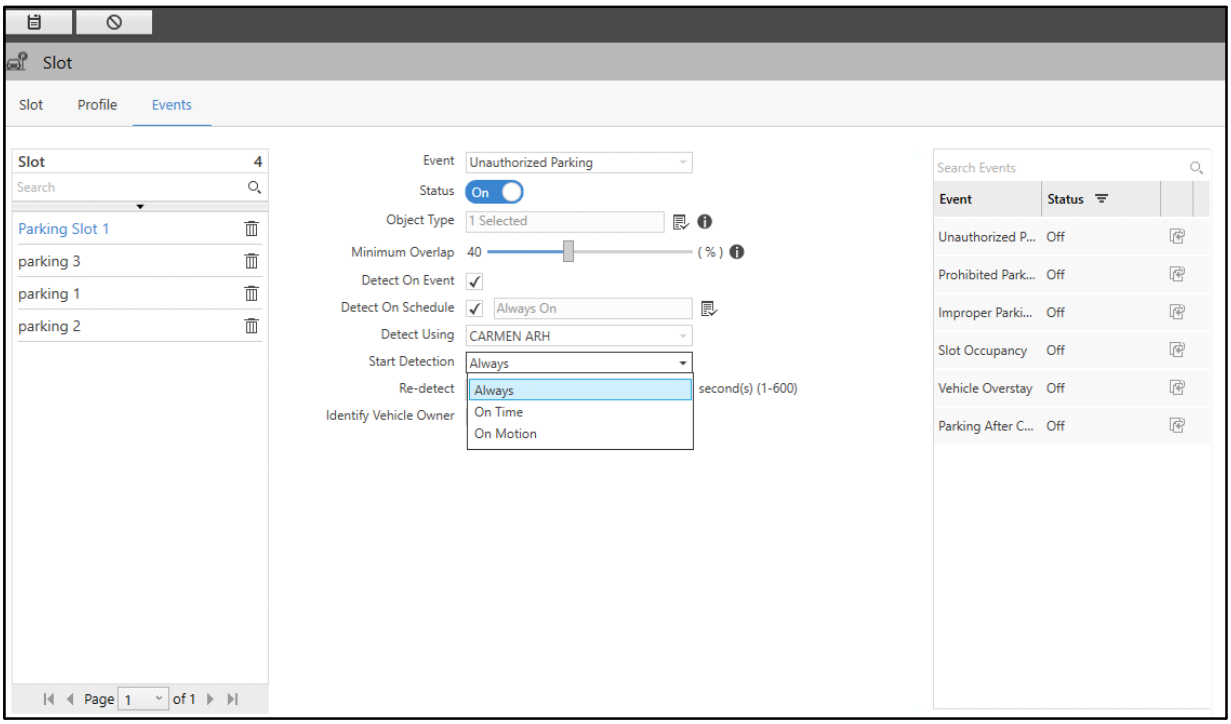
  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Detect Using**: Select the detection method from the drop-down list options — Native ANPR or CARMEN ARH.

  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Slot Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.
  If you select the detection method as **CARMEN ARH**, configure the following parameters:

- **Start Detection**: Select the start detection method from the drop-down list — Always, On Time or On Motion.

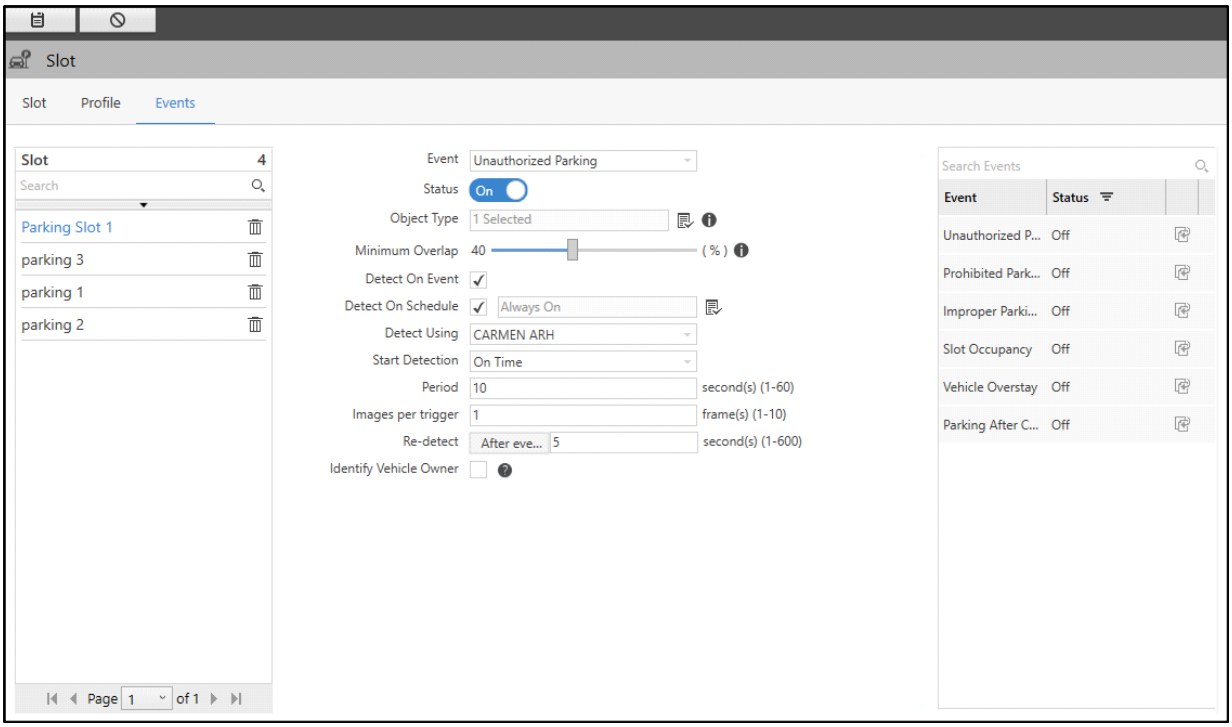


If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images per Trigger is higher than frames received in the configured period, the maximum FPS is sent to ARH. For example, Period = 1 sec and Images Per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters:

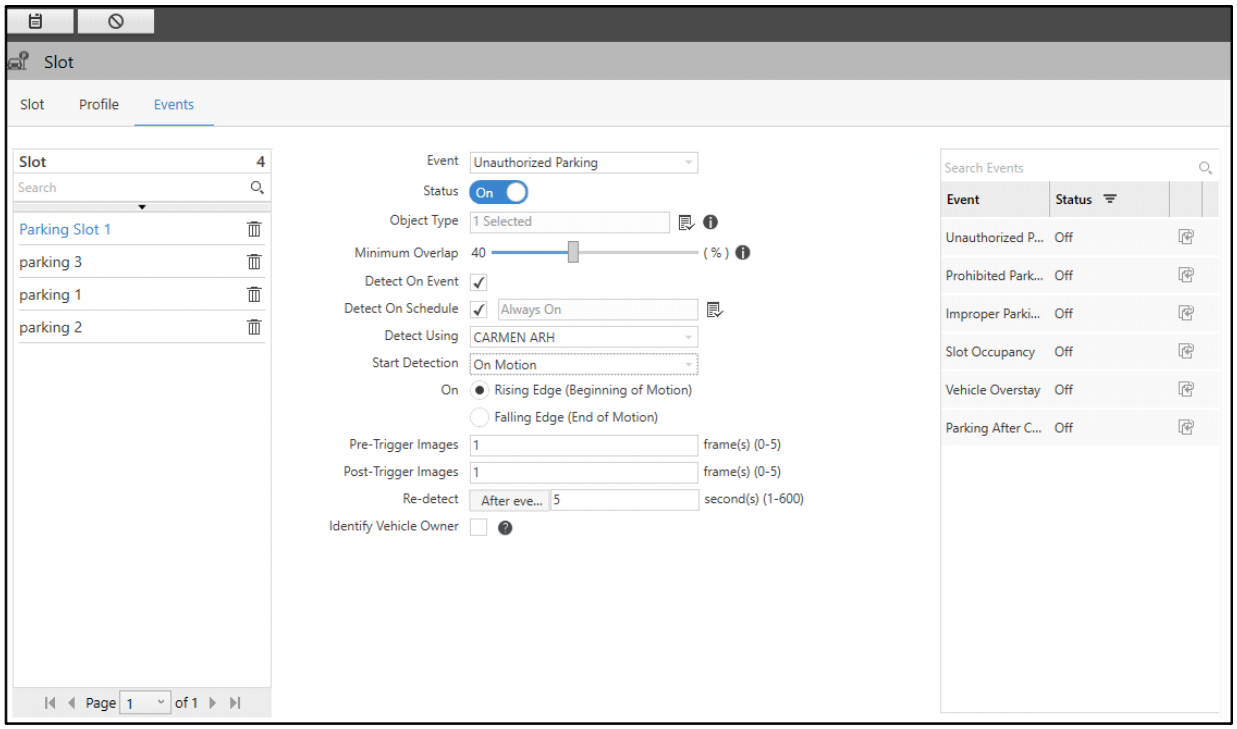
- **Period**: Specify the time interval after which the images will be sent to the ARH Engine. Valid Range:1-60 seconds. Default: 10.
- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range: 1-10 frames. Default:1.



If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as to when the images should be passed to the ARH Engine — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).
- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0-5 frames. Default: 1.
- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion. Valid Range: 0-5 frames. Default: 1.



- **Re-detect**: Specify the Re-detect time after which the Unauthorized Parking Event will be detected again after the previous detection.Valid Range: 0 to 600 seconds. Default: 5.

- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

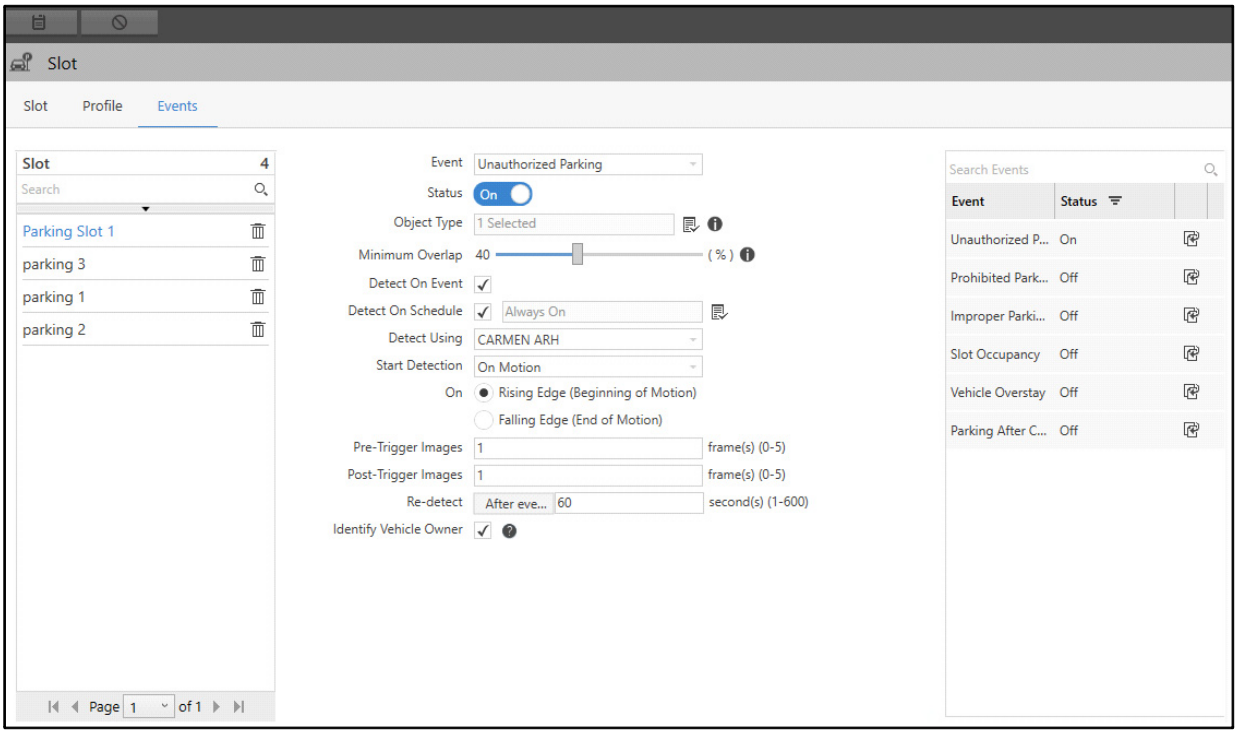
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

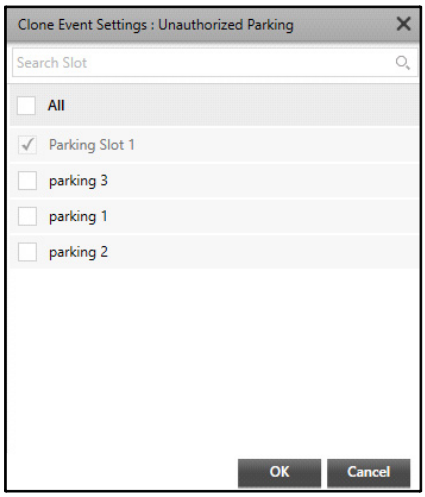
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of slot is created, the **Clone Event Settings** option will be enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Unauthorized Parking** pop-up appears.



- Select the desired slots to which you wish to copy these configurations.

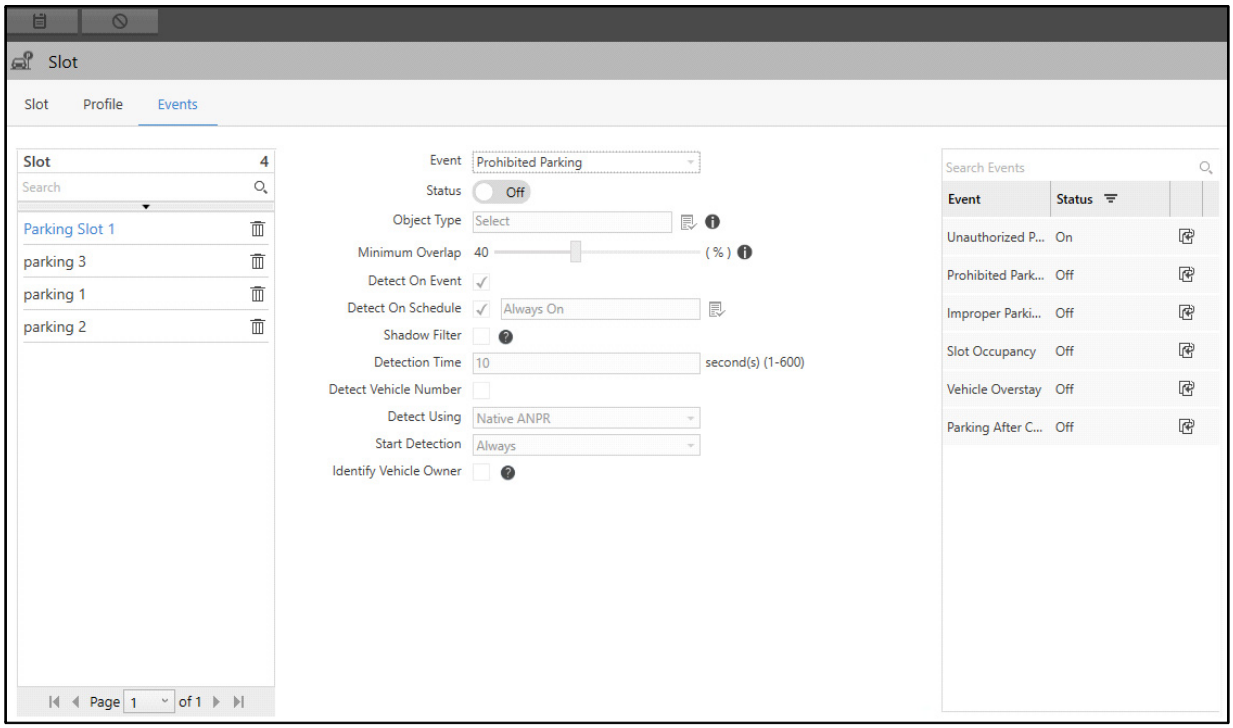
- Click **OK** to confirm or click **Cancel** to discard.

Prohibited Parking

The Prohibited Parking feature enables you to allot a particular zone where no parking is allowed. This feature is used in Traffic Management System. It can also be useful in parkings in mall or building or roadside parking. Thus, you can detect vehicles which are illegally parked in a No Parking Zone.

To configure Prohibited Parking Event for slots,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

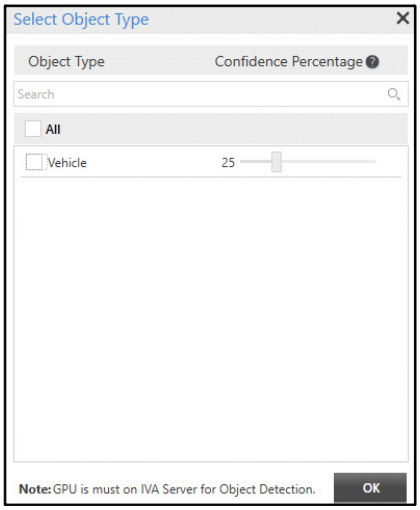


Configure the following parameters:

- **Event:** Select the Prohibited Parking Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

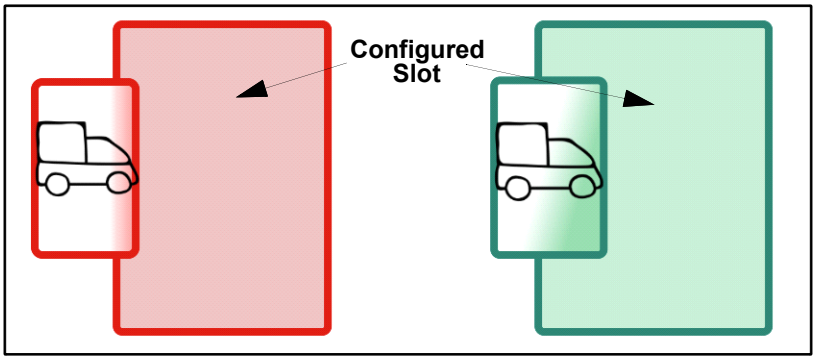


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection.Valid Range: 0-100%. Default: 25. Click **OK**.

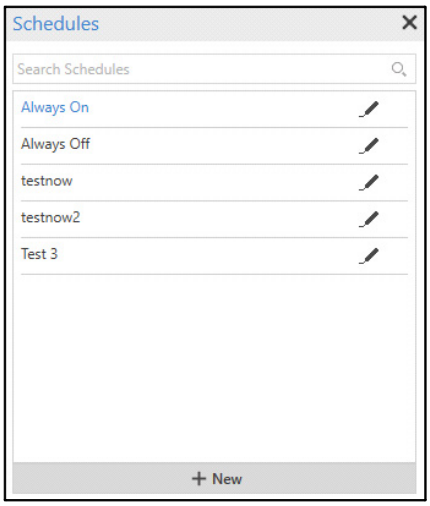
- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the slot to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the slot will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the slot will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Slot, the event will be triggered when 30% of the vehicle is overlapping the configured slot. Whereas, in the Red Slot, the event will not be triggered as, only 10% of the vehicle is overlapping the configured slot.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".

- **Shadow Filter**: Select the check box to ignore the shadow of the people/objects crossing the zone and reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Detection Time**: Specify the detection time in seconds after which the prohibited parking Event should be generated, provided the configured zone is empty initially. The Prohibited Parking Event wont be generated, if the zone already contains a vehicle before configuring the Event. Valid Range: 1-600 seconds. Default: 10.

- **Detect Vehicle Number**: Select the check box to enable vehicle detection through License Plate Recognition.

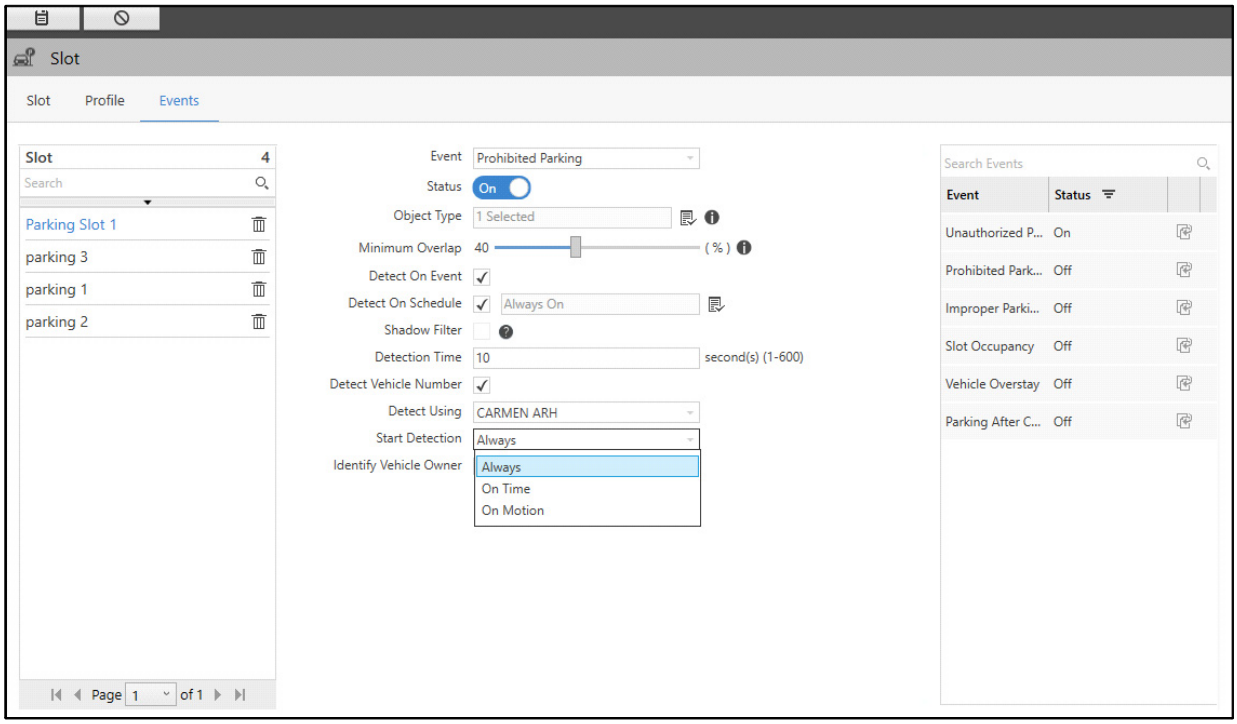
- **Detect Using**: Select the desired detection method from the drop-down list — Native ANPR or CARMEN ARH.

  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Slot Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.

  If you select the detection method as **CARMEN ARH**, configure the following parameters:

- **Start Detection**: Select the start detection method from the drop-down list — Always, On Time or On Motion.

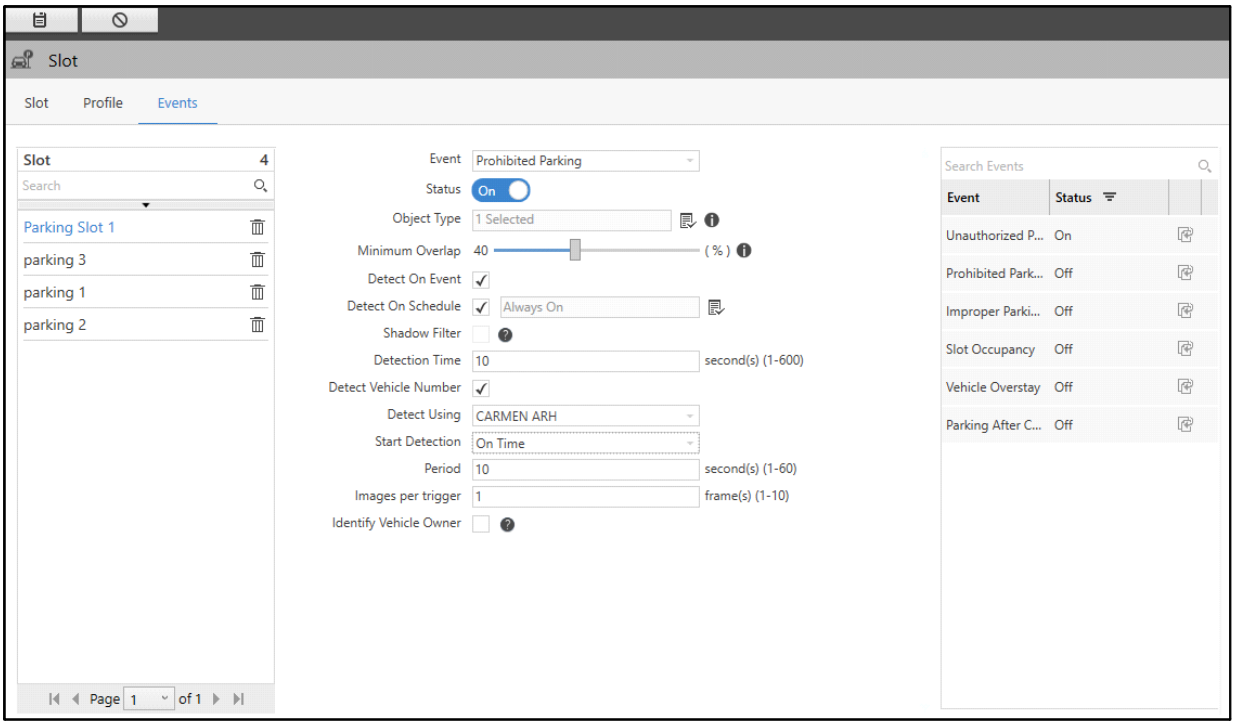


If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images per Trigger is higher than frames received in the configured period, the maximum FPS is sent to ARH. For example, Period = 1 sec & Images per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters.:

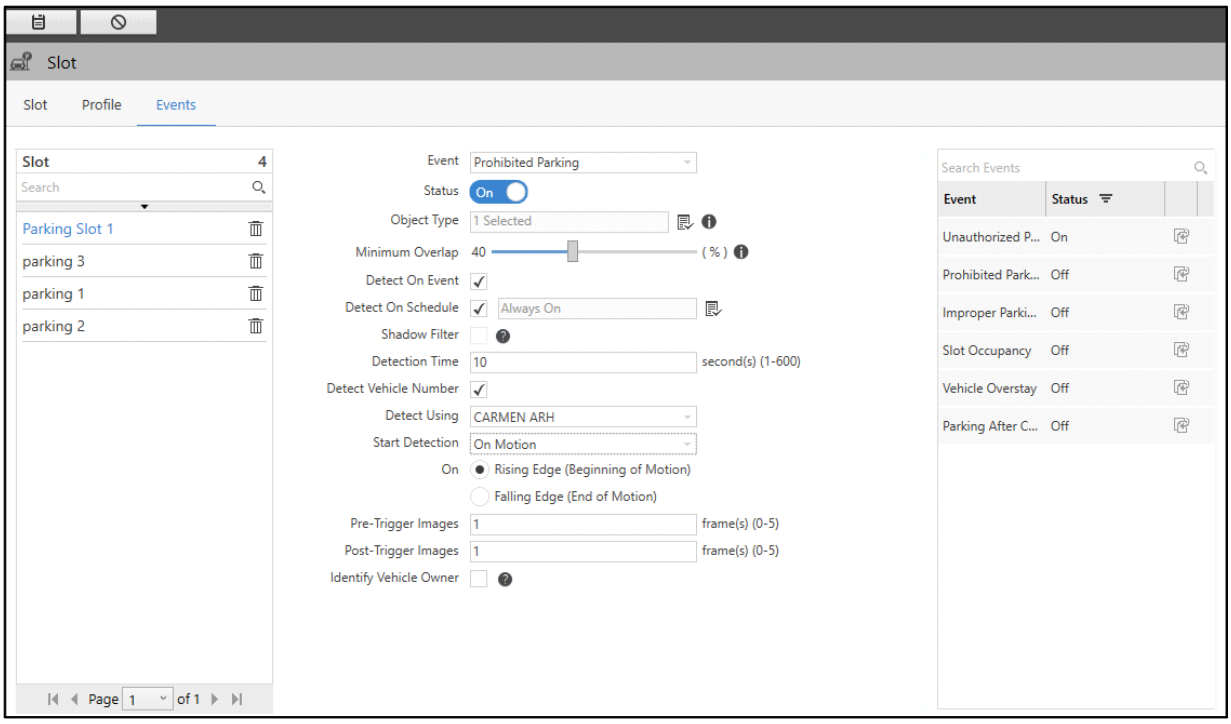
- **Period**: Specify the time interval after which the images will be sent to the ARH Engine. Valid Range: 1-60 seconds. Default: 10.
- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range:0-10 frames. Default:1.



If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as per which you wish the images to be passed to the ARH Engine — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).
- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0-5 frames. Default:1.
- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion. Valid Range: 0-5 frames. Default:1



- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

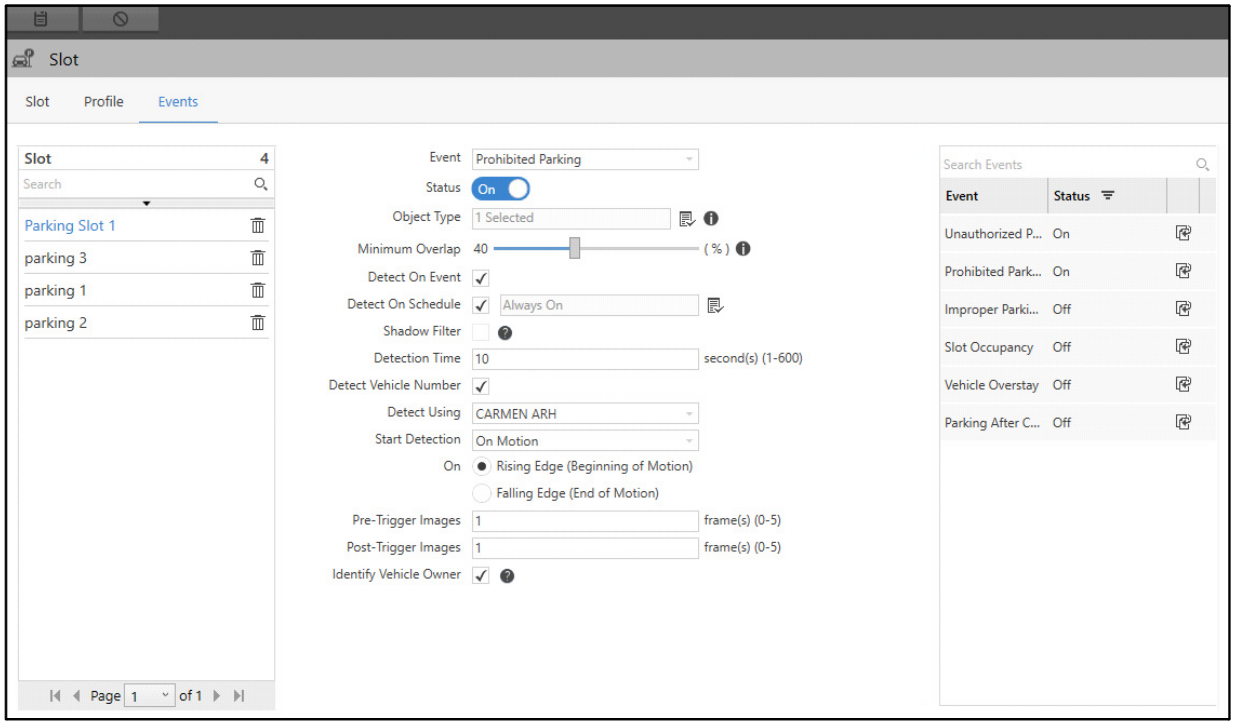
- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Prohibited Parking** pop-up appears.



- Select the desired slots to which you wish to copy the configurations.

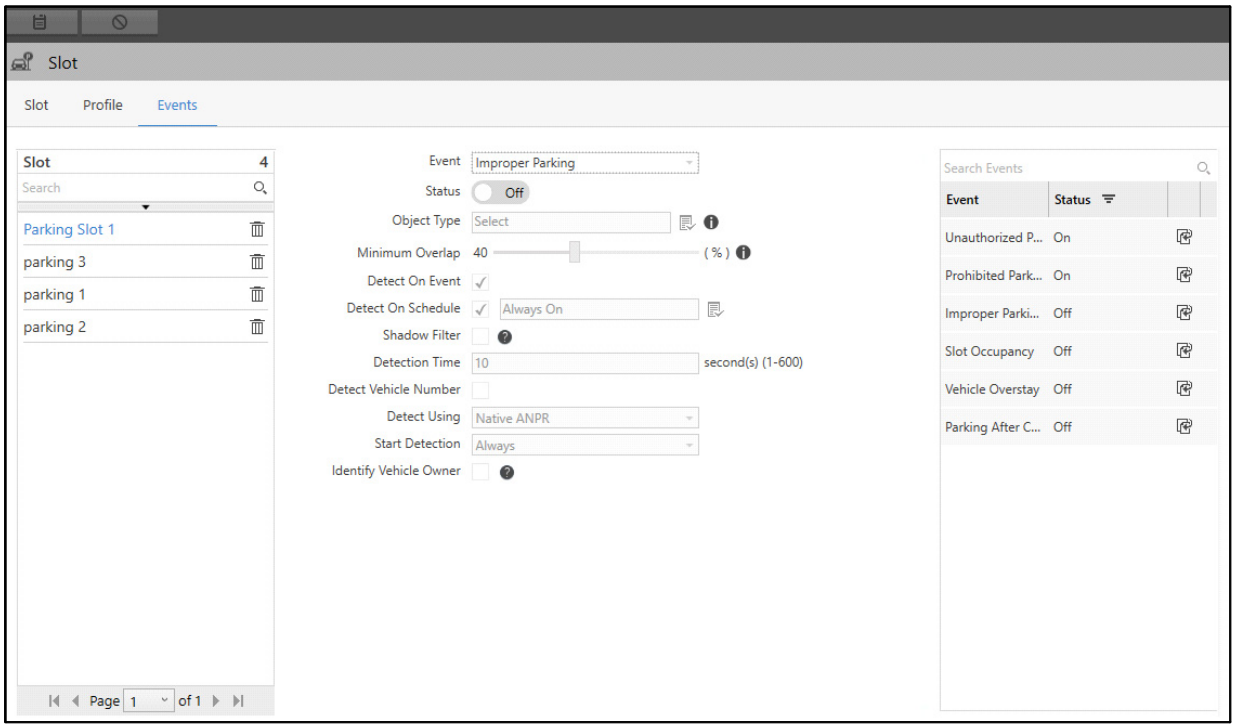
- Click **OK** to confirm or click **Cancel** to discard.

Improper Parking

The Improper Parking feature enables you to generate alerts when a vehicle is not parked as per the rules in the parking area. Based on these alerts, appropriate actions can be taken. The Improper Parking Event detects vehicles which are not parked as per the set rules.

To configure Improper Parking Event for slots,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

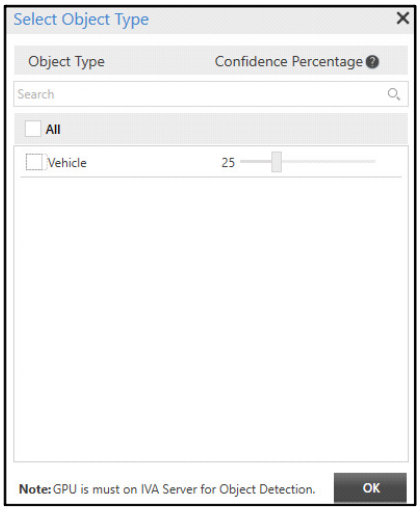


Configure the following parameters:

- **Event:** Select the Improper Parking Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

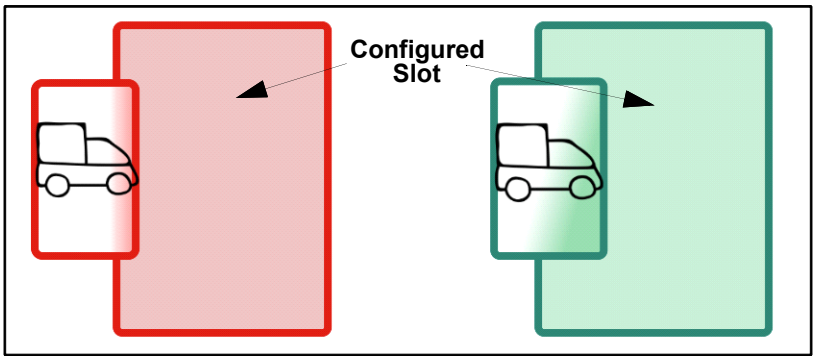


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection.Valid Range: 0-100%. Default: 25. Click **OK**.

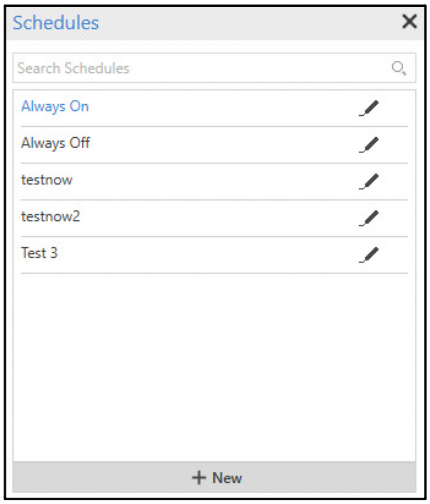
- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the slot to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the slot will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the slot will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Slot, the event will be triggered when 30% of the vehicle is overlapping the configured slot. Whereas, in the Red Slot, the event will not be triggered as, only 10% of the vehicle is overlapping the configured slot.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Shadow Filter**: Select the check box to ignore the shadow of the people/objects crossing the zone and reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Detection Time**: Specify the detection time in seconds after which the Improper Parking Event should be generated, provided the configured zone is empty initially. The Improper Parking Event wont be generated, if the zone already contains an improperly parked vehicle before configuring the Event. Valid Range: 1-600 seconds. Default: 10.

- **Detect Vehicle Number**: Select the check box to enable vehicle detection through License Plate Recognition.

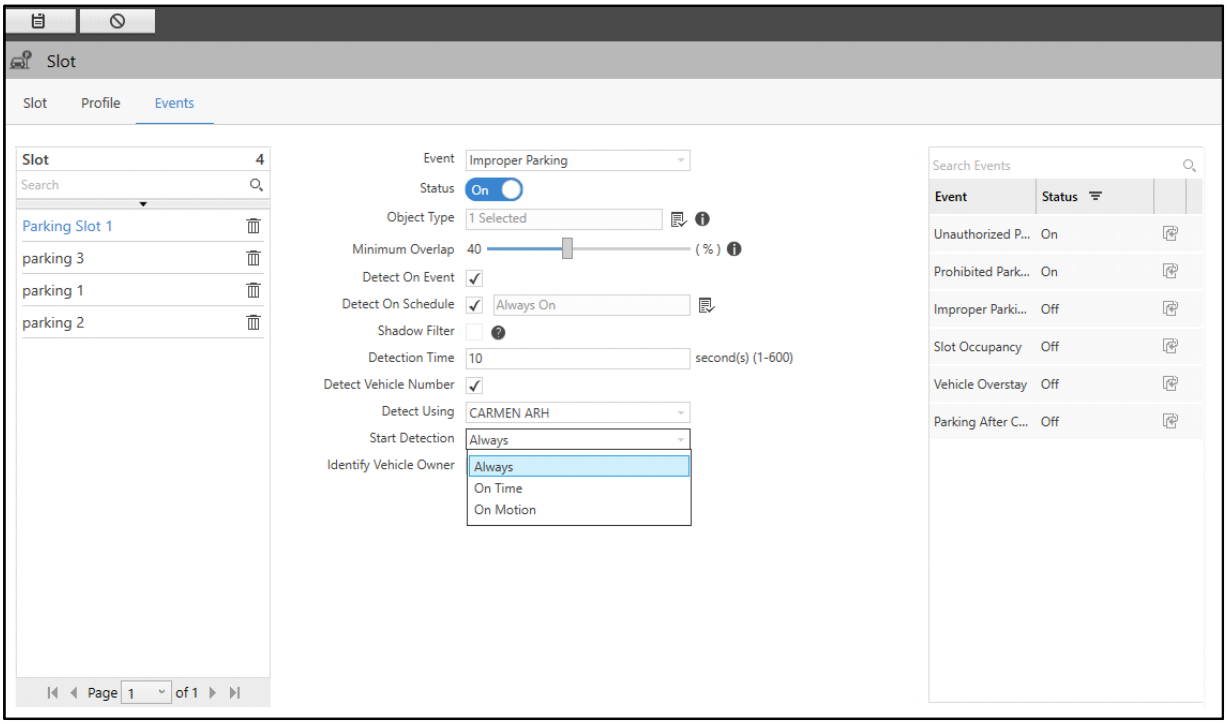
- **Detect Using**: Select the desired detection method from the drop-down list — Native ANPR or CARMEN ARH.

  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Slot Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.

  If you select the detection method as **CARMEN ARH**, configure the following parameters:

- **Start Detection**: Select the desired start detection method from the drop-down list — Always, On Time or On Motion.

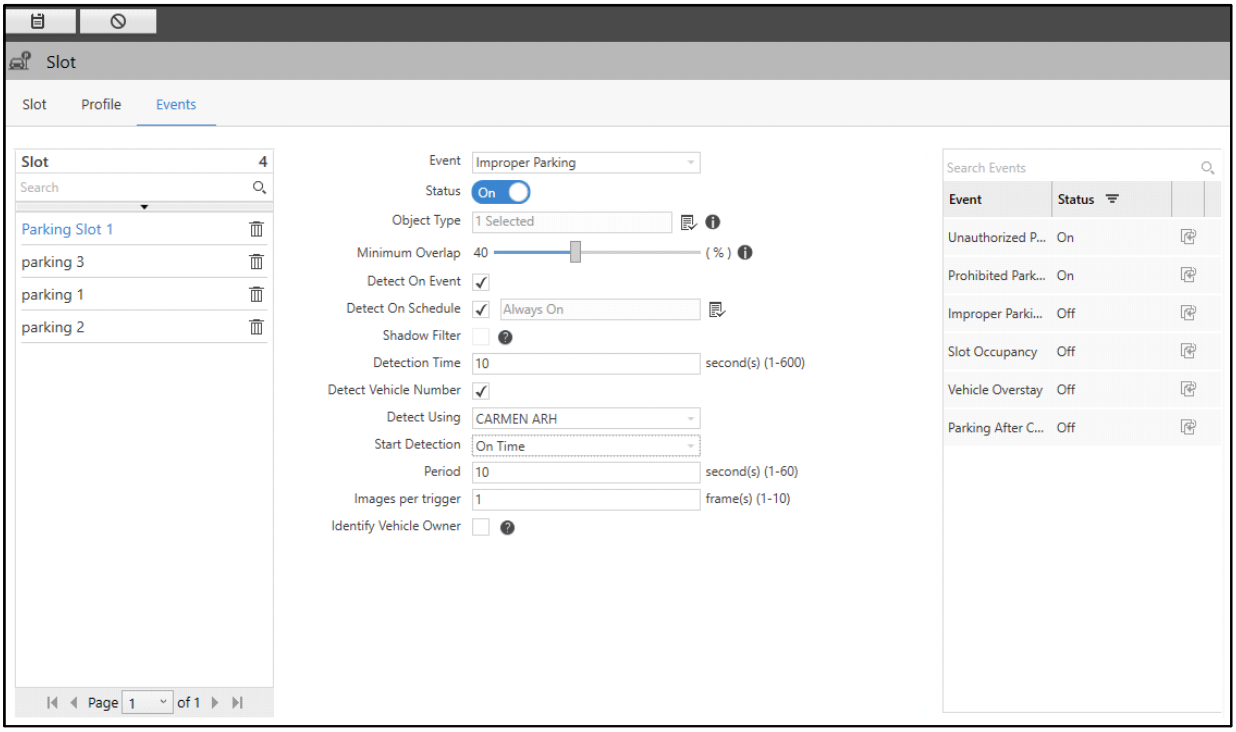


If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images per trigger is higher then frames received in the configured period, the maximum FPS is sent to ARH. For example, Period = 1 sec & Images per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters:

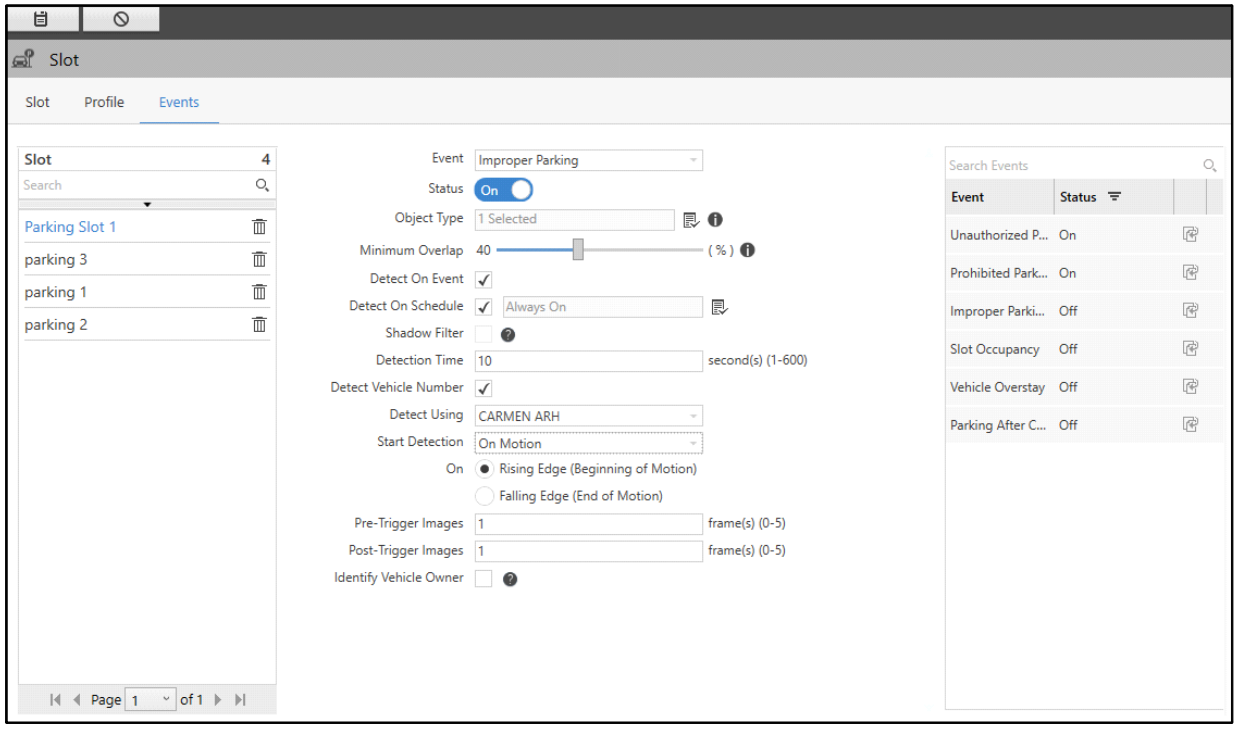
- **Period**: Specify the time interval after which the images will be sent to the ARH Engine. Valid Range: 1-60 seconds. Default:10.
- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range: 1-10 frames. Default: 1.



If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as per which the images to be passed to the ARH Engine — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).
- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0-5 frames. Default: 1.
- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion. Valid Range: 0-5 frames. Default: 1.



- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

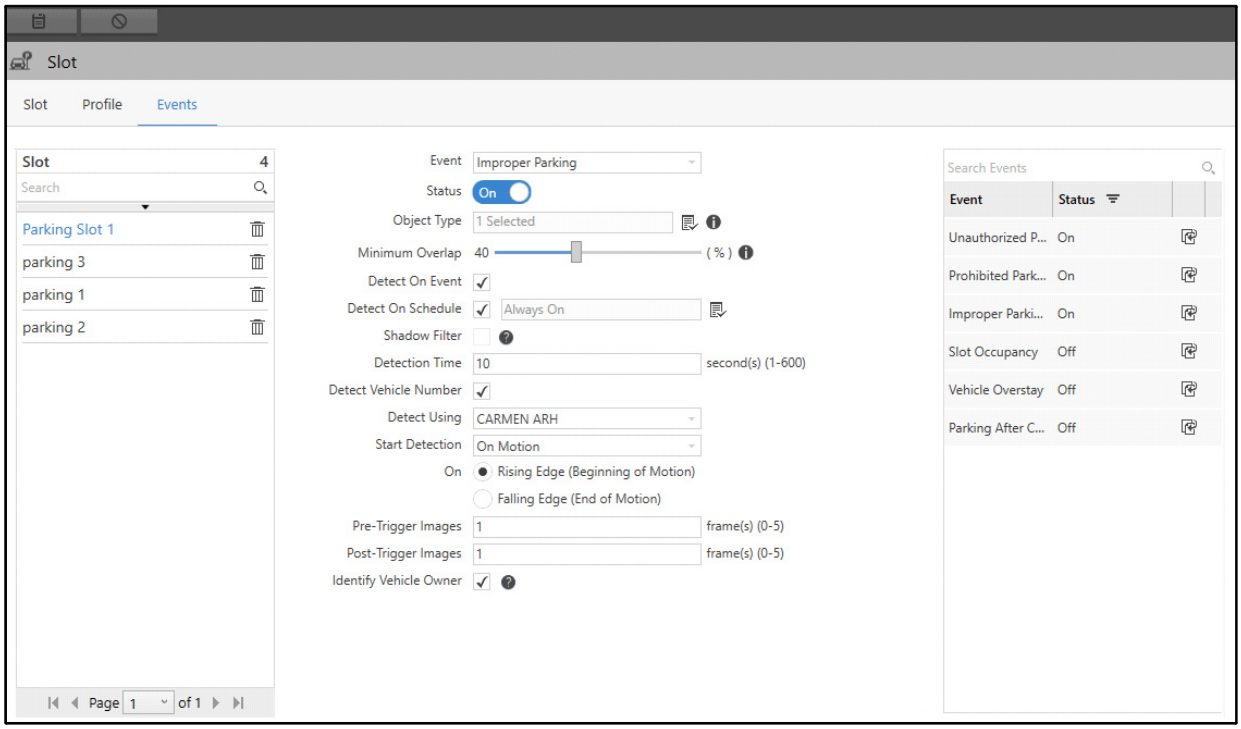
- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

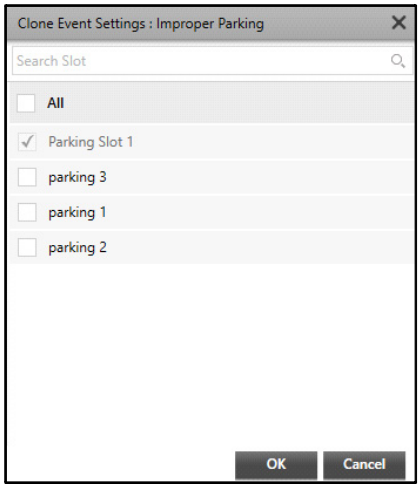
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Improper Parking** pop-up appears.



- Select the desired slots to which you wish to copy these configurations.

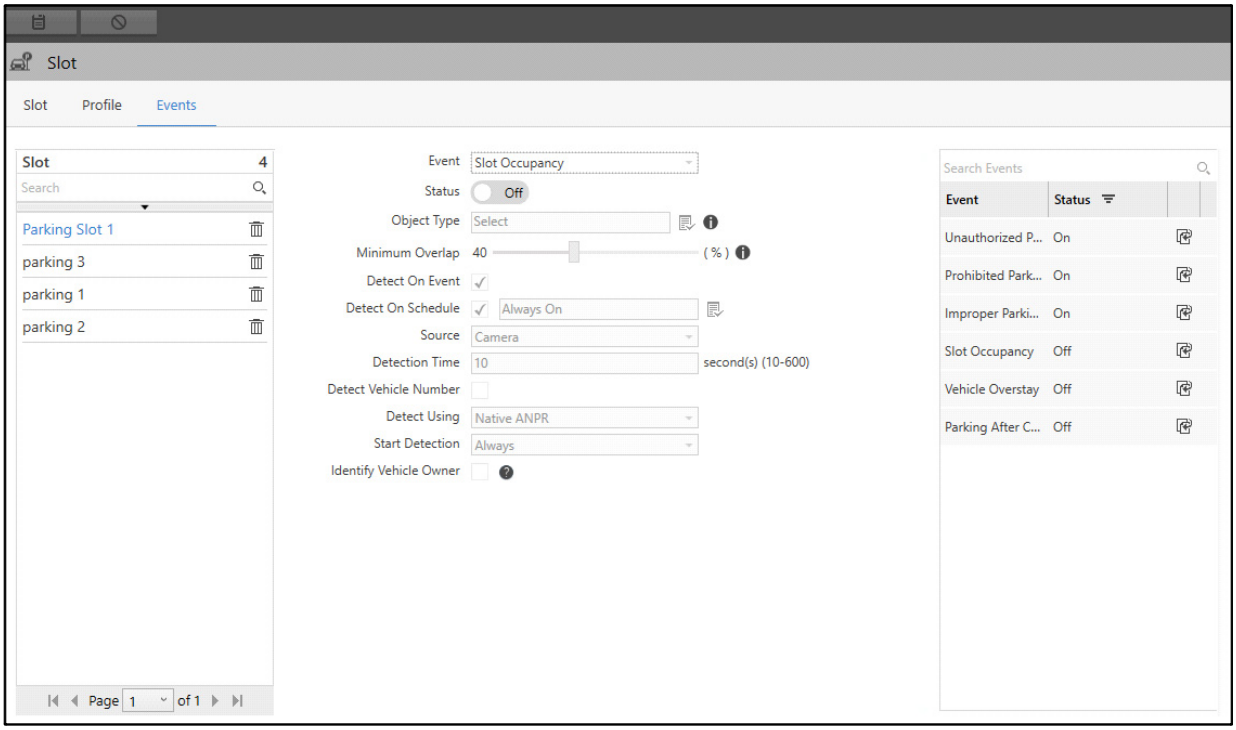
- Click **OK** to confirm or click **Cancel** to discard.

Slot Occupancy

The Slot Occupancy feature enables you to manage a Multilevel Parking facility efficiently. This feature helps you to detect whether the slots are occupied or available for parking. In Admin Client, Slot Occupancy Event can be configured on the basis of Slot Object Size, vehicle number or AUX Input of IO Controller.

To configure Slot Occupancy Event for slots,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

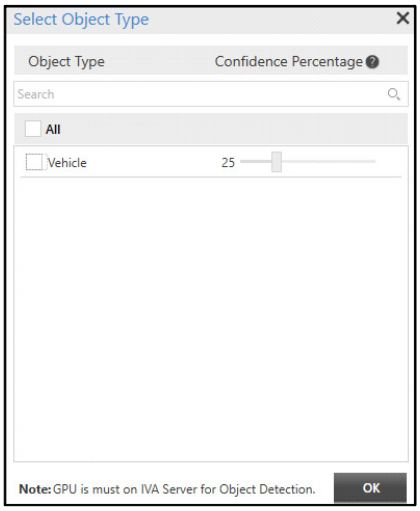


Configure the following parameters:

- **Event:** Select the Slot Occupancy Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

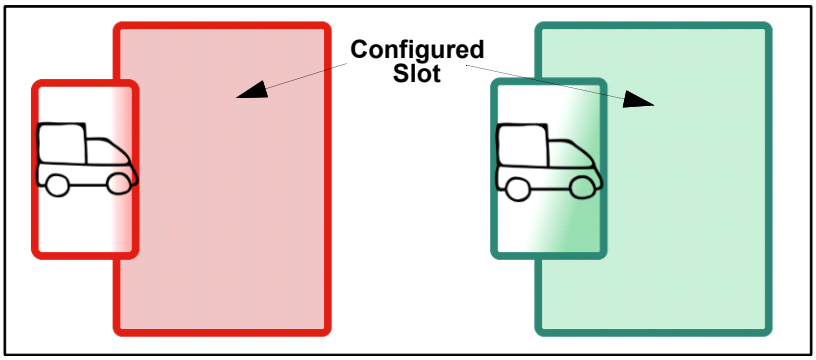


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

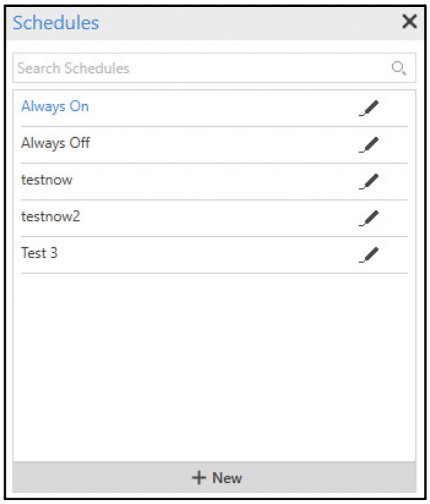
- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the slot to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the slot will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the slot will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Slot, the event will be triggered when 30% of the vehicle is overlapping the configured slot. Whereas, in the Red Slot, the event will not be triggered as, only 10% of the vehicle is overlapping the configured slot.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Source**: Select the source type using which the slot occupancy is to be detected from the drop-down list — Camera, Sensor.

  If Source is selected as Camera, the detection of Slot Occupancy will be based on Slot Object Size or Vehicle Number

  If Source is selected as Sensor, the Occupancy of Slot will be detected based on AUX Input status of IO Controller assigned to a particular slot. Whenever AUX Input is active, **Slot Occupied** Event will be generated for particular slot and for AUX Input Normal, **Slot Available** Event will be generated.

- **Detection Time**: Consider the following conditions to define the Detection Time as per the selected source for the detection of Slot Occupancy Event. Valid Range: 10-600 seconds. Default:10.

  If the Source is selected as a **Camera**, specify the time duration in seconds until which IVA Server will check the change in the given frame. If the same vehicle number is found until the end of the detection time, then IVA Server will ignore that frame and will not generate the Event for the same vehicle number.
  If the Source is selected as a **Sensor**, specify the time duration in seconds until which the Management Server will check for **Sensor Normal** Event once it receives the **Sensor Active** Event.

  If the Sensor gets normal until the end of the detection time, the Management Server will not generate the Event. If the sensor does not get normal after the specified detection time, the **Slot Occupied** Event is generated by MS.

  For example, if the Re-detection time is configured as 60 seconds, once the sensor gets active and MS receives the **Sensor Active** Event, the MS will wait till 60 seconds to check if the sensor gets normal again. If the sensor gets normal, no Event will be generated. Else, **Slot Occupied** Event will be generated by the MS after 60 seconds.

- **Detect Vehicle Number**: Select the check box to enable vehicle detection through License Plate Recognition.

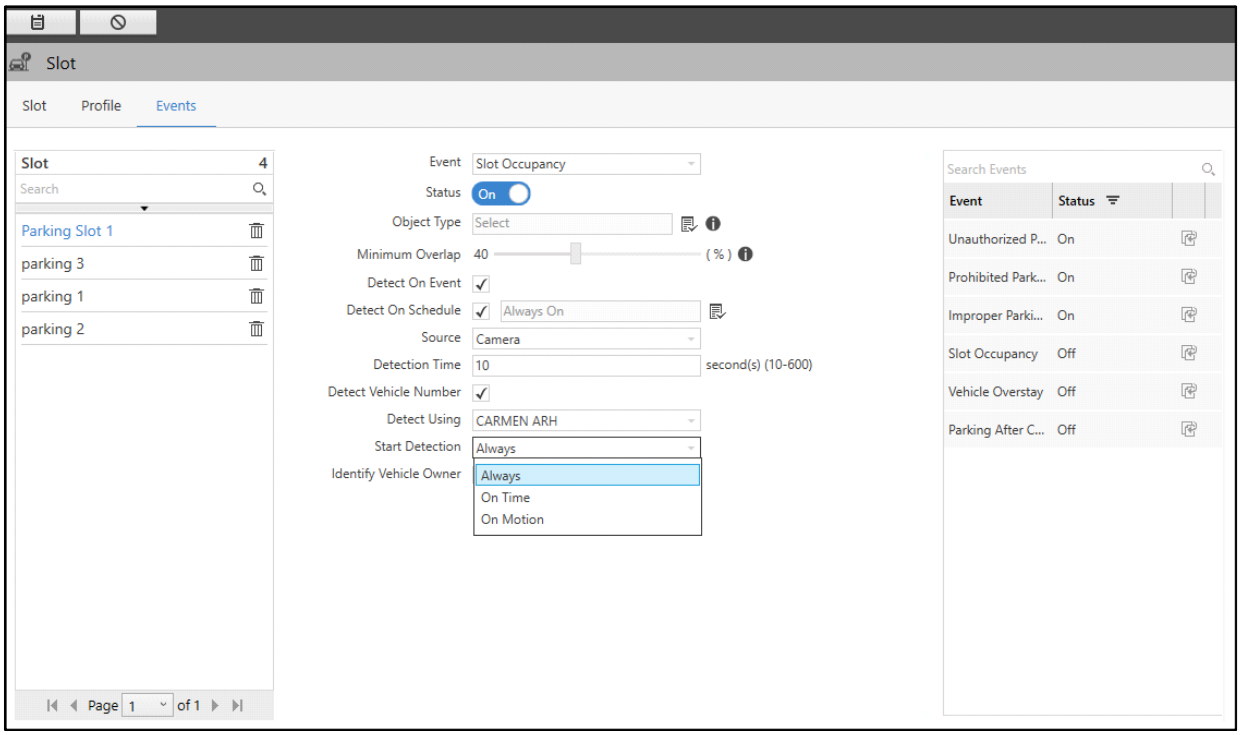
- **Detect Using**: Select the desired detection method from the drop-down list — Native ANPR or CARMEN ARH.

  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Slot Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.

  If you select the detection method as **CARMEN ARH**, configure the following parameters:

- **Start Detection**: Select the desired start detection method from the drop-down list — Always, On Time or On Motion.

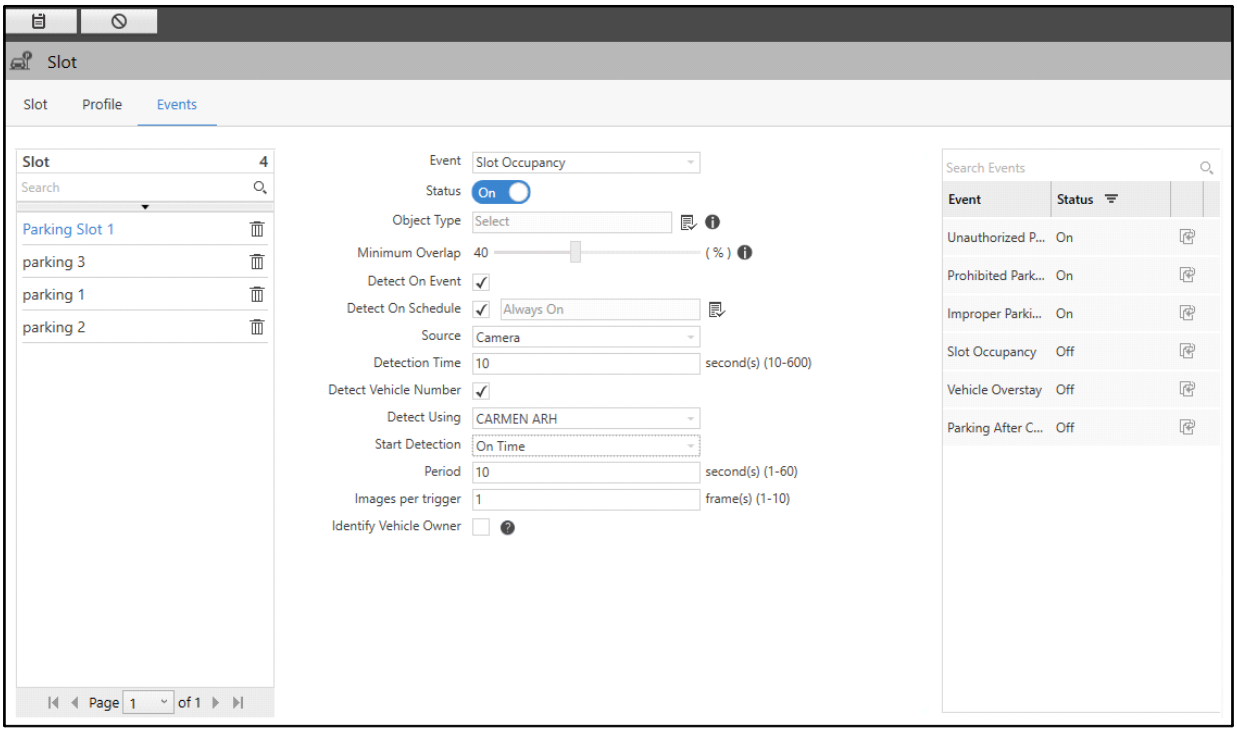


If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images per Trigger is higher than frames received in the configured period, the maximum FPS is sent to ARH. For example, Period = 1 sec and Images per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters:

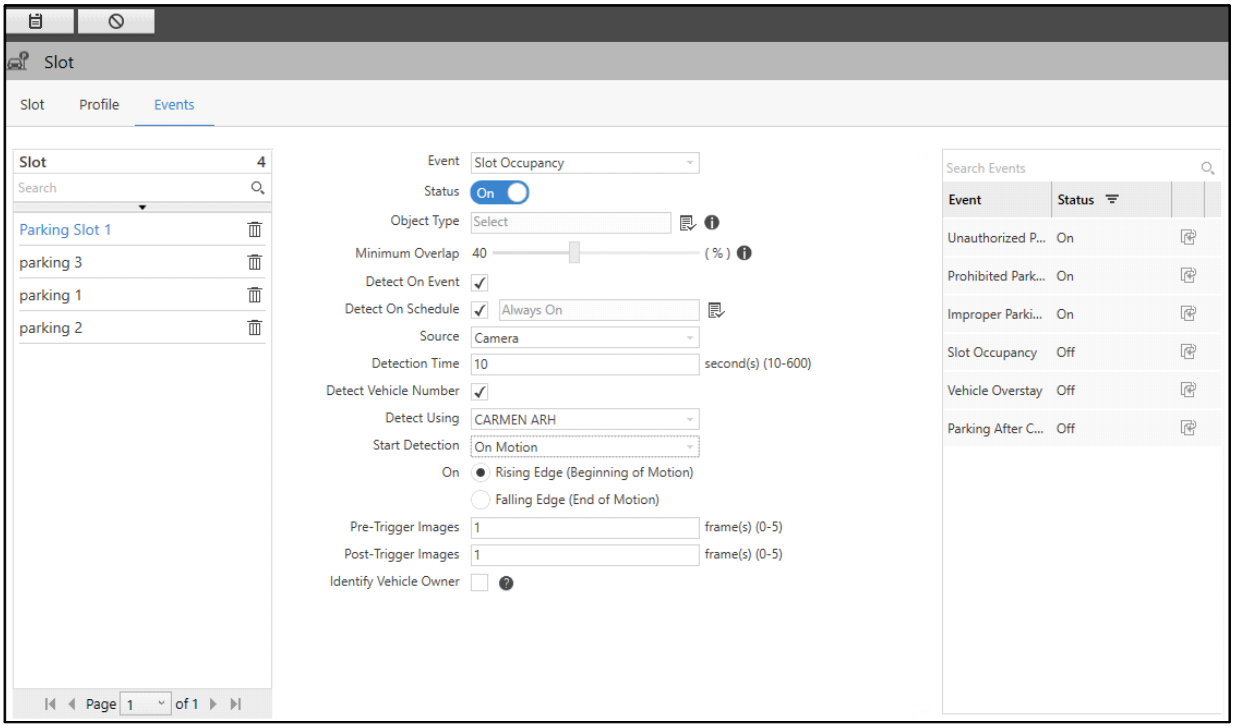
- **Period**: Specify the time interval after which the images will be sent to the ARH Engine. Valid Range:1-60 seconds. Default:10.
- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range: 1-10 frames. Default: 1.



If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as to when you wish the images should be passed to the ARH Engine — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).
- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0-5 frames. Default: 1.
- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion.Valid Range: 0-5 frames. Default: 1.



- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

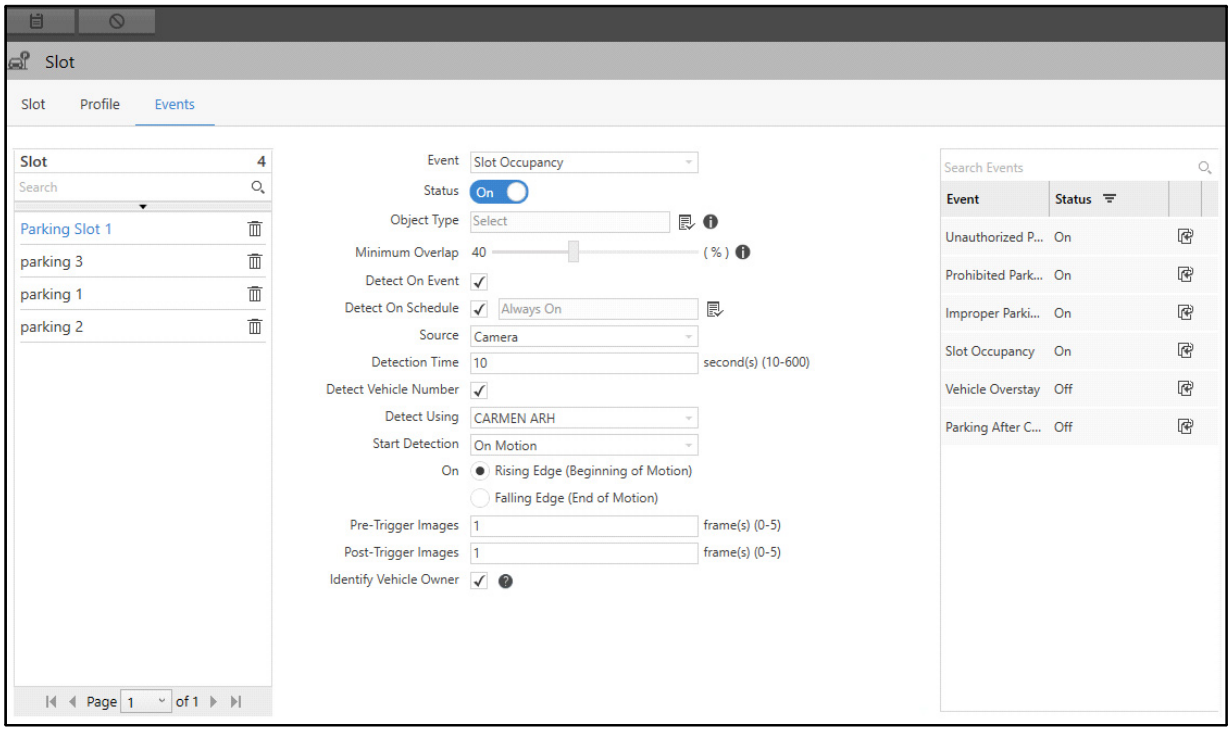
- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Slot Occupancy** pop-up appears.



- Select the desired slots to which you wish to copy these configurations.

- Click **OK** to confirm or click **Cancel** to discard.

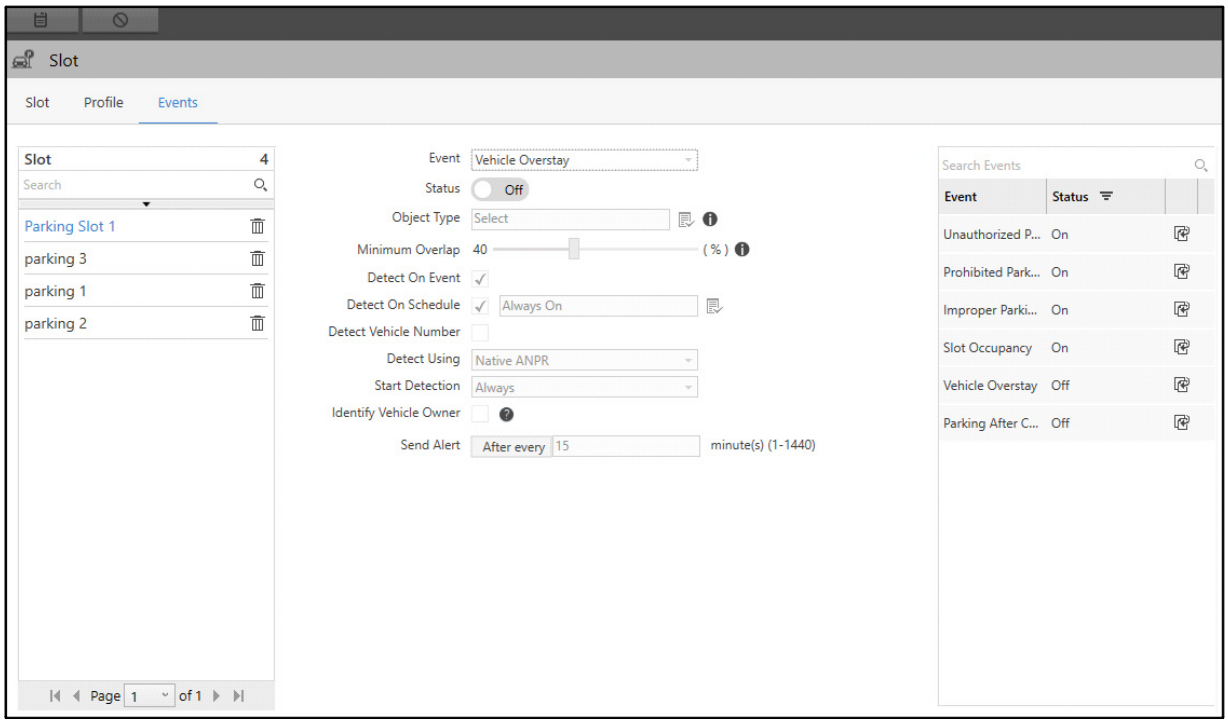
Vehicle Overstay

The Vehicle Overstay feature enables you to get an alert if a vehicle has been parked for more than the duration defined by an organization in the configured slot.

Consider a scenario wherein the organization provides a parking facility for 4 hours between 7 AM to 11 PM. Now, if a person is found to park his/her vehicle for more than the permitted duration, an alert will be sent to the user notifying him/her about the total overstay of the vehicle.

To configure Vehicle Overstay Event for slots,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

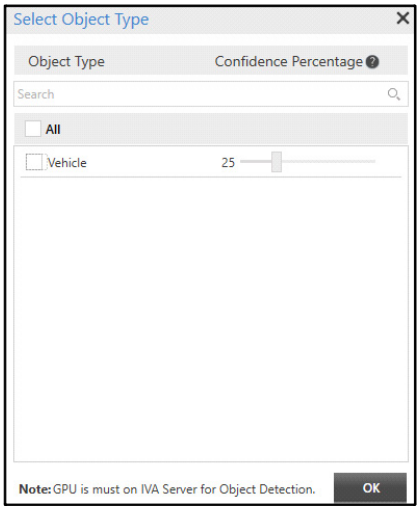


Configure the following parameters:

- **Event:** Select the Vehicle Overstay Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

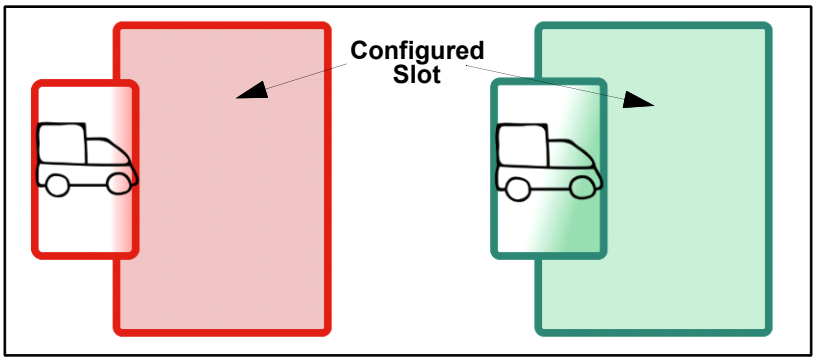


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection.Valid Range: 0-100%. Default: 25. Click **OK**.

- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the slot to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the slot will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the slot will trigger the event. Valid Range: 0-100%. Default: 40.

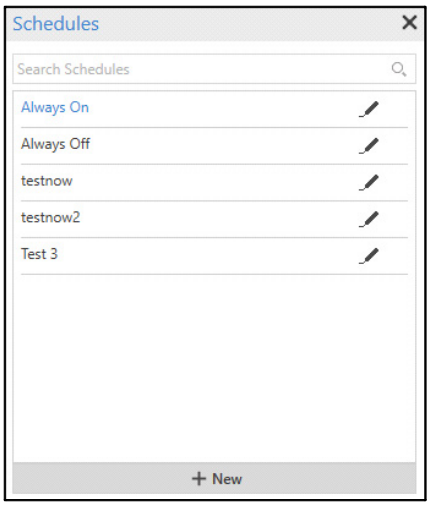
  For example, if you have configured Minimum Overlap as 30%, then as per the Green Slot, the event will be triggered when 30% of the vehicle is overlapping the configured slot as well the time configured for parking exceeds. Whereas, in the Red Slot, the event will not be triggered as, only 10% of the vehicle is overlapping the configured slot even though the time configured for parking exceeds.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of the Event.

- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.

- Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Detect Vehicle Number**: Select the check box to enable vehicle detection through License Plate Recognition.

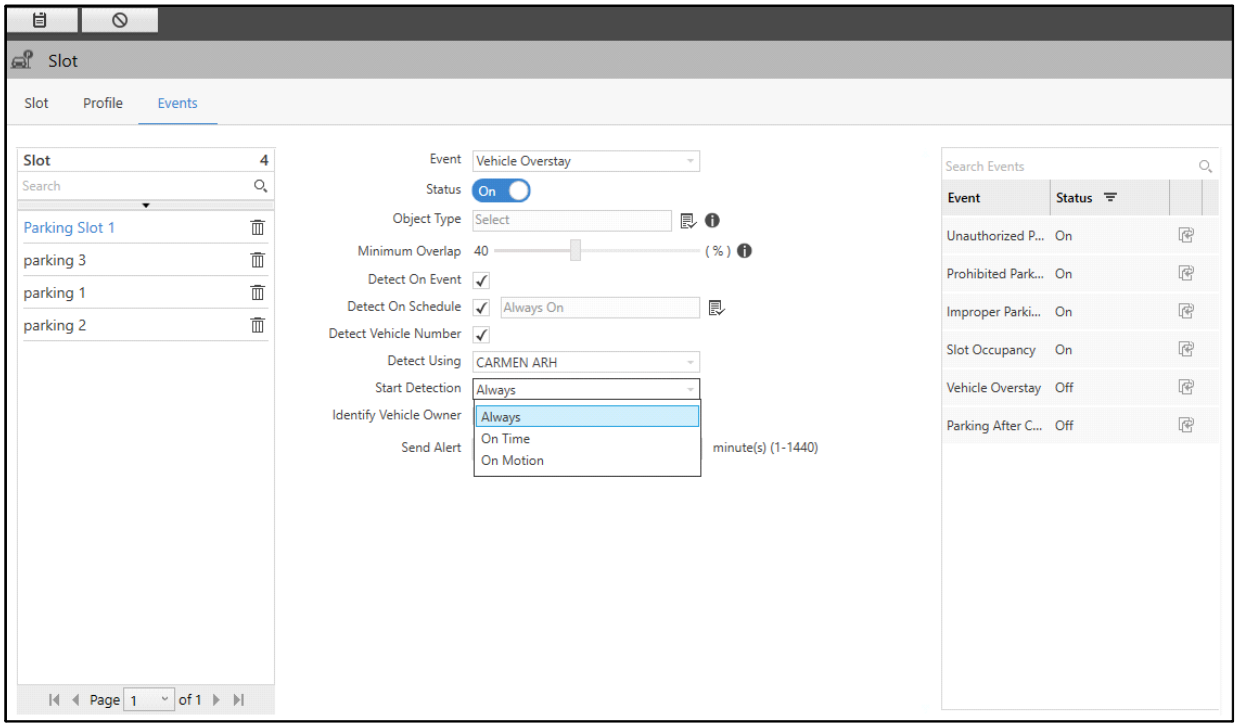
- **Detect Using**: Select the desired detection method from the drop-down list — Native ANPR or CARMEN ARH.

  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Slot Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.

  If you select the detection method as **CARMEN ARH**, configure the following parameters:

- **Start Detection**: Select the desired start detection method from the drop-down list — Always, On Time or On Motion.

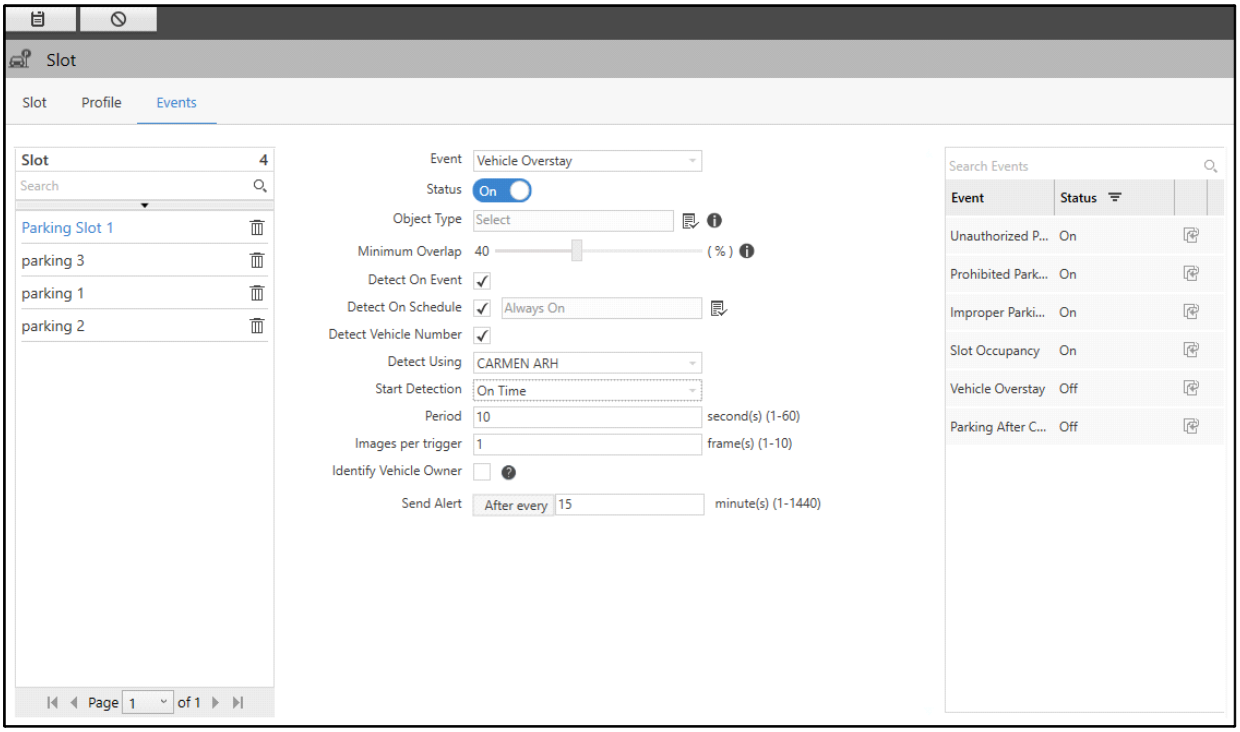


If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images Per trigger is higher than frames received in the configured period, the maximum FPS is sent to ARH. For example, Period = 1 sec and Images per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters:

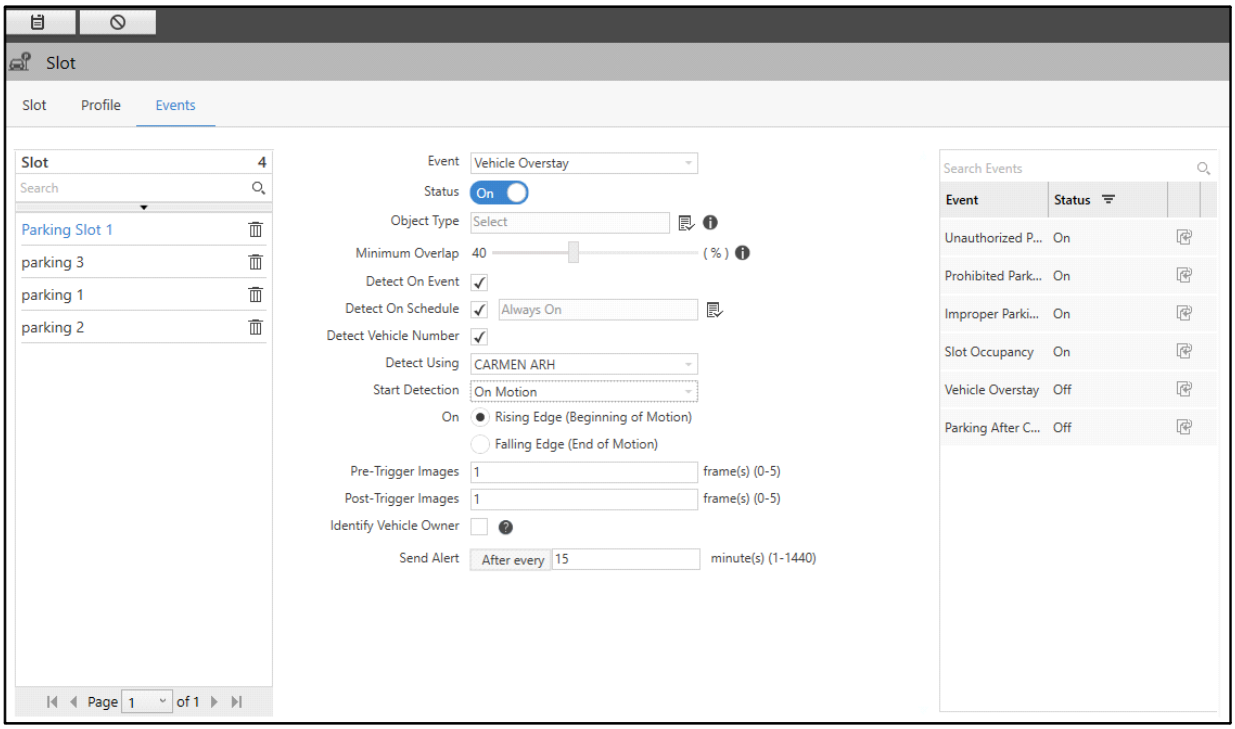
- **Period**: Specify the time interval after which the images will be sent to the ARH Engine. Valid Range:1-60 seconds. Default: 10.
- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range: 1-10 frames. Default: 1.



If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as to when you wish the images should be passed to the ARH Engine from the options — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).
- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0-5 frames. Default: 1.
- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion. Valid Range: 0-5 frames. Default: 1.



- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

- **Send Alert**: Specify the time interval after which alerts will be sent. Valid Range: 1-1440 minutes. Default: 15.

  If send alert time is configured as 15 seconds, the IVA Server will check if there is a change in the license plate or not. If the same license plate is recognized after the end of the permitted duration, the IVA Server will generate an alert after every 15 seconds until the same license plate is recognized.

- Click **Save** to save the settings or **Cancel** to discard.

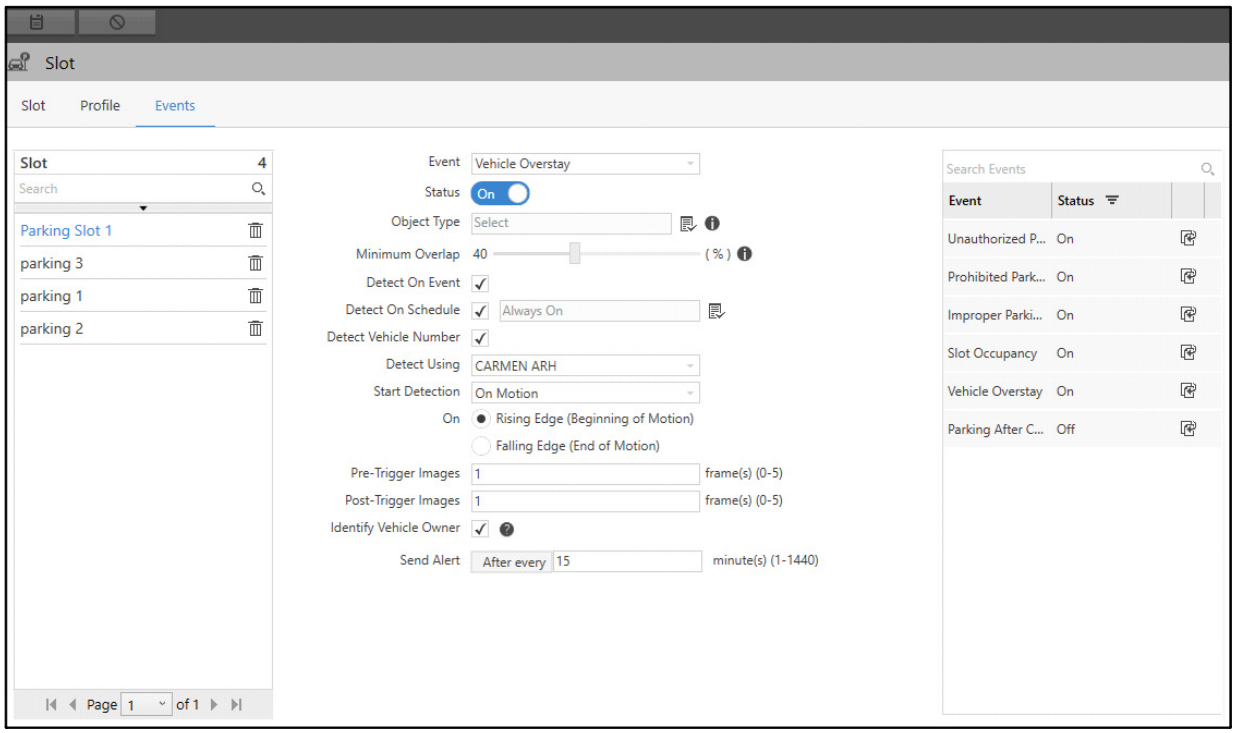
Once you have configured the Event, you can edit its configurations or disable it.

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

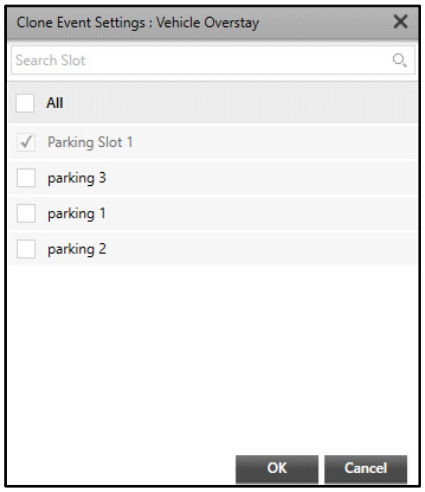
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Vehicle Overstay** pop-up appears.



- Select the desired slots to which you wish to copy the Event configurations.

- Click **OK** to confirm or click **Cancel** to discard.

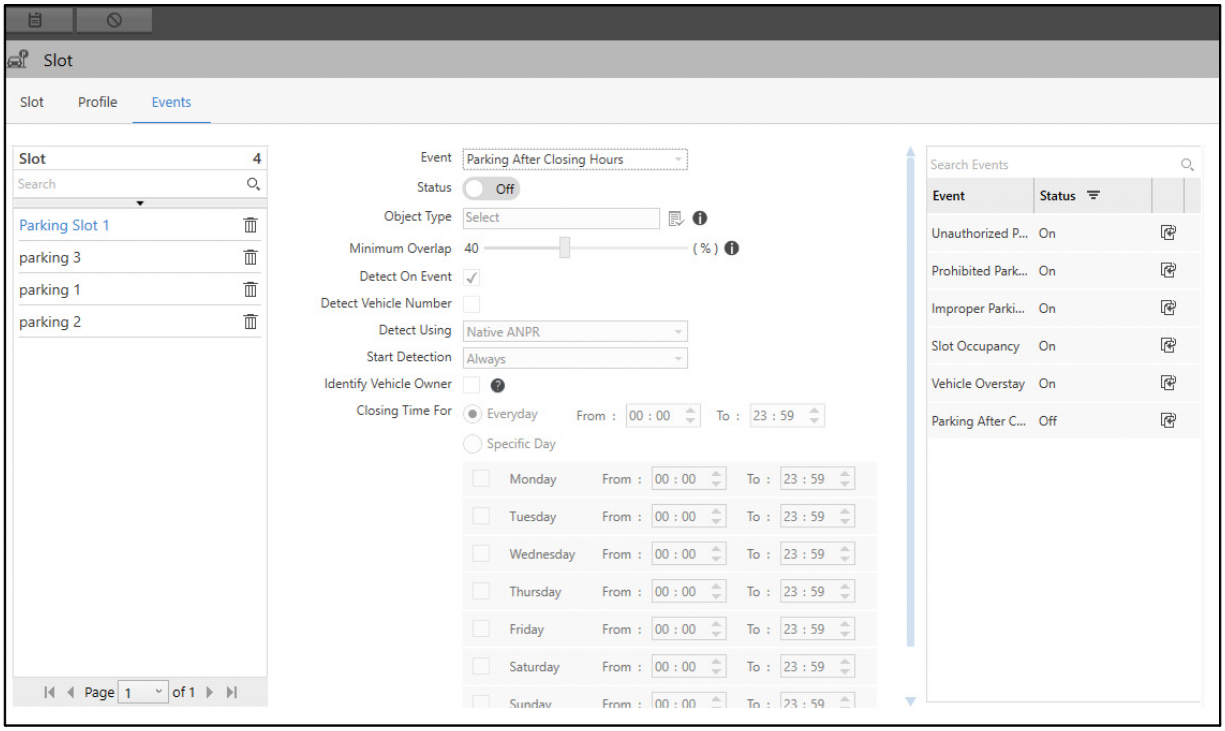
Parking After Closing Hours

The Parking After Closing Hours feature enables you to get an alert if a vehicle is parked in the premises after the parking hours are closed.

Consider a scenario wherein the organization provides a parking facility from 7 AM to 11 PM. Now, if any vehicle is found in the premises after the closing hours, the vehicle owner will get an alert to move the vehicle out of the parking premises.

To configure Parking After Closing Hours Event for slots,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

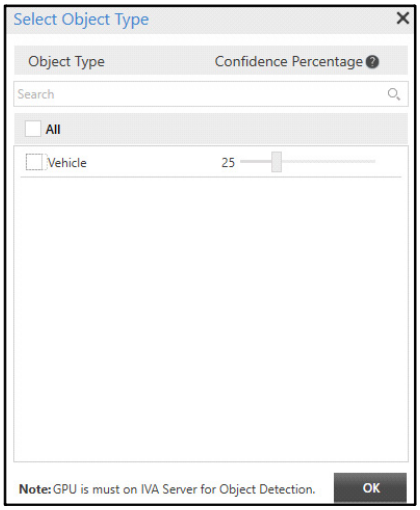


Configure the following parameters:

- **Event:** Select the Parking After Closing Hours Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

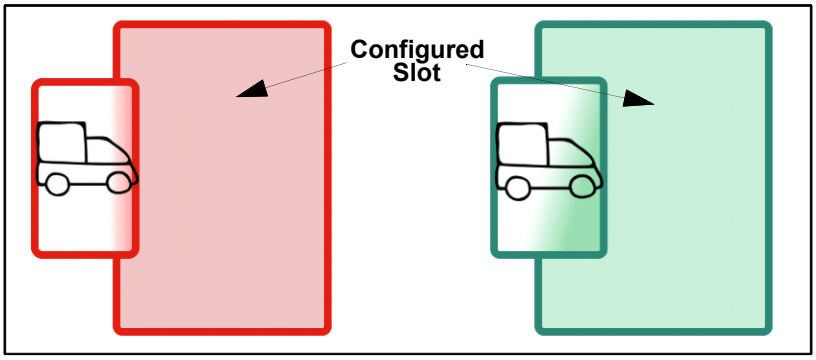


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100% Default: 25. Click **OK**.

- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the slot to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the slot will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the slot will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Slot, the event will be triggered when 30% of the vehicle is overlapping the configured slot as well the time configured for parking exceeds. Whereas, in the Red Slot, the event will not be triggered as, only 10% of the vehicle is overlapping the configured slot even though the time configured for parking exceeds.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.

- **Detect Vehicle Number**: Select the check box to enable vehicle detection through License Plate Recognition.

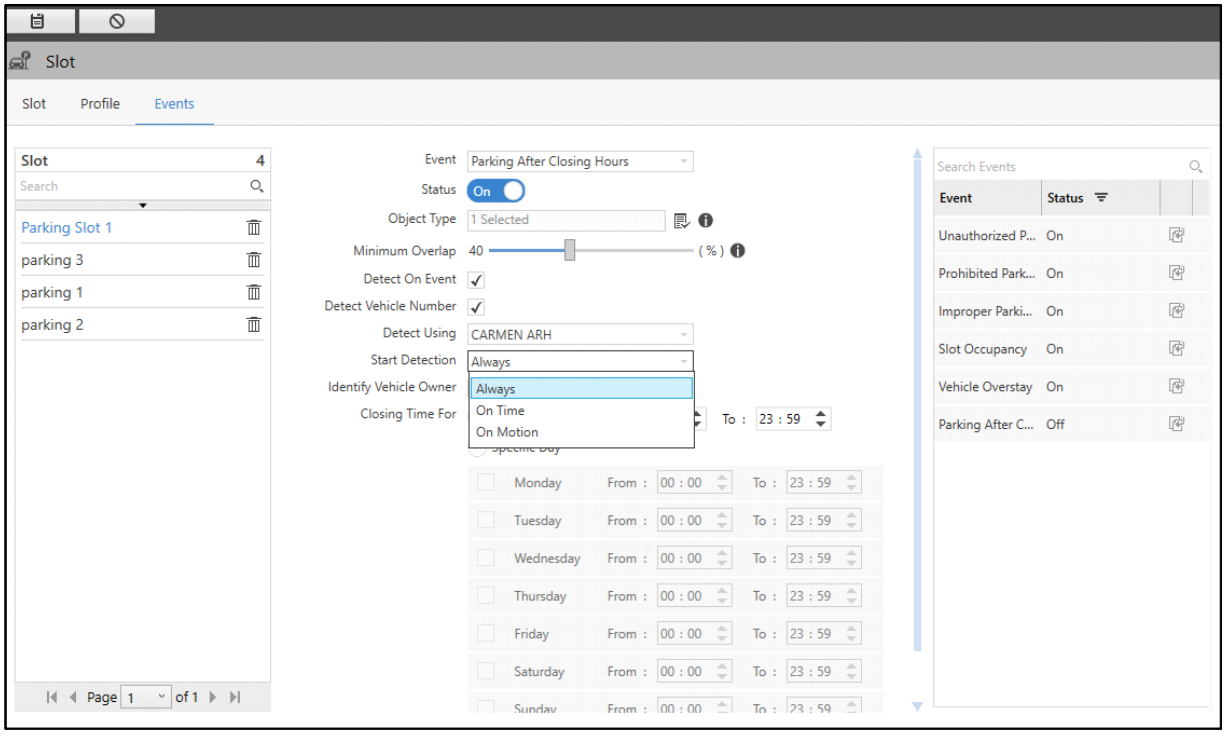
- **Detect Using**: Select the desired detection method from the drop-down list — Native ANPR or CARMEN ARH.

  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Slot Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.

  If you select the detection method as **CARMEN ARH**, configure the following parameters:

- **Start Detection**: Select the desired start detection method from the drop-down list — Always, On Time or On Motion.



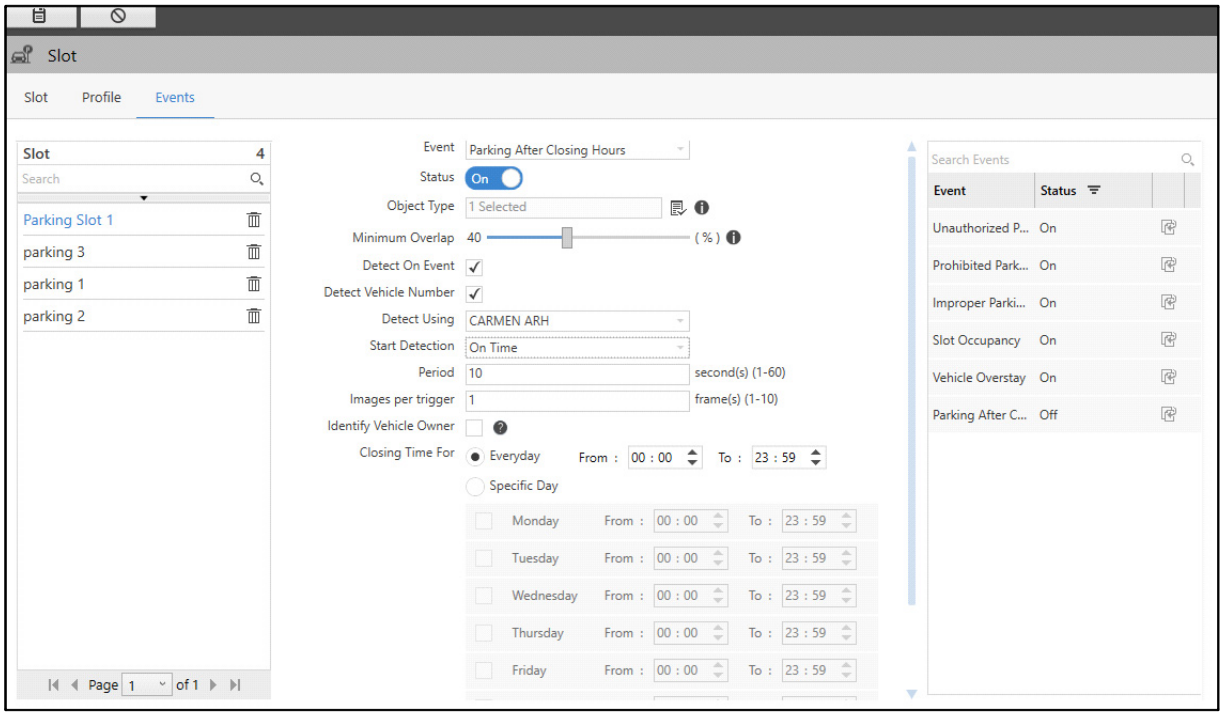
If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images per Trigger is higher than frames received in the configured period, the maximum FPS is sent to ARH. For example, Period = 1 sec and Images per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters:

- **Period**: Specify the time interval after which the images will be sent to the ARH Engine. Valid Range:1-60 seconds. Default:10.

- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range: 1-10 frames. Default:1.



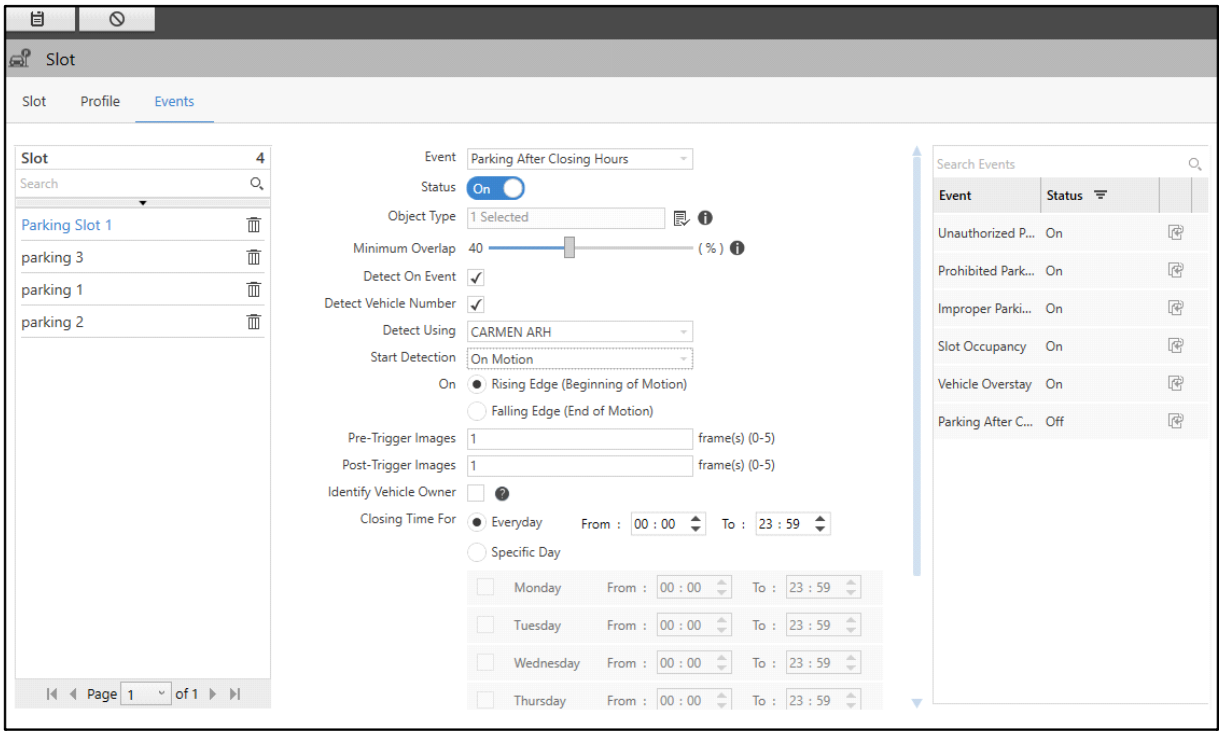
If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as to when you wish the images should be passed to the ARH Engine — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0-5 frames. Default:1.

- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion.Valid Range: 0-5 frames. Default:1.



- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

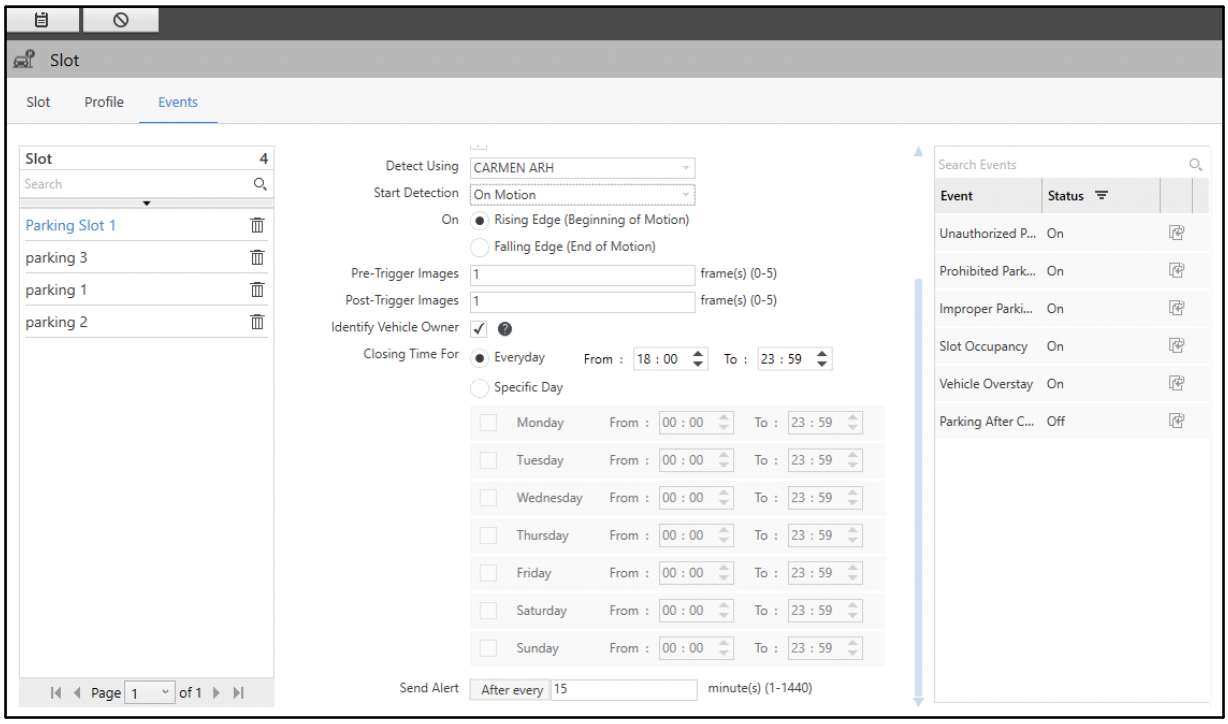
- **Closing Time For**: Set the closing time for parking by selecting the desired options — Everyday or Specific Day.

  If you select **Everyday**, set the Closing **From** time and Closing **To** time for parking.

  If you select **Specific Day**, select the check boxes for the days on which you wish to set the closing hours and set the Closing **From** time and Closing **To** time.

  The time duration will include the **From** time but not the **To** time. For example, if you wish to set Closing Hours from 18:00 to 06:00 on Monday, then you need to:

  - select **Monday** check box and set the **From** time as 18:00 and **To** time as 06:01.



- **Send Alert**: Specify the time interval after which alerts will be sent. Valid Range: 1-1440 minutes. Default:15.

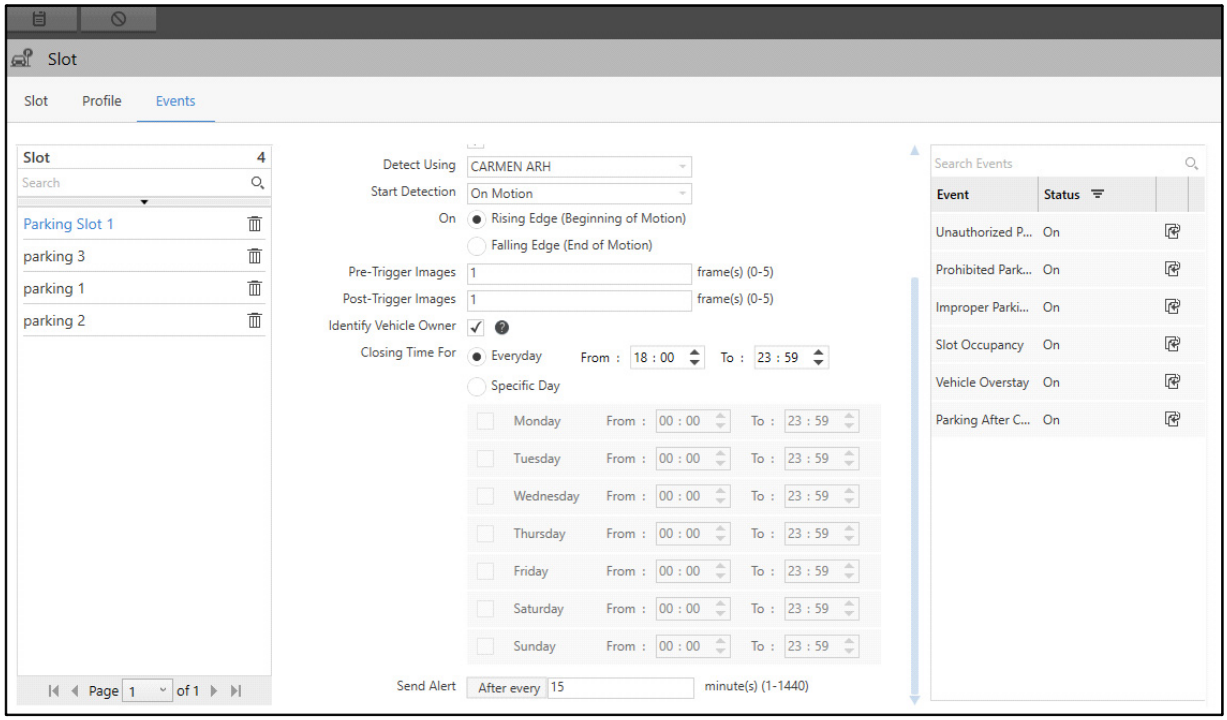
  If send alert time is configured as 1 minute, the IVA Server will check if there is a change in the license plate or not, that is, whether the vehicle is present or not. If the same license plate is recognized after the end of the permitted duration, the IVA Server will generate an alert after every 1 minute until the same license plate is recognized.

Once you have configured the Event, you can edit its configurations or disable it.

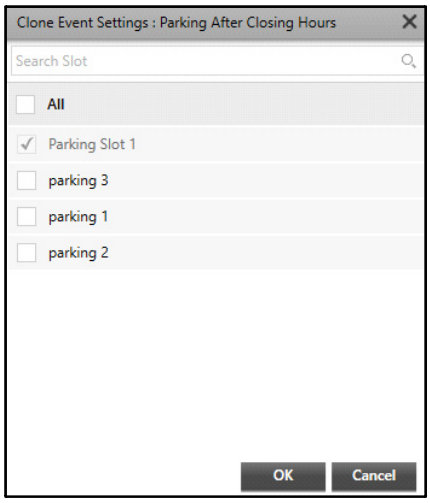
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Parking After Closing Hours** pop-up appears.



- Select the desired slots to which you wish to copy these configurations.

- Click **OK** to confirm or click **Cancel** to discard.

Slot Group

Slot is the first level of the Multilevel Parking configuration, where the parking area is divided into the multiple defined slots. Multiple slots are grouped together to form various **Slot Groups**.



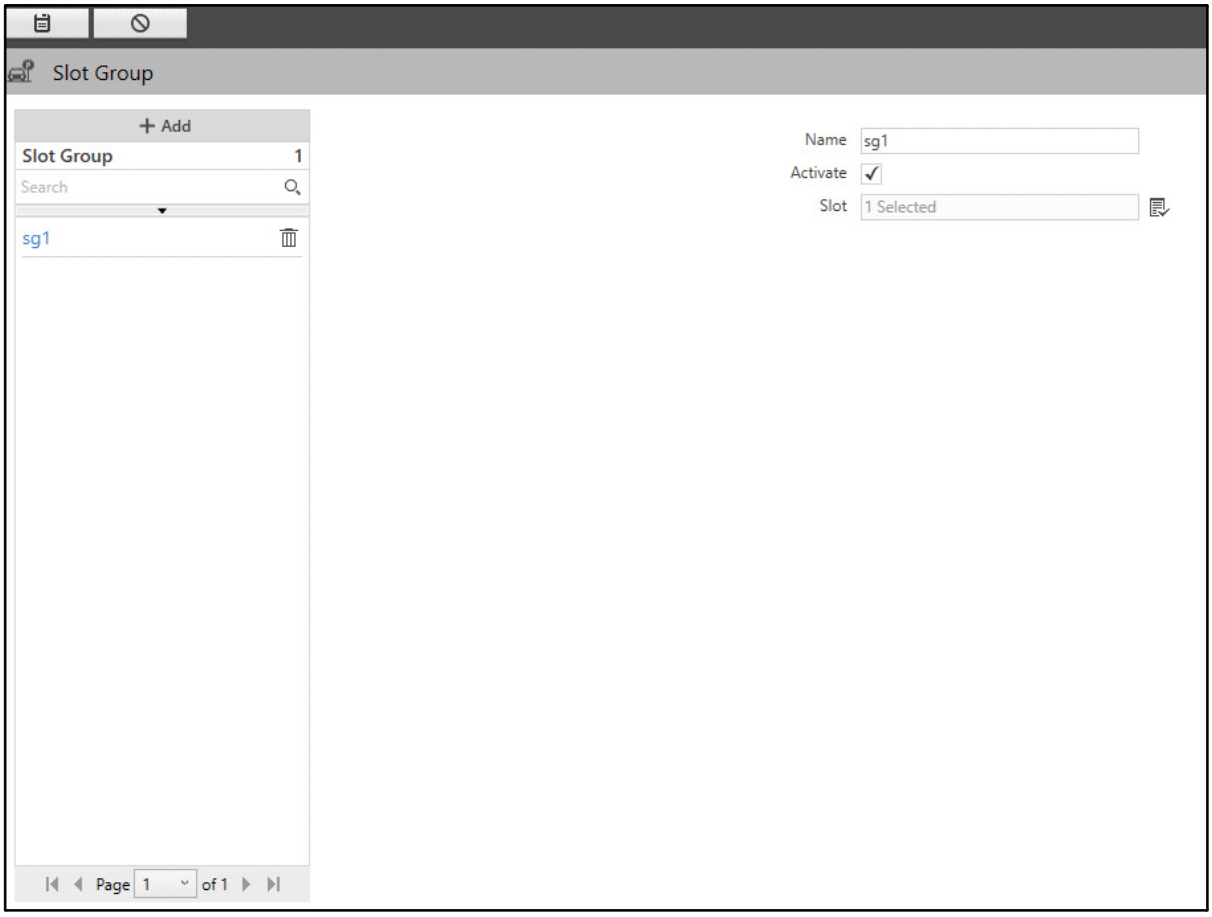
Multiple Slot Groups can also be formed by combining different slots.



The Slot Group page displays all the configured Slot Groups. You can view and configure the Slot Groups from this page.

To configure Slot Groups,

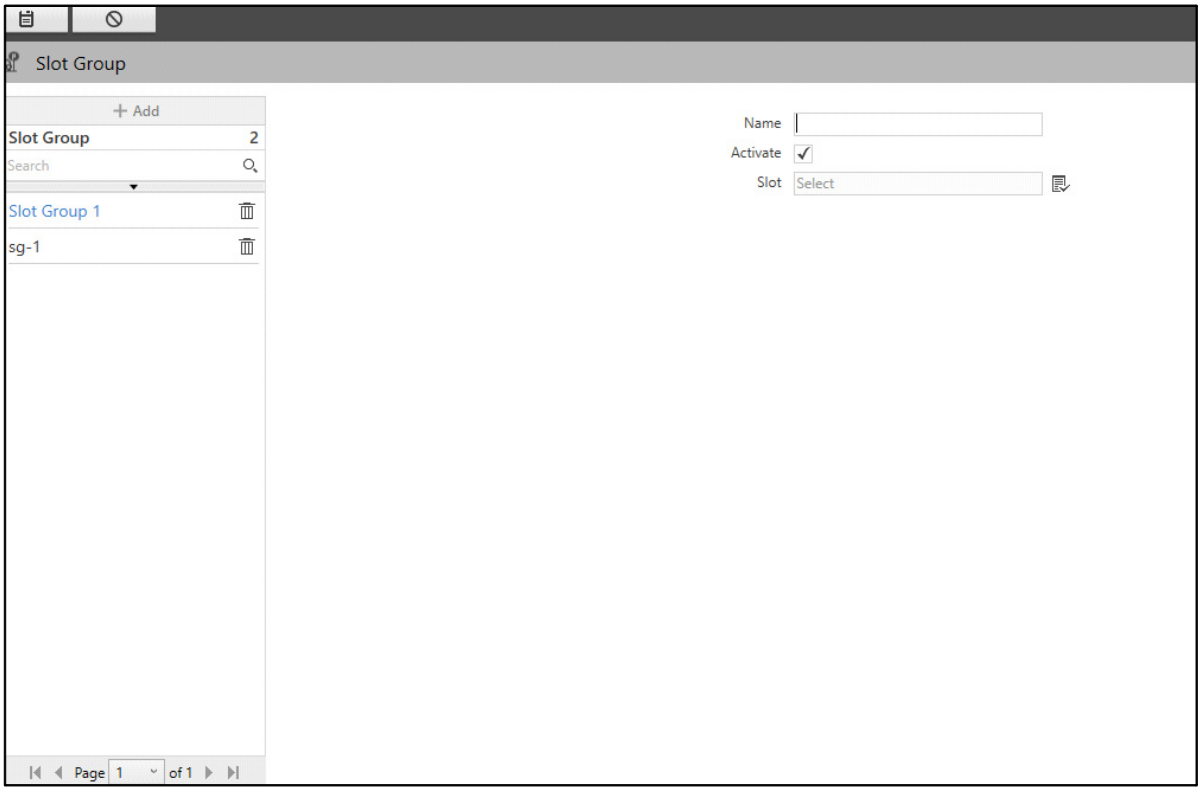
- Click **Parking Management > Multilevel Parking > Slot Group**.



The entity name (Slot Group) can also be changed from the Rename Entity section, for more details, Refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

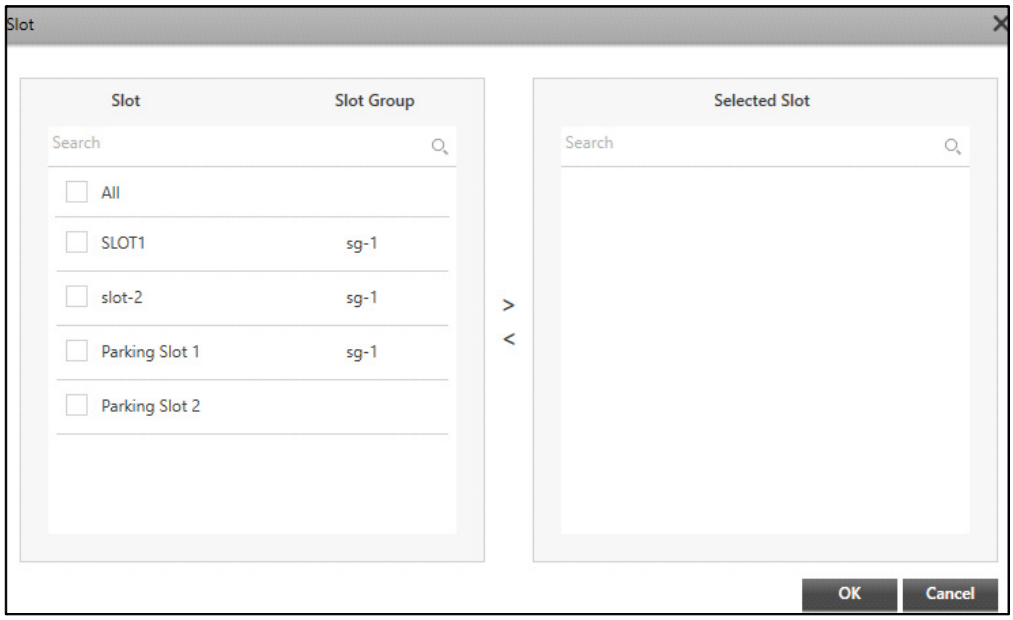
*The **Add** button is disabled when you are configuring Slot Group for the first time. You can directly configure the parameters and save the Slot Group.*

- Click **Add**.



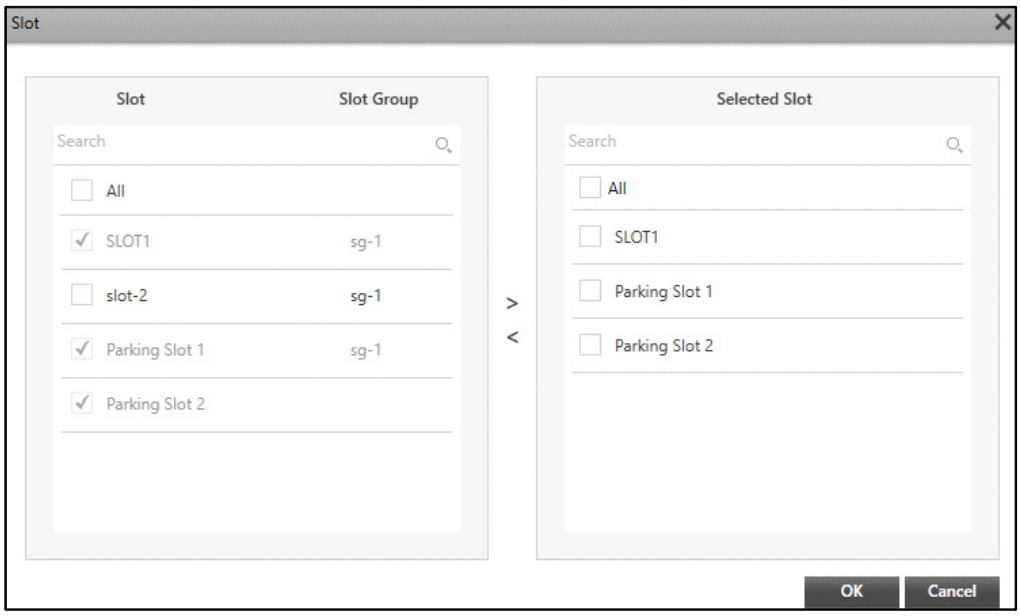
Configure the following parameters:

- **Name:** Specify a suitable name for the Slot Group. In Name, you can enter upto 50 characters. Default: Blank.
- **Activate**: Select the check box to enable the Slot Group.
- **Slot:** Select the desired slots which you wish to assign to the Slot Group using the **Select Slot** picklist.
  - Click **Select Slot** picklist. The **Slot** pop-up appears.



- All the configured slots appear in the list. To configure slots, refer to "Slot". The Slot Group to which the slots belong to is indicated next to the slots. Select the check boxes of the desired slots you wish to select from the list. Click the right arrow button to add those slots in the **Selected Slot** list. You can also search for the desired slots using the search bar.

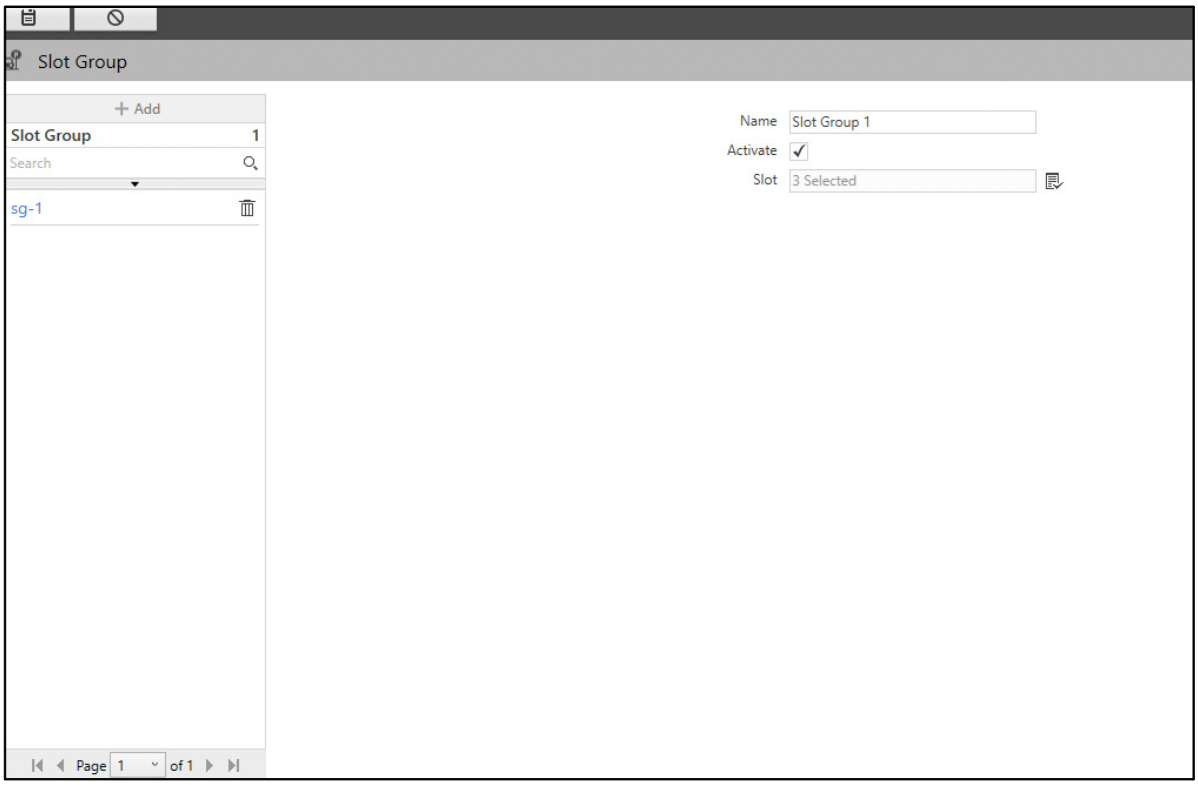
  To remove slots, select the check boxes of the desired slots you wish to remove from the Selected Slot list. Click the left arrow button to remove the slots from the Selected Slot list.



- Click **OK** to confirm or click **Cancel** to discard. The number of slots added to the group appear in **Slot**.

  The Slot Group will appear in the list on the left hand side.

  You can edit the configurations of the Slot Group or delete it.



- Select the desired Slot Group from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Slot Group.

Lane

Lane is the next level of the Multilevel Parking configuration, where multiple Slot Groups are combined together to form a **Lane.**



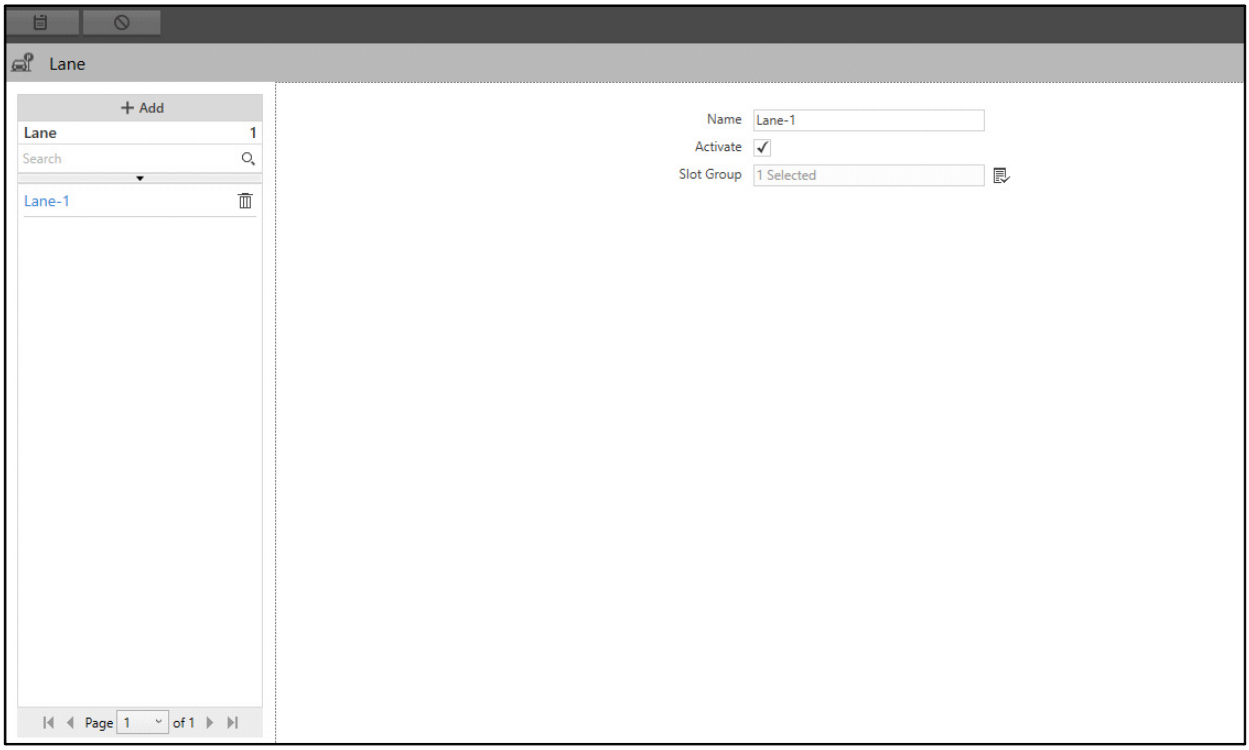
Multiple Lanes can also be formed by combining different Slot Groups.



The Lane page displays all the configured Lanes. You can view and configure the Lanes from this page.

To configure Lanes,

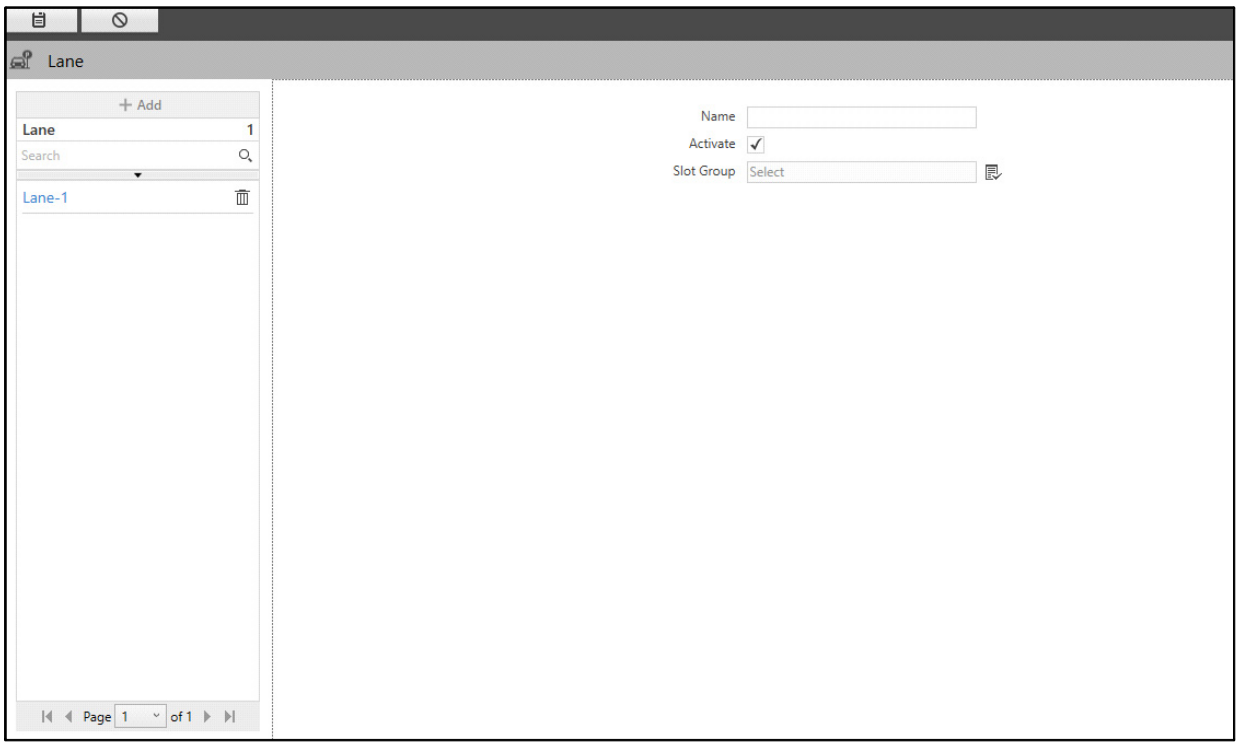
- Click **Parking Management > Multilevel Parking > Lane**.



The entity name (Lane) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

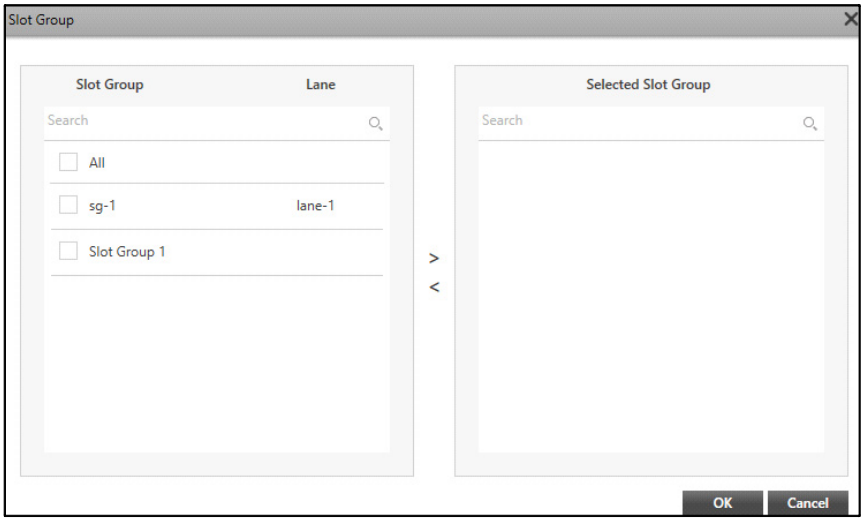
*The **Add** button is disabled when you are configuring lane for the first time. You can directly configure the parameters and save the lane.*

- Click **Add**.



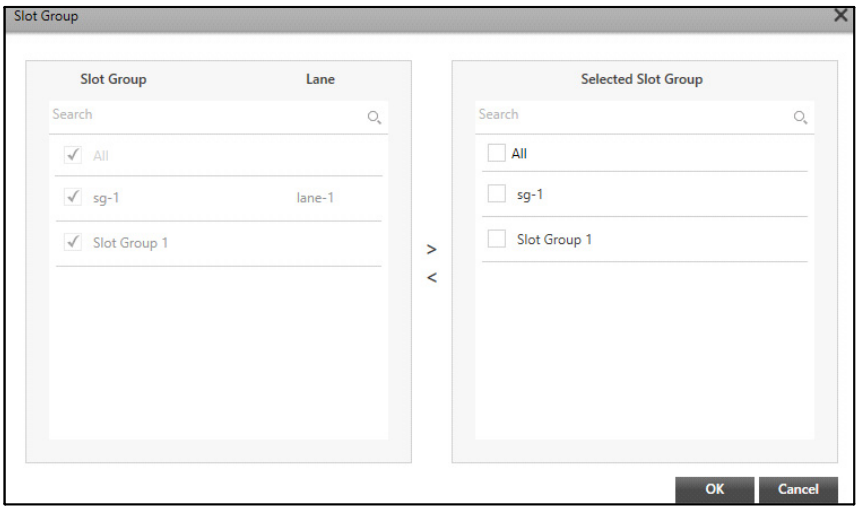
Configure the following parameters:

- **Name:** Specify a suitable name for the Lane.In Name, you can enter upto 50 characters. Default: Blank.
- **Activate**: Select the check box to enable the Lane.
- **Slot Group:** Select the desired Slot Groups which you wish to assign to the Lane using the **Select Slot Group** picklist.
    - Click **Select Slot Group** picklist. The **Slot Group** pop-up appears.



- All the configured Slot Groups appear in the list. To configure Slot Groups, refer to "Slot Group". The Lanes to which the Slot Groups belong to is indicated next to the Slot Groups. Select the check boxes for the desired Slot Groups you wish to select from the list. Click the right arrow button to add those Slot Groups in the **Selected Slot Group** list. You can also search for the desired Slot Groups using the search bar.

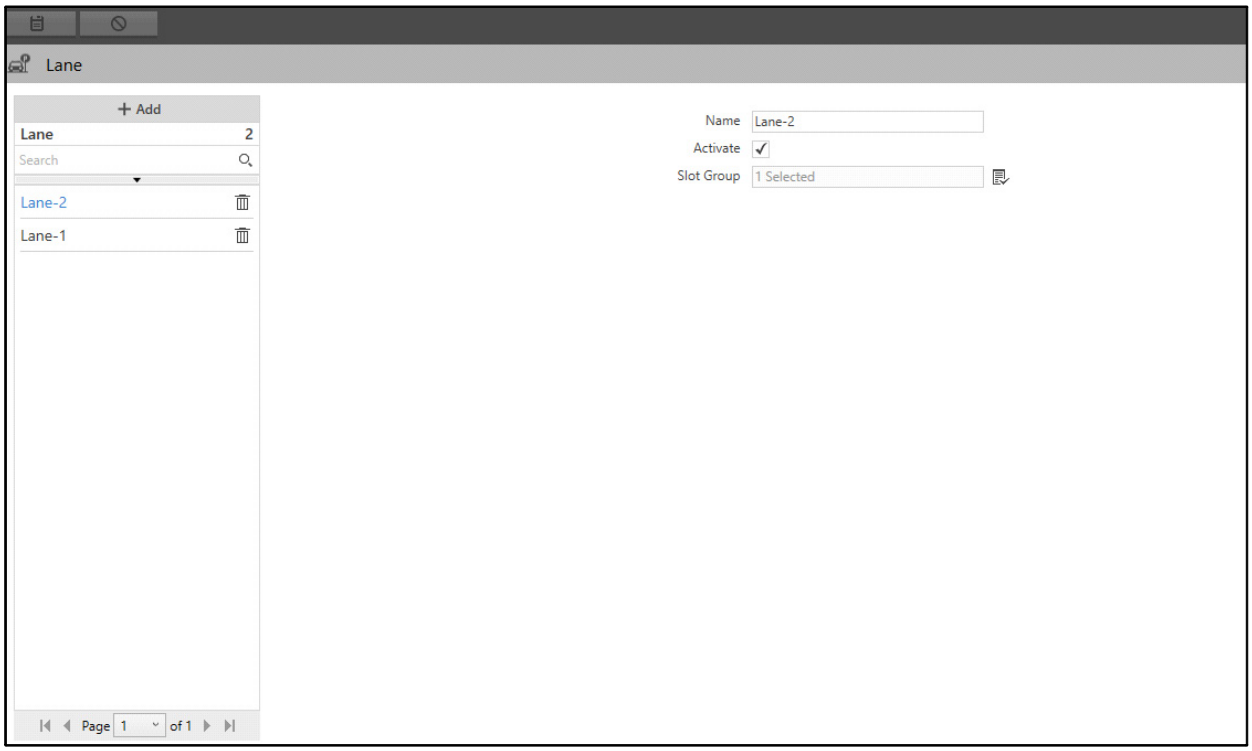
  To remove Slot Groups, select the desired check boxes for the Slot Groups you wish to remove from the Selected Slot Group list. Click the left arrow button to remove the Slot Groups from the Selected Slot Group list.



- Click **OK** to confirm or click **Cancel** to discard. The number of Slot Groups added to the Lane appear in **Slot Group**.

  The Lane will appear in the list on the left hand side.

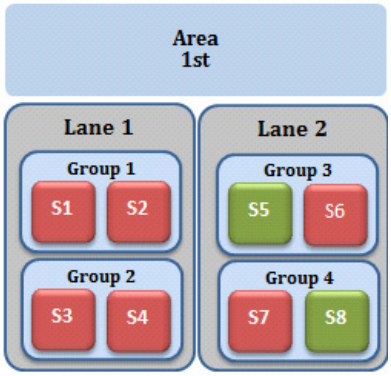
  You can edit the configurations of the Lane or delete it.



- Select the desired Lane from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Lane.

Area

Area is the second level of the Multilevel Parking configuration, where multiple Lanes are combined together to form an **Area.**



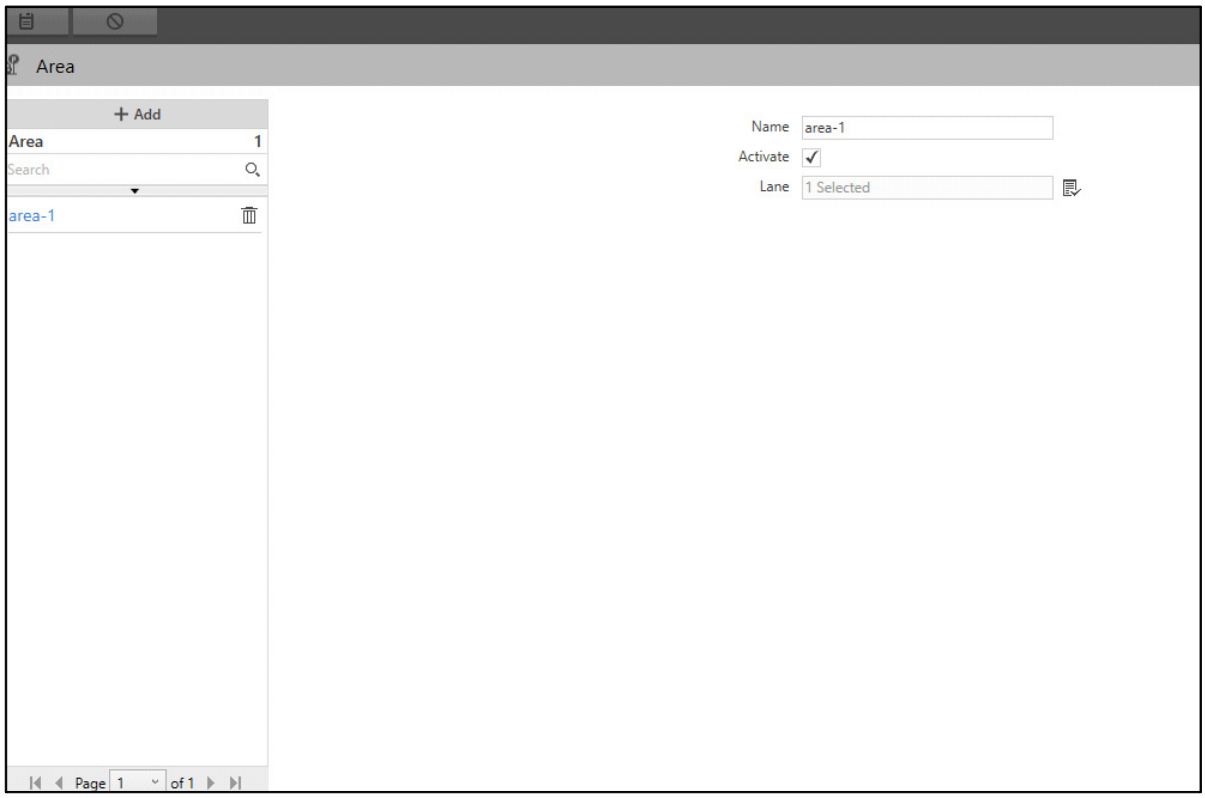
Multiple Areas can also be formed by combining different Lanes.



The Area page displays all the configured Areas. You can view and configure the Areas from this page.

To configure Areas,

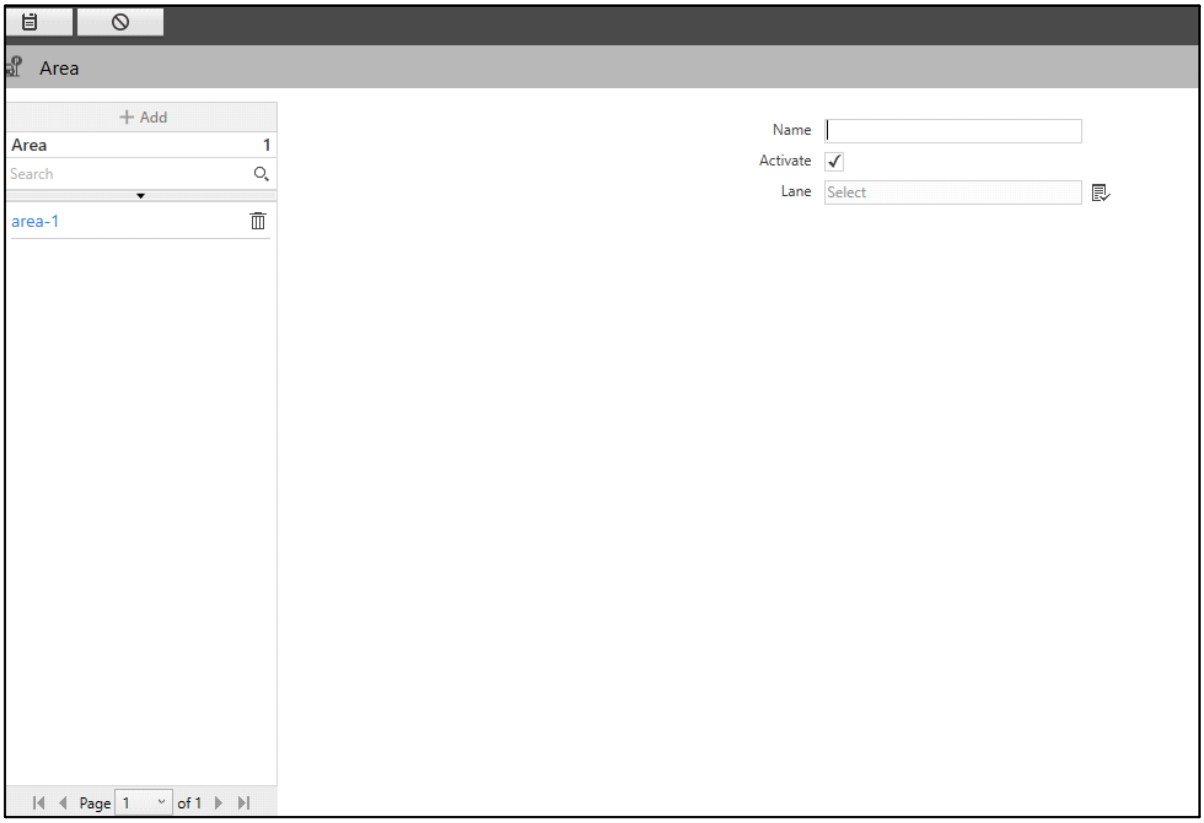
- Click **Parking Management > Multilevel Parking > Area**.



The entity name (Area) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

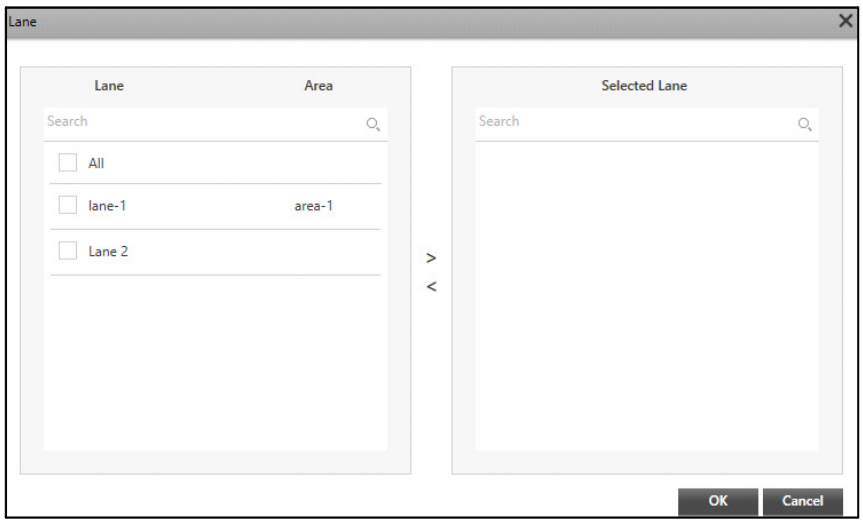
*The **Add** button is disabled when you are configuring Area for the first time. You can directly configure the parameters and save the Area.*

- Click **Add**.



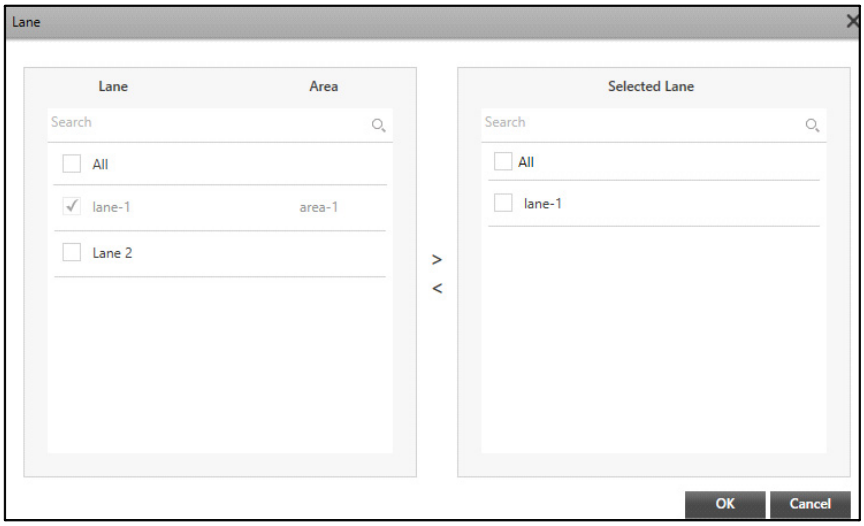
Configure the following parameters:

- **Name:** Specify a suitable name for the Area. In Name, you can enter upto 50 characters. Default: Blank.
- **Activate**: Select the check box to enable the Area.
- **Lane:** Select the desired Lanes which you wish to assign to the Area using the **Select Lane** picklist.
    - Click **Select Lane** picklist. The **Lane** pop-up appears.



- All the configured Lanes appear in the list. To configure Lanes, refer to “Lane”. The Areas to which the Lanes belong to is indicated next to the Lanes. Select the check boxes of the desired Lanes you wish to select from the list. Click the right arrow button to add those Lanes in the **Selected Lane** list. You can also search for the desired Lanes using the search bar.

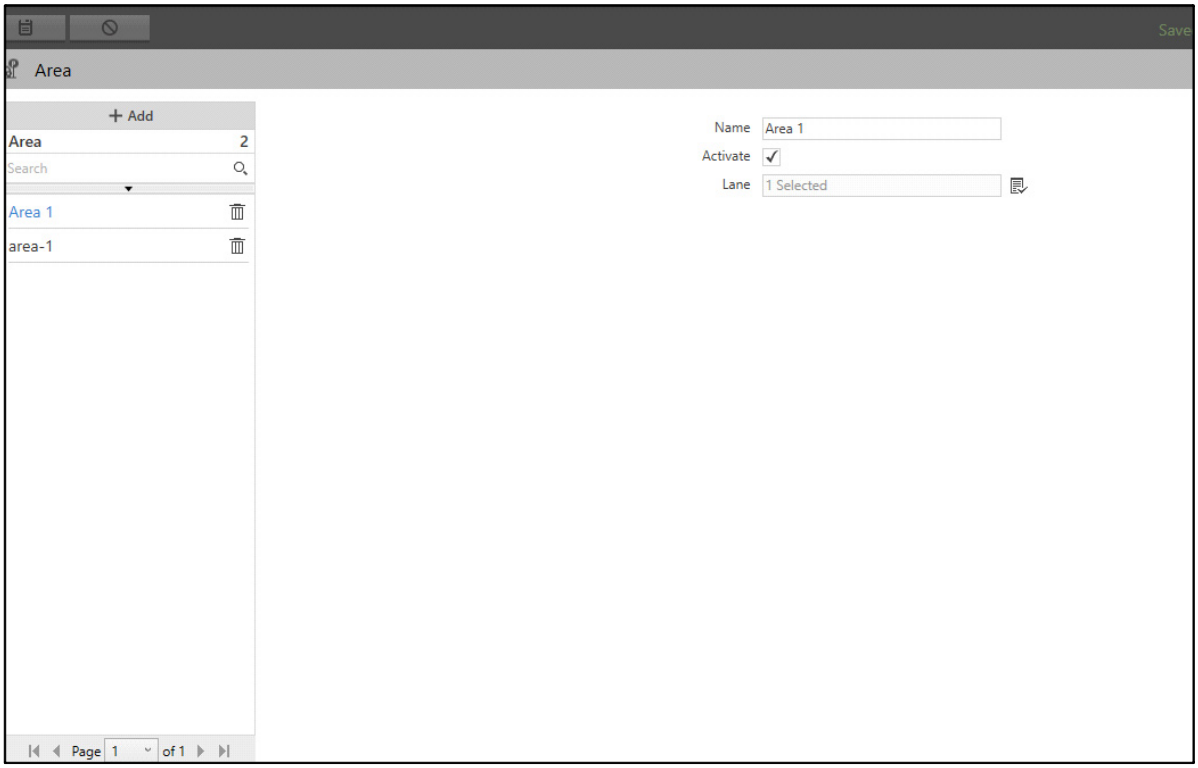
  To remove Lanes, select the check boxes of the desired Lanes you wish to remove from the Selected Lane list. Click the left arrow button to remove the Lanes from the Selected Lane list.



- Click **OK** to confirm or click **Cancel** to discard.

  The number of Lanes added to the Area appear in **Lane**.

  You can edit the configurations of the Area or delete it.



- Select the desired Area from the list and edit the configurations on the right hand side.
- Click **Save**  to save the settings or **Cancel**  to discard.
- Click **Delete**  to delete the desired Area.

Level

Level is the third level of the Multilevel Parking configuration, where multiple Areas are combined together to form a Level.

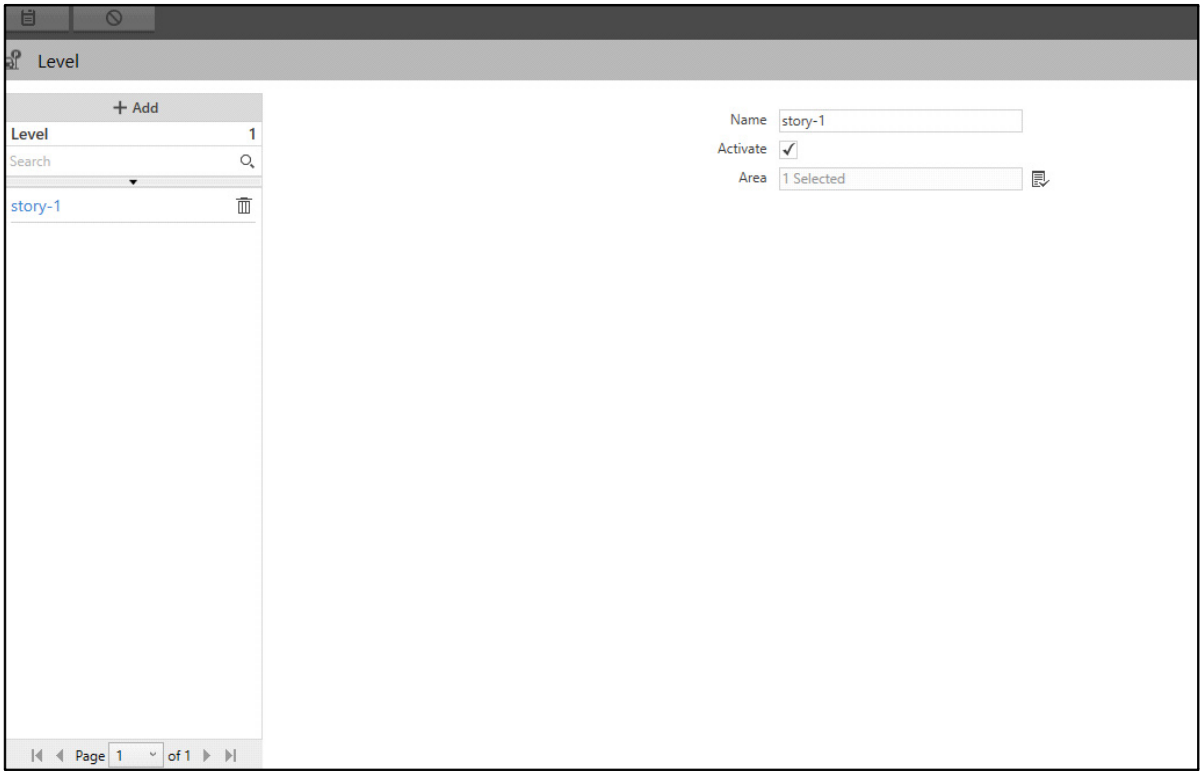
For example, multiple regions of Areas can be grouped to form a Floor of the Multilevel Parking.



The Level page displays all the configured Levels. You can view and configure the Levels from this page.

To configure Levels,

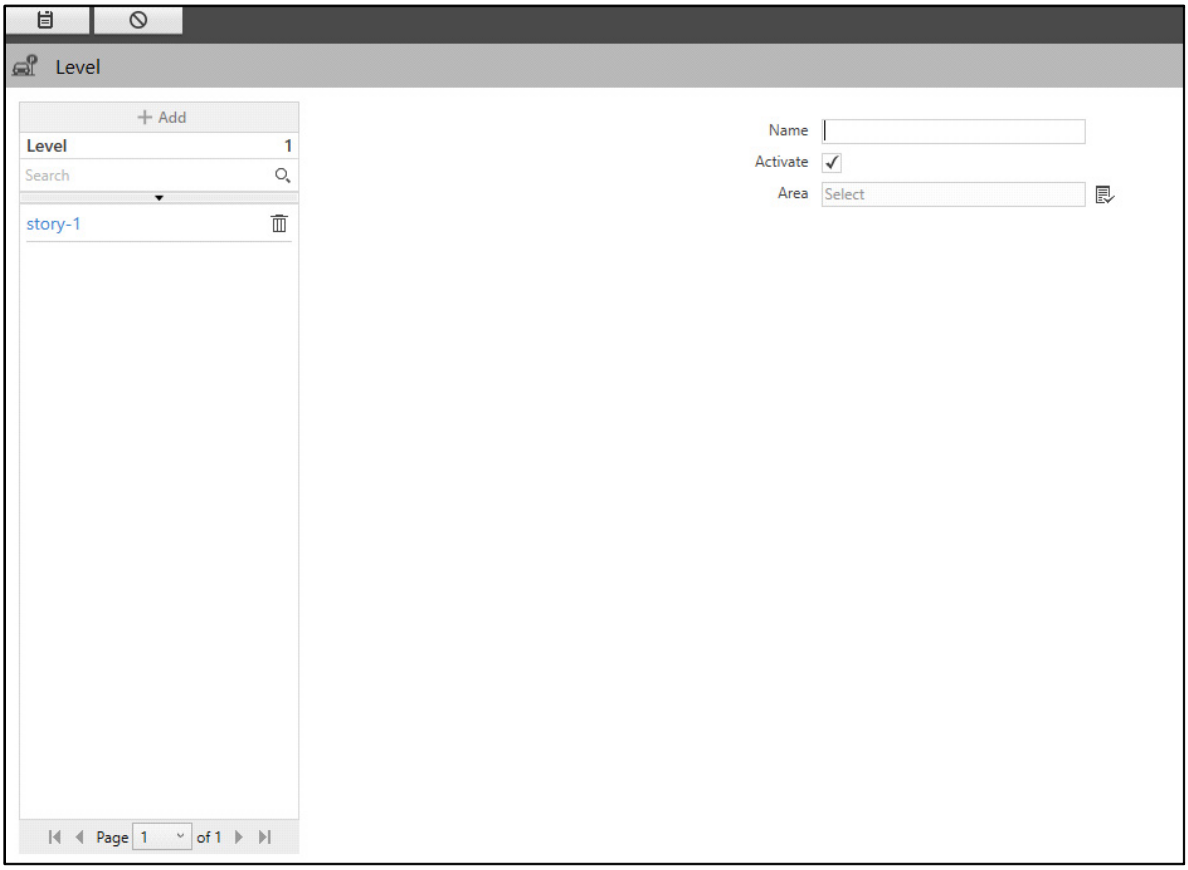
- Click **Parking Management > Multilevel Parking > Level**.



The entity name (Level) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

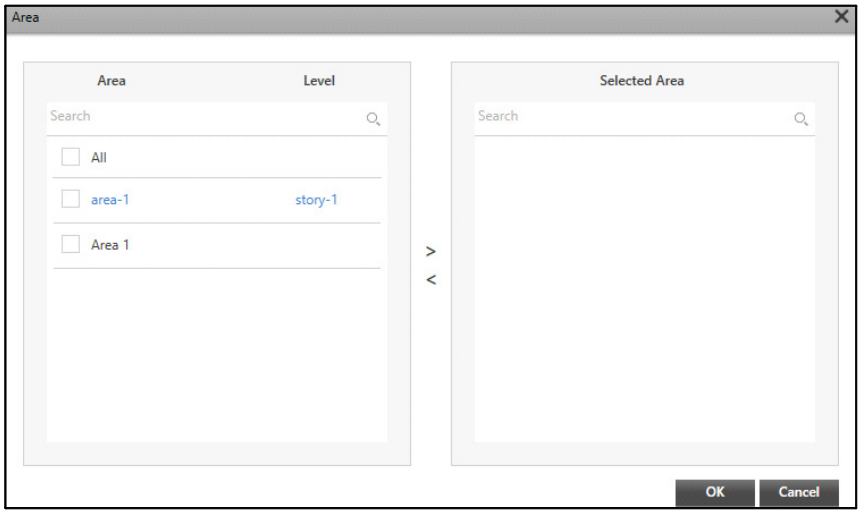
*The **Add** button is disabled when you are configuring Level for the first time. You can directly configure the parameters and save the Level.*

- Click **Add**.



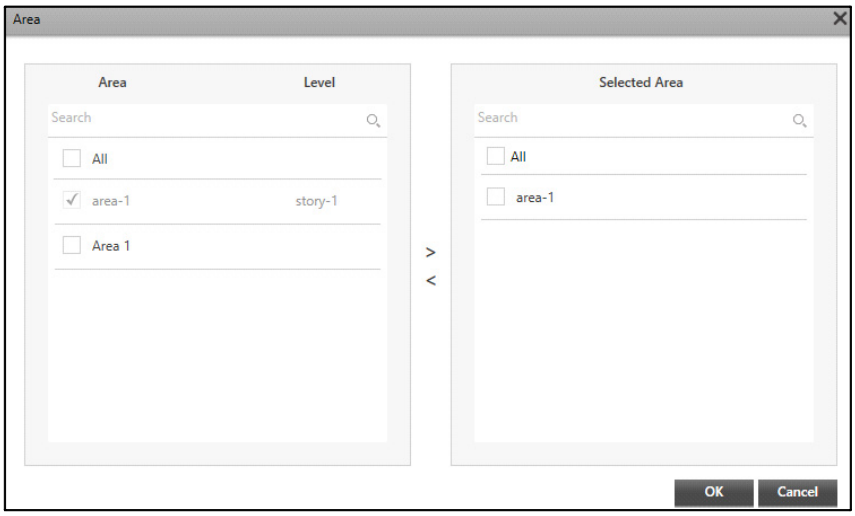
Configure the following parameters:

- **Name:** Specify a suitable name for the Level. In Name, you can enter upto 50 characters. Default: Blank.
- **Activate**: Select the check box to enable the Level.
- **Area:** Select the desired Areas which you wish to assign to the Level using the **Select Area** picklist.
  - Click **Select Area** picklist. The **Area** pop-up appears.



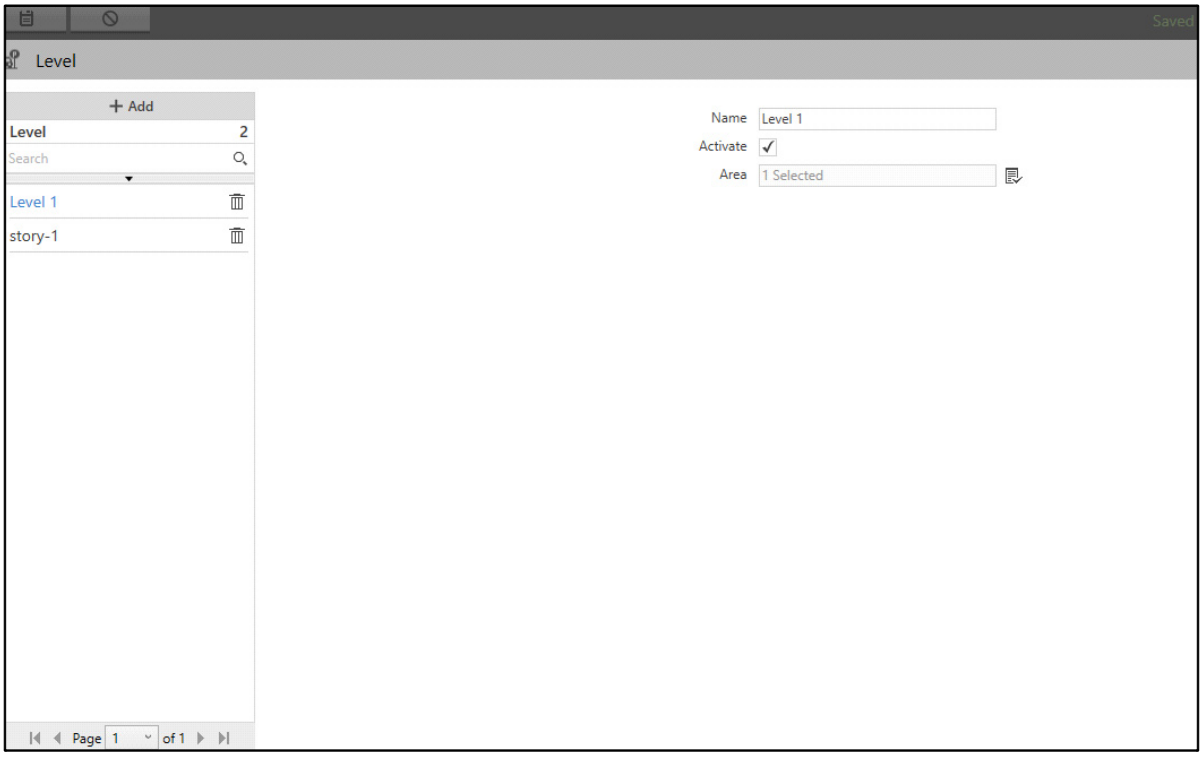
- All the configured Areas appear in the list. To configure Areas, refer to “Area”. The Levels to which the Areas belong to is indicated neat the Areas. Select the check boxes of the desired Areas you wish to select from the list. Click the right arrow button to add these Areas in the **Selected Area** list. You can also search for the desired Areas using the search bar.

  To remove Areas, select the check boxes of the desired Areas you wish to remove from the Selected Area lists. Click the left arrow button to remove the Areas from the Selected Area list.



- Click **OK** to confirm or click **Cancel** to discard. The number of Areas added to the Level appear in **Area**.

  You can change the configurations of the Level or delete it.



- Select the desired Level from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Level.

Facility

Facility is the fourth level of the Multilevel Parking configuration, where multiple Levels are combined together to form a Facility.

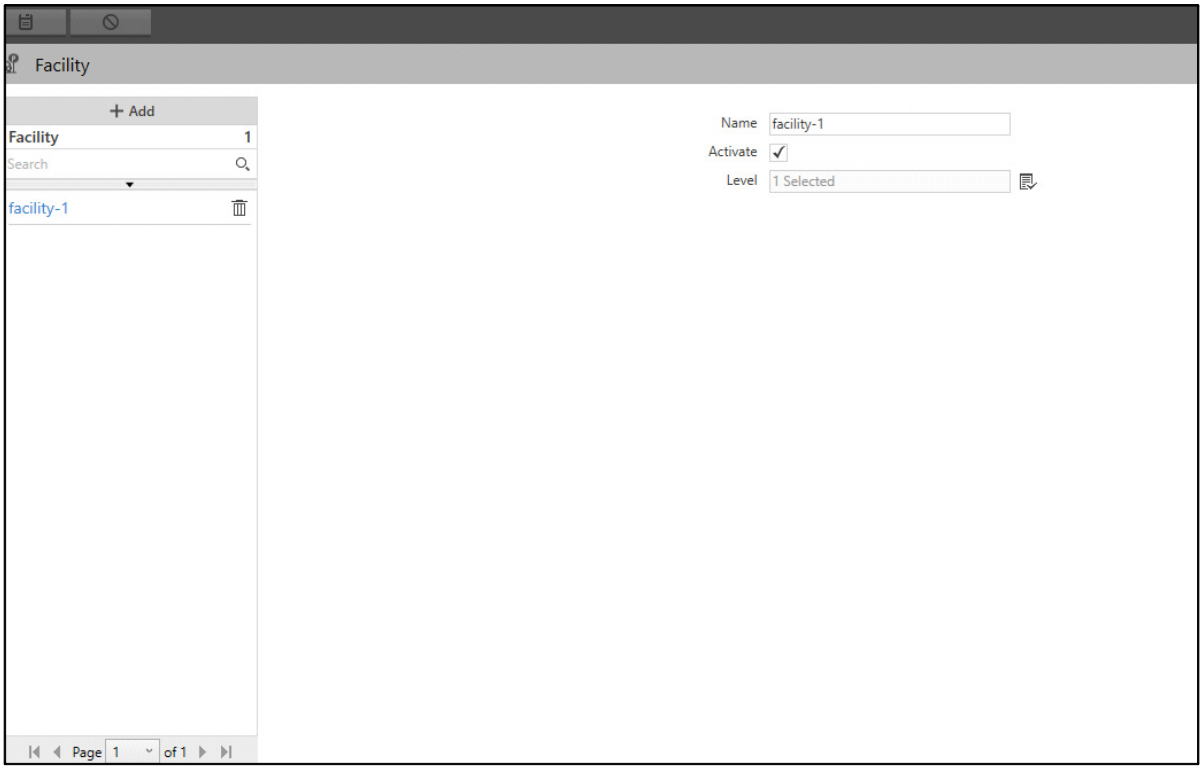
For example, multiple Floors can be grouped to form a Building of the Multilevel Parking.



The Facility page displays all the configured Facilities. You can view and configure the Facilities from this page.

To configure Facilities,

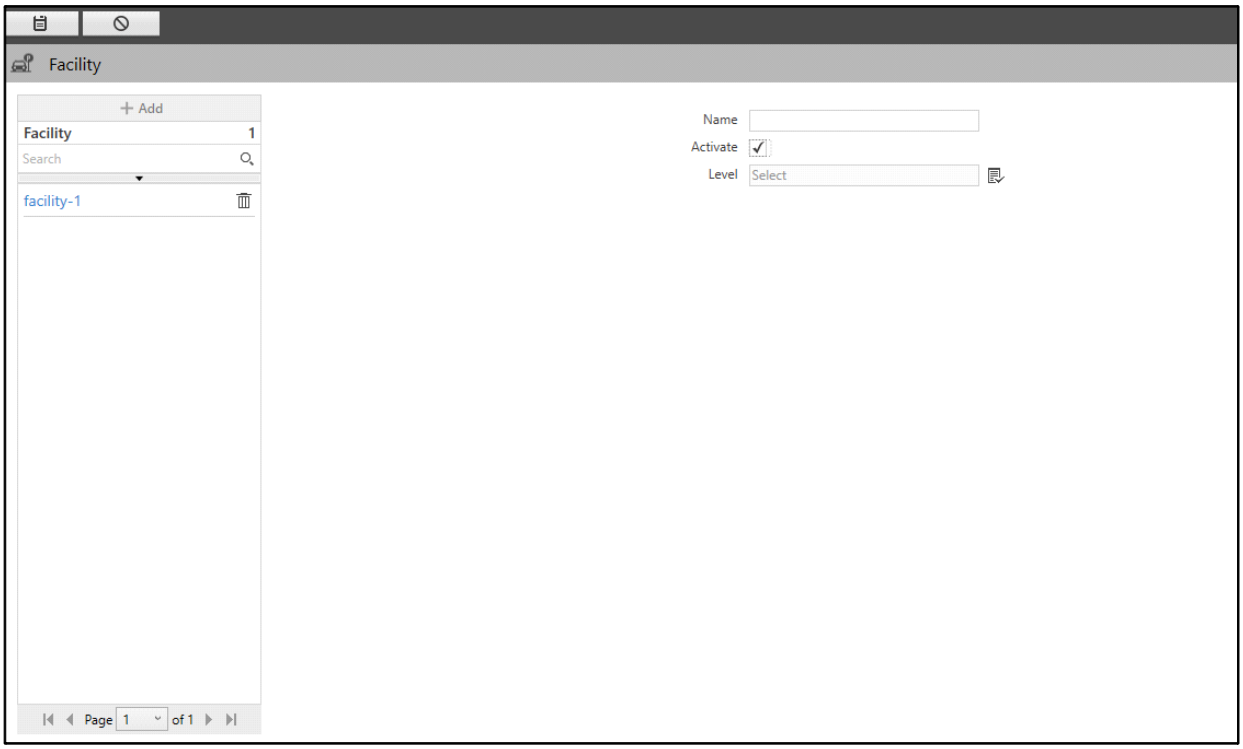
- Click **Parking Management > Multilevel Parking > Facility**.



The entity name (Facility) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

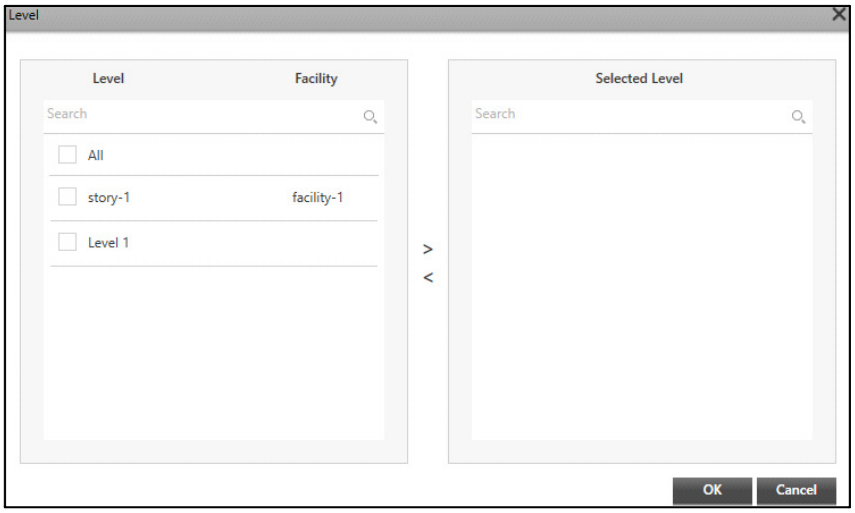
*The **Add** button is disabled when you are configuring Facility for the first time. You can directly configure the parameters and save the Facility.*

- Click **Add**.



Configure the following parameters:

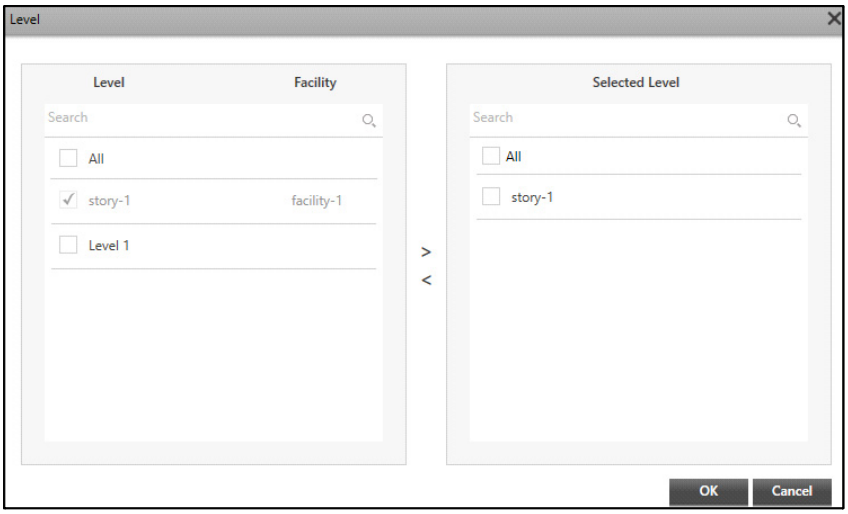
- **Name:** Specify a suitable name for the Facility. In Name, you can enter upto 50 characters. Default: Blank.
- **Activate**: Select the check box to enable the Facility.
- **Level:** Select the desired Levels which you wish to assign to the Facility using the **Select Level** picklist.
  - Click **Select Level** picklist. The **Level** pop-up appears.



  - All the configured Levels appear in the list. To configure Levels, refer to "Level". The Facilities to which the Levels belong to is indicated next to the Levels. Select the check boxes of the desired

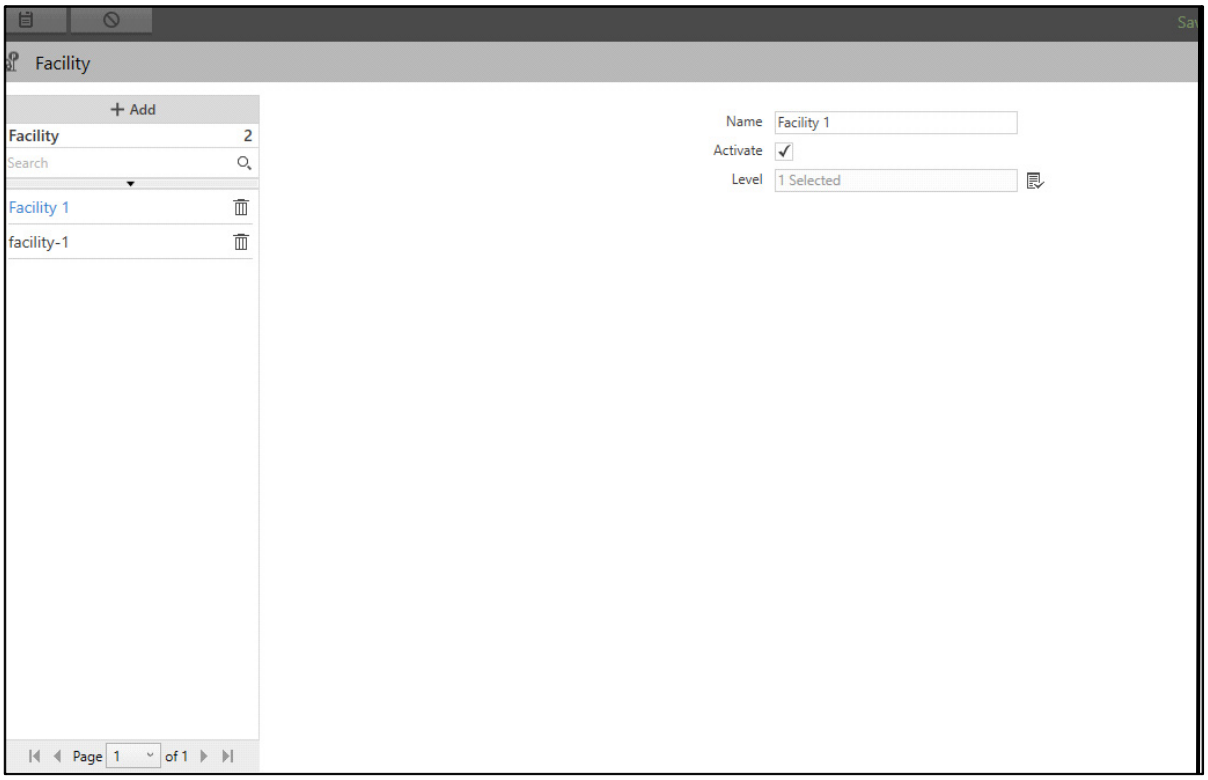
Levels you wish to select from the list. Click the right arrow button to add these Levels in the **Selected Level** list. You can also search for the desired Levels using the search bar.

To remove Levels, select the check boxes of the desired Levels you wish to remove from the Selected Level list. Click the left arrow button to remove the Levels from the Selected Level list.



- Click **OK** to confirm or click **Cancel** to discard. The number of Levels added to the Facility appear in **Level**.

  You can edit the configurations of the Facility or delete it.



- Select the desired Facility from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

- Click **Delete**  to delete the desired Facility.

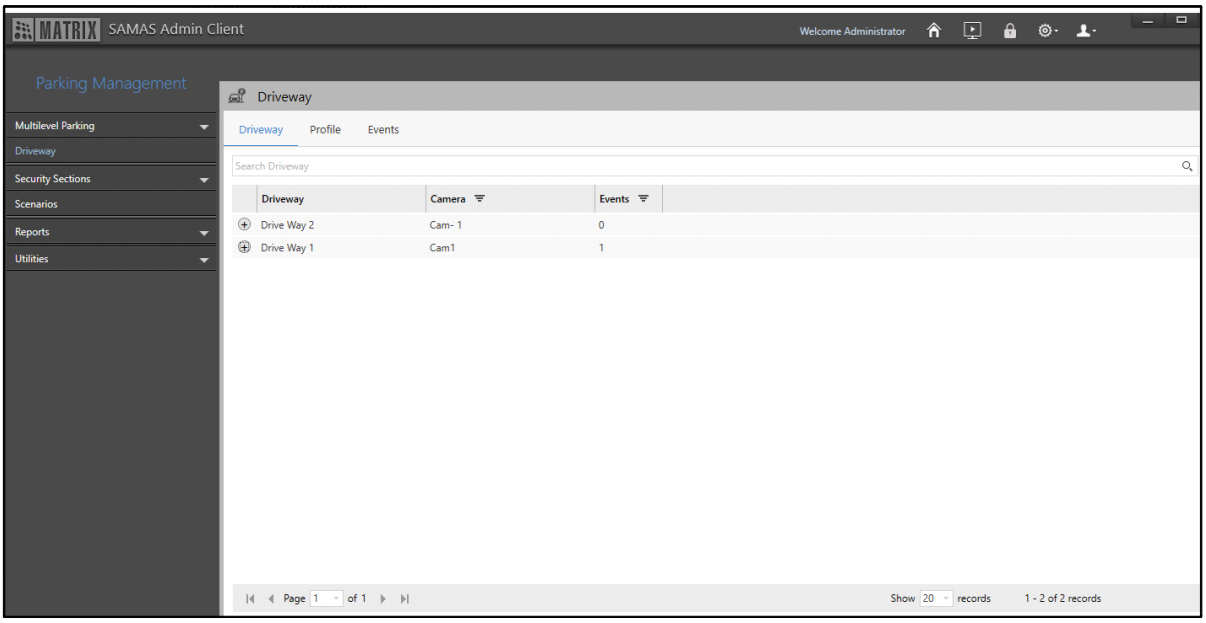
Driveway

The Parking Management module allows you to configure Driveway profiles. The Driveway feature is useful at places like malls, parking areas etc. to detect any Events (For example, Wrong Way Detection) in these premises. These Events can help security person or management to detect vehicles moving in the wrong direction and take actions accordingly. The Event that can be configured against a configured Driveway is Wrong Way Detection.

The Drive Way page displays all the configured Driveways. You can view and configure the Driveways from this page.

To configure Driveways,

- Click **Parking Management > Driveway**.



The entity name (Driveway) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

The Driveway page consists of the following tabs:

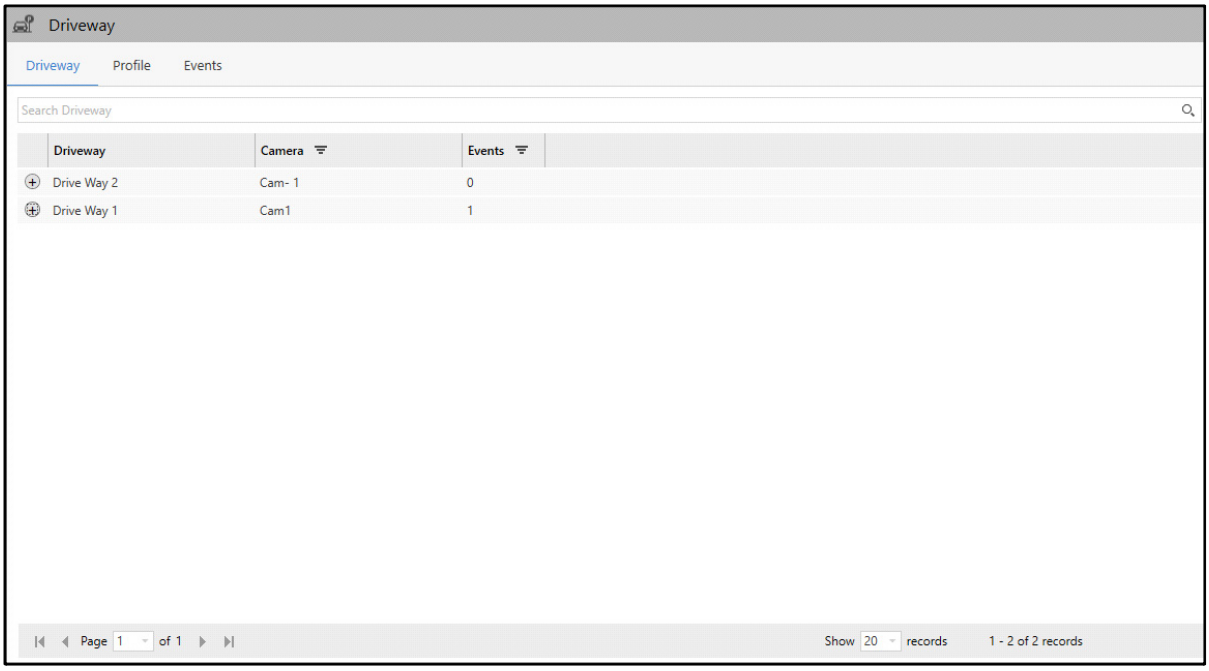
- "Driveway"
- "Profile"
- "Events"

Driveway

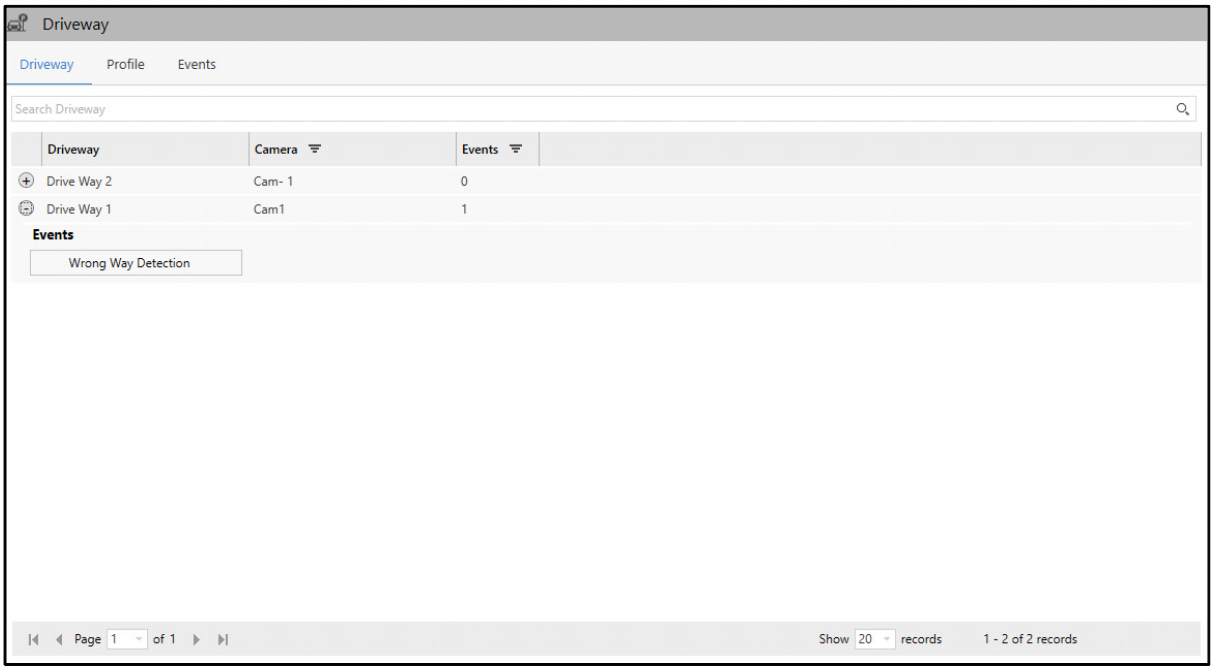
This tab enables you to view Driveways. You can configure the Zones from "Profile". All the Driveways and the Events configured for them appear under this tab. The Driveway details displayed are — Driveway, Camera and Events.

To view Driveways,

- Click the **Driveway** tab.



- Click **Show Events** ⊕ to view the Events configured for the Driveway.



- Click **Filter** ▼ of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** ▼ and then click **CLEAR FILTER**.

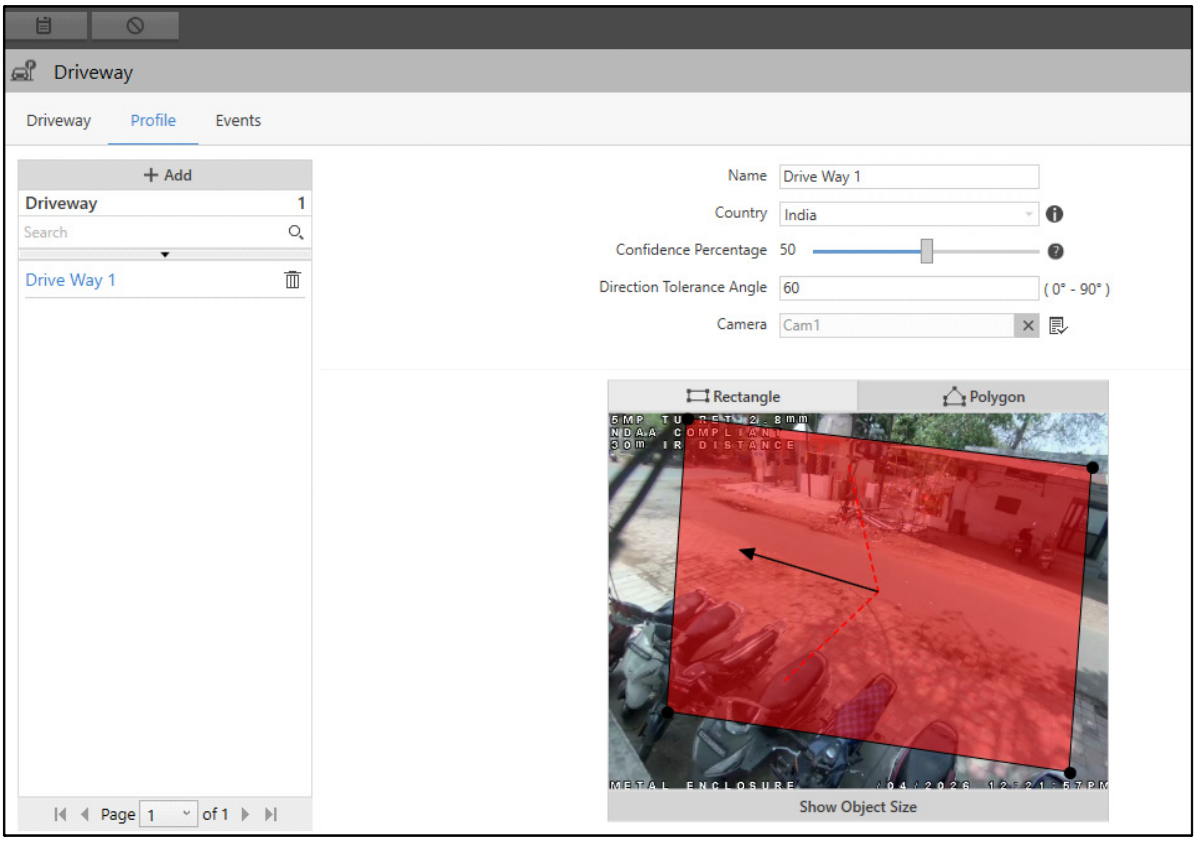
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

This tab enables you to configure Driveways. All the Driveways configured here appear under the **Driveway** tab.

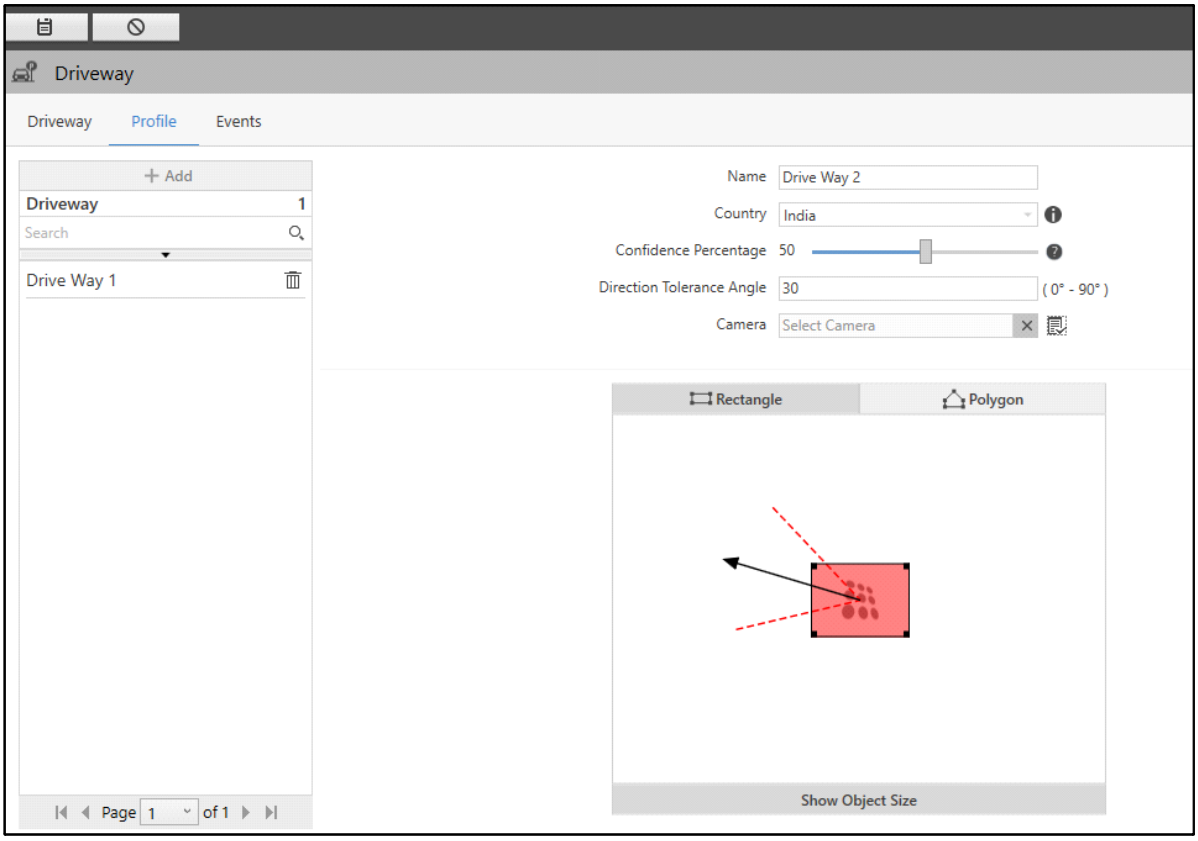
To configure Driveways,

- Click the **Profile** tab.



*The **Add** button is disabled when you are configuring Driveway profile for the first time. You can directly configure the parameters and save the Driveway.*

- Click **Add**.



Configure the following parameters:

- **Name**: Specify a suitable name for the Driveway. In Name, you can enter upto 50 characters. Default: Blank.

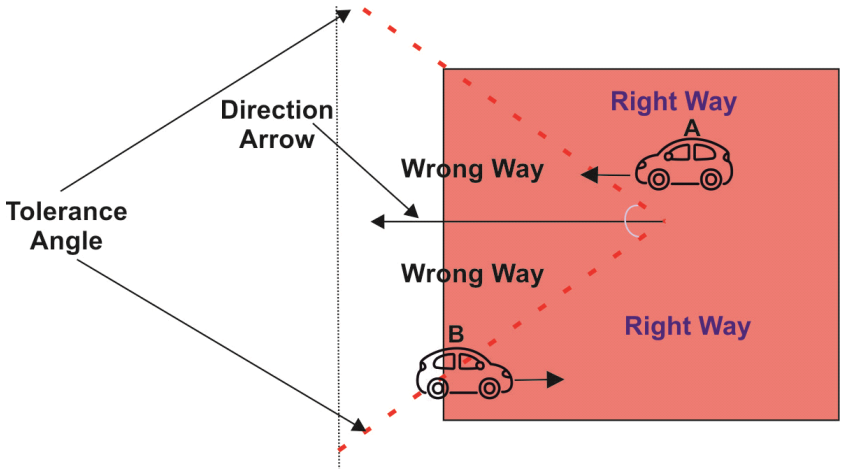
- **Country**: Select the country from the drop-down list where the camera is installed. This option is helpful in increasing the efficiency of vehicle recognition.

*The **Country** option will be applicable only when Number Plate Detection is done using Native ANPR.*

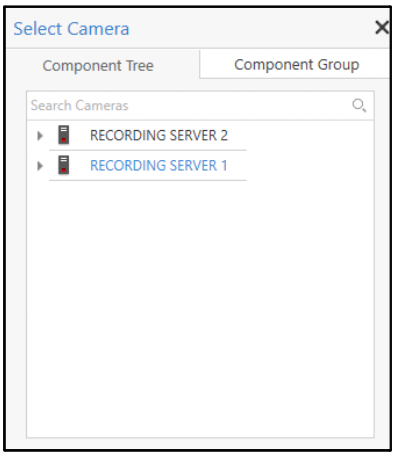
- **Confidence Percentage**: Set the Confidence Percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the percentage of success between image plate recognized and the text which is recognized from the image plate. This will be the minimal percentage allowed for successful vehicle detection. Valid Range: 0-100%. Default: 50.

- **Direction Tolerance Angle**: Configure the Direction Tolerance Angle. This indicates that vehicles coming in within the configured angle, on either side of the direction arrow are in wrong direction. Any vehicles coming from an angle on either sides beyond the configured Tolerance Angle are in right direction.

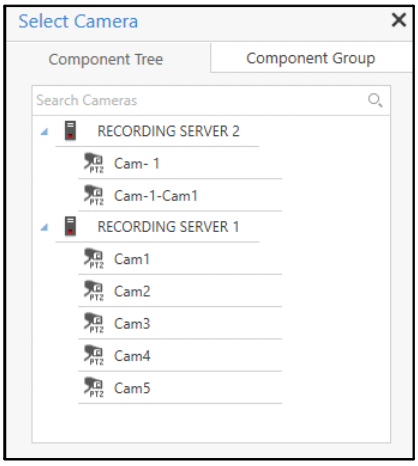
  For example, in the diagram below, consider you have set Direction Tolerance Angle at 30 degrees. Then, vehicle **A** coming in the zone within 30 degrees from the direction arrow is in wrong direction. Vehicle **B** coming in the zone in the opposite direction as that of **Direction Arrow** is said to be in right direction, irrespective of whether it falls within the Tolerance Angle or not.



- **Camera**: Select the desired camera which you wish to assign to the Driveway using the **Camera** picklist.
    - Click **Camera** picklist. The **Select Camera** pop-up appears.

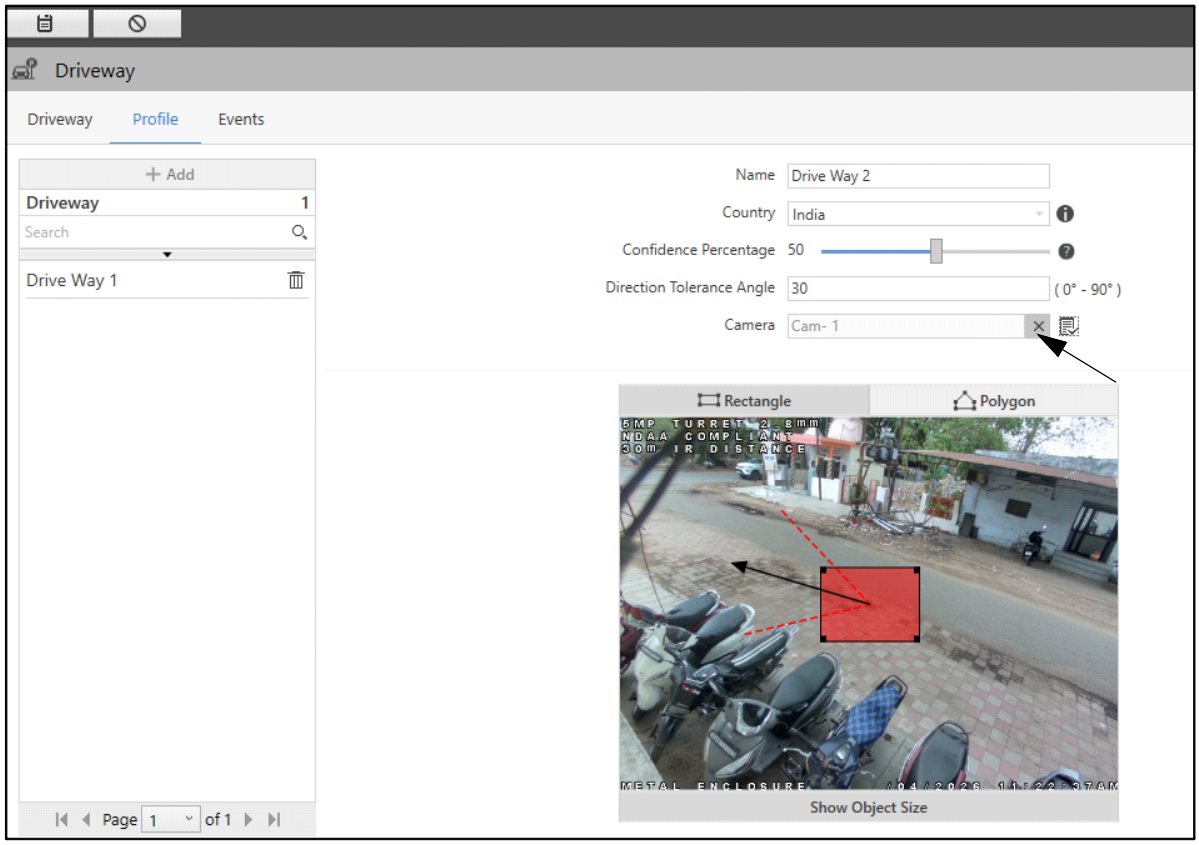


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to "Component Group". Double-click the desired camera to assign it to the Driveway. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

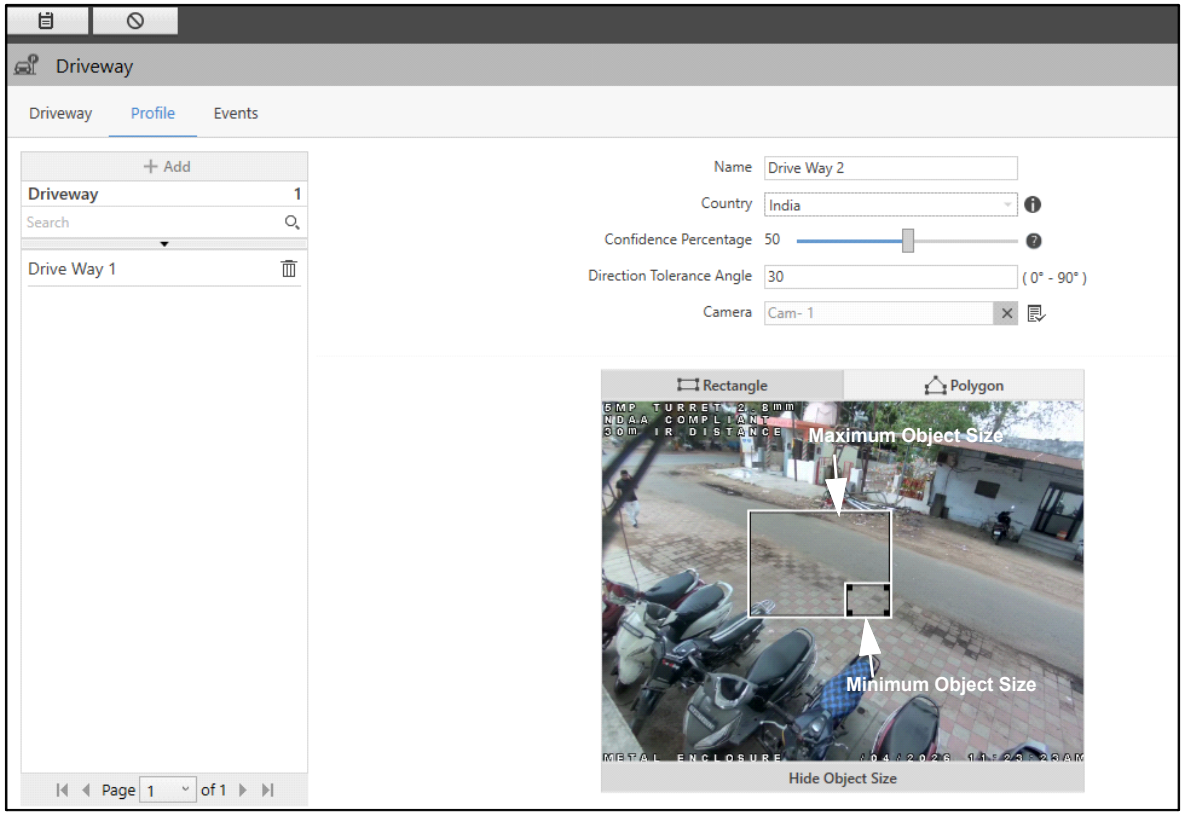
- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click to select the desired option.
  - Click **Go to selected position** to move the camera to the selected preset position.
  - To remove the camera, click **Remove** .



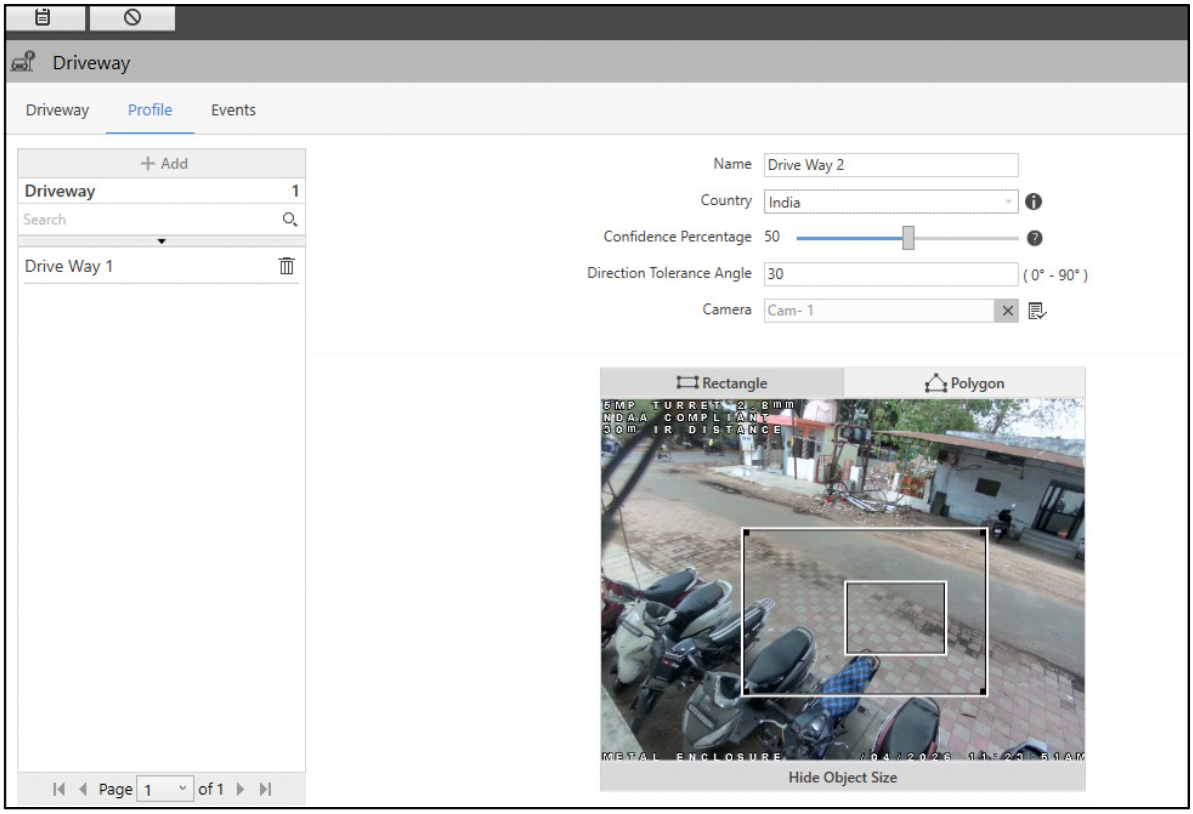
Once a camera is assigned, you can draw a Driveway on the live view of the camera. You can also define the **Minimum** and **Maximum Object Size**. You can either draw a **Rectangle** or **Polygon** to define the Driveway.

Object Size will not be applicable if you select Object Type in any Event. For details, refer to "Events".

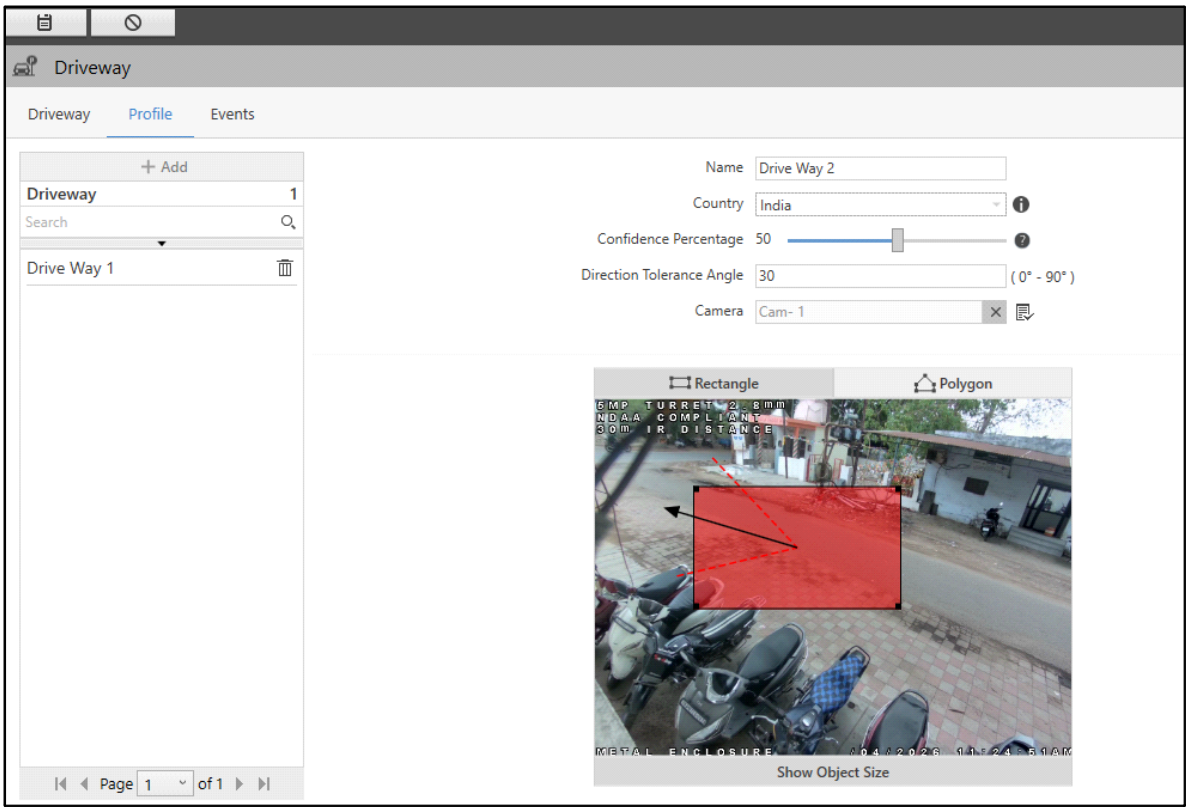
- Click **Show Object Size**. The default **Minimum** and **Maximum Object Size** appear.



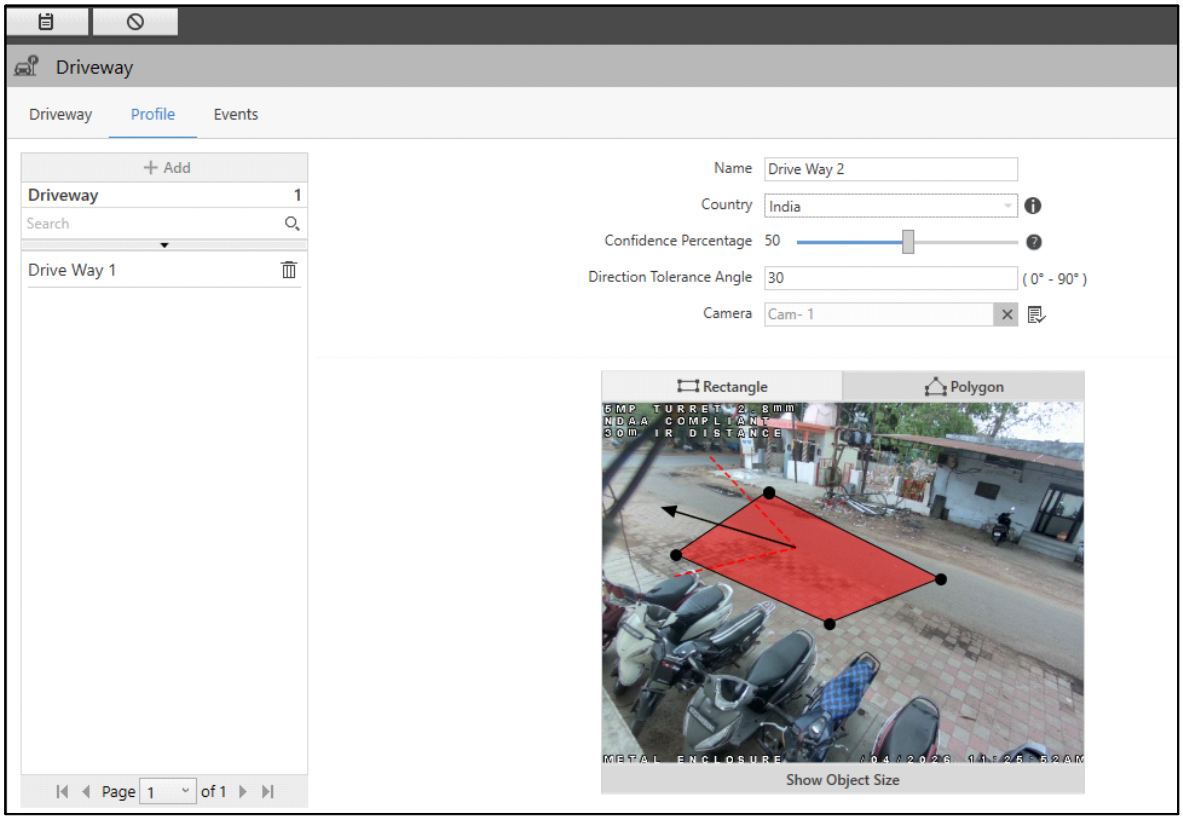
- Drag the corners of the rectangles to configure the minimum and maximum object size to be detected in the Event, if required. When the object size meant to be detected in the Event does not fit in the default Minimum and Maximum Object Size, you can configure it to match the desired object size.



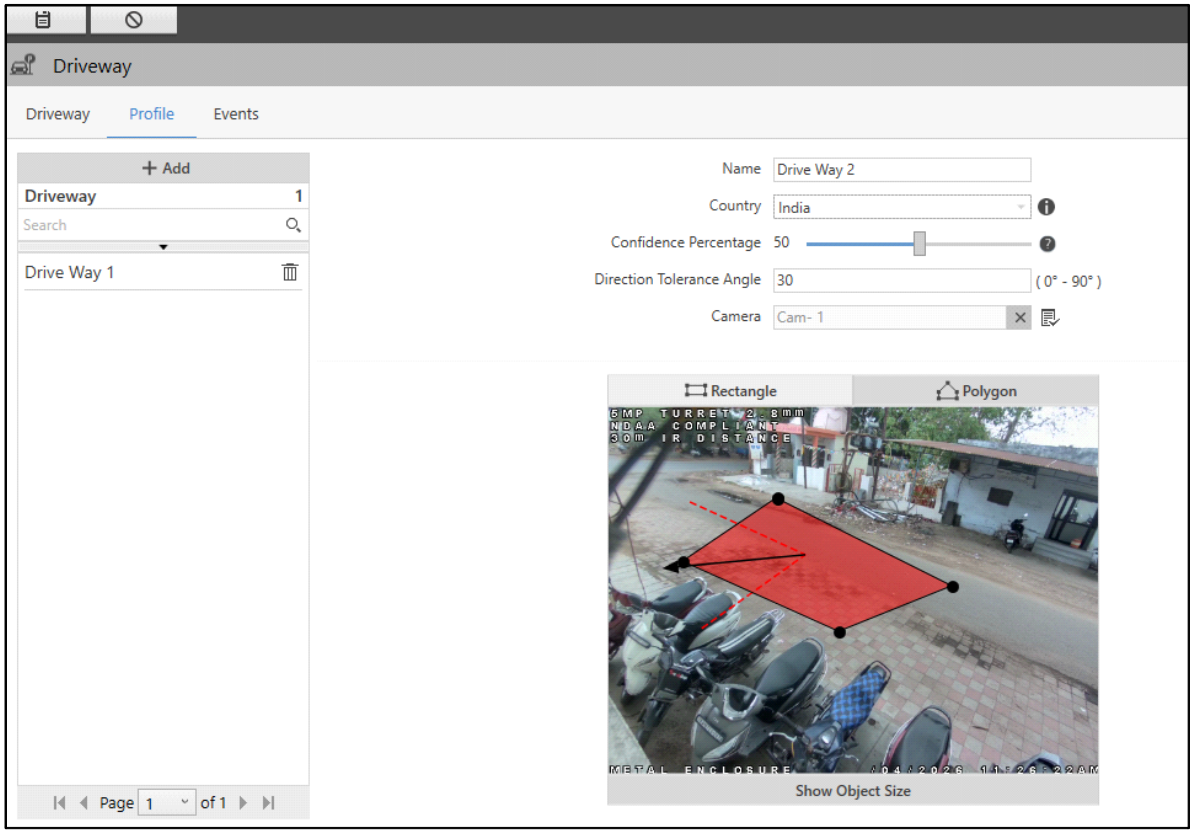
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Hide Object Size** to hide the size and draw the Driveway.
  - Select either **Rectangle** or **Polygon** to draw the Driveway.
  - If you select **Rectangle**, drag the corners and sides of the rectangle to configure the Driveway.



  - If you select **Polygon**, click on the live view to place the vertex of the polygon. Click again on the desired place to join the previous vertex with a new vertex. Continue this process to complete the polygon.



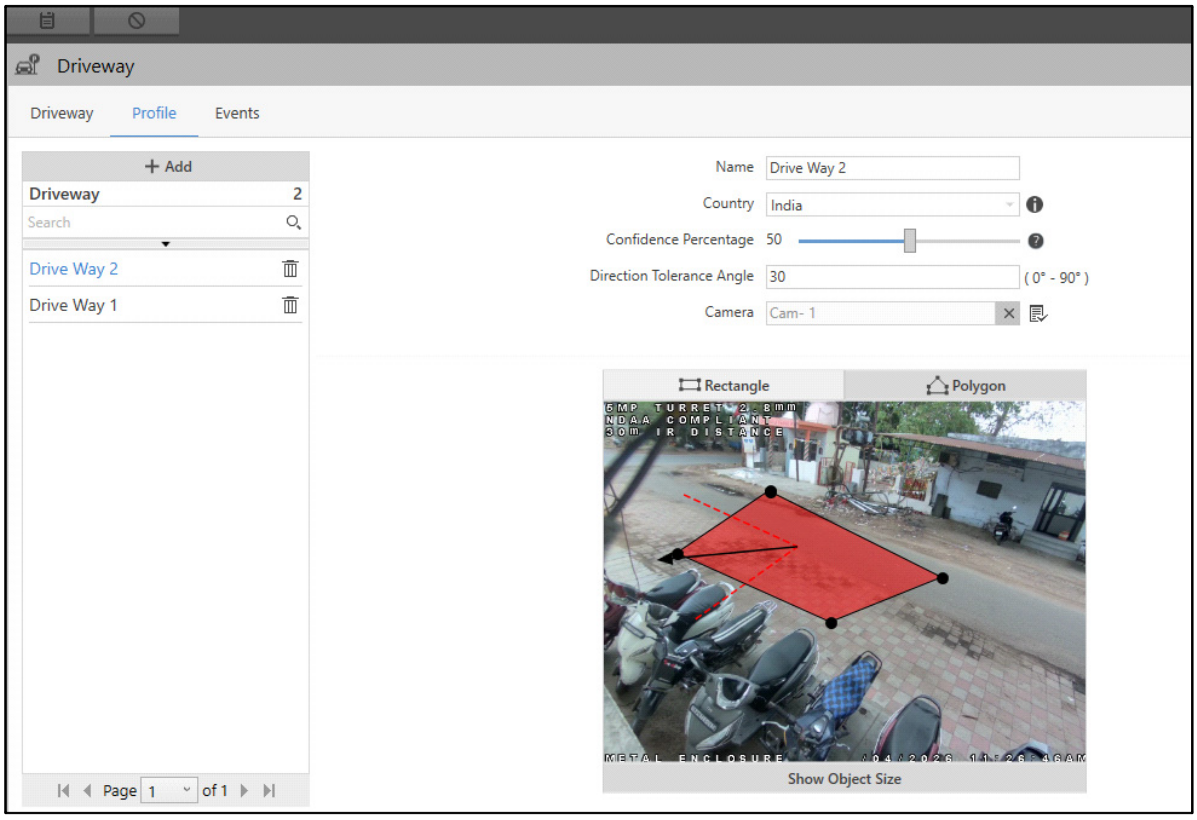
Once the Polygon or Rectangle shaped Driveway is configured along with Direction Tolerance Angle, the direction is set automatically depicted by the arrow. If you wish to change the direction of the arrow, hover-over the arrow. When the two direction arrow appears, click and drag in the desired direction.



- Click **Save** to save the settings or **Cancel** to discard.

The new Driveway will appear in the list on the left hand side.

You can edit the configurations of the Driveway or delete it.



- Select the desired Driveway from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Driveway.

Similarly, you can configure the other Driveways.

Events

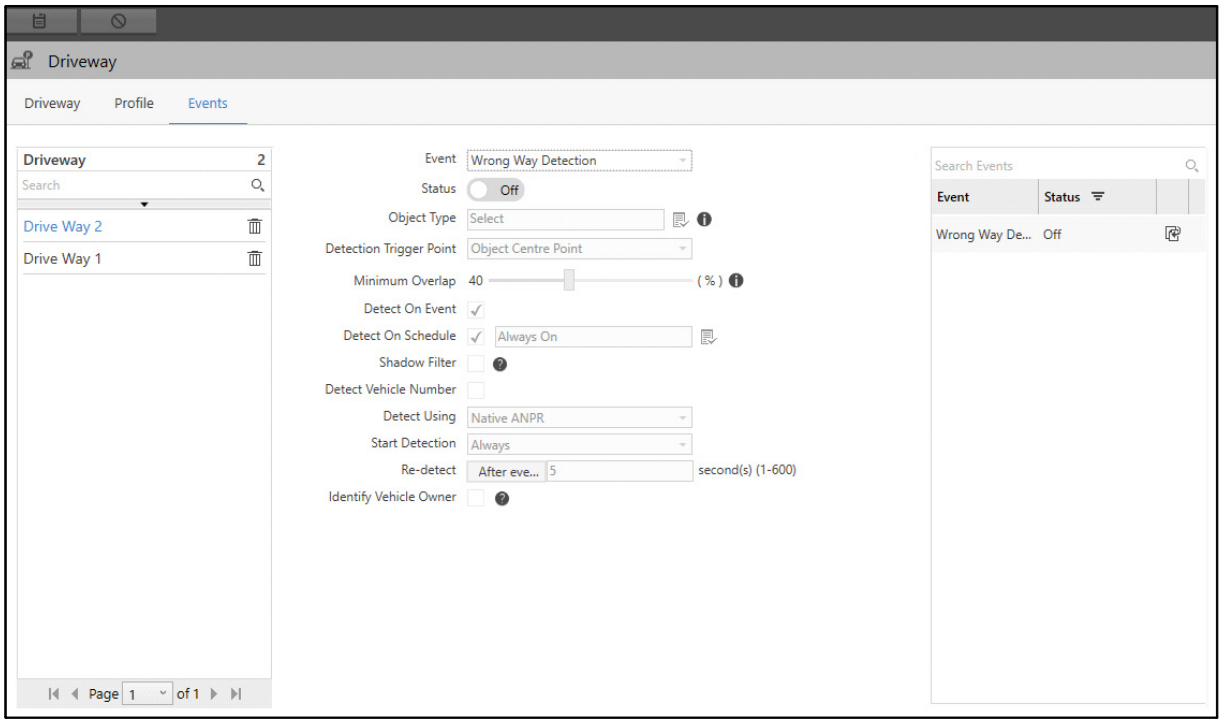
This tab enables you to configure the Wrong Way Detection Event for the Driveways. All the configured Events appear under the **Driveway** tab.

The Wrong Way Detection Event enables you to control people or vehicles moving in a wrong direction. This is useful at places like malls, parking areas etc. where only one entry and exit door is present. At such places, this Event proves to be very helpful in detecting people or vehicle moving in the wrong direction and take actions accordingly.

Object Size configured in any "Profile" will not be applicable if you select Object Type in any Event.

To configure Wrong Way Detection Event,

- Click the **Events** tab.
- Select the desired Profile from the left hand side for which you wish to configure the Event.

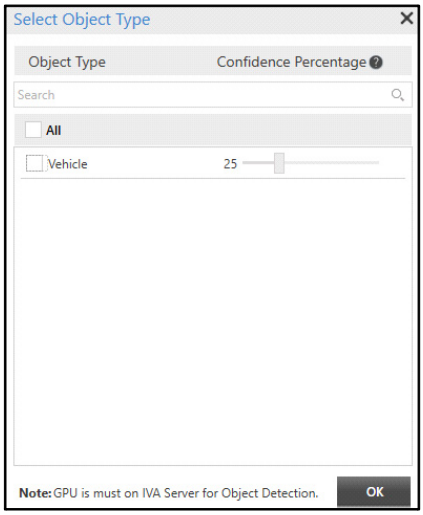


Configure the following parameters:

- **Event:** Select the Wrong Way Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

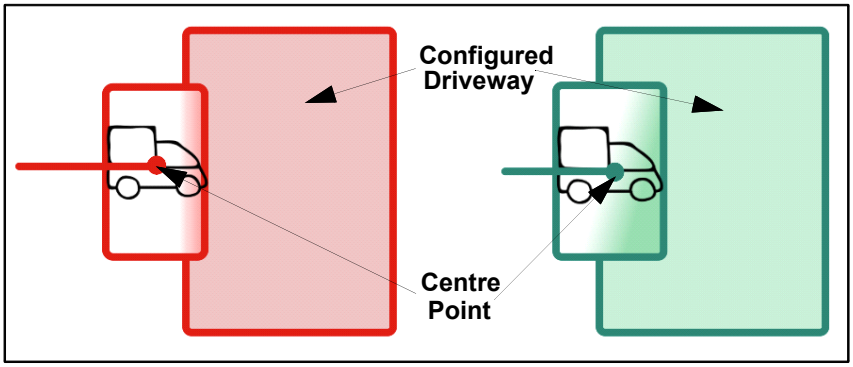


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point, Minimum Overlap. Based on the selected option, the IVA engine will detect the selected Object Type. The **Wrong Way Detection** event will be triggered based on the selected **Detection Trigger Point** and the **Direction Tolerance Angle** as configured in “Profile”.

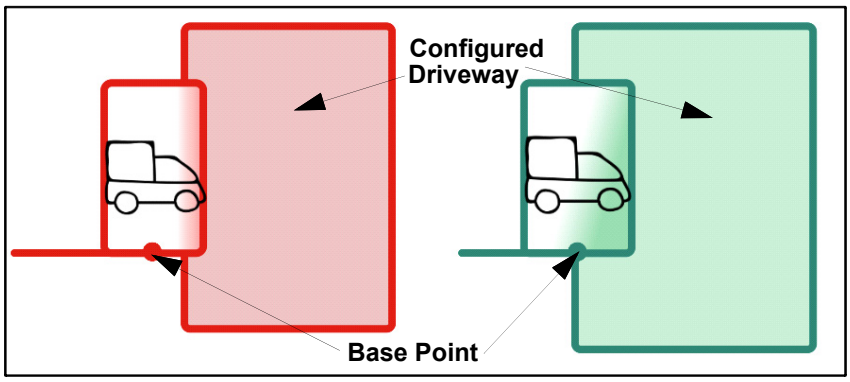
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured driveway.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point of the object crosses the configured driveway, an event will be generated if the object is moving in the direction same as that of the Direction Arrow.



  If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured driveway.

  In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured driveway, an event will be generated if the object is moving in the direction same as that of the Direction Arrow.

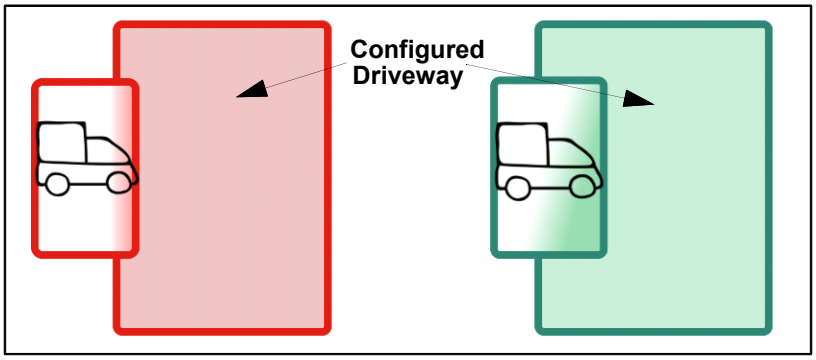


If you select **Minimum Overlap**, the IVA engine will detect the event based on the minimum percentage of overlap of detected object across the configured driveway.

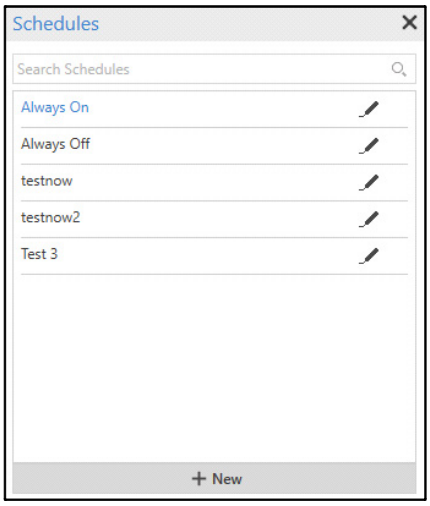
- **Minimum Overlap**: If you have selected **Detection Trigger Point** as **Minimum Overlap**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the driveway to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the driveway will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the driveway will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Slot, the event will be triggered when 30% of the vehicle is overlapping the configured driveway and is moving in the direction same as that of the Direction Arrow. Whereas, in the Red Slot, the event will not be triggered as, only 10% of the vehicle is overlapping the configured driveway even if it is moving in the direction same as that of the Direction Arrow.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of the Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Shadow Filter**: Select the check box to ignore the shadow of the people/objects crossing the Driveway and reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Detect Vehicle Number**: Select the check box to enable vehicle detection through License Plate Recognition.

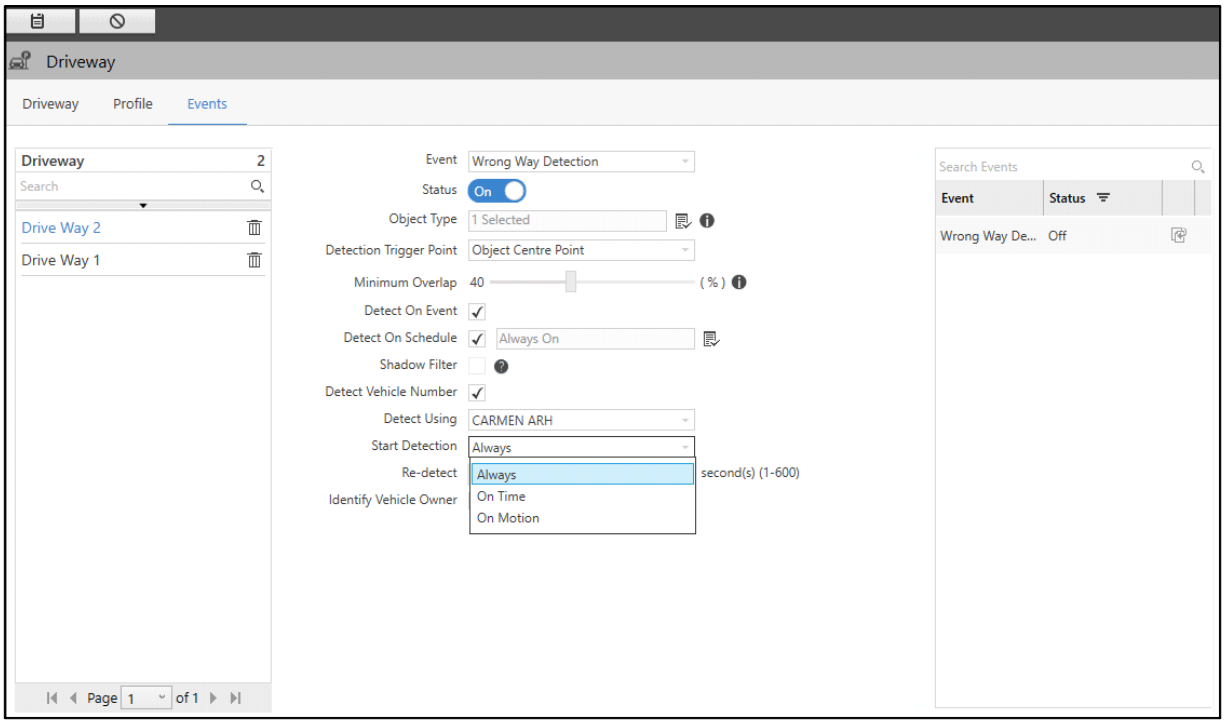
- **Detect Using**: Select the detection method from the drop-down list options — Native ANPR or CARMEN ARH.

  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Driveway Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.
  If you select the detection method as **CARMEN ARH**, configure the following parameters:

There will be a delay of 10 seconds to check for the License (dongle), if it is not found (or removed in-between) during the process of Event generation for all Vehicle based Events where the CARMEN ARH has been used.

- **Start Detection**: Select the start detection method from the drop-down list options — Always, On Time or On Motion.

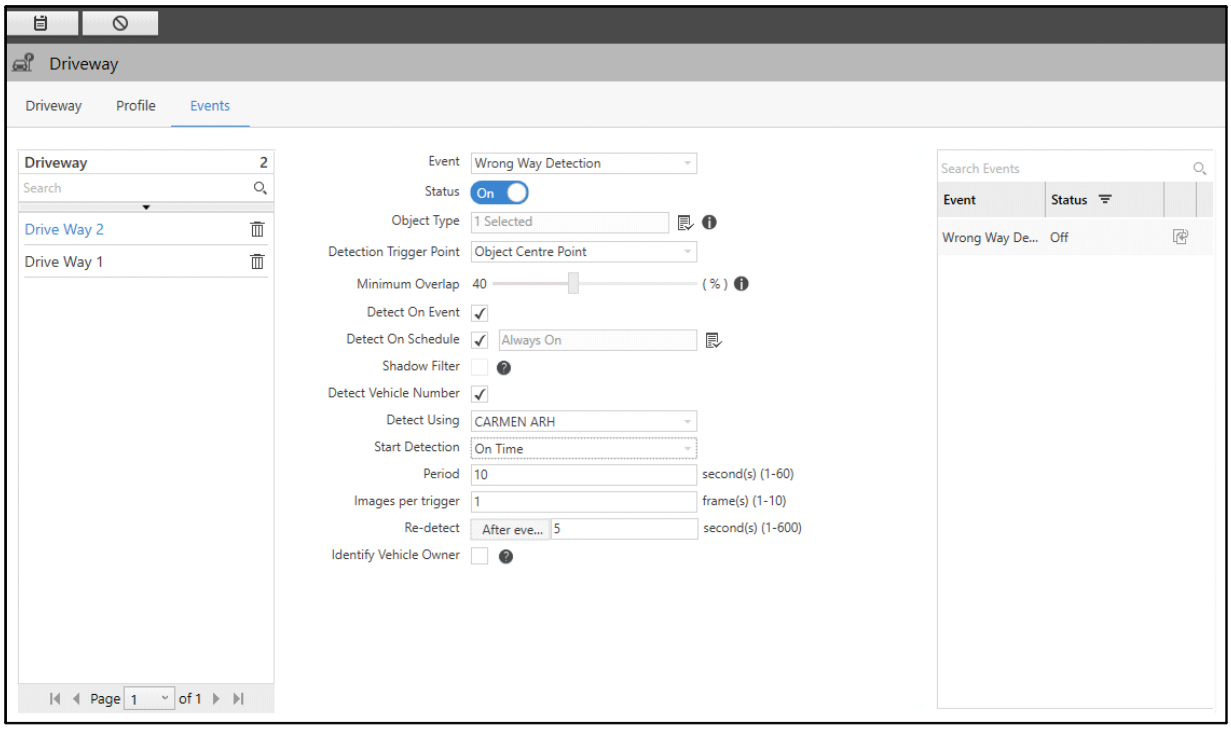


If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images per Trigger is higher than frames received in the configured period, the maximum FPS is sent to ARH. For example, Period = 1 sec and Images per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters:

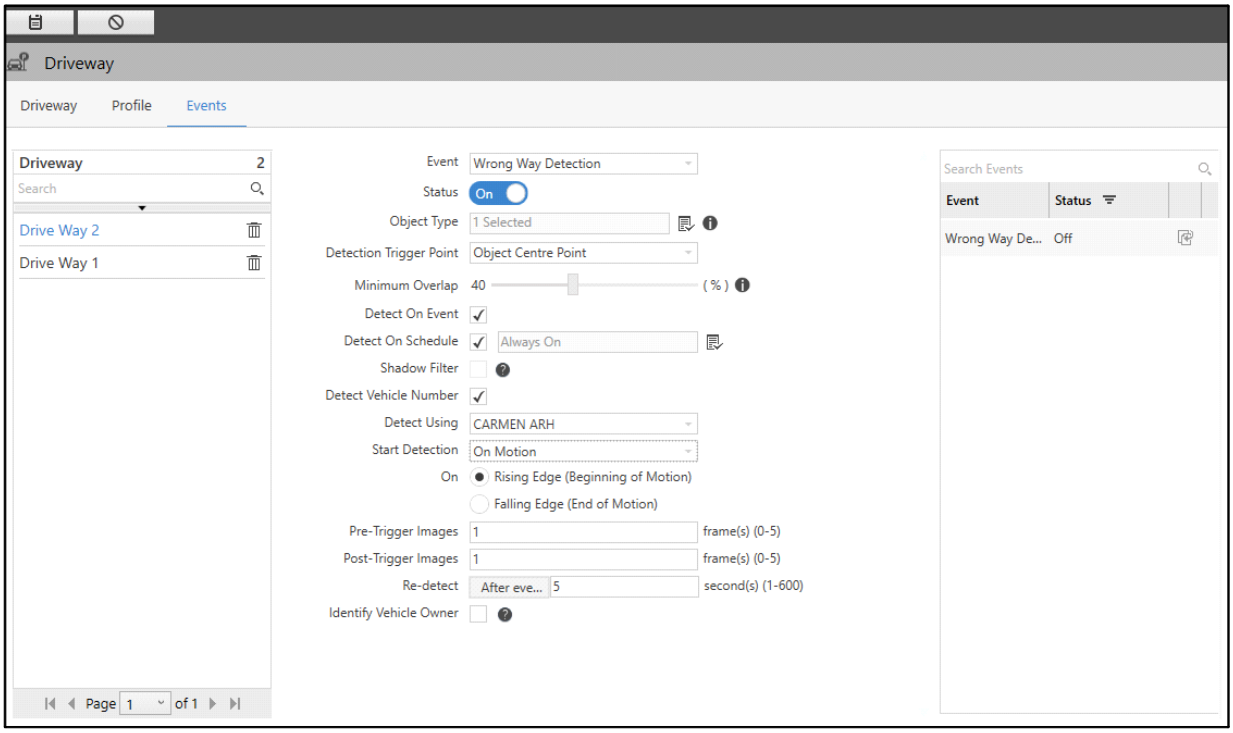
- **Period**: Specify the time interval after which the images will be sent to the ARH Engine. Valid Range:1-60 seconds. Default: 10.
- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range: 1-10 frames. Default: 1.



If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as per which you wish the images to be passed to the ARH Engine — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).
- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0-5 frames. Default: 1.
- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion. Valid Range: 0-5 frames. Default: 1.



- **Re-detect After every**: Specify the time after which the Wrong Way Detection Event will be detected again after the previous detection. Valid Range: 1-600 seconds. Default: 5.

- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

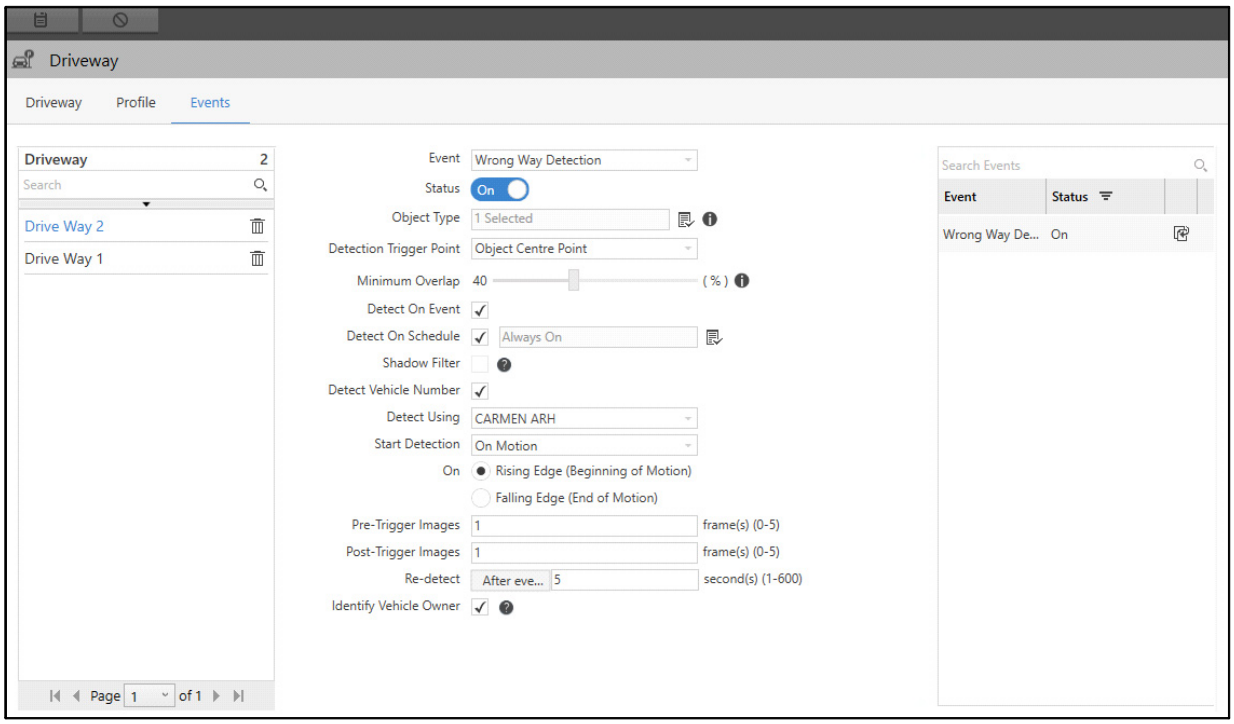
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.

- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

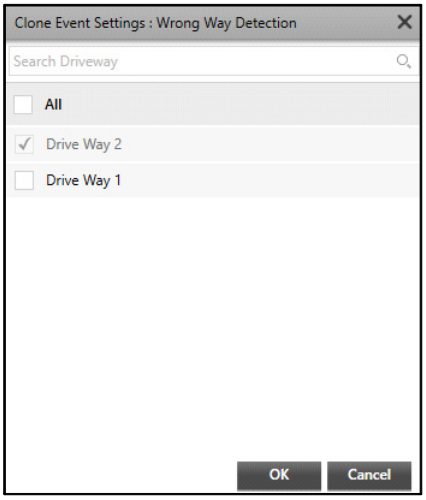
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Driveway is created, the **Clone Event Settings** option gets enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Wrong Way Detection** pop-up appears.



- Select the desired driveways to which you wish to copy the Event configurations.

- Click **OK** to confirm or click **Cancel** to discard.

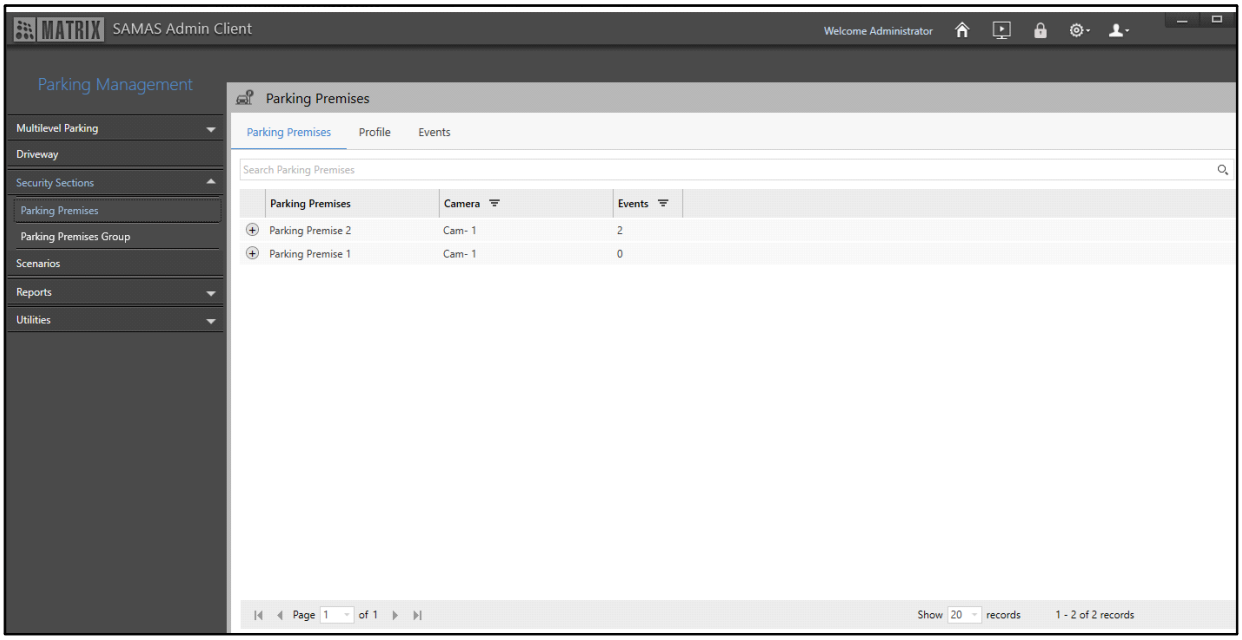
Security Sections

The Parking Management module allows you to configure Parking Premise profiles. The Parking Premises feature is useful at places like malls, parking areas etc. to detect any Events (For example, Parking Premises Availability) in the premises. These Events can help security person or management to know about the remaining space at the parking zone. Events that can be configured against the configured Parking Premises profile are: Parking Premises Availability and Vehicle Counting.

The Parking Premises page displays all the configured Parking Premises. You can view and configure the Parking Premises from this page.

To configure Parking Premises,

- Click **Parking Management > Security Sections**. The **Parking Premises** page appears by default.



The entity name (Parking Premises) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

The Parking Premises page consists of the following tabs.

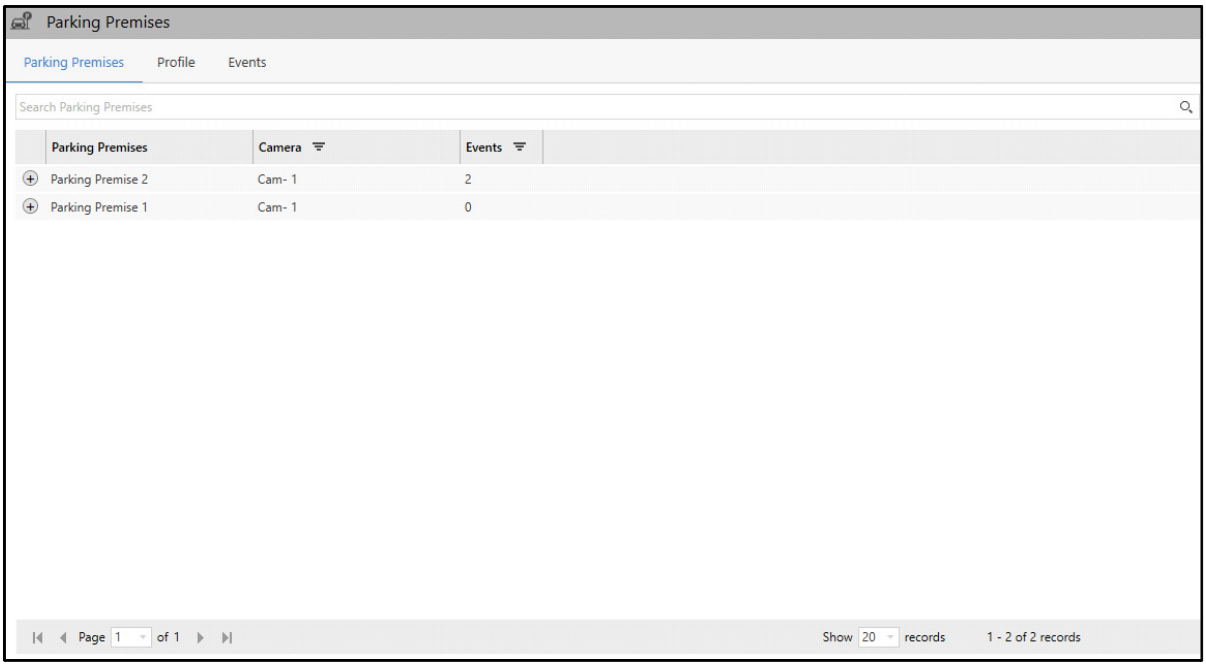
- "Parking Premises"
- "Profile"
- "Events"

Parking Premises

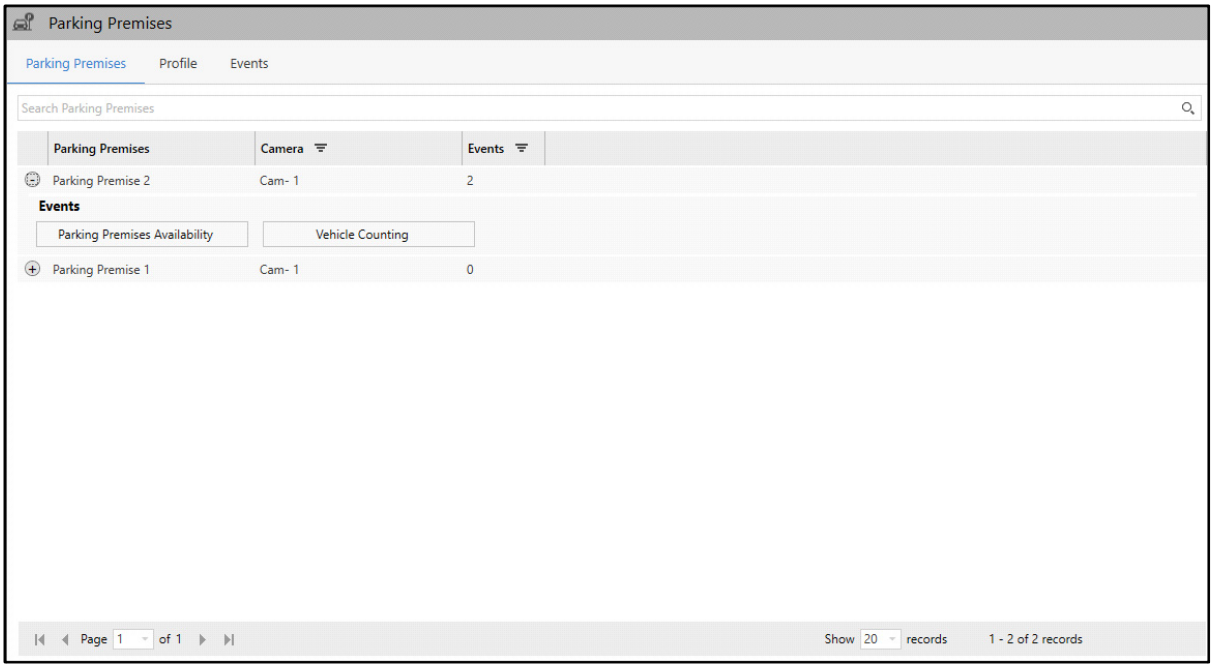
This tab enables you to view Parking Premises. You can configure the Parking Premises from "Profile". All the Parking Premises and the Events configured for them appear under this tab. The Parking Premises details displayed are — Parking Premises, Camera and Events.

To view Parking Premises,

- Click the **Parking Premises** tab.



- Click **Show Events** to view the Events configured for the Parking Premises.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR FILTER**.

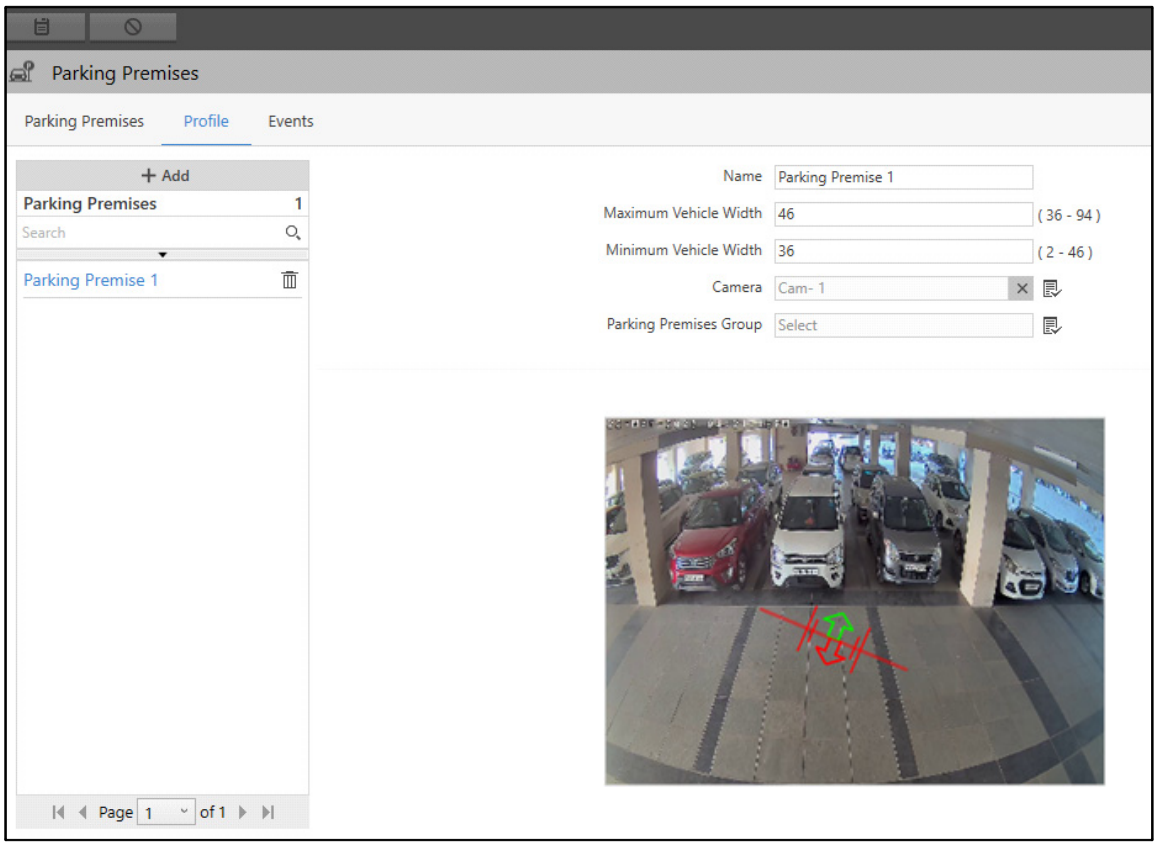
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

This tab enables you to configure Parking Premises. All the Parking Premises configured here appear under the **Parking Premises** tab.

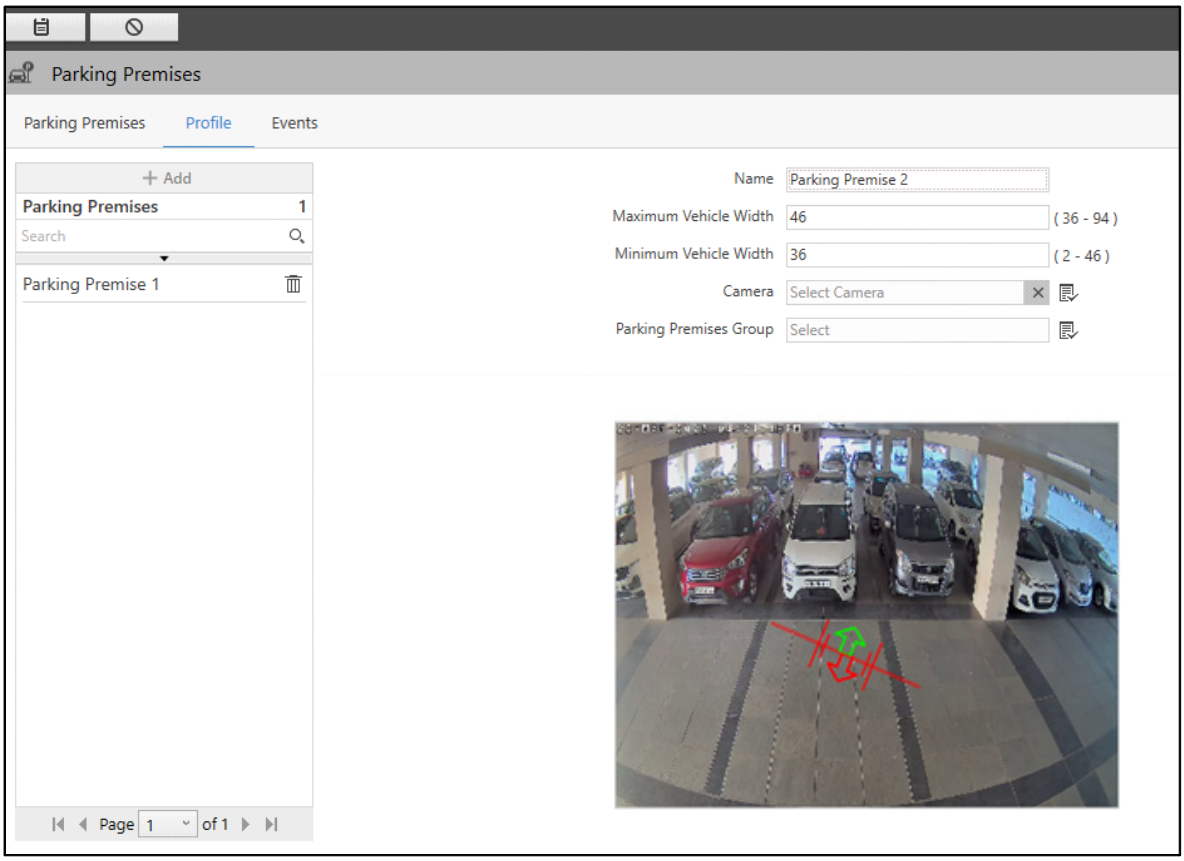
To configure Parking Premises,

- Click the **Profile** tab.



*The **Add** button is disabled when you are configuring Parking Premises profile for the first time. You can directly configure the parameters and save the Parking Premises.*

- Click **Add**.



Configure the following parameters:

- **Name**: Specify a suitable name for the Parking Premise. In Name, you can enter upto 50 characters. Default: Blank.

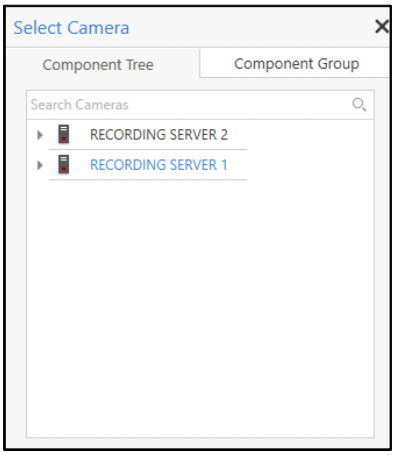
Maximum and Minimum Vehicle Width will not be applicable if you select Object Type in any Event. For details, refer to "Events".

- **Maximum Vehicle Width**: Specify the maximum width of the vehicle which is meant to be detected in the Event in the live view. Default Range: 36 to 492. Maximum Size will vary as per the line configured by you. Default:46.

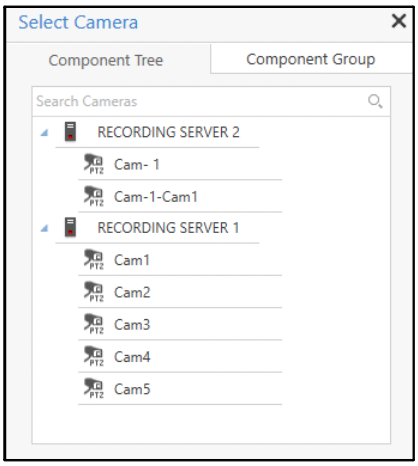
- **Minimum Vehicle Width**: Specify the minimum width of the vehicle which is meant to be detected in the Event in the live view. Default Minimum Vehicle Width: 2 (Lower limit). The Upper limit of Minimum Vehicle Width will vary as per the Maximum Vehicle Width configured by you. Default:36.

- **Camera**: Select the desired camera which you wish to assign to the Parking Premise using the **Camera** picklist.

  - Click **Camera** picklist. The **Select Camera** pop-up appears.

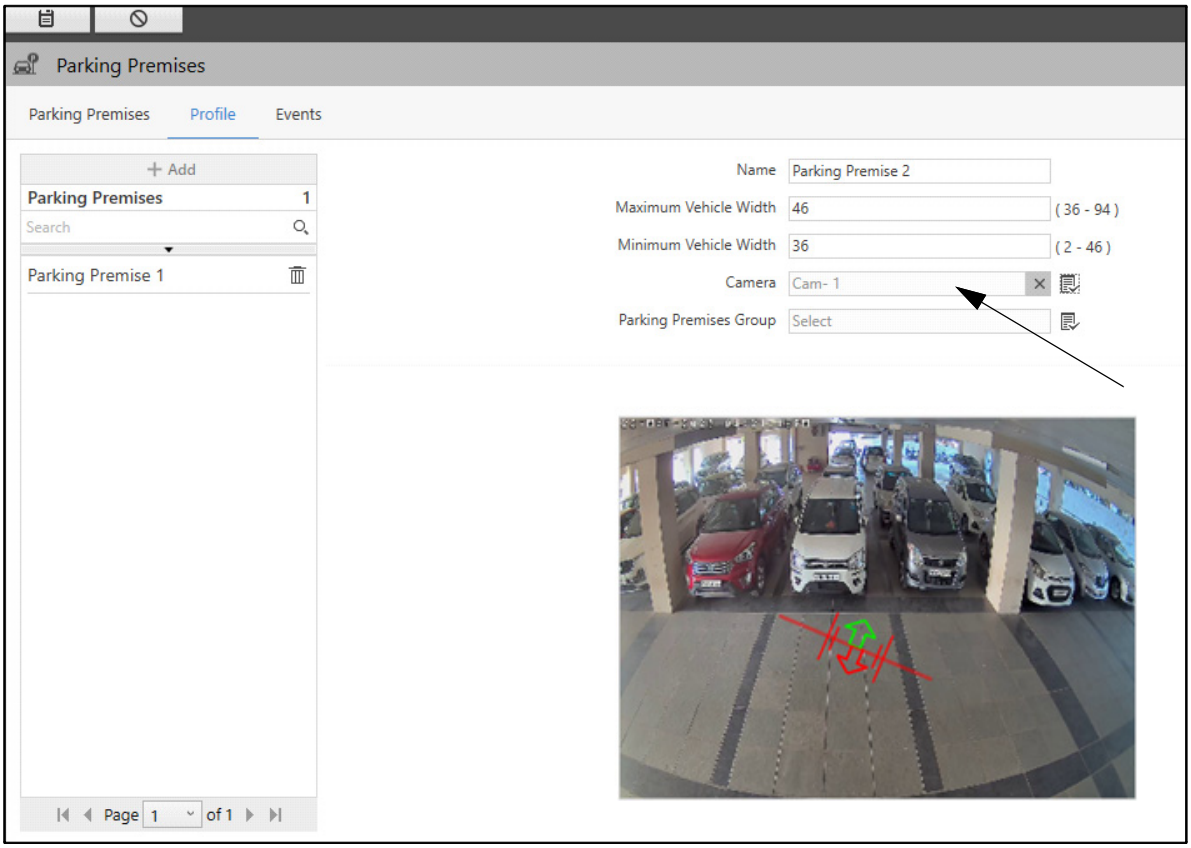


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to "Component Group". Double-click the desired camera to assign it to the Parking Premises. You can also search for the desired cameras using the **Search Cameras** search bar.

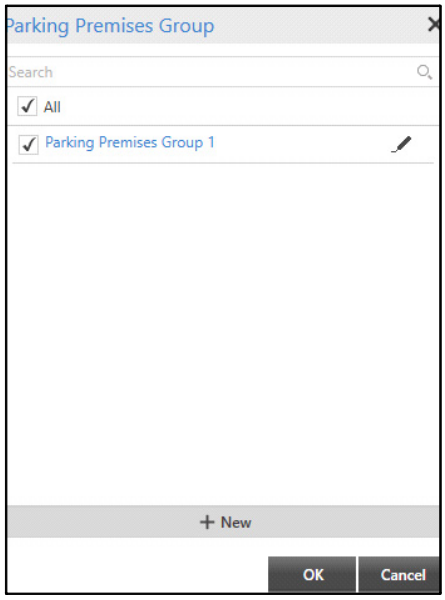


If you select a PTZ camera, you need to select the preset positions for it.

- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click to select the desired option.
  - Click **Go to selected position** , to move the camera to the selected preset position..
- To remove the camera, click **Remove** .



- **Parking Premises Group**: Select the desired Parking Premises Group which you wish to assign to the Parking Premise using the **Parking Premises Group** picklist.
    - Click **Parking Premises Group** picklist. The **Parking Premises Group** pop-up appears.



- Select the desired Parking Premises from the list. You can edit an existing Parking Premises Group by clicking on **Edit** . You can also configure a new Parking Premises Group by clicking **New**. For more details, refer to “Parking Premises Group”.

- Click **OK** to confirm or click **Cancel** to discard.

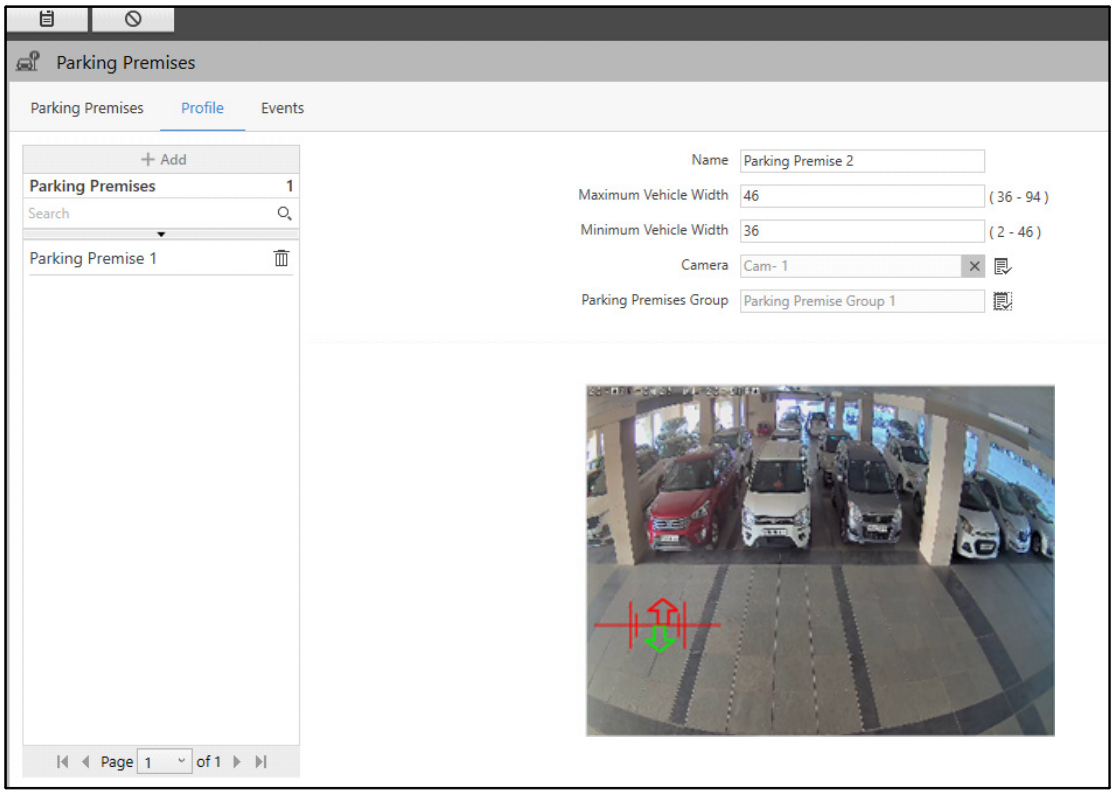
Once a camera is assigned, you can draw the Parking Premises on the live view of the camera.

- Drag the line to increase or decrease the length of the line and set it as desired.

  You can also drag it to change the Entry (Green arrow) and Exit (Red arrow) direction. To do so,

  Move the mouse pointer to any one end of the line, a four direction arrow appears.

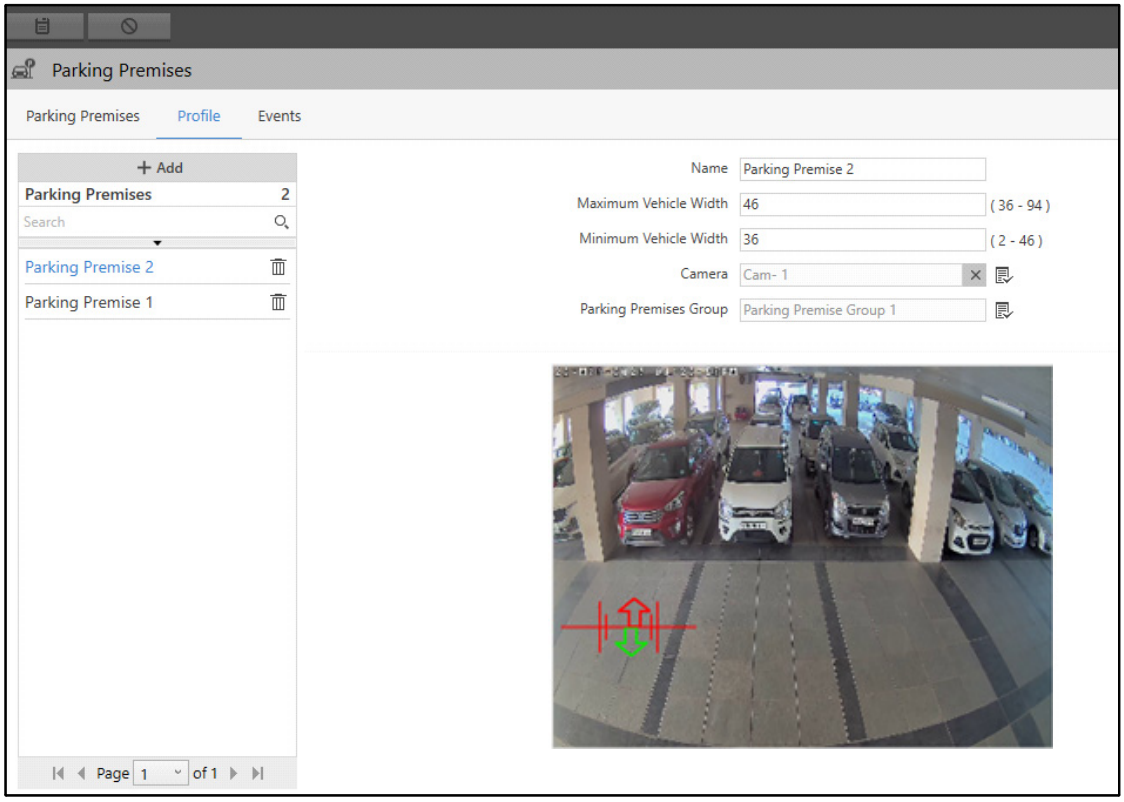
  Now, drag it in the desired direction.



- Click **Save** to save the settings or **Cancel** to discard.

The new Parking Premise will appear in the list on the left hand side.

You can edit the configurations of the Parking Premise or delete it.



- Select the desired Parking Premise from the list and edit the details on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the Parking Premise.

Similarly, you can configure the other Parking Premises.

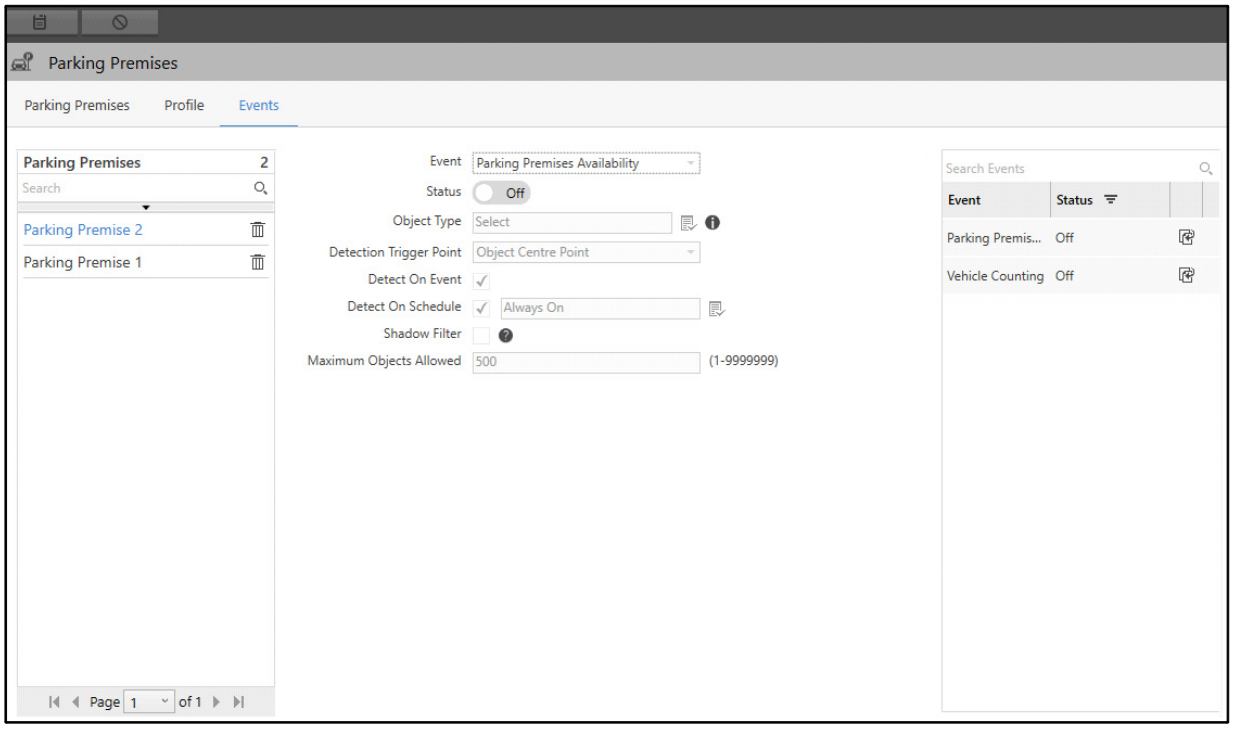
Events

This tab enables you to configure the Events for the Parking Premises. All the configured Events appear under the **Parking Premises** tab.

Maximum and Minimum Vehicle Width configured in any "Profile" will not be applicable if you select Object Type in any Event.

To configure an Event,

- Click the **Events** tab.



For Parking Premises, you can configure two types of Events — “Parking Premises Availability” and “Vehicle Counting”.

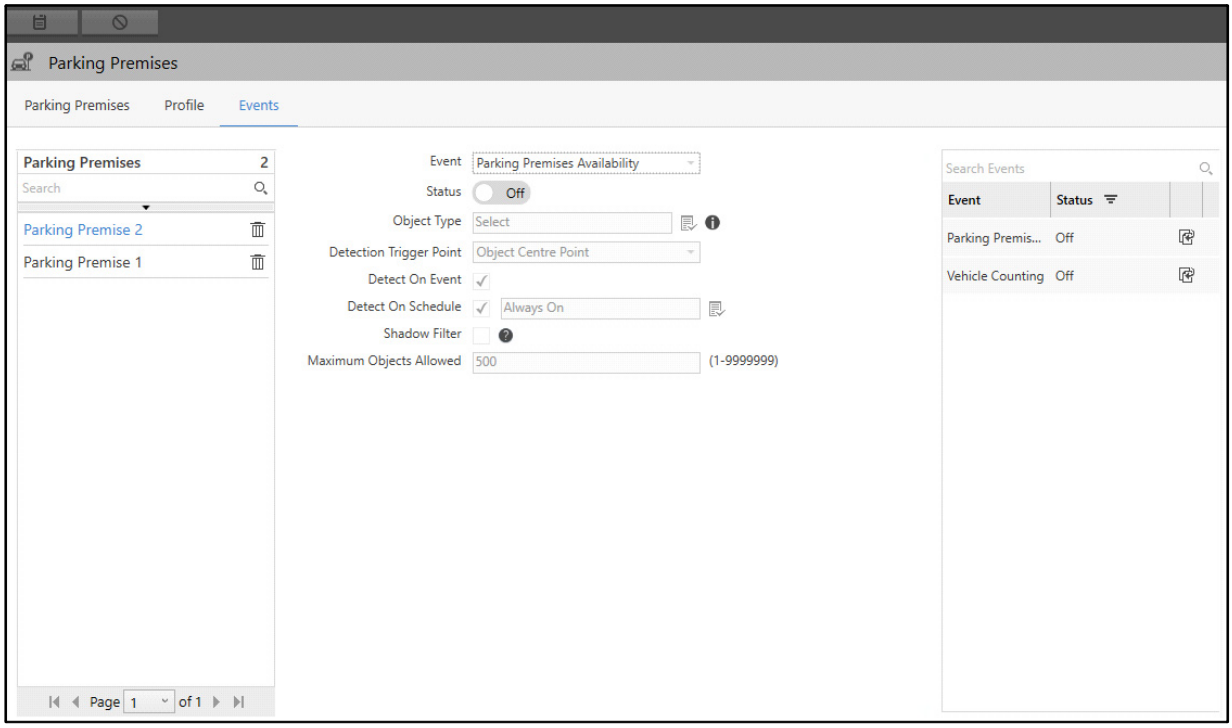
Parking Premises Availability

The Parking Premises Availability feature is used for keeping records of Premise availability for parking. This helps you to know whether the configured premise is full or not and if not full then how much space is remaining in the premises.

Based on the configured **Maximum Objects Allowed** count, if a vehicle moves towards Red Arrow (Exit), then **Premise Availability** event will be generated, whereas if a vehicle moves towards the Green Arrow (Entry), the **Premise Full** event will be generated.

To configure Parking Premises Availability Event for Parking Premises,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

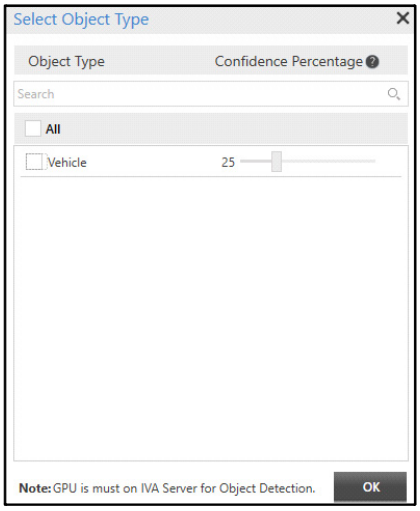


Configure the following parameters:

- **Event**: Select the Parking Premises Availability Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

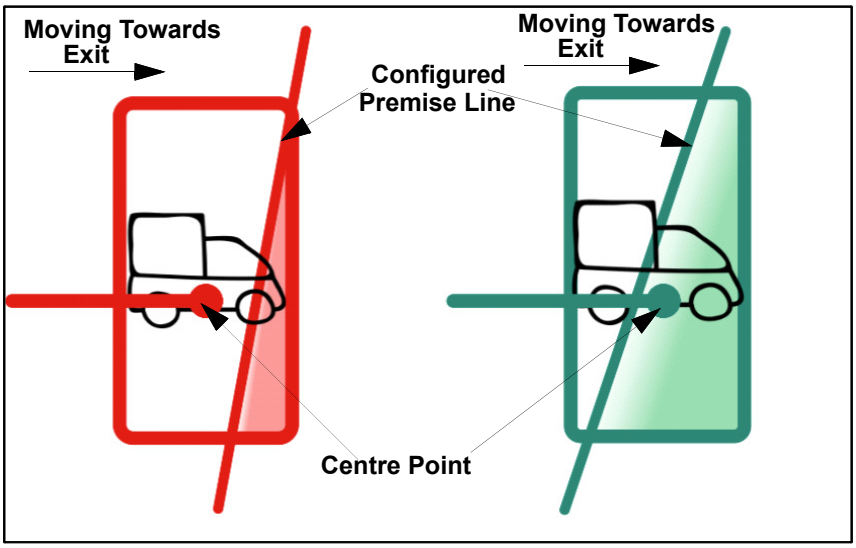


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point. Based on the selected option, the IVA engine will detect the selected Object Type.

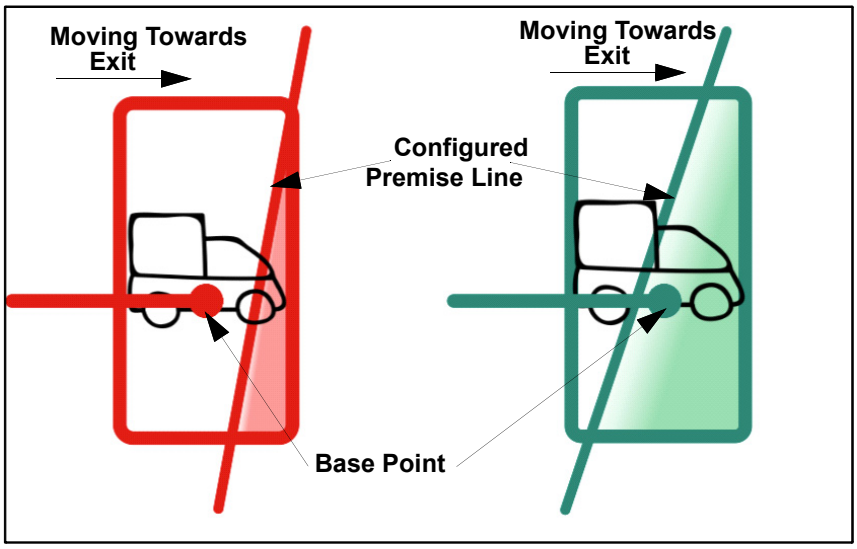
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured premise line.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point crosses the configured premise line, an event will be generated if the object is moving away from the premise line. That is, the Premise will be said to be Available for parking when the vehicle moves away from the premise line in the direction of Red Arrow (Exit) on the configured premise line.

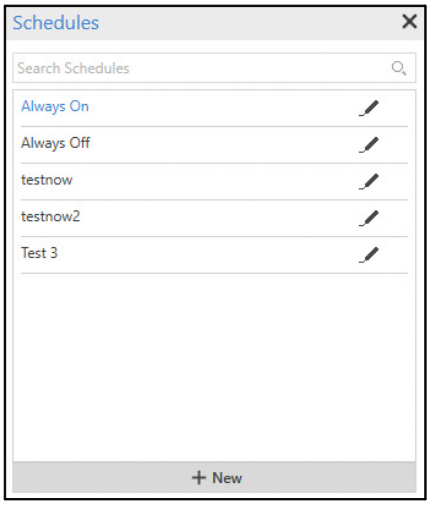


  If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured premise line.

  In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured premise line, an event will be generated if the object is moving away from the premise line. That is, the Premise will be said to be Available for parking when the vehicle moves away from the premise line in the direction of Red Arrow (Exit) on the configured premise line.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.
- **Shadow Filter**: Select the check box to ignore the shadow of the people/objects crossing the Parking Premises and reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Maximum Objects Allowed**: Specify the number of objects/vehicles allowed in the Parking Premises. Valid Range: 1 to 9999999. Default: 500.

- Click **Save** to save the settings or **Cancel** to discard.

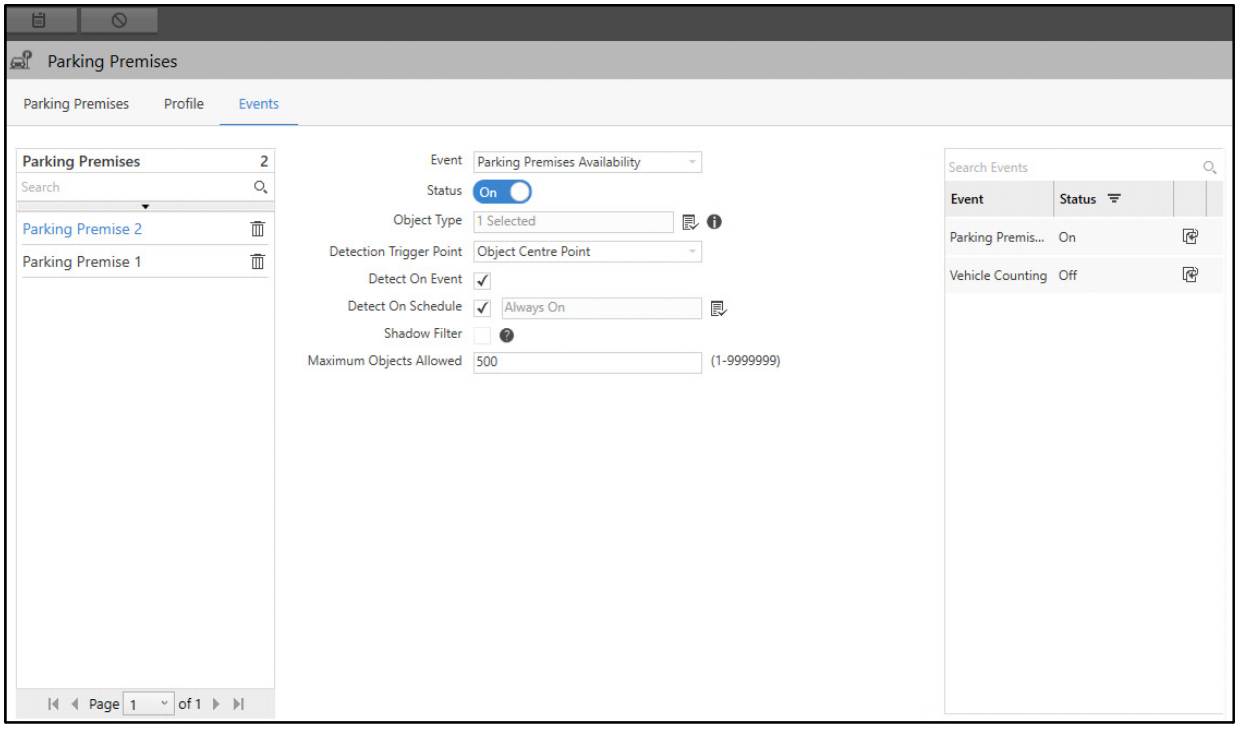
Once you have configured the Event, you can edit its configurations or disable it.

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

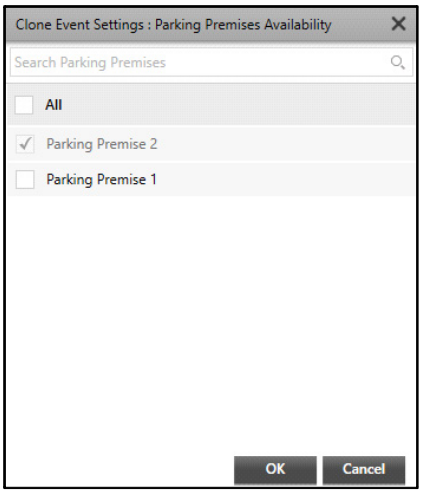
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Parking Premises is created, the **Clone Event Settings** option gets enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Parking Premises Availability** pop-up appears.



- Select the desired parking premises to which you wish to copy the Event configurations.

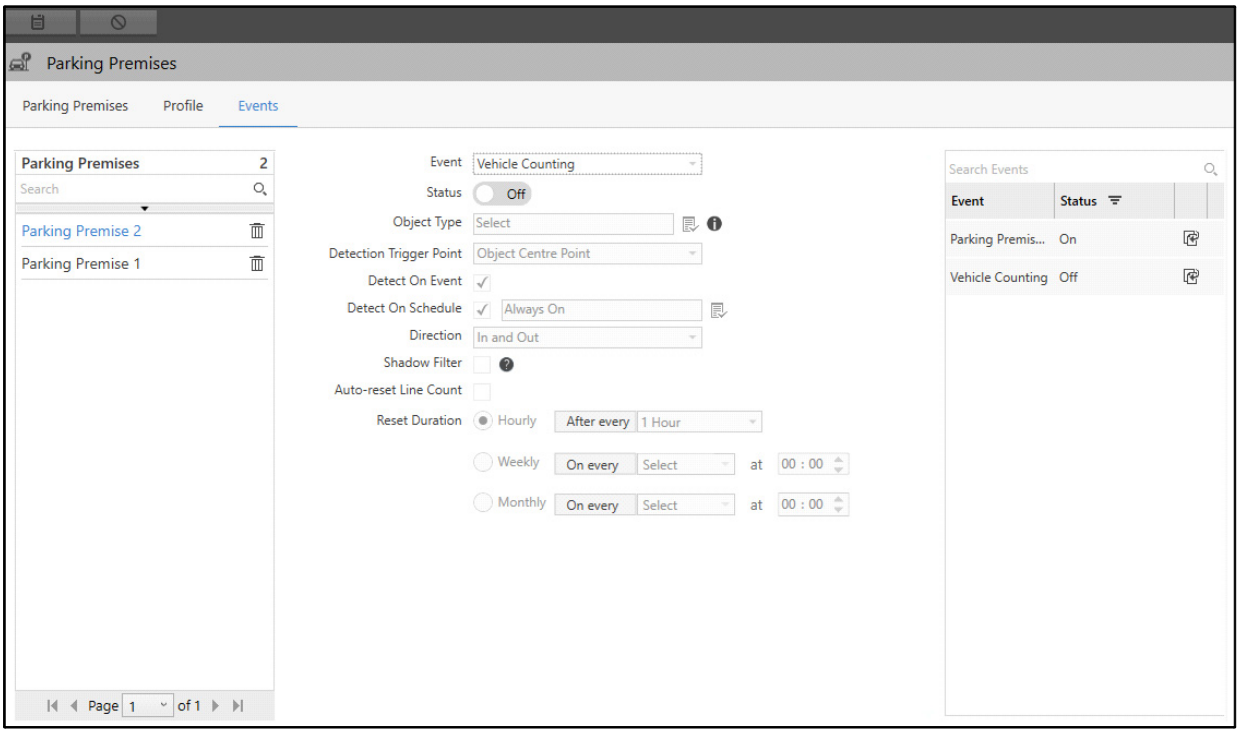
- Click **OK** to confirm or click **Cancel** to discard.

Vehicle Counting

The Vehicle Counting feature is used for keeping records of vehicle count in a Parking Premise.

To configure Vehicle Counting Event for Parking Premises,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

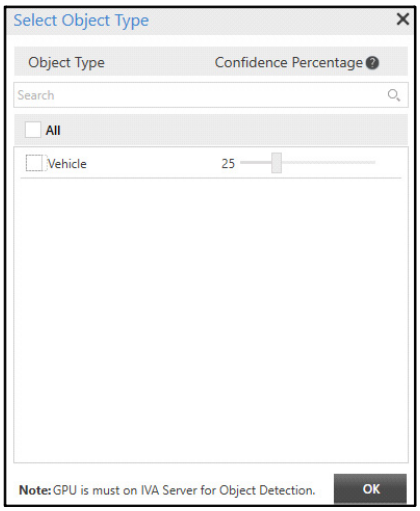


Configure the following parameters:

- **Event**: Select the Vehicle Counting Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

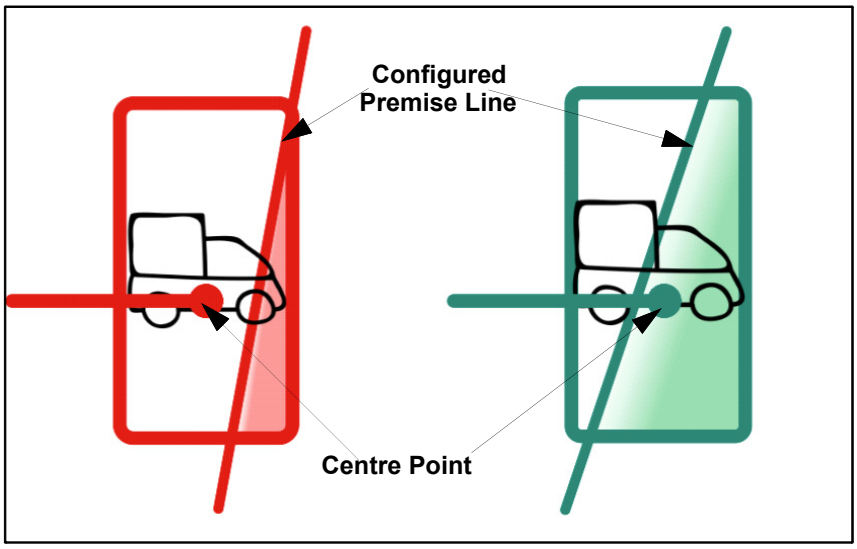


  - Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection.Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point. Based on the selected option, the IVA engine will detect the selected Object Type.

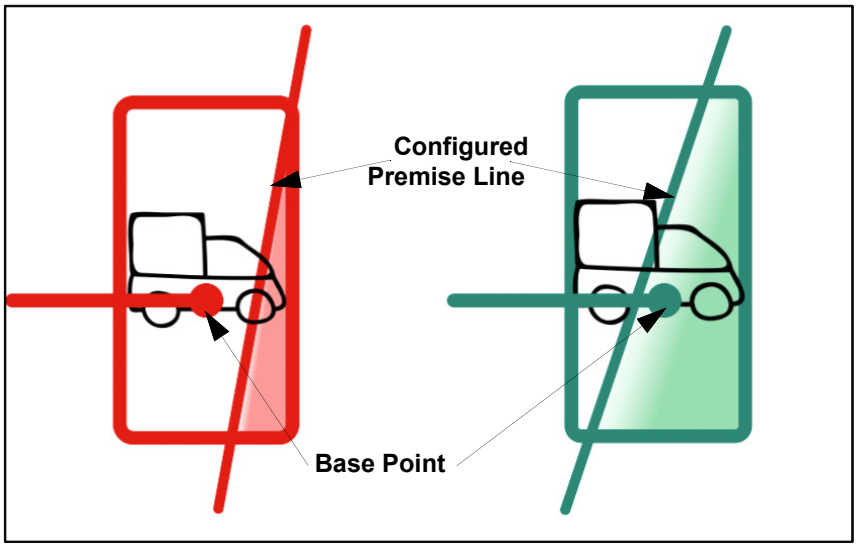
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured premise line.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point of the object crosses the configured premise line in the direction of Red (Exit)/Green (Entry) Arrow, an event will be generated.

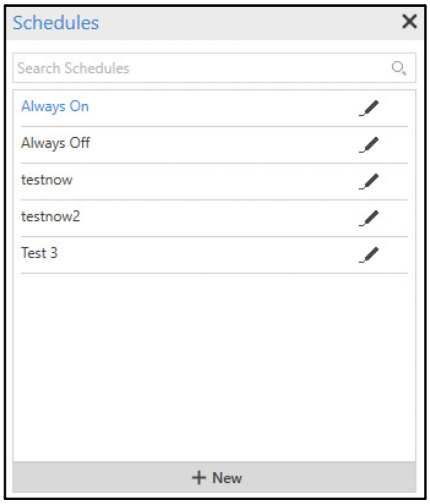


If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured premise line.

In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured premise line in the direction of Red (Exit)/Green (Entry) Arrow, an event will be generated.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Direction**: Select the direction for the vehicle count from the drop-down list options — In and Out, In, Out.

  Select **In**, if the Event should occur only when a vehicle enters the premises.

  Select **Out**, if the Event should occur only when a vehicle moves out of the premises.

  Select **In and Out**, if the Event should occur when a vehicle enters or moves out of the premises.

- **Shadow Filter**: Select the check box to ignore the shadow of the people/objects crossing the Parking Premises and reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Auto-reset Line Count**: Select the check box if you wish the Vehicle Counting Line counter to reset to zero. If you enable this option, you must configure the Reset Duration.

By default counter will not be reset till 99999999. You can reset the counter by selecting a value from the drop-down list.

- **Reset Duration**: Select the Reset Duration from the options — Hourly, Weekly or Monthly to auto-reset the Line counter.

  - **Hourly:** Select this option to auto-reset the Line counter hourly and select the desired interval from the drop-down list. The Line counter will reset automatically as per the selected interval.

    For example, if you select **1 Hour**, from the drop-down list, then Line counter will be reset automatically after every 1 Hour.

  - **Weekly:** Select this option to auto-reset the Line counter on a particular day of the week and at the chosen time. You can select multiple days of week. Select the desired day from the drop-down list and specify the desired time.

For example, if you select **Monday** and **Wednesday** from the drop-down list and set the time as 18:00, the Line counter will reset on every Monday and Wednesday of the week at 6 PM.

- **Monthly:** Select this option to auto-reset the Line counter on a particular date of the month and at the chosen time. You can select multiple dates of the month. Select the desired date from the drop-down list and specify the desired time.

  For example, if you select 1st and 25th date from the drop-down list and set the time as 18:00, the Line counter will reset on every 1st and 25th date of the month at 6 PM.

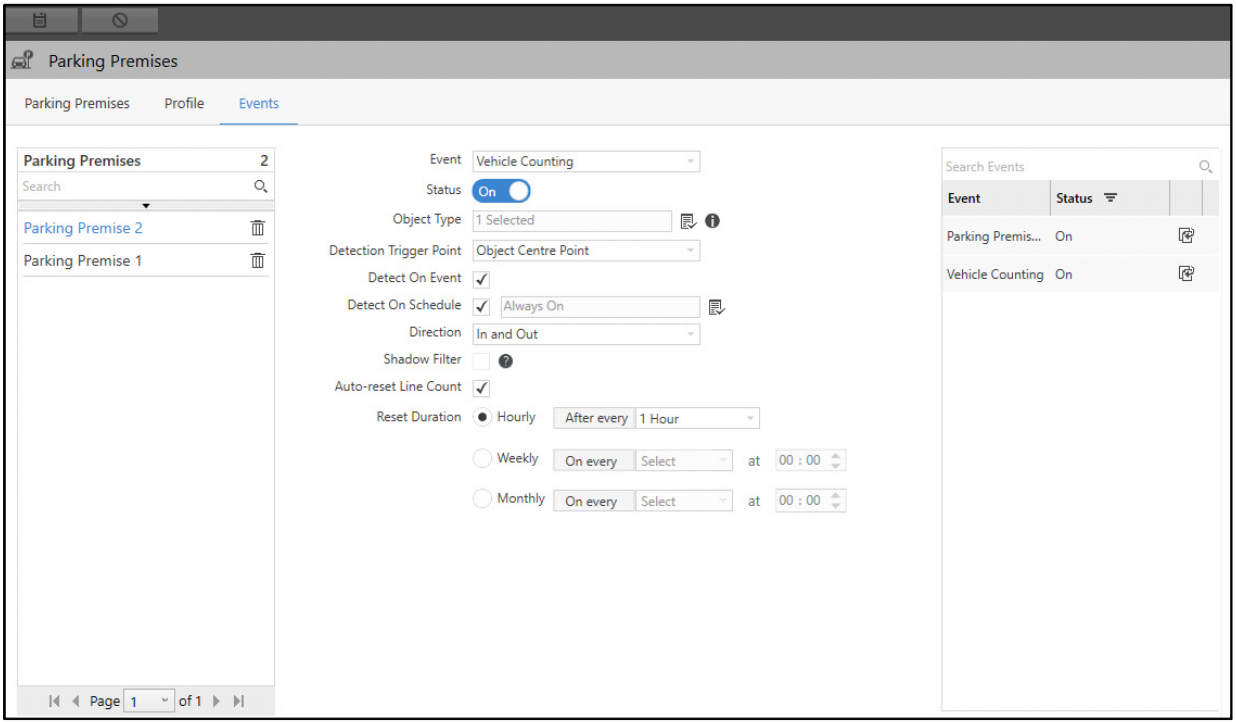
- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

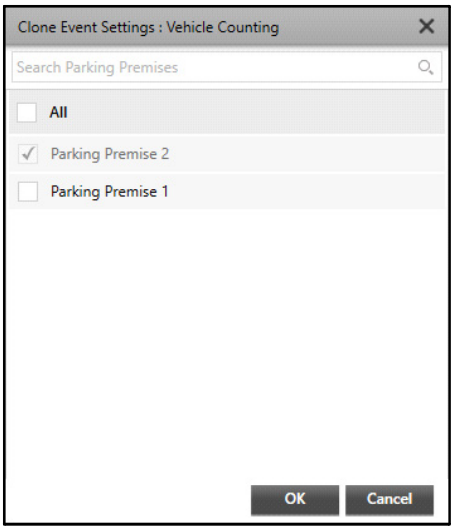
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Vehicle Counting** pop-up appears.



- Select the desired parking premises to which you wish to copy the Event configurations.

- Click **OK** to confirm or click **Cancel** to discard.

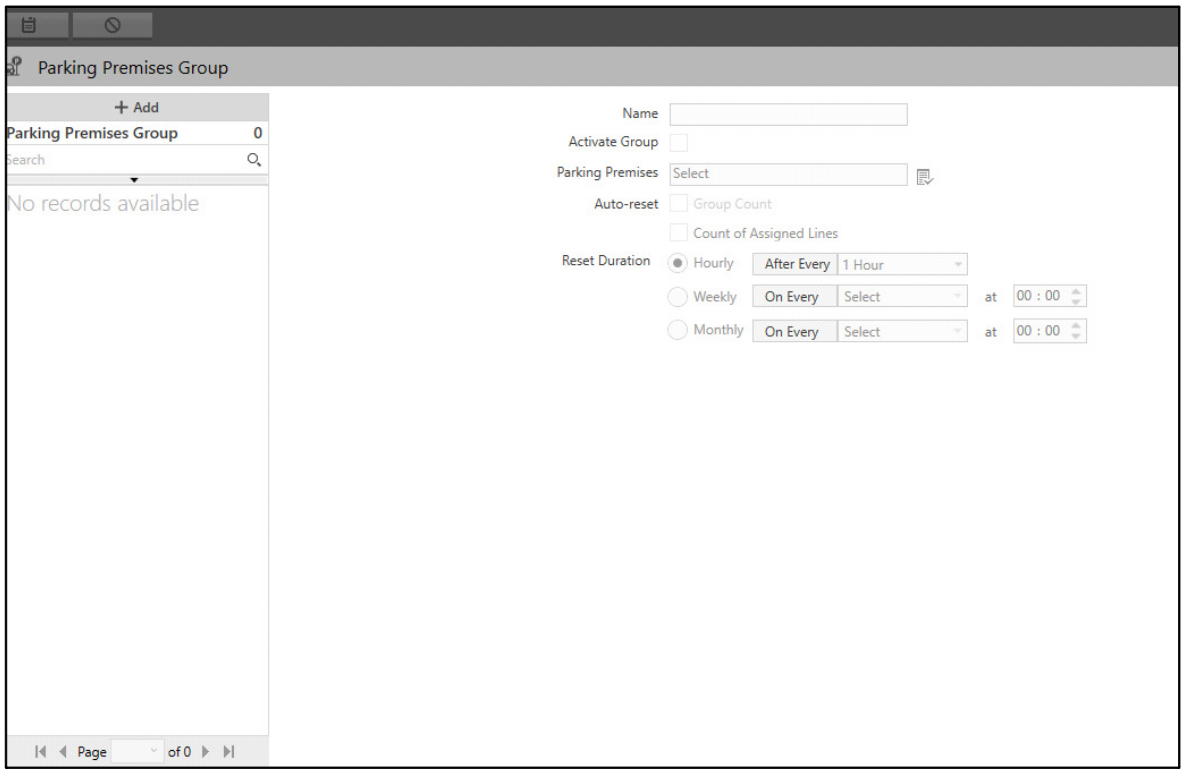
Parking Premises Group

Parking Premises Groups are the logical groups of Parking Premises configured for the Parking Premises Events. This feature is useful in a situation where a premise has different entry and exit gates and the user needs a cumulative sum of all these entry and exit points. This helps the user to get a clear view of the number of vehicles entering and exiting the premise.

The Parking Premises Group page displays all the configured Parking Premises Groups. You can view and configure Parking Premises Groups from this page.

To configure Parking Premises Group,

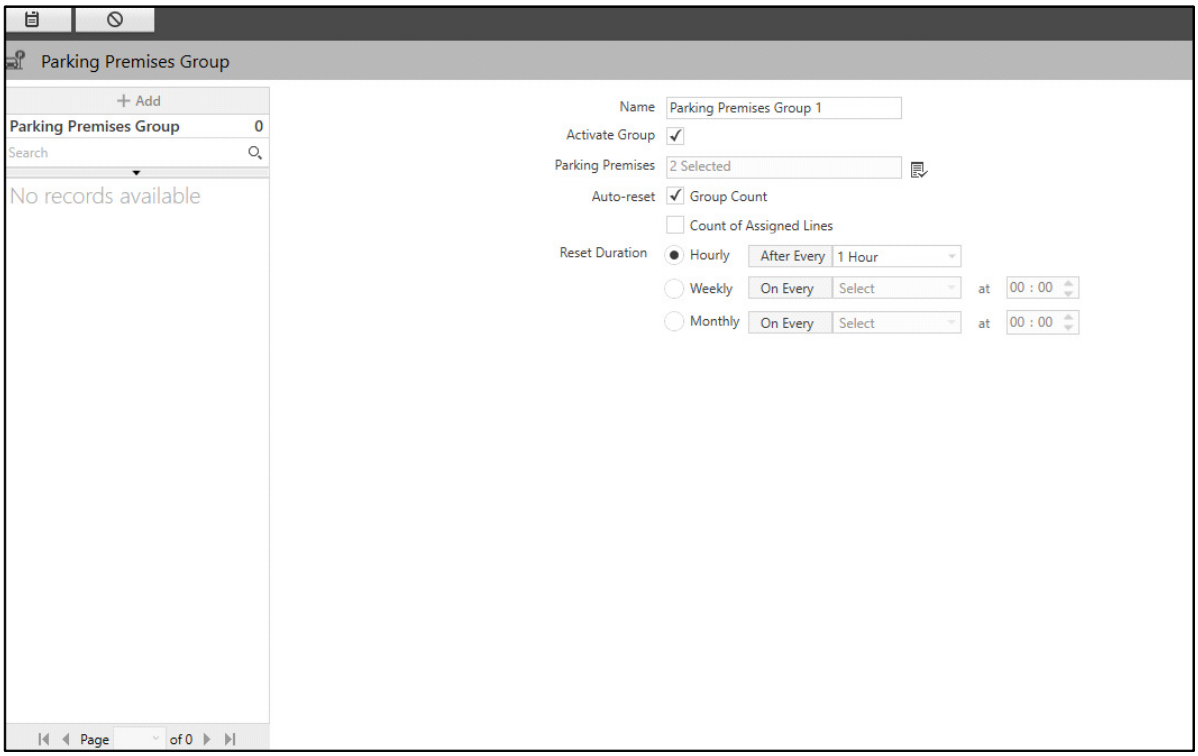
- Click **Parking Management > Security Sections > Parking Premises Group**.



The entity name (Parking Premises Group) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities". The reflection will be seen everywhere in Admin Client.

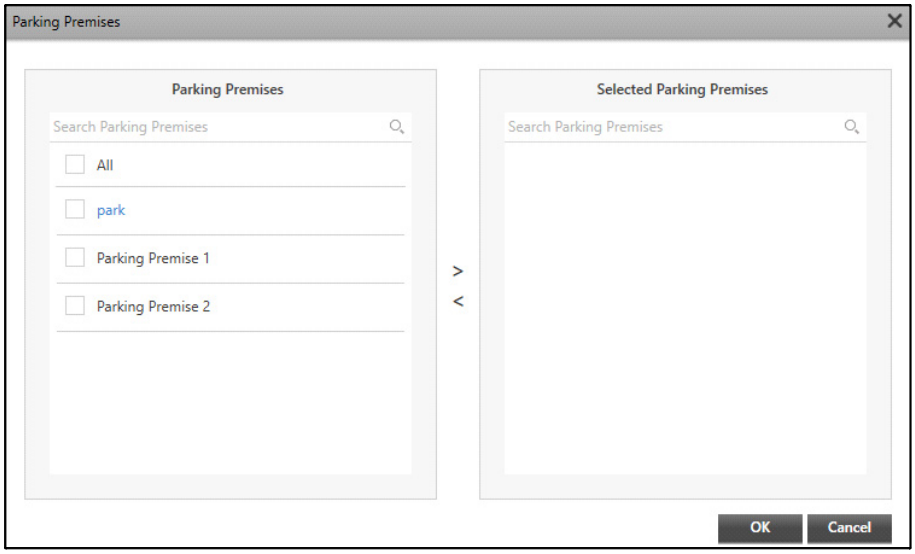
*The **Add** button is disabled when you are configuring Level for the first time. You can directly configure the parameters and save the Level.*

- Click **Add**.



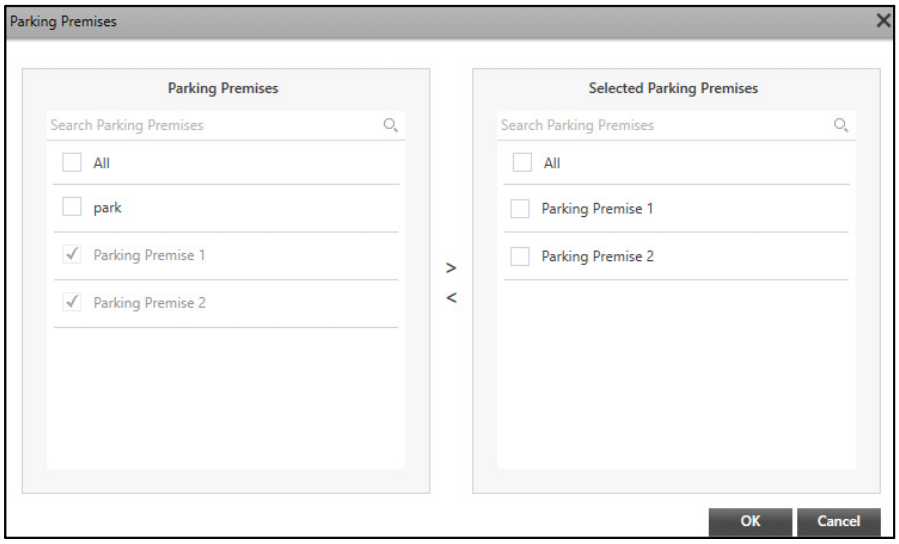
Configure the following parameters:

- **Name:** Specify a suitable name for the Parking Premises Group.In Name, you can enter upto 50 characters. Default: Blank.
- **Activate Group:** Select the check box to activate the group.
- **Parking Premises**: Select the desired Parking Premises which you wish to assign to the Parking Premises Group using the **Select Parking Premises** picklist.
  - Click **Select Parking Premises** picklist. The **Parking Premises** pop-up appears.



- All the configured Parking Premises appear in the list. To configure Parking Premises, refer to "Parking Premises". Select the check boxes of the desired Parking Premises you wish to select from the list. Click the right arrow button to add those Parking Premises in the **Selected Parking Premises** list. You can also search for the desired Parking Premises using the **Search Parking Premises** search bar.

  To remove Parking Premises, select the check boxes of the desired Parking Premises you wish to remove from the Selected Parking Premises list. Click the left arrow button to remove the Parking Premises from the Selected Parking Premises list.



- Click **OK** to confirm or click **Cancel** to discard.

Auto-reset

- **Auto-reset Group Count**: Select the check box to automatically reset the Group Count of the Parking Premises Events. If this check box is enabled then the other parameters can be configured.

- **Count of Assigned Lines**: If Group Count is enabled, then only you can select this check box. Select the check box to automatically reset the count of the Lines assigned to the Group. If the same Lines are assigned to multiple groups, the Line count is reset for all the Groups.

If Auto-reset check box is not enabled, then the counter will not reset automatically. It can be reset either manually or when the counter reaches its limit, that is, till 999999999. Reset is done by the Management Server for selected Group.

- **Reset Duration**: Select the Reset Duration from the options — Hourly, Weekly or Monthly to auto-reset the Line counter.

  - **Hourly:** Select this option to auto-reset the Group/Line counter hourly and select the desired interval from the drop-down list. The Group/Line counter will reset automatically as per the selected interval.

    For example, if you select **1 Hour**, from the drop-down list, then Group/Line counter will be reset automatically after every 1 Hour.

- **Weekly:** Select this option to auto-reset the Group/Line counter on a particular day of the week and at the chosen time. You can select multiple days of week. Select the desired day from the drop-down list and specify the desired time.

  For example, if you select **Monday** and **Wednesday** from the drop-down list and set the time as 18:00, the Group/Line counter will reset on every Monday and Wednesday of the week at 6 PM.

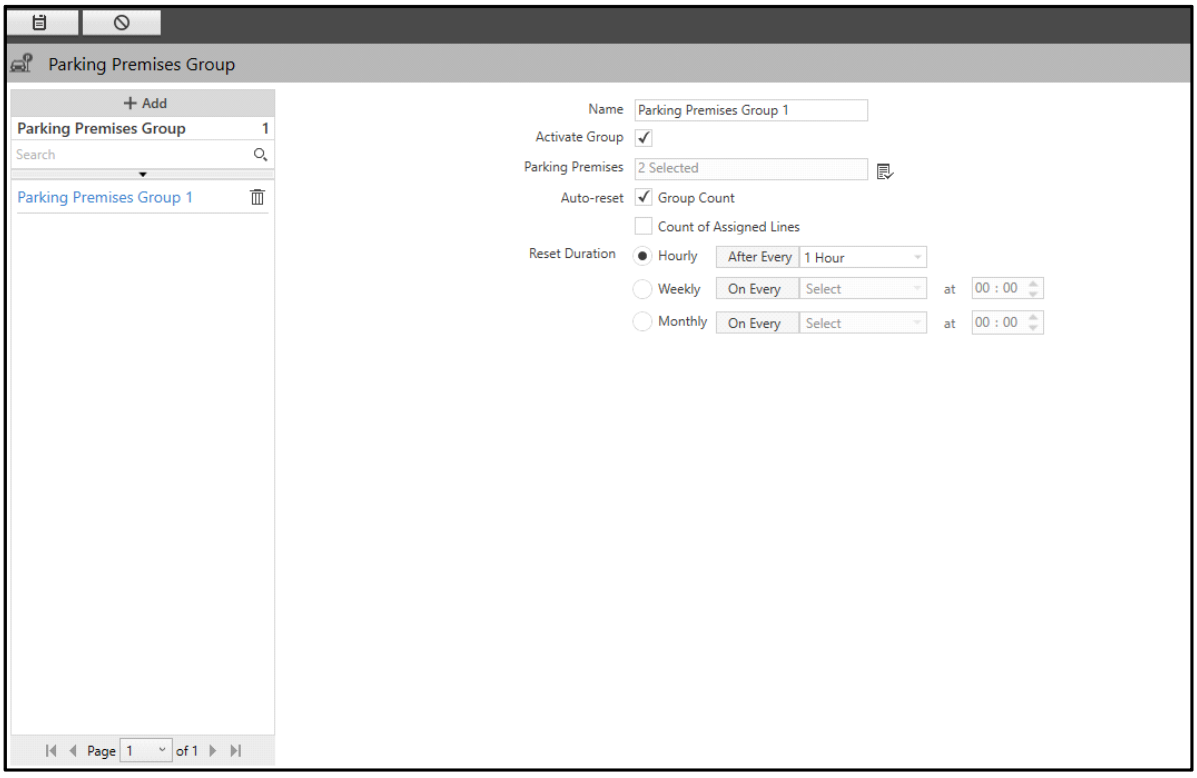
- **Monthly:** Select this option to auto-reset the Group/Line counter on a particular date of the month and at the chosen time. You can select multiple dates of the month. Select the desired date from the drop-down list and specify the desired time.

  For example, if you select 1st and 25th date from the drop-down list and set the time as 18:00, the Group/Line counter will reset on every 1st and 25th date of the month at 6 PM.

- Click **Save** to save the settings or **Cancel** to discard.

The Parking Premises Group appears in the list on the left hand side.

You can edit the configurations of the Parking Premises Group or delete it.



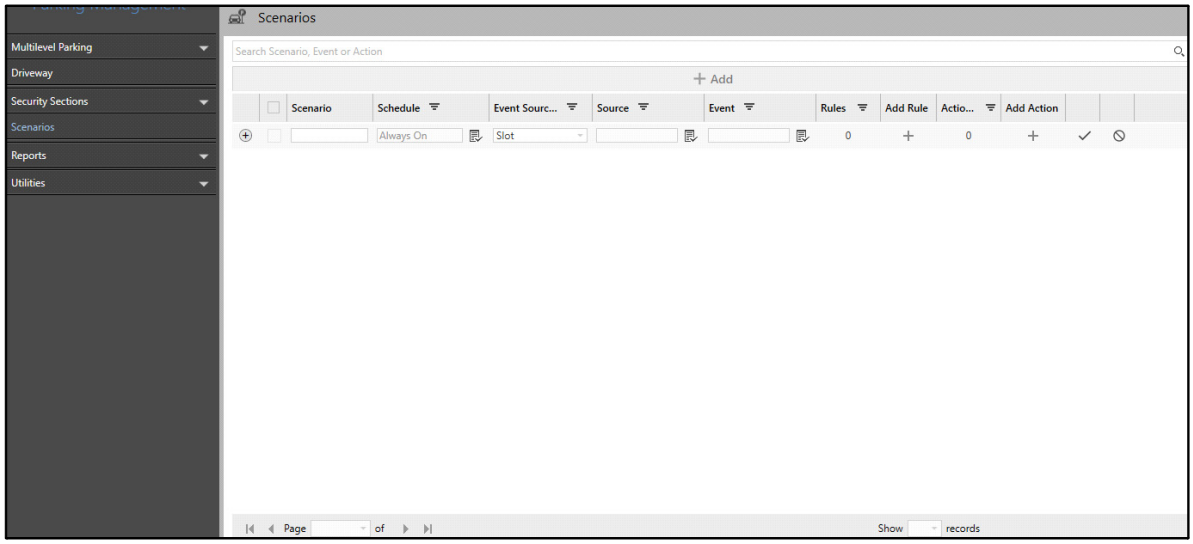
- Select the desired Parking Premises Group from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
  - Click **Delete** to delete the Parking Premises Group.

Parking Management- Scenarios

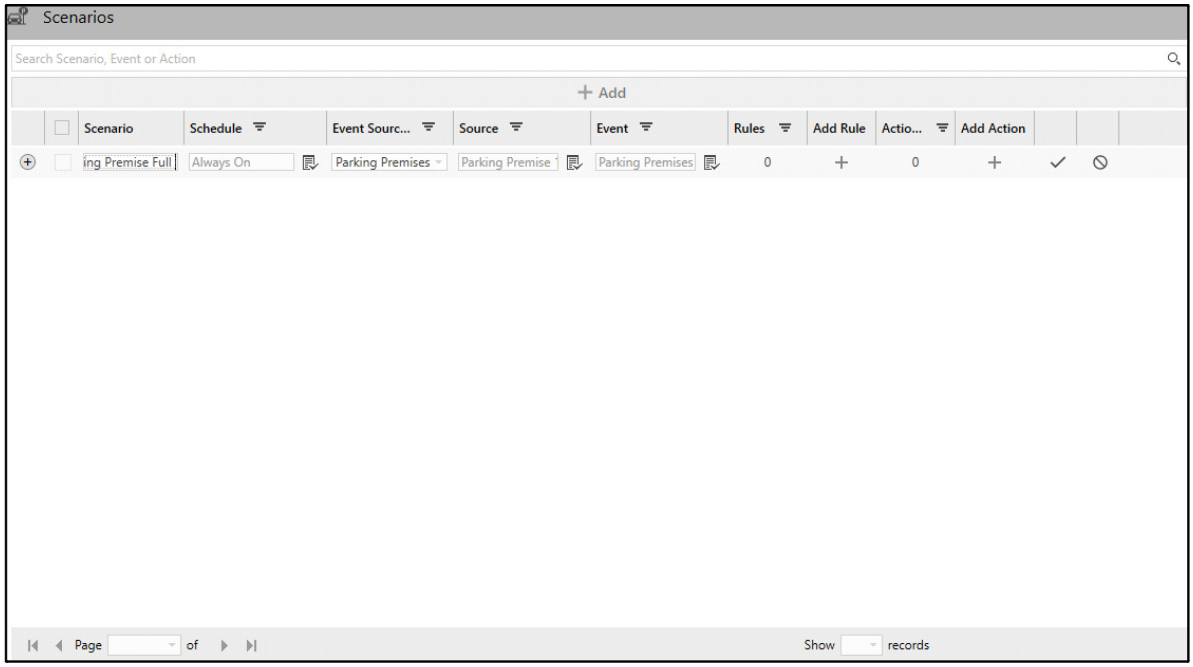
In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send SMS) on Events occurring at certain sources (For example, Parking Premises Full). The Scenarios page displays all the Scenarios configured for Parking Management. You can view and configure the Scenarios for all the configured Slots, Slot Groups, Lanes, Areas, Levels, Facilities and Driveways.

To configure Scenarios,

- Click **Parking Management > Scenarios**.



- Click **Add.**



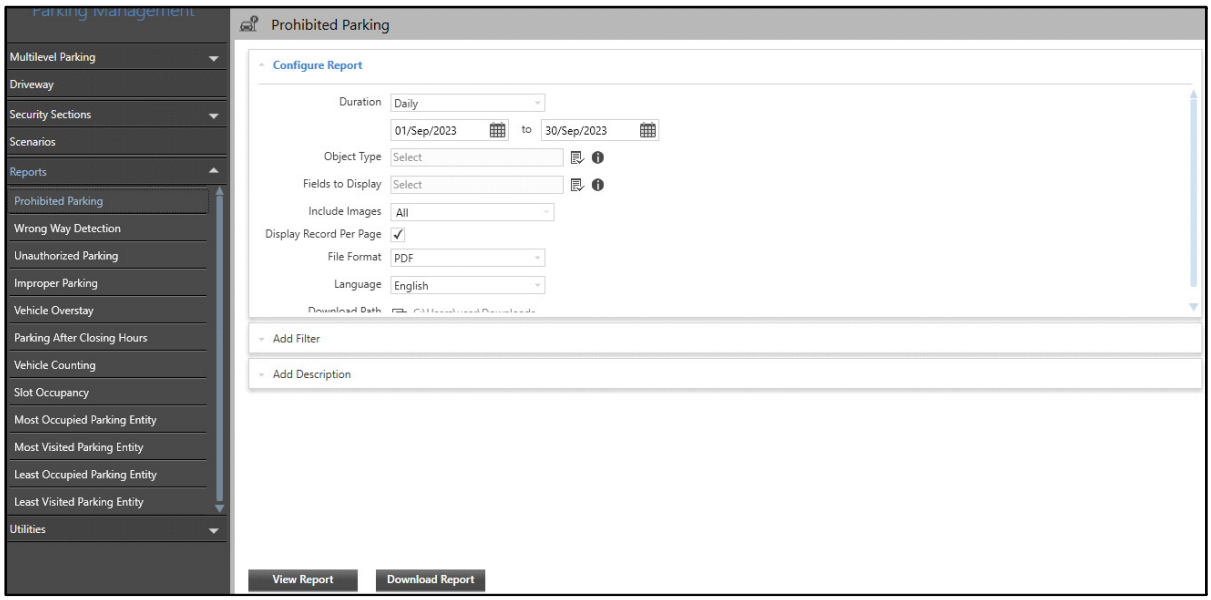
The configurations of Scenarios for Parking Management are similar to the Basic Scenario. For details, refer to “Basic Scenario”.

Parking Management - Reports

The Reports page enables you to generate, view and download different types of Parking Event reports, such as Prohibited Parking, Wrong Way Detection, Unauthorized Parking, Improper Parking etc.

To configure Reports,

- Click **Parking Management > Reports**.



Refer to the following links for the configuration details of each type of report.

- “Prohibited Parking Report”
- “Wrong Way Detection Report”
- “Unauthorized Parking Report”
- “Improper Parking Report”
- “Vehicle Overstay Report”
- “Parking After Closing Hours Report”
- “Vehicle Counting Report”
- “Slot Occupancy Reports”
- “Most Occupied Parking Entity Report”
- “Most Visited Parking Entity Report”
- “Least Occupied Parking Entity Report”
- “Least Visited Parking Entity Report”

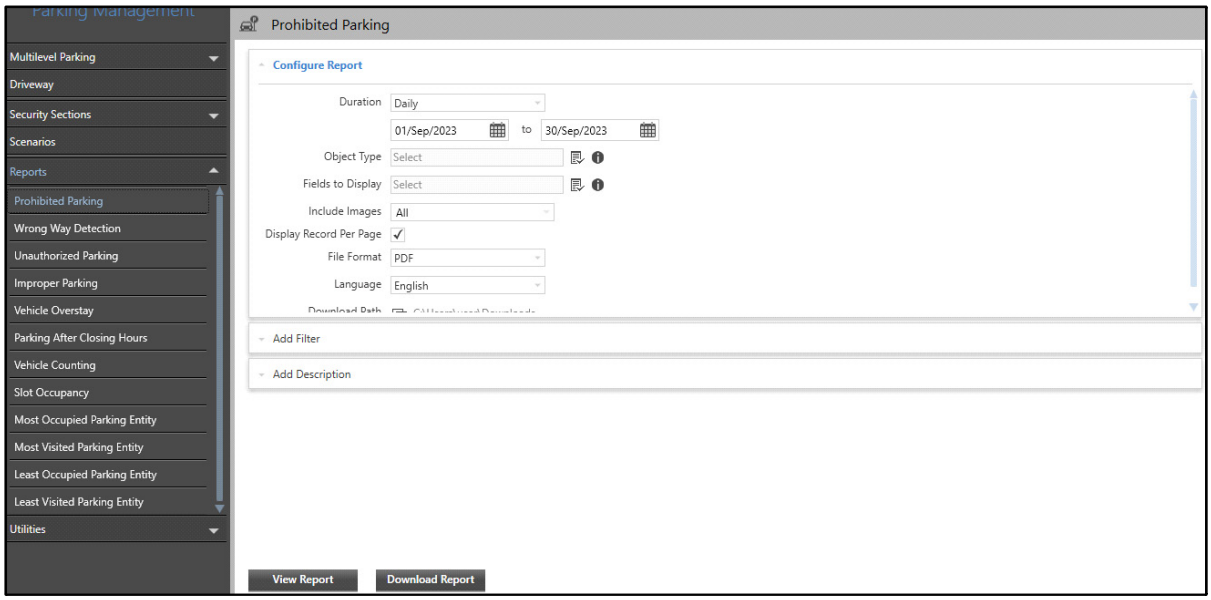
Prohibited Parking Report

Prohibited Parking Report can play a vital role to manage traffic and prevent illegal parking. This report is useful in Traffic Management System. It can also be useful at places such as parking of a mall or building or roadside. Based on this report, illegal parking can be tracked efficiently and actions can be taken accordingly.

The Prohibited Parking page enables you to configure parameters for Prohibited Parking Reports. You can view and configure Prohibited Parking Reports on Daily, Monthly and Hourly basis.

To configure Prohibited Parking Report,

- Click **Parking Management > Reports > Prohibited Parking**.



The Prohibited Parking page contains three collapsible panels — Configure Report, Add Filter and Add Description. For detailed configurations of the report, refer to “Report Configurations”.

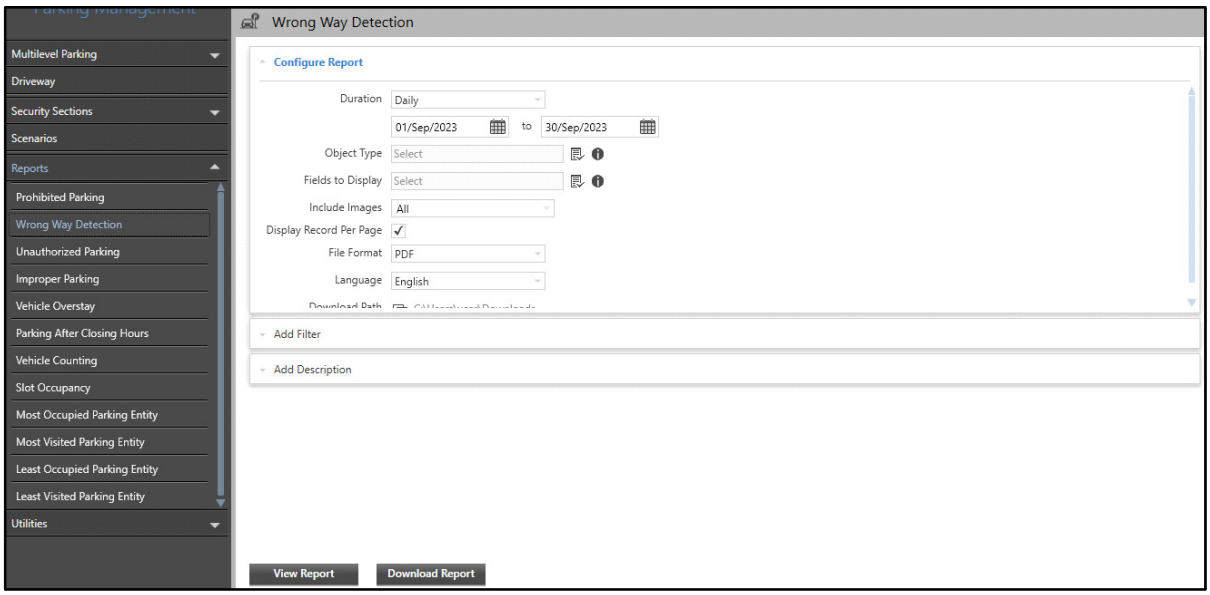
Wrong Way Detection Report

Wrong Way Detection Report can play a vital role to control the vehicles moving in the wrong direction. This report is useful at places such as malls, parking areas, buildings (school, colleges etc.) where only one entry and exit is present. Based on this report, wrong way movement can be tracked efficiently and actions can be taken accordingly.

The Wrong Way Detection page enables you to configure parameters for Wrong Way Detection Reports. You can view and configure Wrong Way Detection Reports on Daily, Monthly and Hourly basis.

To configure Wrong Way Detection Report,

- Click **Parking Management > Reports > Wrong Way Detection**.



The Wrong Way Detection page contains three collapsible panels — Configure Report, Add Filter and Add Description. For detailed configurations of the report, refer to “Report Configurations”.

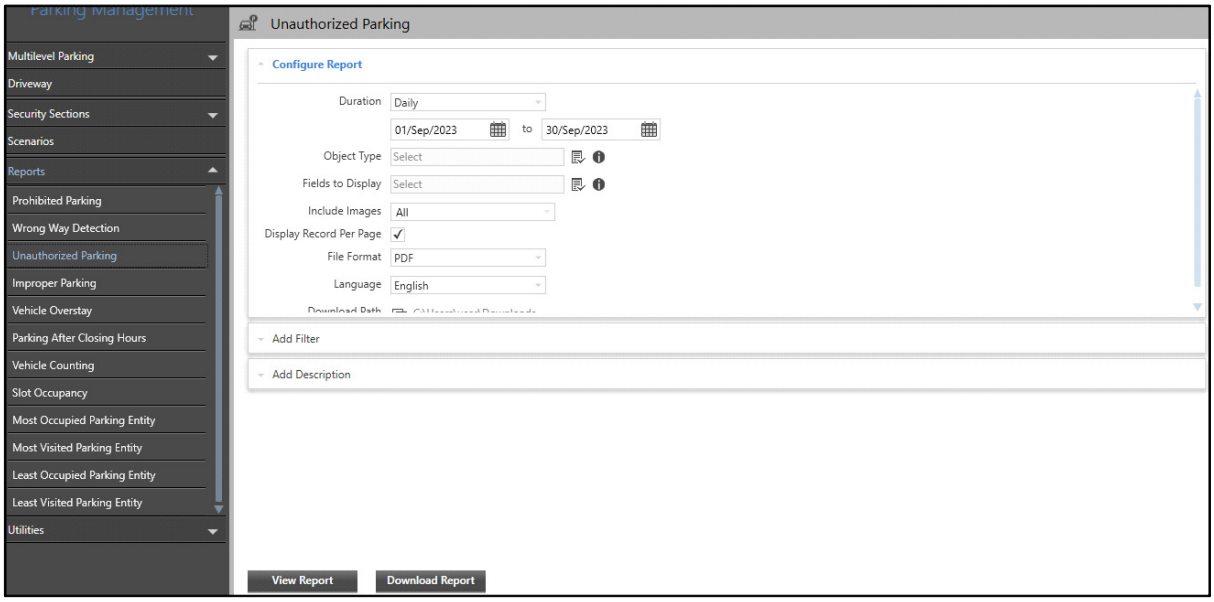
Unauthorized Parking Report

Unauthorized Parking Report can play a vital role at places such as office parking or residential parking, where the user is alloted a parking area based on an unique Vehicle Number. Based on this report, Unauthorized Parking can be tracked efficiently and actions can be taken accordingly.

The Unauthorized Parking page enables you to configure parameters for Unauthorized Parking Reports. You can view and configure Unauthorized Parking Reports on Daily, Monthly and Hourly basis.

To configure Unauthorized Parking Report,

- Click **Parking Management > Reports > Unauthorized Parking**.



The Unauthorized Parking page contains three collapsible panels — Configure Report, Add Filter and Add Description. For detailed configurations of the report, refer to “Report Configurations”.

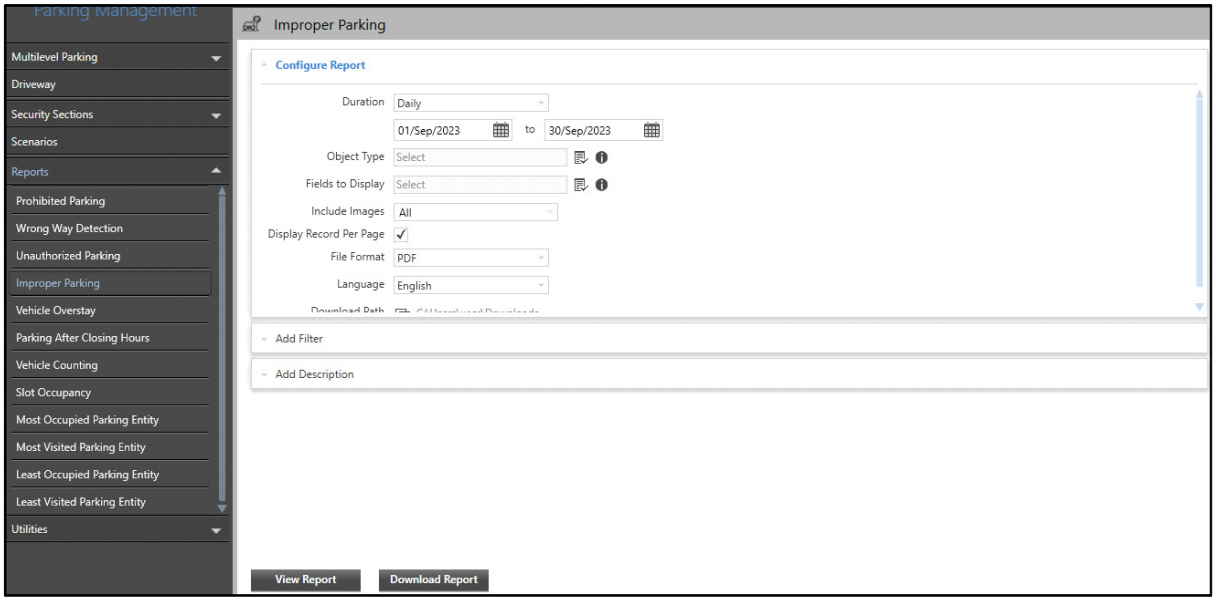
Improper Parking Report

Improper Parking Report can play a vital role at parking areas to track those vehicles which are not parked properly as per the defined parking slot in the parking area. Based on this report, Improper Parking can be tracked efficiently and actions can be taken accordingly.

The Improper Parking page enables you to configure parameters for Improper Parking Reports. You can view and configure Improper Parking Reports on Daily, Monthly and Hourly basis.

To configure Improper Parking Report,

- Click **Parking Management > Reports > Improper Parking**.



The Improper Parking page contains three collapsible panels — Configure Report, Add Filter and Add Description. For detailed configurations of the report, refer to “Report Configurations”.

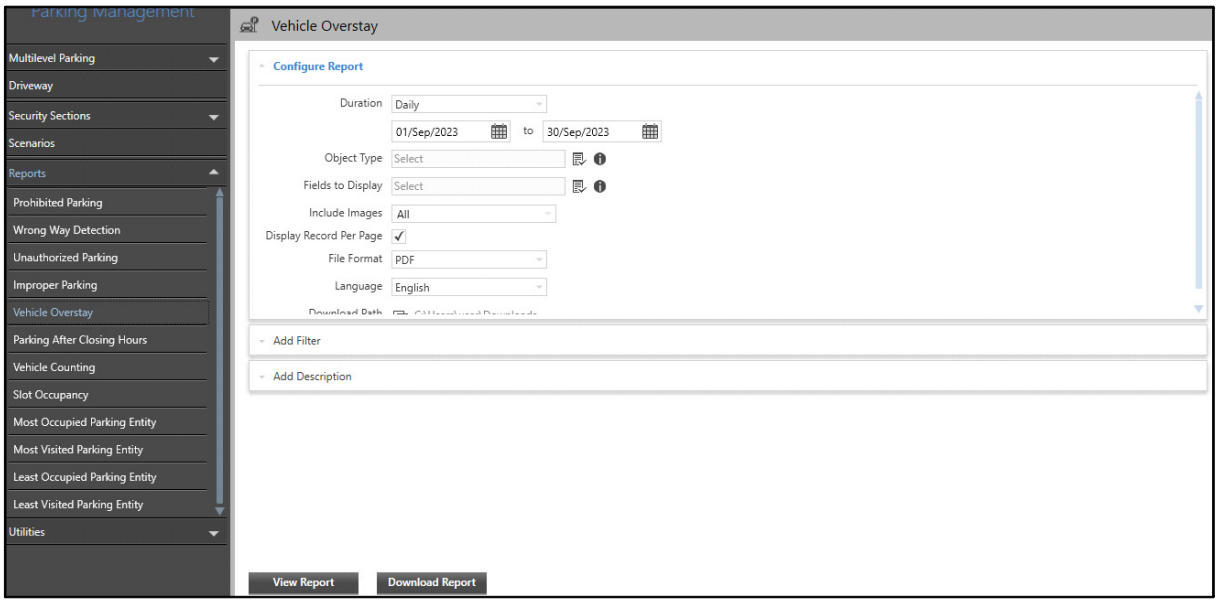
Vehicle Overstay Report

Vehicle Overstay Report can play a vital role in optimum utilization of the parking area. This report is useful at places such as mall parking, where the permitted duration for parking is defined. Based on this report, if a vehicle is found to be parked for more than the defined time, it can be tracked efficiently and actions can be taken accordingly.

The Vehicle Overstay page enables you to configure parameters for Vehicle Overstay Reports. You can view and configure Vehicle Overstay Reports on Daily, Monthly and Hourly basis.

To configure Vehicle Overstay Report,

- Click **Parking Management > Reports > Vehicle Overstay**.



The Vehicle Overstay page contains three collapsible panels — Configure Report, Add Filter and Add Description. For detailed configurations of the report, refer to “Report Configurations”.

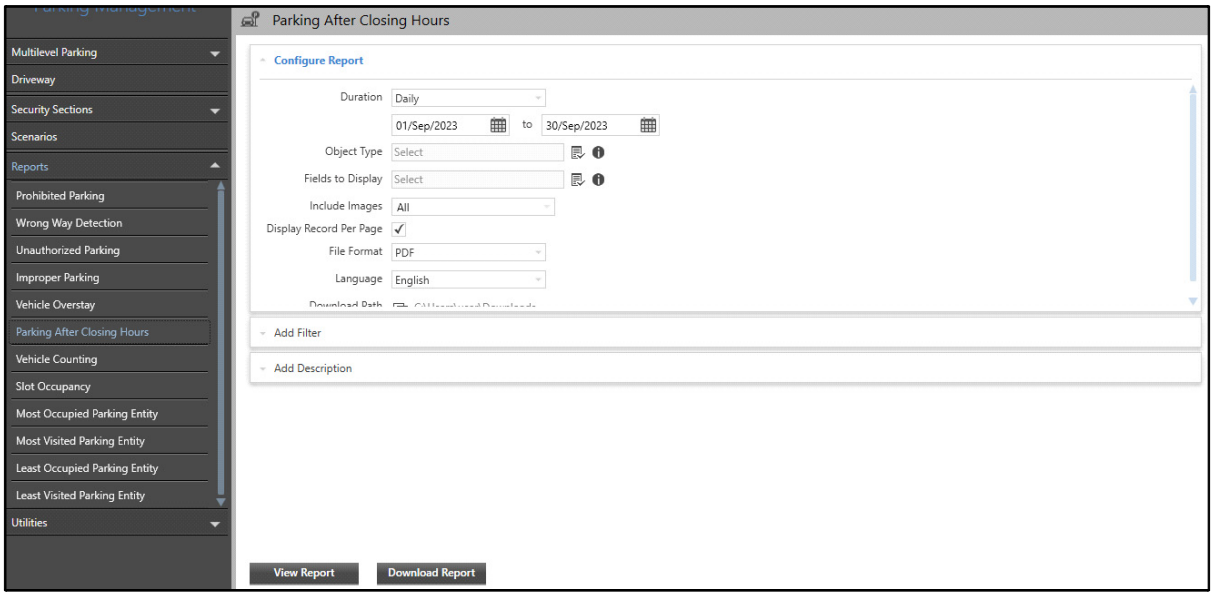
Parking After Closing Hours Report

Parking After Closing Hours Report can play a vital role to track those vehicles that are still parked in the premises even after the parking hours are over. This report is useful at the places such as mall parking, where security guard has to vacate the parking premises as per the mall closure timings. Based on this report, Parking After Closing Hours can be tracked efficiently and actions can be taken accordingly.

The Parking After Closing Hours page enables you to configure parameters for Parking After Closing Hours Reports. You can view and configure Parking After Closing Hours Reports on Daily, Monthly and Hourly basis.

To configure Parking After Closing Hours Report,

- Click **Parking Management > Reports > Parking After Closing Hours**.



The Parking After Closing Hours page contains three collapsible panels — Configure Report, Add Filter and Add Description. For detailed configurations of the report, refer to “Report Configurations”.

Report Configurations

Report configuration allows you to configure the desired reports and generate them as per your requirement. The generated report includes summarized data that can be analyzed and helps you to use the features more accurately and efficiently.

The report configurations are the same for the following types of reports.

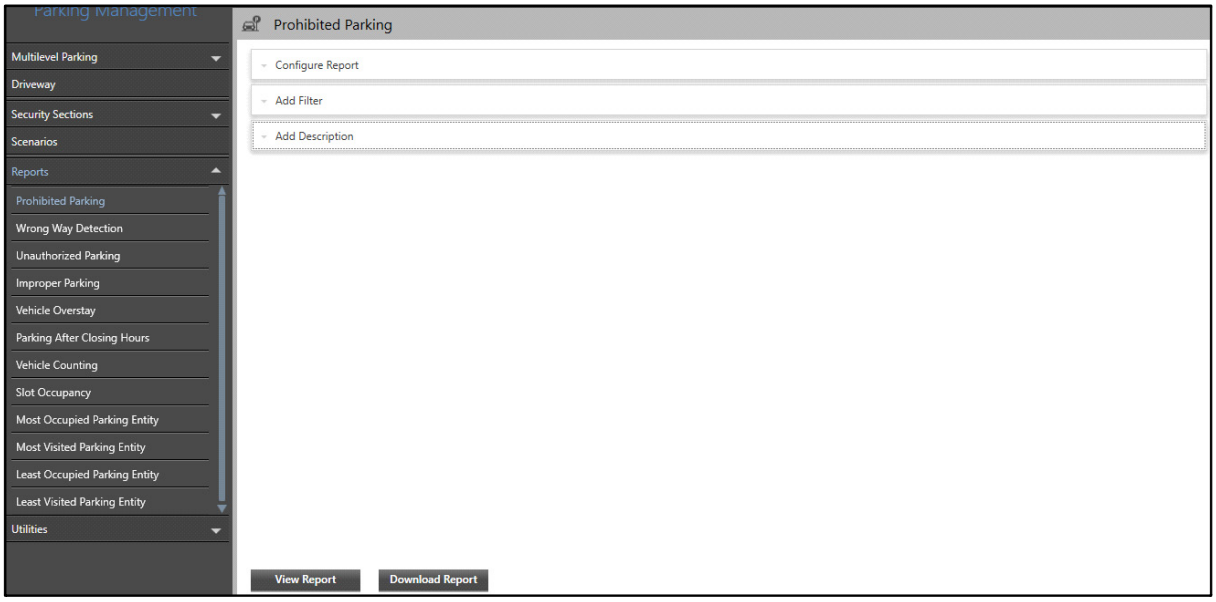
- “Prohibited Parking Report”
- “Wrong Way Detection Report”
- “Unauthorized Parking Report”
- “Improper Parking Report”
- “Vehicle Overstay Report”
- “Parking After Closing Hours Report”

For the above mentioned Reports the configurations are explained in this topic itself.

For Vehicle Counting Report, refer to “Vehicle Counting Report”.
For Slot Occupancy Report, refer to “Slot Occupancy Reports”.
For Most Occupied Parking Entity Report, refer to “Most Occupied Parking Entity Report”.
For Most Visited Parking Entity Report, refer to “Most Visited Parking Entity Report”.
For Least Occupied Parking Entity Report, refer to “Least Occupied Parking Entity Report”.
For Least Visited Parking Entity Report, refer to “Least Visited Parking Entity Report”.

To configure a report,

- Click **Parking Management > Reports**.



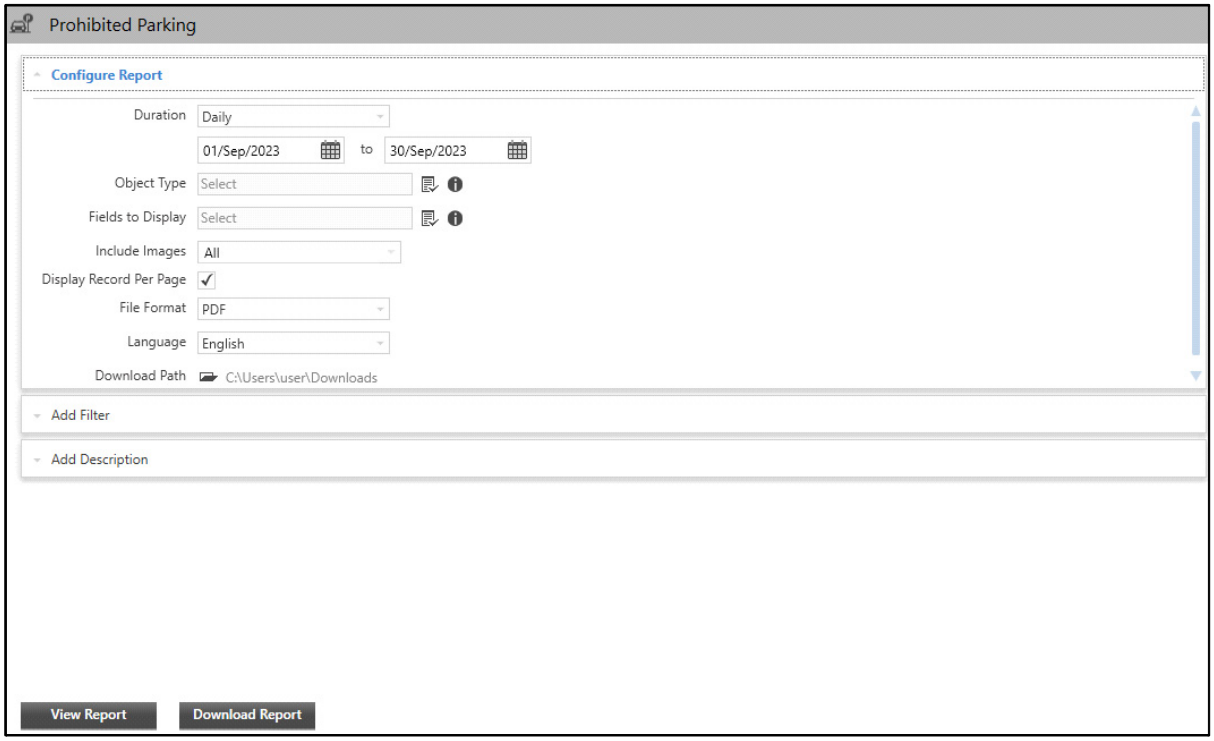
The Prohibited Parking page contains three collapsible panels — “Configure Report”, “Add Filter” and “Add Description”.

Configure Report

This panel displays the report configurations and you can configure various report parameters. You can generate monthly, daily or hourly reports with captured images against specific events selected from the drop-down list along with event source and time details.

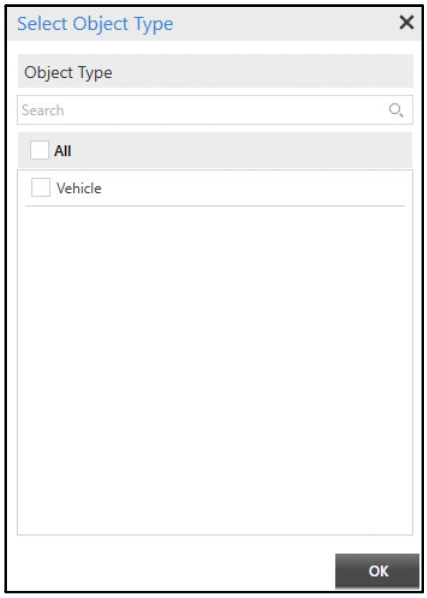
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



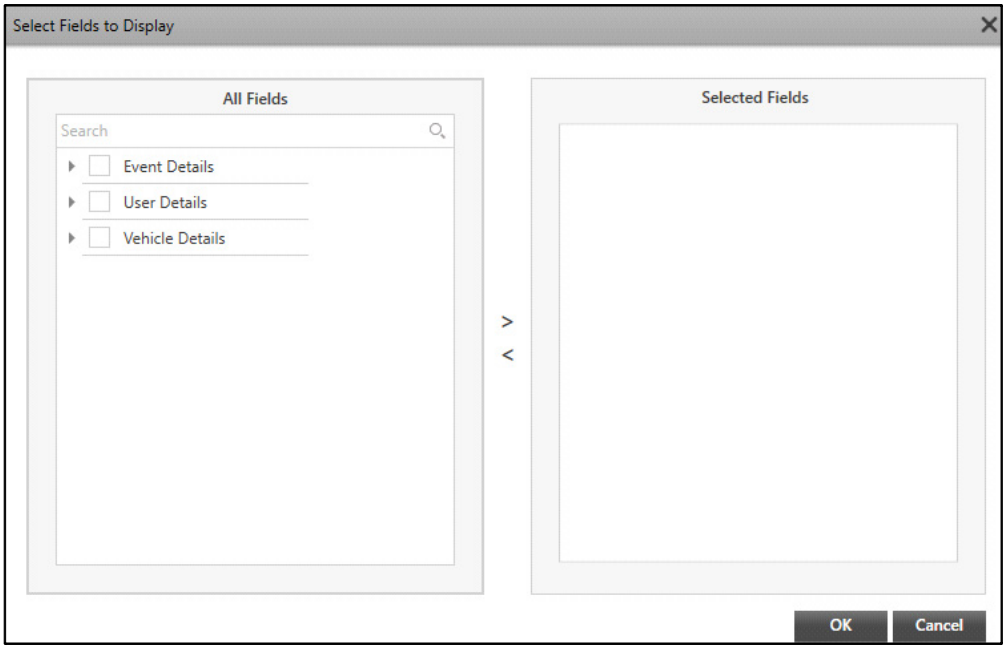
Configure the following parameters:

- **Duration**: Select the desired Duration from the drop-down list — Monthly, Daily or Hourly.
  - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
  - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
  - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
- **Object Type**: Select the desired Object Type for which you wish to generate reports using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



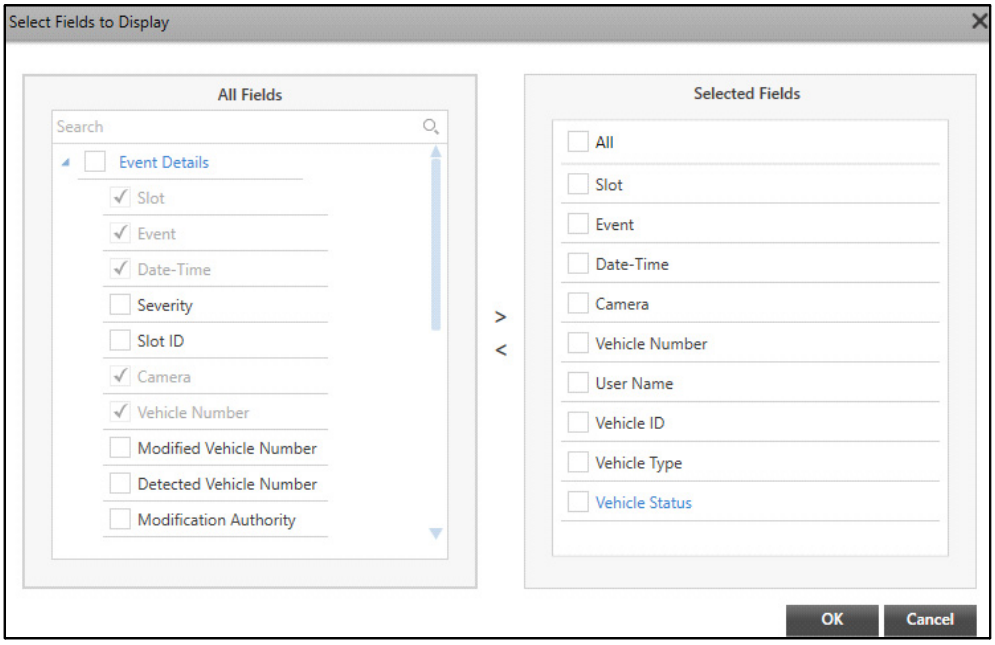
- Select the **Vehicle** check box. Click **OK**.

- **Fields to Display**: Select the desired fields which you wish to include in the report using the **Fields to Display** picklist.
  - Click **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



- Select the check boxes of the desired fields you wish to add from the **All Fields** list. Click the right arrow button to add these fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

  To remove fields, select the check boxes for the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields from the Selected Fields list.



- Click **OK** to confirm or click **Cancel** to discard.



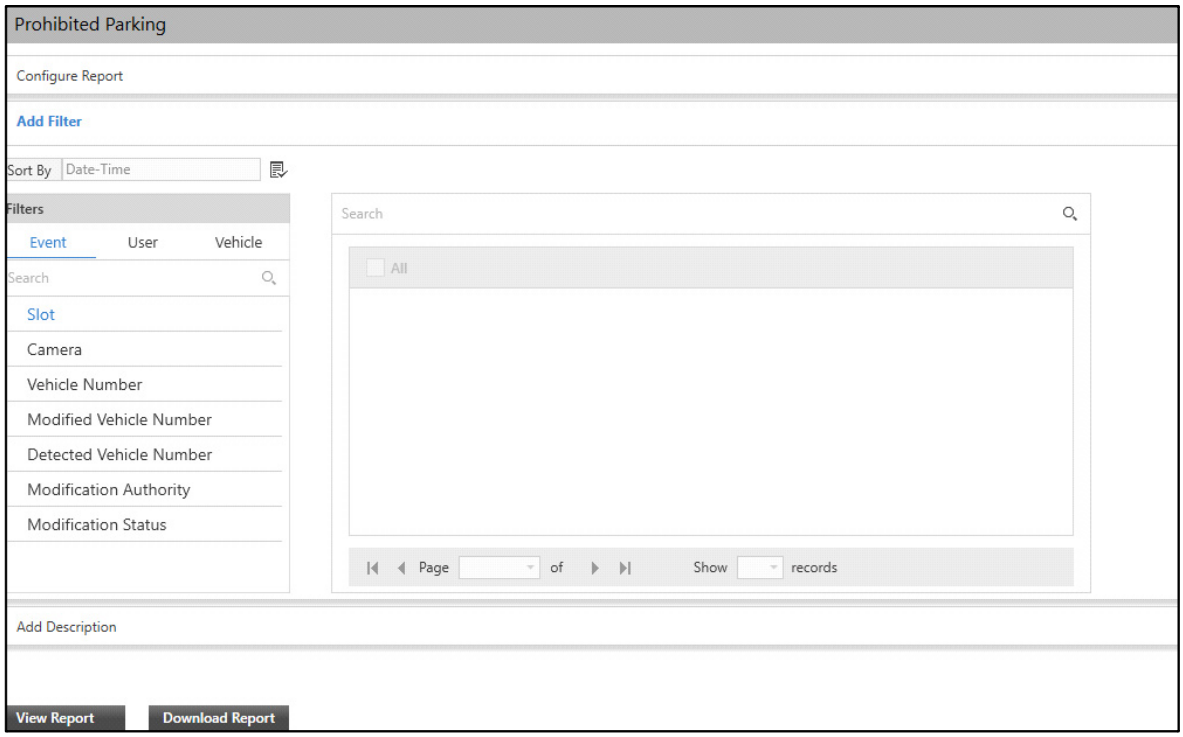
- **Include Images**: Select the type of images that you wish to include in the report using the drop-down list.
- **Display Record per Page**: Select the check box to display each record for the selected fields on a new page.
- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Filter

This panel allows you to add filters for the Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters. You can view and edit the filters from this collapsible panel

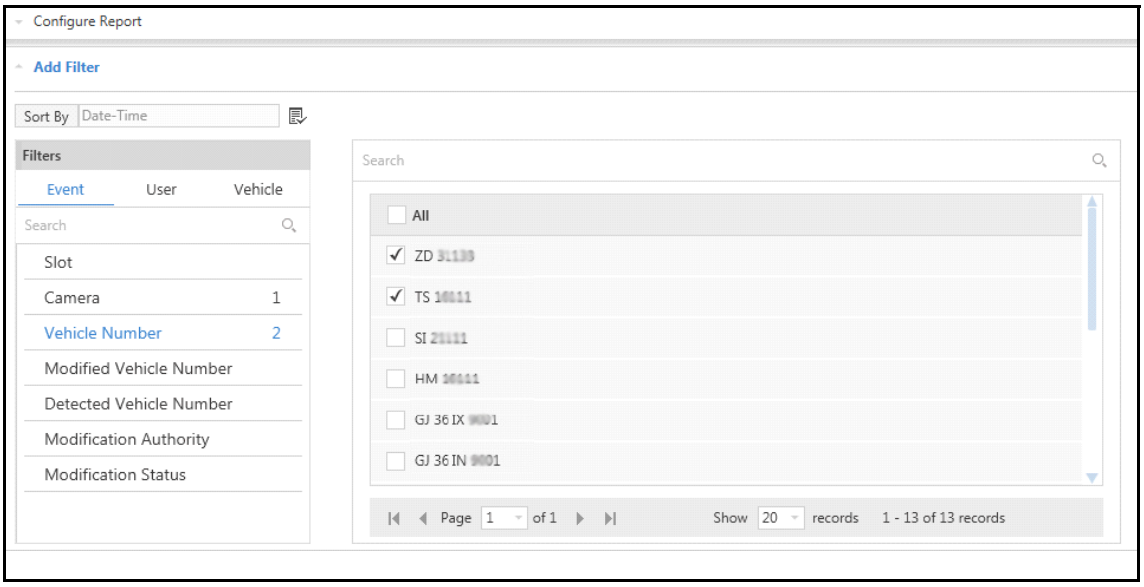
To configure the filters,

- Click the **Add Filter** collapsible panel.



Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data — Event Details, User Details or Vehicle Details in the report using the **Sort By** picklist. Double-click to select the desired option. By default, the sorting is done as per the Date and Time of the Event Occurrence.
- **Filters**: You can set the Filters as per your requirements to get the data for the report. The Filters section contains three tabs — Event, User and Vehicle.
  - Select the desired tab, for example Event.
  - The list of the filter parameters appear. Click the desired parameter on the left, its associated entities are displayed on the right. For example, if you select Vehicle Number on the right, all the Vehicle Numbers are displayed on the right hand side. Select the check boxes of the desired Vehicle Numbers you wish to include in the report.



- Similarly, you can click the tabs — User or Vehicle and then set the filters as per your requirement.

Add Description

This panel allows you to add a description for the Report once the report configurations are done. This description is visible in the generated report.

To configure the Description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report on-screen.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

Vehicle Counting Report

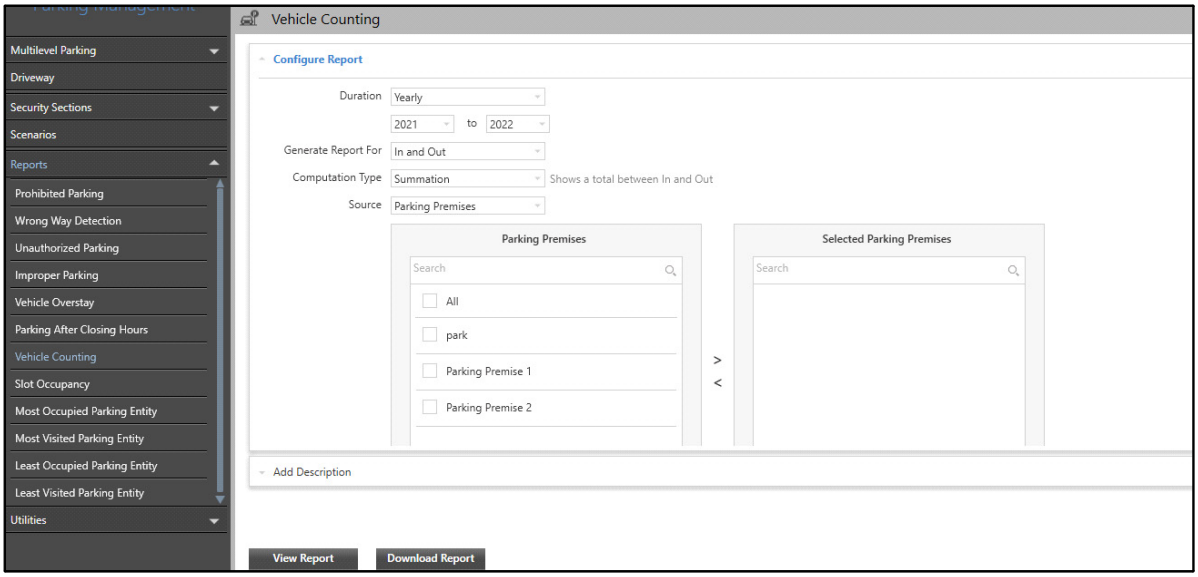
Vehicle Counting Report provides a tabular as well as graphical statistics on vehicle congestion. These statistics can be useful in managing the traffic at various locations by sitting at one place. It allows the user to track the number of vehicles passing-by within the defined duration at any place. The report includes the count of vehicles detected at camera across multiple entries/exits.

For example, consider a shop having various outlets at different locations. Based on this report, the user can track the number of vehicles entering and exiting the various outlets by sitting at one place. If traffic increases at a particular outlet, it can be managed by taking appropriate actions.

The Vehicle Counting Report page enables you to configure parameters for Vehicle Counting Reports. You can view and configure Vehicle Counting Reports on Yearly, Monthly, Weekly, Daily, Hourly and Peak Hour basis.

To configure Vehicle Counting Report,

- Click **Parking Management > Reports > Vehicle Counting**.



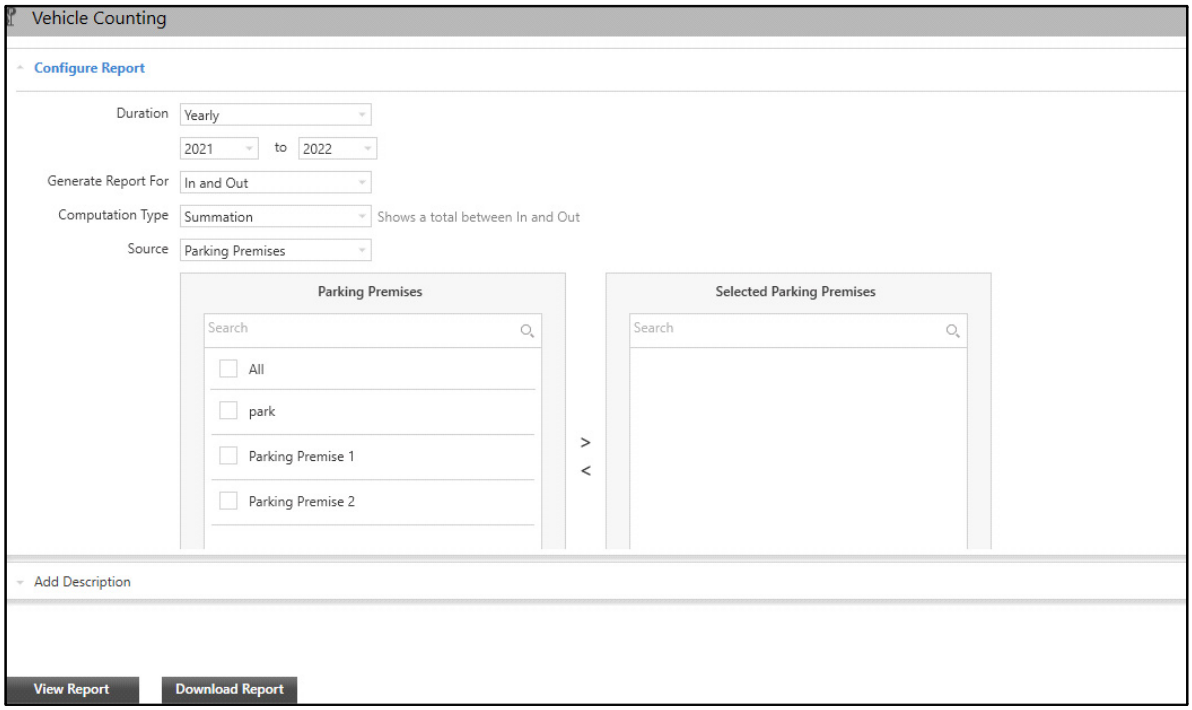
The Vehicle Counting page contains two collapsible panels — “Configure Report”and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Vehicle Counting Report from this collapsible panel.

To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

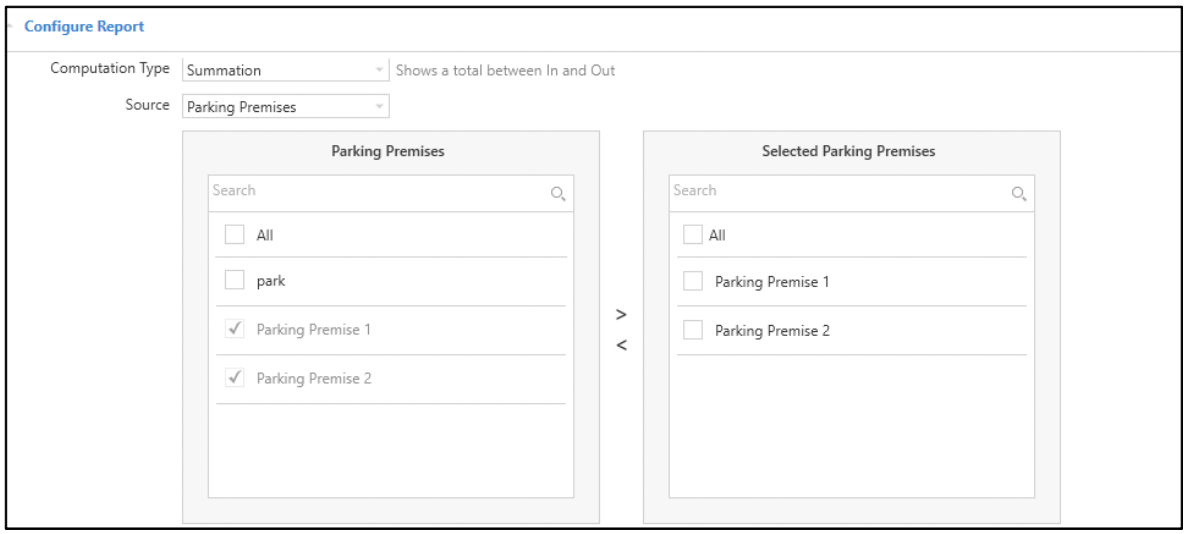
- **Duration**: Select the desired Duration from the drop-down list — Yearly, Monthly, Daily, Hourly, Weekly and Peak Hour Reports.
    - **Yearly**: Select this option to generate yearly reports. Select the desired From and To year from the drop-down lists.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
    - **Weekly**: Select this option to generate weekly reports. Select the desired From and To dates from the calendar. Select the day of the week from when you wish the weekly report from the **Start Week From** drop-down list.
    - **Peak Hour**: Select this option to generate reports for the peak hours. Select the period for which you wish the report from the **Period** drop-down list. Select the year, month or day to configure the peak period duration. Specify the **Peak Period** time.
- **Generate Report For**: Select the parameter for which you wish to generate the report from the drop-down list — In, Out and In and Out.
    - If you select **In**, the report will include only **In** counts of the vehicles from various locations.
    - If you select **Out**, the report will include only **Out** counts of the vehicles from various locations.

- If you select **In and Out,** the report will include both **In** and **Out** counts of the vehicles from various locations.

- **Computation Type**: Select the type of computation for the report from the drop-down list — Summation, Differentiation and Maximum Count. The data will be processed according to the selected computation type option.

  - **Summation**: This report will give you total counts between In and Out for the selected Parking Premises or Parking Premises Group.
  - **Differentiation**: This report will give you difference between In and Out count for the selected Parking Premises or Parking Premises Group.
  - **Maximum Count**: This report will give the maximum count of In or Out count for the selected Parking Premises or Parking Premises Group.

- **Source**: Select the source from the drop-down list — Parking Premises or Parking Premises Group.



  - Select the check boxes of the desired Parking Premises or Parking Premises Group you wish to select for the report from the **Parking Premises** or **Parking Premises Group** list. Click the right arrow button to add these Parking Premises or Parking Premises Group in the **Selected Parking Premises** or **Selected Parking Premises Group** list. You can also search for the desired Parking Premises or Parking Premises Group using the search bar.

    To remove Parking Premises or Parking Premises Group, select the check boxes of the desired the Parking Premises or Parking Premises Group you wish to remove from the Selected Parking Premises or Selected Parking Premises Group list. Click the left arrow button to remove the Parking Premises or Parking Premises Group from the list.

- **Representation Format**: Select the format in which you wish the report to be generated from the drop-down list.



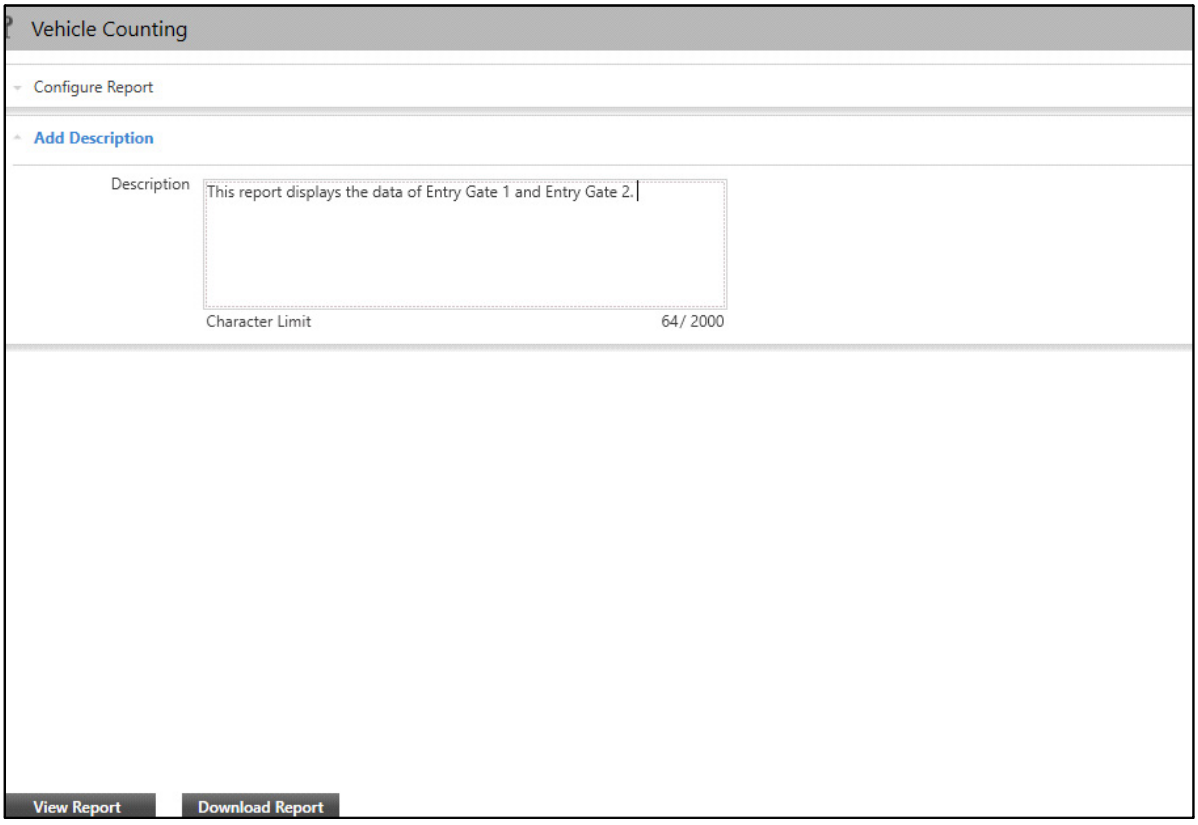
- **Graph Type**: Select the Graph Type from the drop-down list if you selected Graph as the Representation Format.
- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all the folders which are in the drive. Select the desired folder.

Add Description

This panel allows you to add a description for the Vehicle Counting Report once the report configurations are done. This description is visible in the generated report.

To configure the description,

- Click the **Add Description** collapsible panel.



The configurations of Add Description for Vehicle Counting Report are similar to that explained in Report Configurations. For details, refer to“Add Description” in “Report Configurations”.

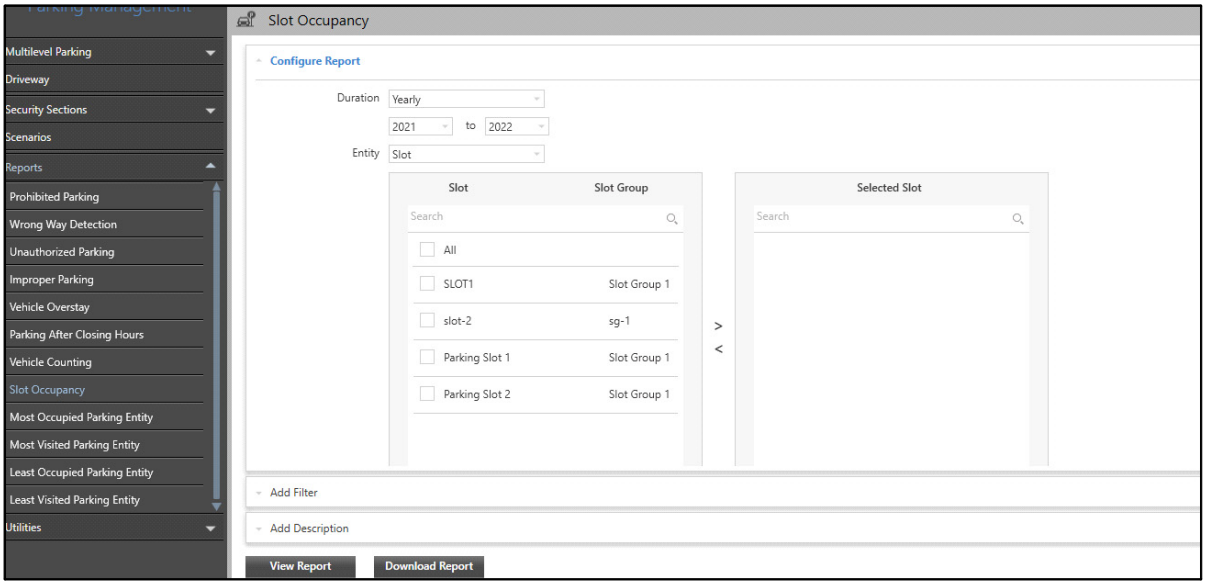
Slot Occupancy Reports

Slot Occupancy Reports can play a vital role to identify for what duration the parking area has been occupied by a particular vehicle. This report is useful at places such as Malls, Multilevel Parking and Multiplexes where the demand for parking slots is high. Based on this report, Slot Occupancy can be tracked and if the vehicle is found to be parked for a longer duration, then actions can be taken accordingly.

The Slot Occupancy page enables you to configure parameters for Slot Occupancy Reports. You can view and configure Slot Occupancy Reports on Yearly, Daily, Monthly and Hourly basis.

To configure Slot Occupancy Report,

- Click **Parking Management > Reports > Slot Occupancy**.



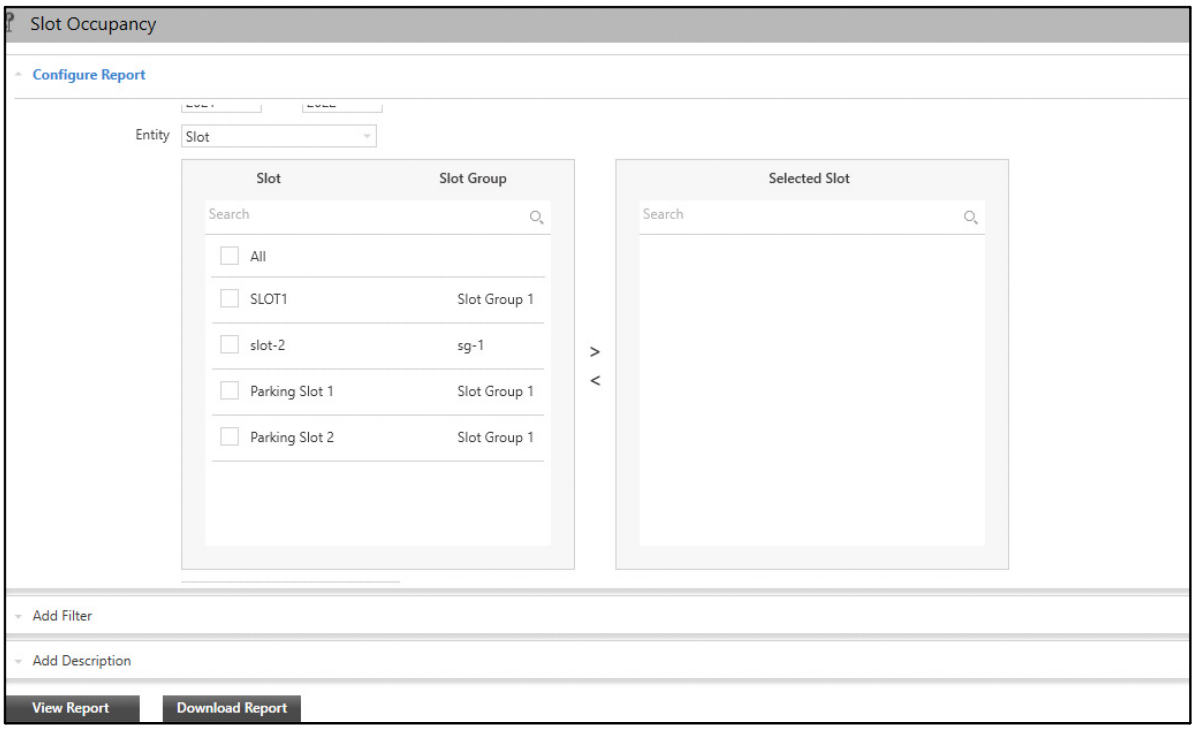
The Slot Occupancy page contains three collapsible panels — “Configure Report”, “Add Filter” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Slot Occupancy Report from this collapsible panel.

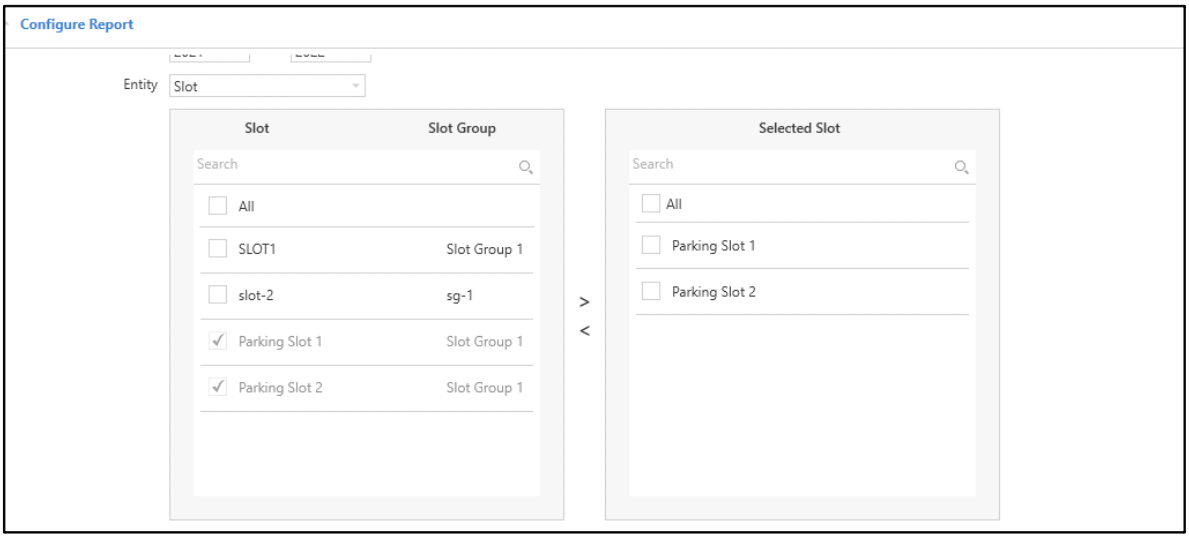
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



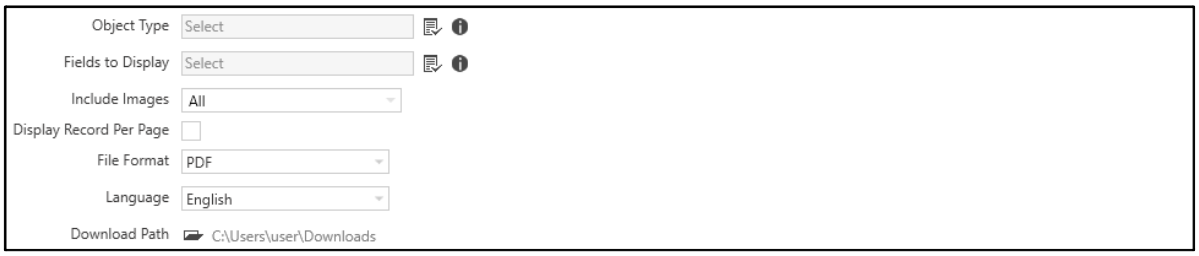
Configure the following parameters:

- **Duration**: Select the desired Duration from the drop-down list options — Yearly, Monthly, Daily and Hourly.
    - **Yearly**: Select this option to generate yearly reports. Select the desired From and To year from the drop-down lists.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
- **Entity**: Select the desired Entity from the drop-down list — Slot, Slot Group, Lane, Area, Level and Facility.

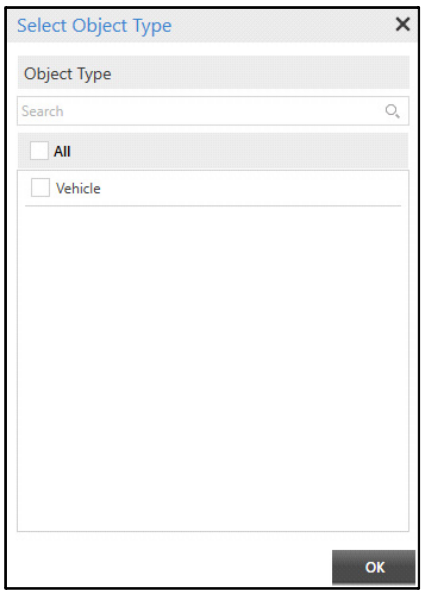


- Select the check boxes of the desired Entities you wish to select for the report from the Entity list. Click the right arrow button to add these Entities in the Selected Entities list. You can also search for the desired Entities using the search bar.

  To remove Entities, select the check boxes of the desired Entities you wish to remove from the Selected Entities list. Click the left arrow button to remove the Entities from the list.

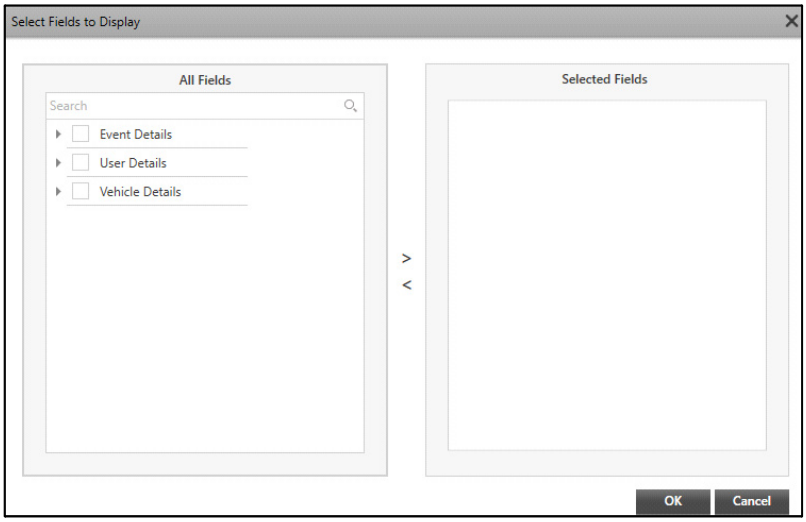


- **Object Type**: Select the desired Object Type for which you wish to generate reports using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



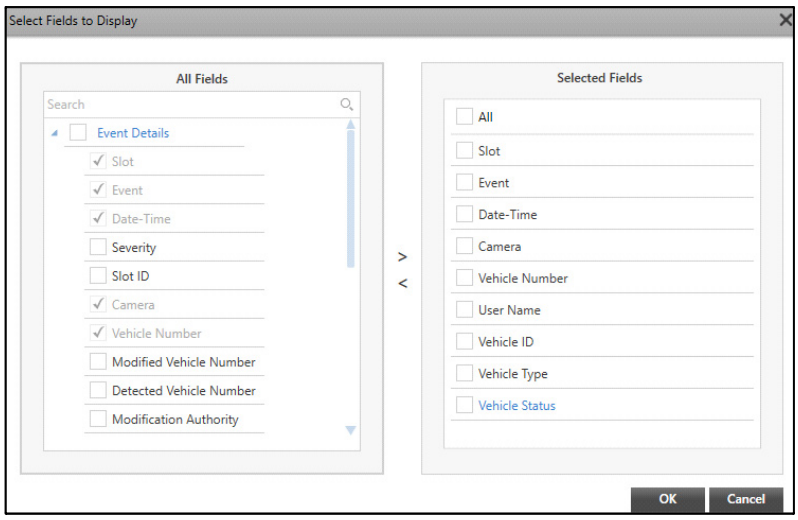
- Select the **Vehicle** check box. Click **OK**.

- **Fields to Display**: Select the desired fields which you wish to include in the report using the **Fields to Display** picklist.
  - Click **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



- Select the check boxes of the desired fields you wish to add from the **All Fields** list. Click the right arrow button to add these fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

  To remove fields, select the desired check boxes for the fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields from the Selected Fields list.



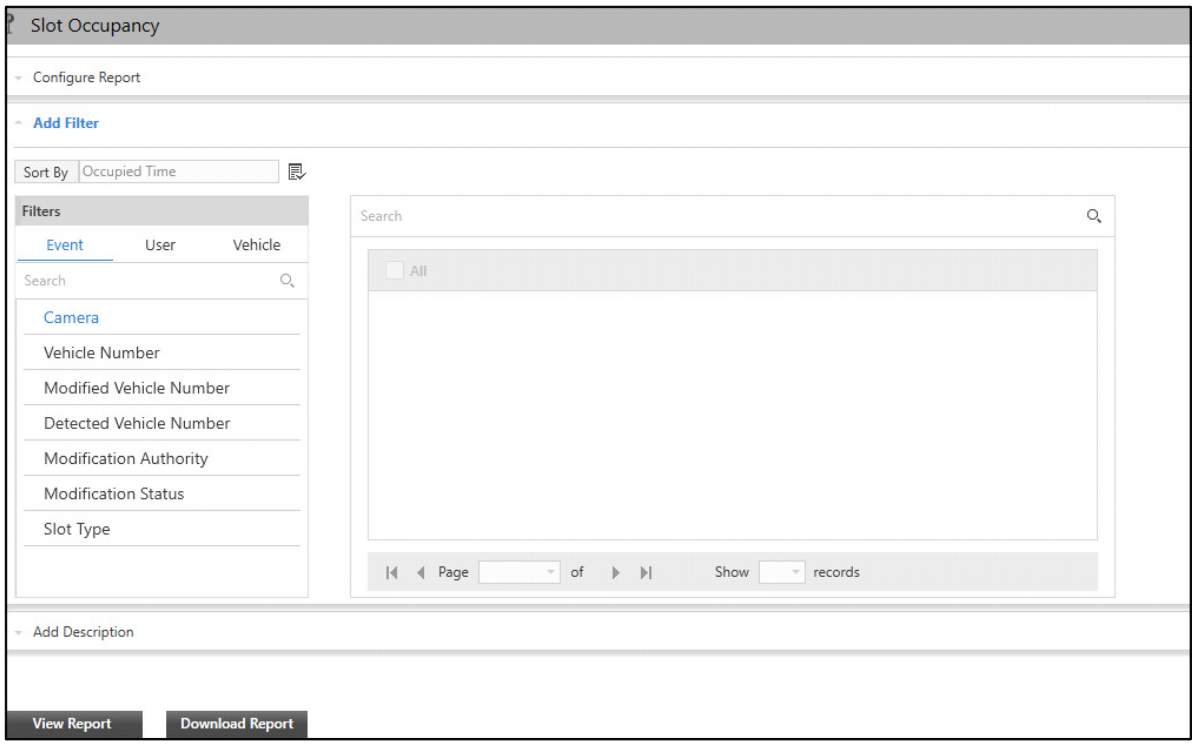
- Click **OK** to confirm or click **Cancel** to discard.
- **Include Images**: Select the type of images that you wish to include in the report from the drop-down list.
- **Display Record per Page**: Select the check box to display each record of the selected fields on a new page.
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the desired Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Filter

This panel allows you to add filters for the Slot Occupancy Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters.

To configure the filters,

- Click the **Add Filter** collapsible panel.



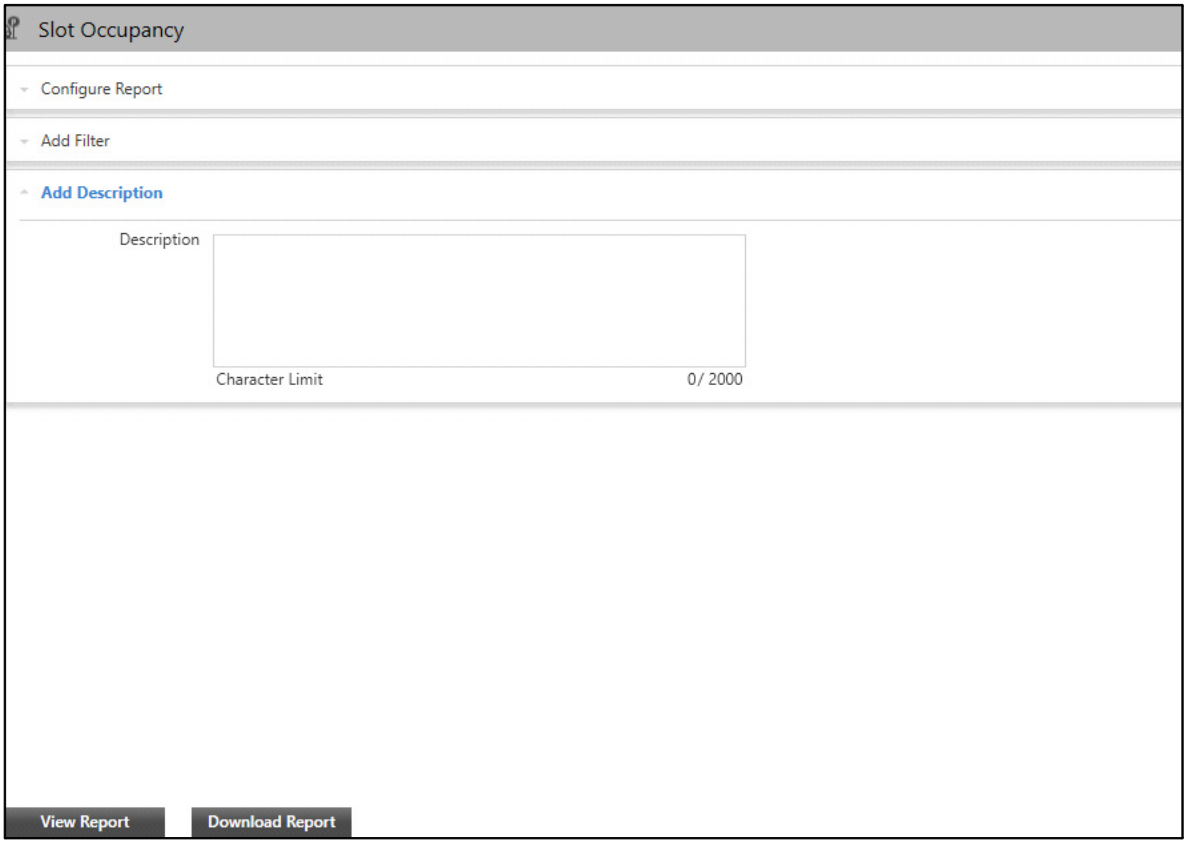
The configurations of Add Filter for Slot Occupancy Report are similar to that explained in Report Configurations. For details, refer to “Add Filter” in “Report Configurations”.

Add Description

This panel allows you to add a description for the Slot Occupancy Report once the report configurations are done. This description is visible in the generated report.

To configure the description,

- Click the **Add Description** collapsible panel.



The configurations of Add Description for Slot Occupancy Report are similar to that explained in Report Configurations. For details, refer to“Add Description” in “Report Configurations”.

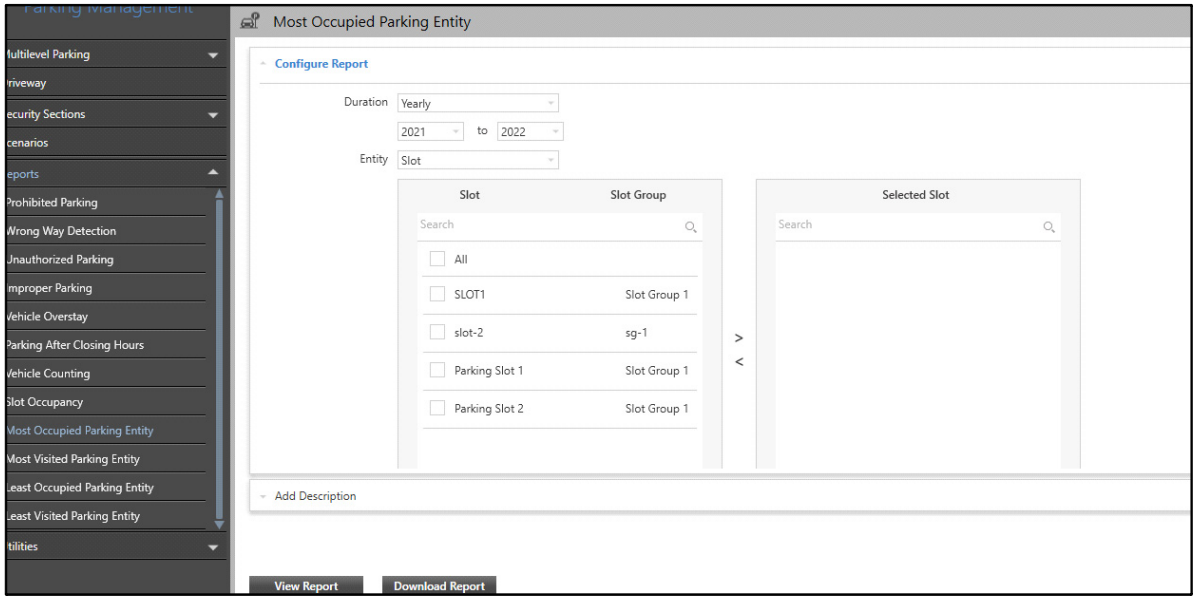
Most Occupied Parking Entity Report

Most Occupied Parking Entity Reports can play a vital role in utilizing the parking facility efficiently. This report is useful at busy parking lots in indicating the entity which is being occupied for the longest duration. Based on this report, Most Occupied Parking Entity can be tracked and some schemes can also be introduced for those entities which are not being much occupied for effective parking premise utilization.

The Most Occupied Parking Entity page enables you to configure parameters for Most Occupied Parking Entity Reports. You can view and configure Most Occupied Parking Entity Reports on Yearly, Daily, Monthly and Hourly basis.

To configure Most Occupied Parking Entity Report,

- Click **Parking Management > Reports > Most Occupied Parking Entity**.



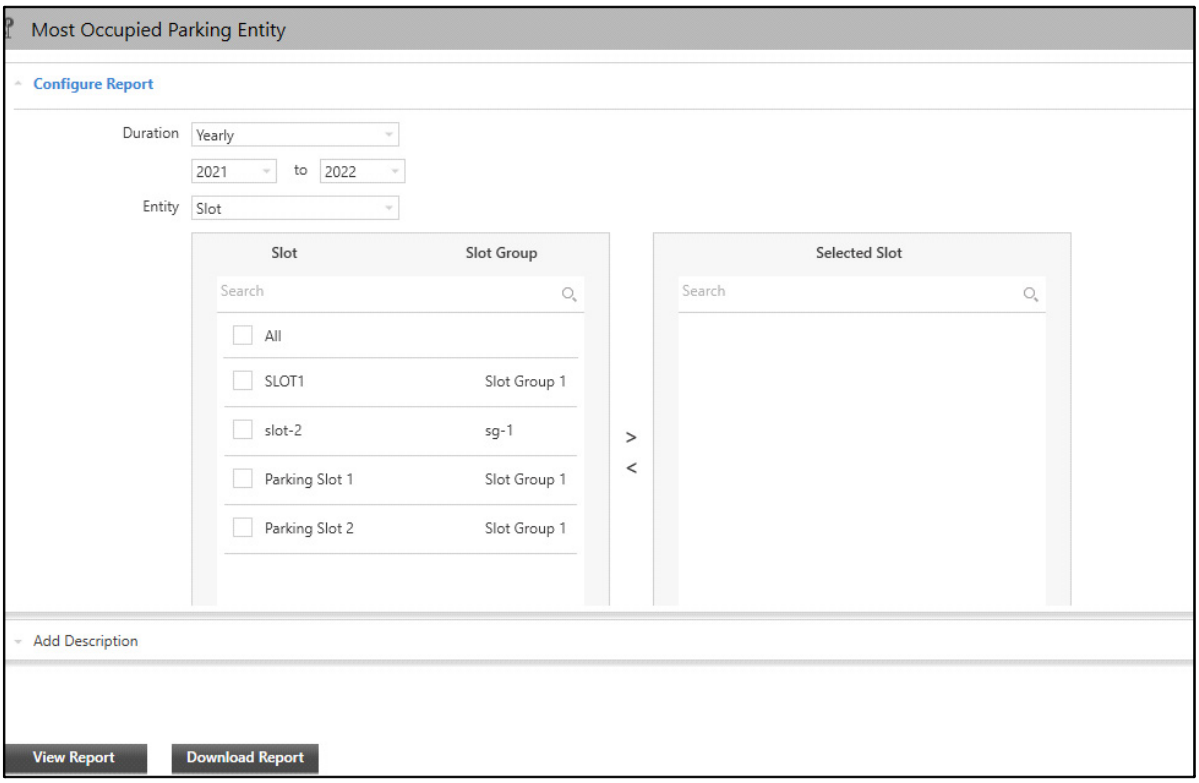
The Most Occupied Parking Entity page contains two collapsible panels — “Configure Report” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Most Occupied Parking Entity Report from this collapsible panel.

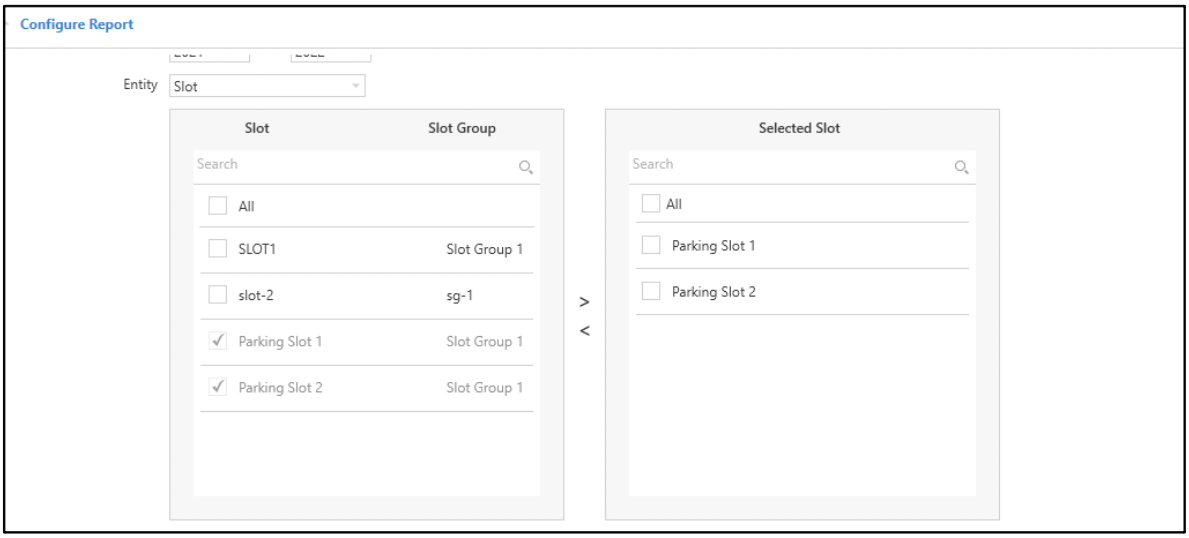
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

- **Duration**: Select the Duration from the drop-down list — Yearly, Monthly, Daily and Hourly.
  - **Yearly**: Select this option to generate yearly reports. Select the desired From and To year from the drop-down lists.
  - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
  - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
  - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
- **Entity**: Select the Entity from the drop-down list — Slot, Slot Group, Lane, Area, Level and Facility.



- Select the check boxes of the desired Entities you wish to select for the report from the Entity list. Click the right arrow button to add these Entities in the Selected Entities list. You can also search for the desired Entities using the search bar.

- To remove Entities, select the desired check boxes for the Entities you wish to remove from the Selected Entities list. Click the left arrow button to remove the Entities from the list.



- **Representation Format**: Select the desired format in which you wish the report to be generated from the drop-down list.

- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.

- **Language**: Select the desired Language in which you wish to generate the report from the drop-down list.

- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

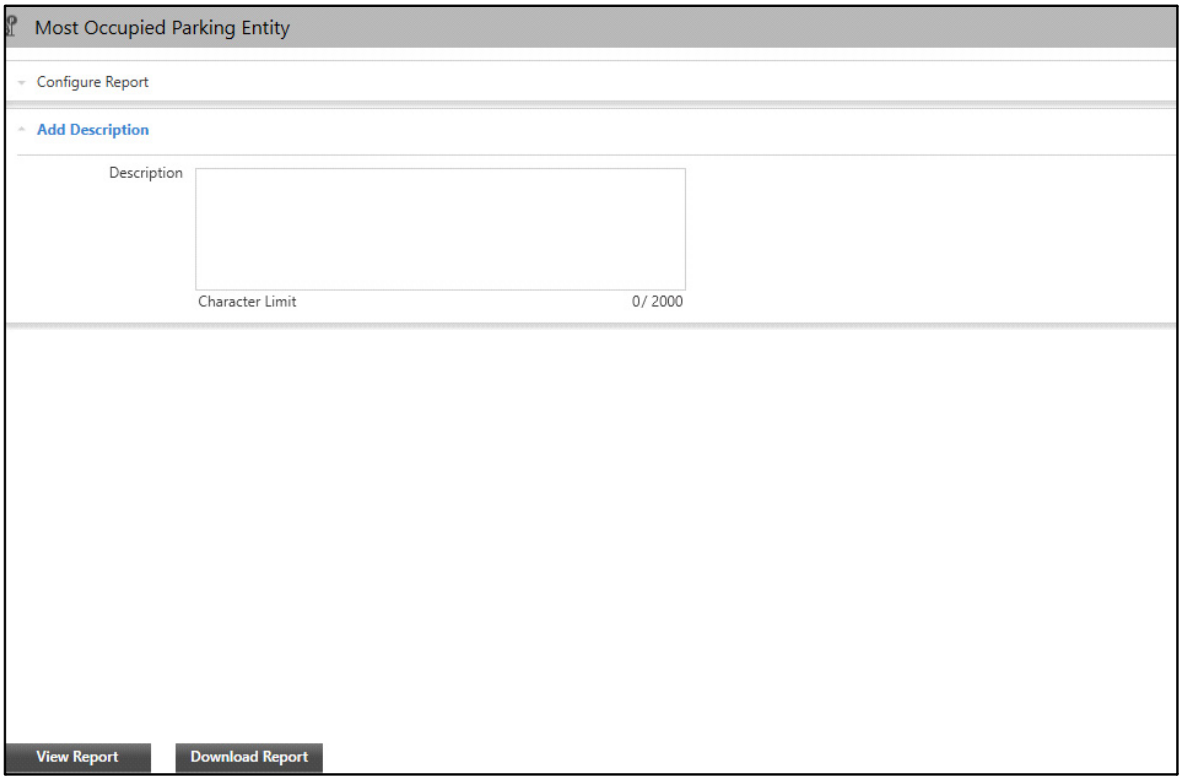
If your Management Server is at PC-2 and you are downloading report at PC-1, ensure that report service at PC-2 (where Management Service is running) must be running.

Add Description

This panel allows you to add a description for the Vehicle Report once the report configurations are done. This description is visible in the generated report.

To configure the description,

- Click the **Add Description** collapsible panel.



The configurations of Add Description for Most Occupied Parking Entity Report are similar to that explained in Report Configurations. For details, refer to “Add Description” in “Report Configurations”.

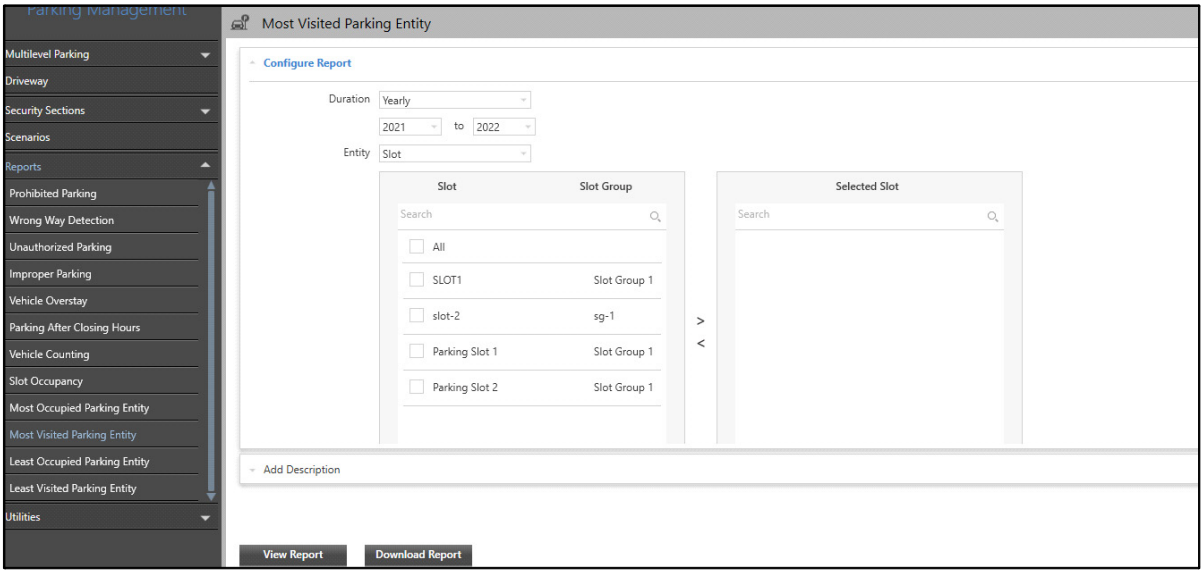
Most Visited Parking Entity Report

Most Visited Parking Entity Reports can play a vital role in utilizing the parking facility efficiently. This report is useful at busy parking lots in indicating the entity which is being used or visited most frequently. Based on this report, Most Visited Parking Entity can be tracked and some schemes can also be introduced for those entities which are not being used frequently for effective parking premise utilization.

The Most Visited Parking Entity page enables you to configure parameters for Most Visited Parking Entity Reports. You can view and configure Most Visited Parking Entity Reports on Yearly, Daily, Monthly and Hourly basis.

To configure Most Visited Parking Entity Report,

- Click **Parking Management > Reports > Most Visited Parking Entity**.



The configurations of Most Visited Parking Entity Report are similar to that explained in Most Occupied Parking Entity Configurations. For details, refer to “Most Occupied Parking Entity Report”.

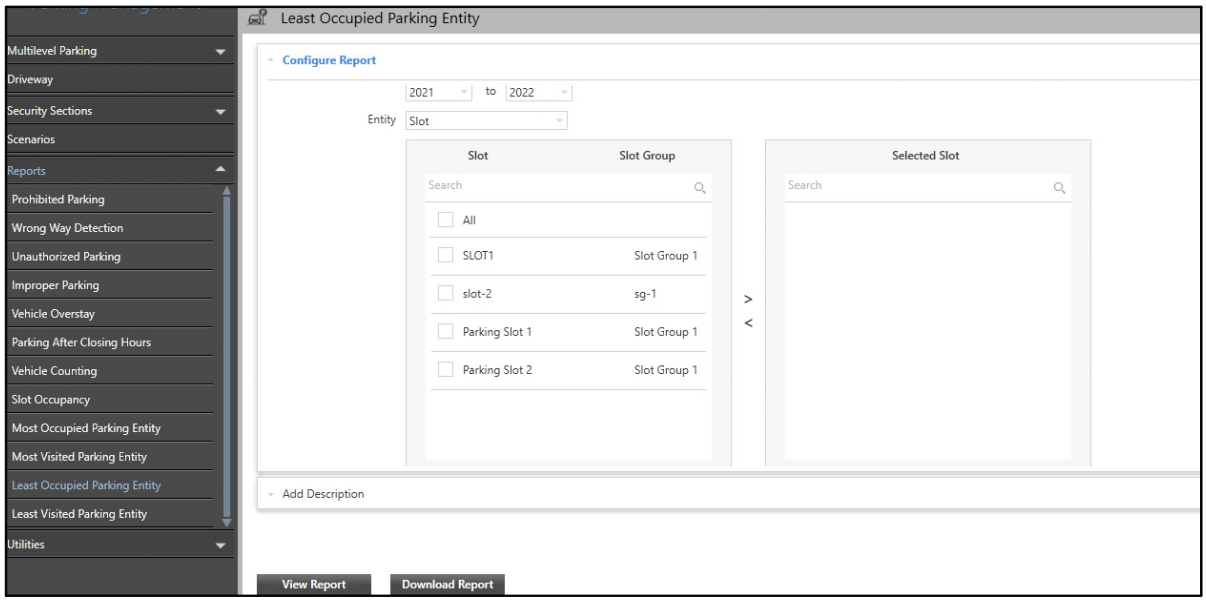
Least Occupied Parking Entity Report

Least Occupied Parking Entity Reports can play a vital role in utilizing the parking facility efficiently. This report is useful at empty or sparsely used as well as busy parking lots in indicating the entity which is being occupied for the least duration. Based on this report, Least Occupied Parking Entity can be tracked and some schemes can be introduced for those entities which are not being used frequently for effective parking premise utilization.

The Least Occupied Parking Entity page enables you to configure parameters for Least Occupied Parking Entity Reports. You can view and configure Least Occupied Parking Entity Reports on Yearly, Daily, Monthly and Hourly basis.

To configure Least Occupied Parking Entity Report,

- Click **Parking Management > Reports > Least Occupied Parking Entity**.



The configurations of Least Occupied Parking Entity Report are similar to that explained in Most Occupied Parking Entity Configurations. For details, refer to “Most Occupied Parking Entity Report”.

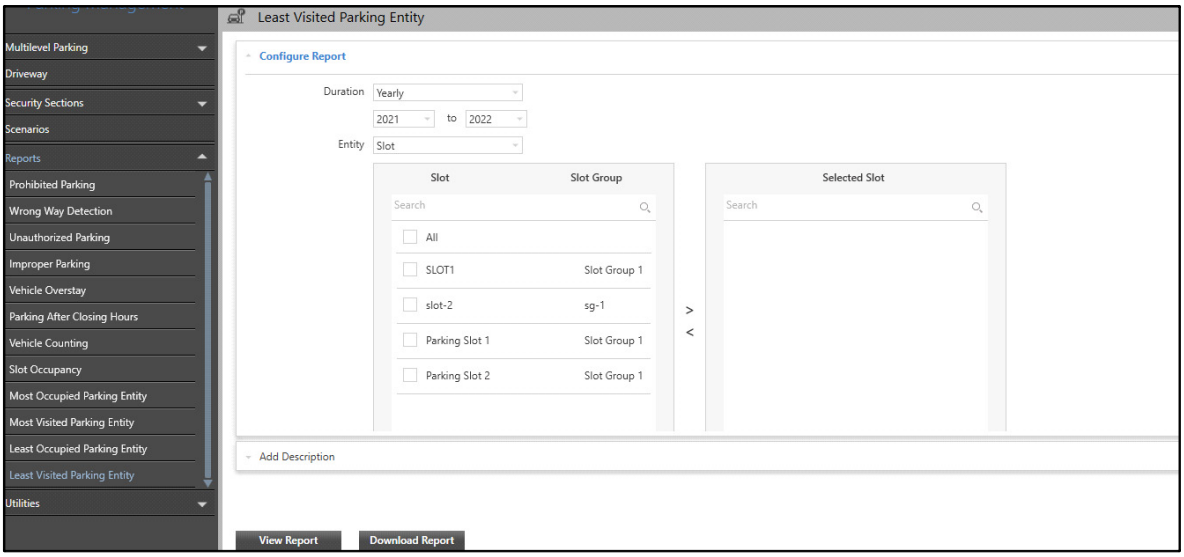
Least Visited Parking Entity Report

Least Visited Entity Reports can play a vital role in utilizing the parking facility efficiently. This report is useful at empty or sparsely used as well as busy parking lots in indicating the entity which is being used least frequently. Based on this report, Least Visited Parking Entity can be tracked and some schemes can be introduced for those entities which are not being used frequently for effective parking premise utilization.

The Least Visited Parking Entity page enables you to configure parameters for Least Visited Parking EntityReports. You can view and configure Least Visited Parking Entity Reports on Yearly, Daily, Monthly and Hourly basis.

To configure Least Visited Parking Entity Report,

- Click **Parking Management > Reports > Least Visited Parking Entity**.



The configurations of Least Visited Parking Entity Report are similar to that explained in Most Occupied Parking Entity Configurations. For details, refer to “Most Occupied Parking Entity Report”.

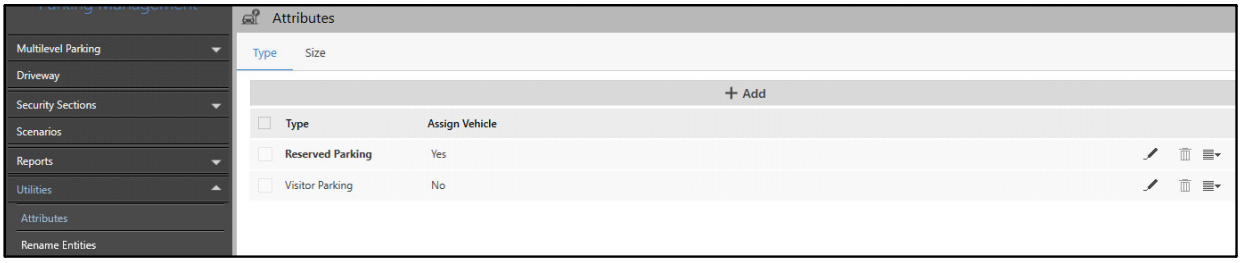
Utilities

Attributes

The Parking Management module allows you to configure various **Types** and **Size** of slots. Attributes created here are available for selection while configuring Slot profiles in Multilevel Parking.

To configure Attributes,

- Click **Parking Management > Utilities > Attributes**.



The Attributes page consists of the following tabs:

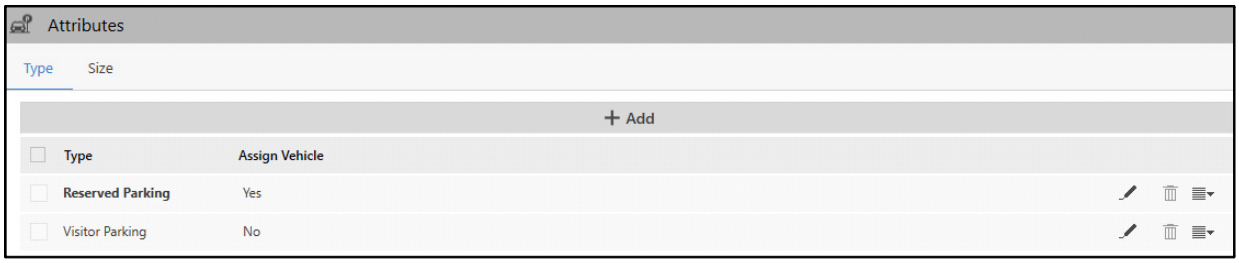
- "Types"
- "Size"

Types

This tab enables you to view and add types of slots. All the slot types appear under this tab. The slot details displayed are — Type and Assign Vehicles.

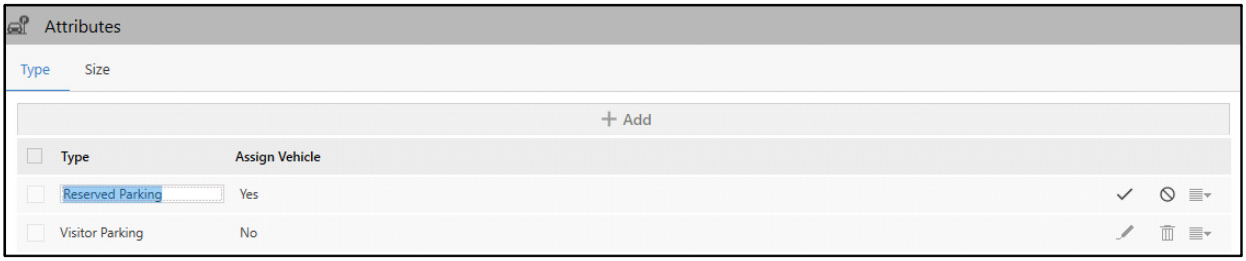
To configure the Types,

- Click the **Type** tab.



The slot types that appear by default are — Reserved Parking and Visitor Parking. You cannot delete the default slot types. You can only edit their names.To do so,

- Click **Edit** corresponding to the slot type you wish to rename.



- Specify the desired name. You can enter upto 30 characters.
- Click **Save** to save the details or click **Cancel** to discard.

You can also add a new slot type. To do so,

- Click **Add**.

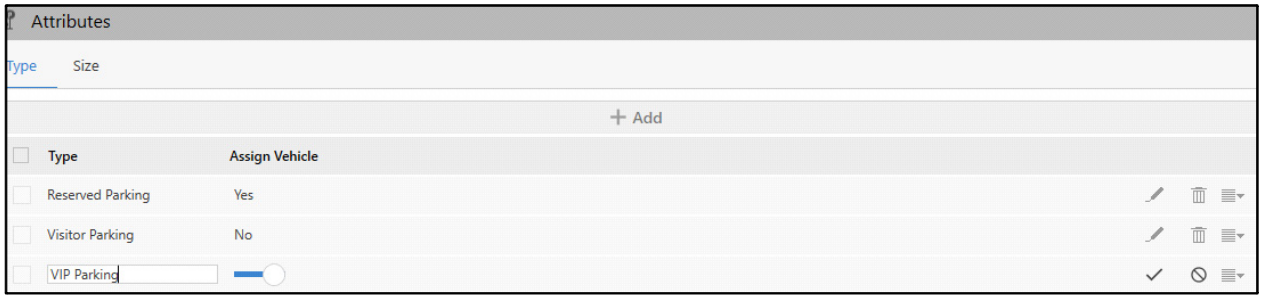


- Specify the desired name. In Type, you can enter upto 30 characters. Default: Blank.
- By default the **Assign Vehicle** Switch of Off. Click to turn it on.
- Click **Save** to save the details or click **Cancel** to discard.

The new slot type appears in the list.

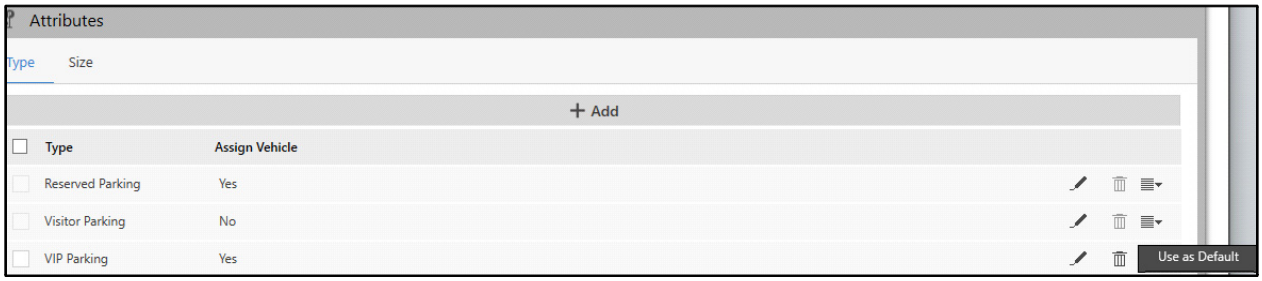
Each Slot Type can be edited, deleted or set as Use as Default.

- Click **Edit** to edit the slot details.



  - Edit the desired details.
- Click **Save** to save the details or click **Cancel** to discard.
- Click **Delete** to delete the added slot type.

- Click **OK** to confirm or click **Cancel** to discard.
- Click **Actions** . The **Use as Default** option appears.



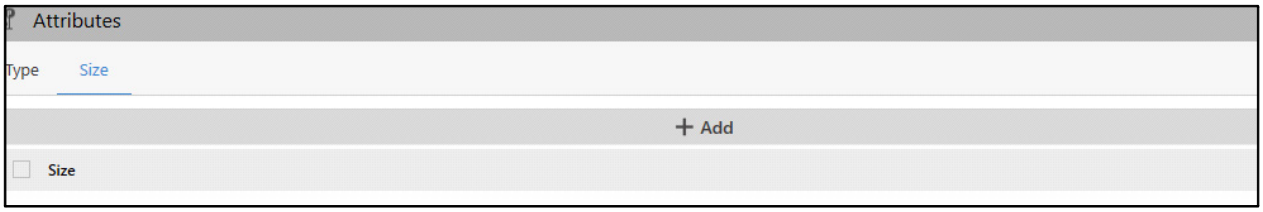
  - Select **Use as Default** if you wish to use this Slot Type as default.

Size

This tab enables you to view and configure the size of the slots. All the existing slot sizes appear under this tab.

To configure the Size,

- Click the **Size** tab.



- Click **Add**.

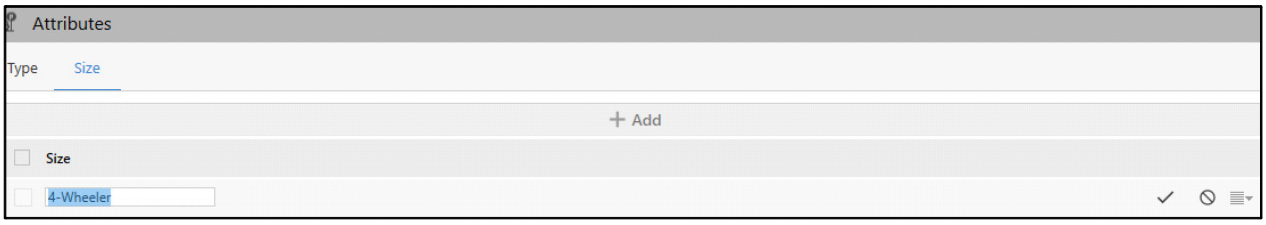


- Specify the desired name for the slot size. In Size, you can enter upto 30 characters. Default: Blank.
- Click **Save** to save the details or click **Cancel** to discard.

The new slot size appears in the list.

Each Slot Size can be edited, deleted or set as Use as Default.

- Click **Edit** to edit the slot details.



- Edit the desired details.

- Click **Save** ✓ to save the details or click **Cancel** ⊘ to discard.
- Click **Delete** 🗑 to delete the added slot size.
- Click **OK** to confirm or click **Cancel** to discard.
- Click **Actions** ☰▾ . The **Use as Default** option appears.



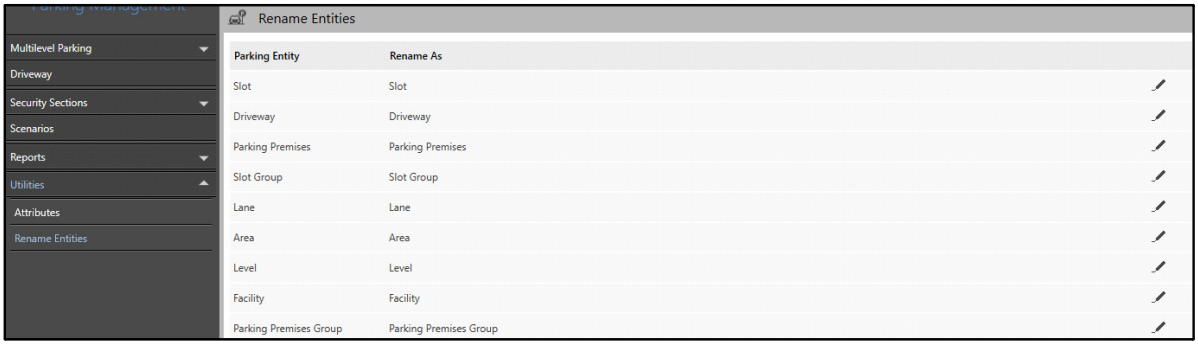
- Select **Use as Default** if you wish to use this Slot Size as default.

Rename Entities

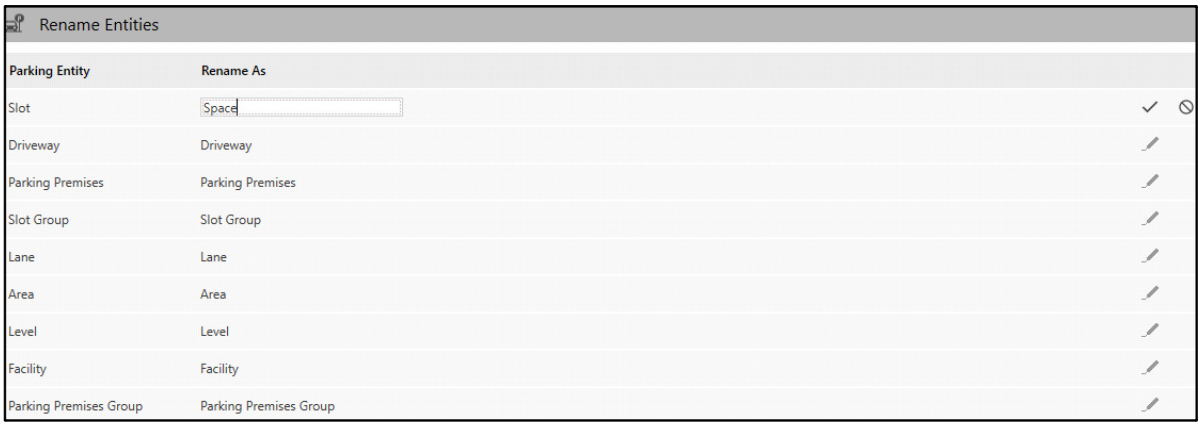
The Parking Management module allows you to change the names of the various Parking Entities. Rename Entities provides you the flexibility to change the names of all the levels of the Multilevel Parking and the other parking Entities as required. The changed names are reflected in the Admin Client wherever applicable.

To configure Entities,

- Click **Parking Management > Utilities > Rename Entities**.



- Click **Edit** corresponding to the Entity you wish to rename.



- Specify the desired name. In Rename As, you can enter upto 30 characters.
- Click **Save** to save the details or click **Cancel** to discard.

CHAPTER 11

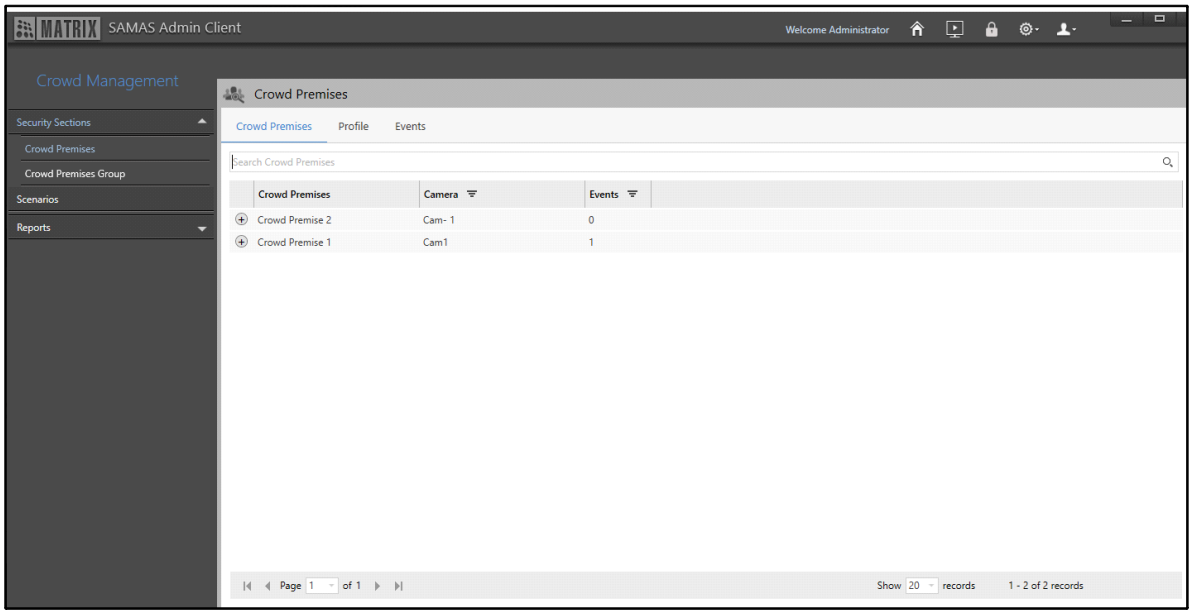
Crowd Management

The Crowd Management module enables you to configure various Crowd Premises and Events for them. Crowd Management uses video content analysis which is effective in detecting Events such as People Counting and Premises Availability based on live stream of a camera. It also enables you to configure Scenarios based on Events.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure Crowd Management,

- Click **Crowd Management**.



The Crowd Management module contains these pages — "Crowd Premises", "Crowd Premises Group", "Crowd Management-Scenarios" and "People Counting Reports".

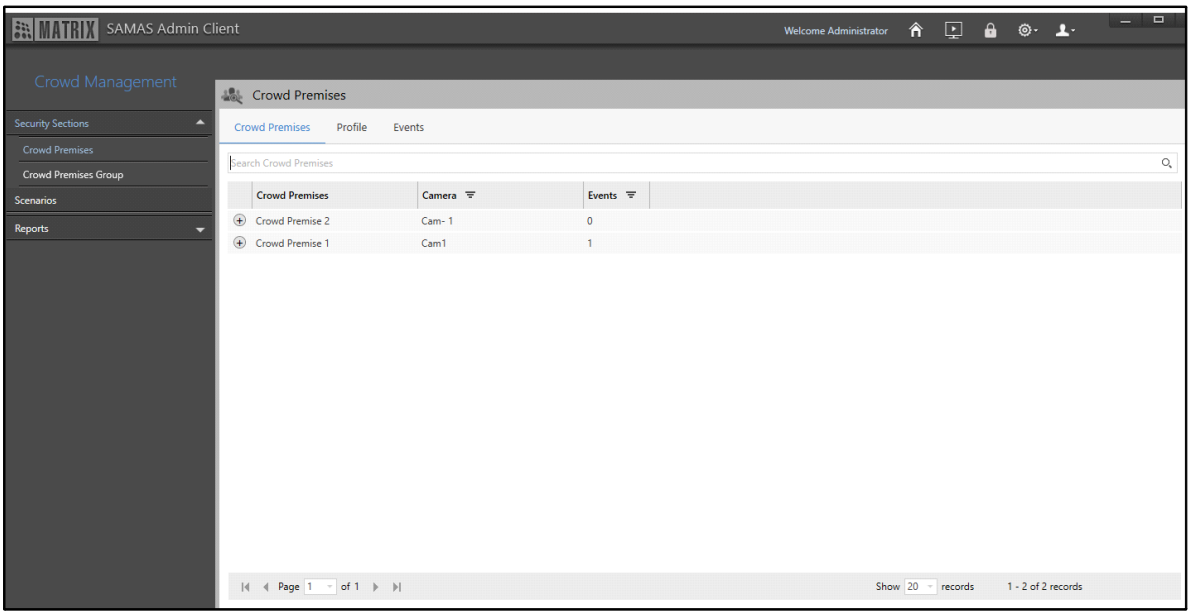
Crowd Premises

The Crowd Management module allows you to configure Crowd Premises profiles. The Crowd Premises feature is useful at places like Exhibition Halls, Open Theaters, Restaurants, Malls, etc. to detect any Events (For example, Premises Availability) in the premises. These Events can help security person or management to know about the remaining space in the area.Events that can be configured against the configured Crowd Premises profile are — Premises Availability and People Counting.

The Crowd Premises page displays all the configured Crowd Premises. You can view and configure the Crowd Premises from this page.

To configure Crowd Premises,

- Click **Crowd Management > Security Sections**. The **Crowd Premises** page appears by default.



The Crowd Premises page consists of the following tabs.

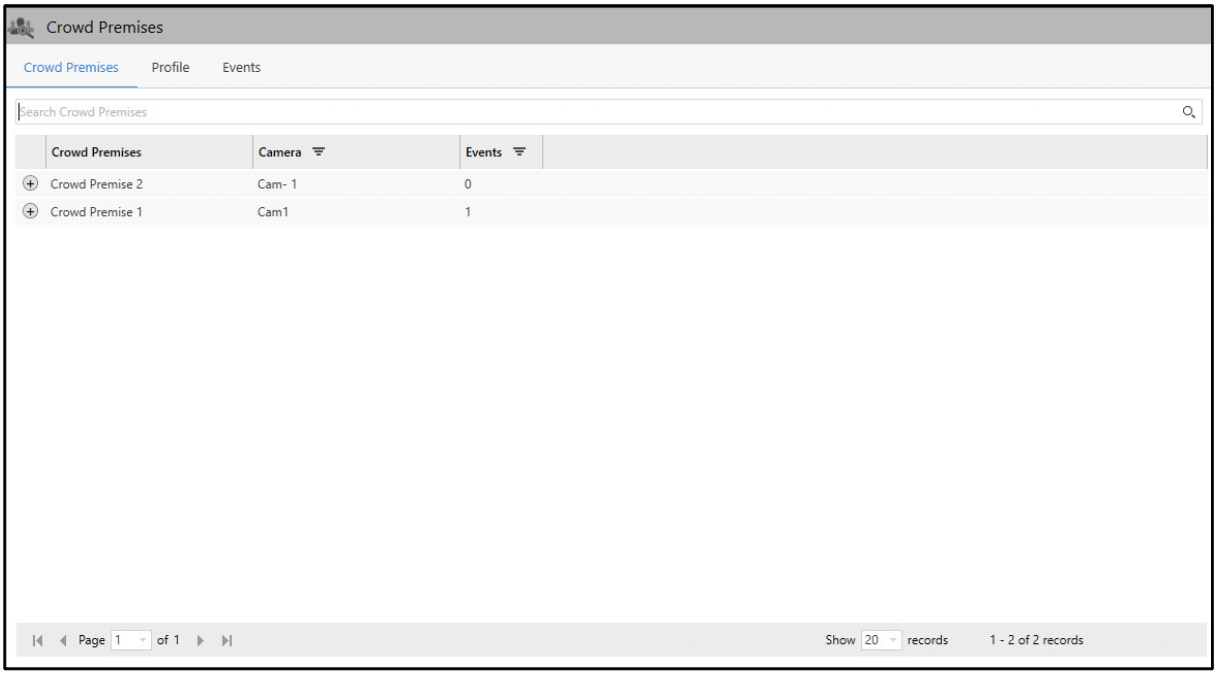
- “Crowd Premises”
- “Profile”
- “Events”

Crowd Premises

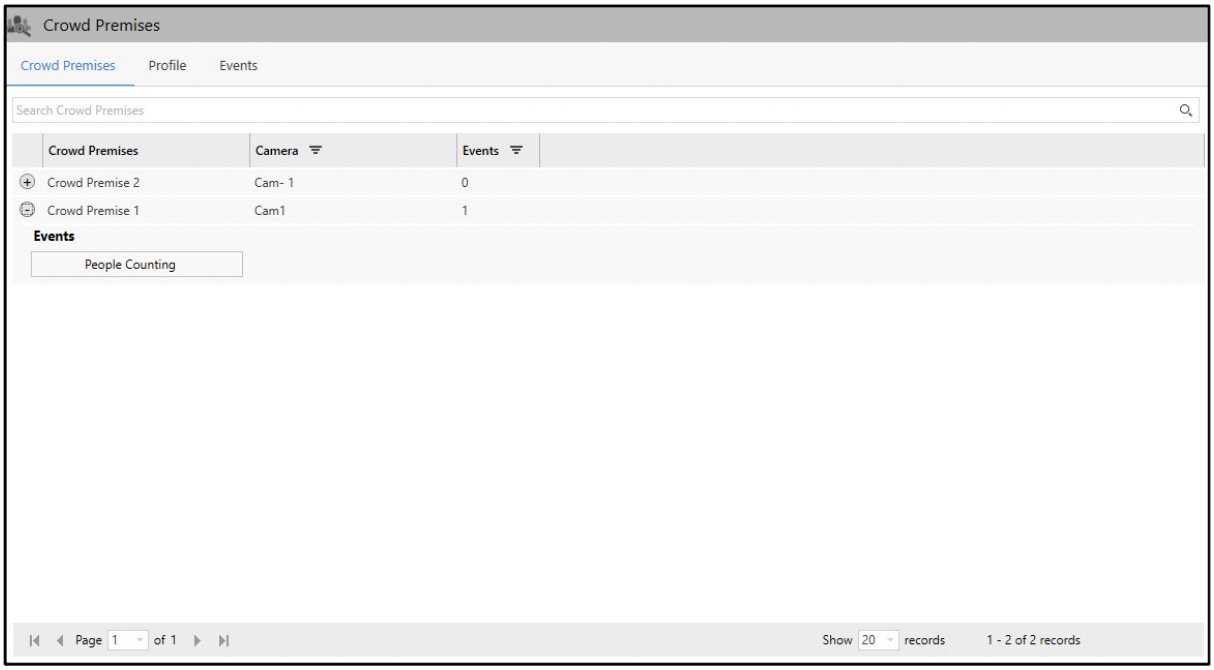
This tab enables you to view Crowd Premises. You can configure the Crowd Premises from “Profile”.All the Crowd Premises and the Events configured for them appear under this tab. The Crowd Premises details displayed are — Crowd Premises, Camera and Events.

To view Crowd Premises,

- Click the **Crowd Premises** tab.



- Click **Show Events** to view the Events configured for the Crowd Premises.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

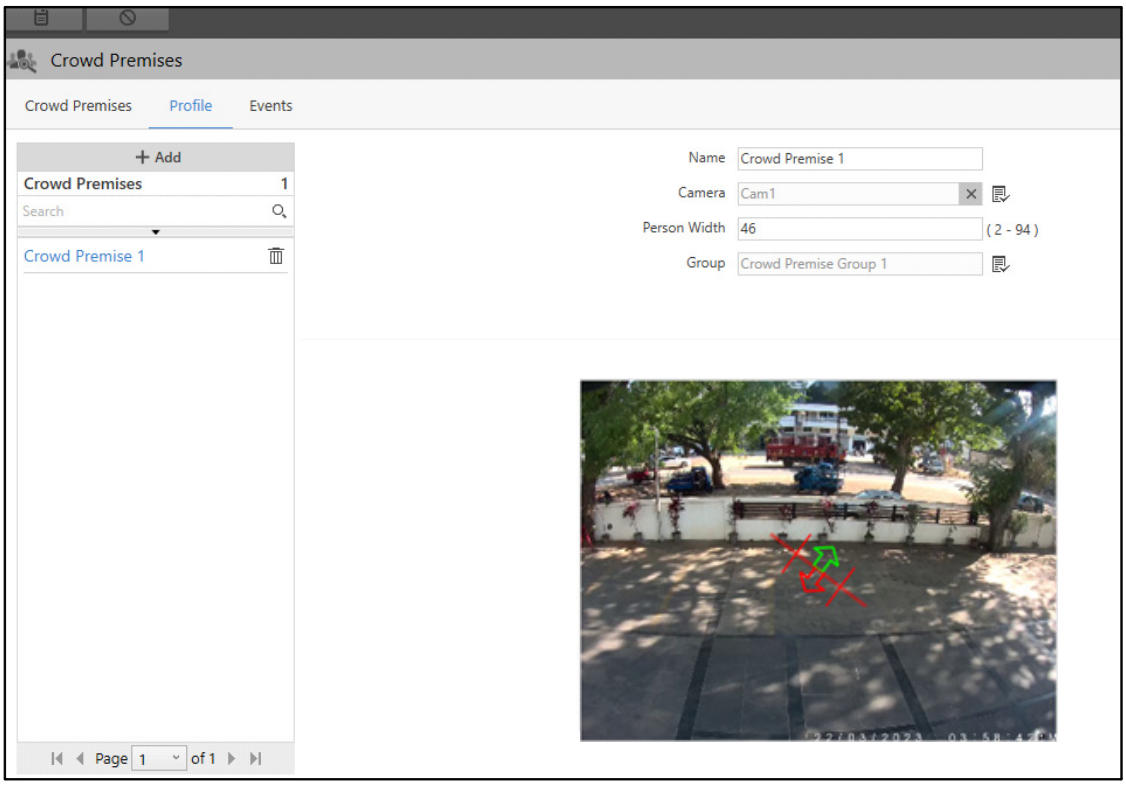
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

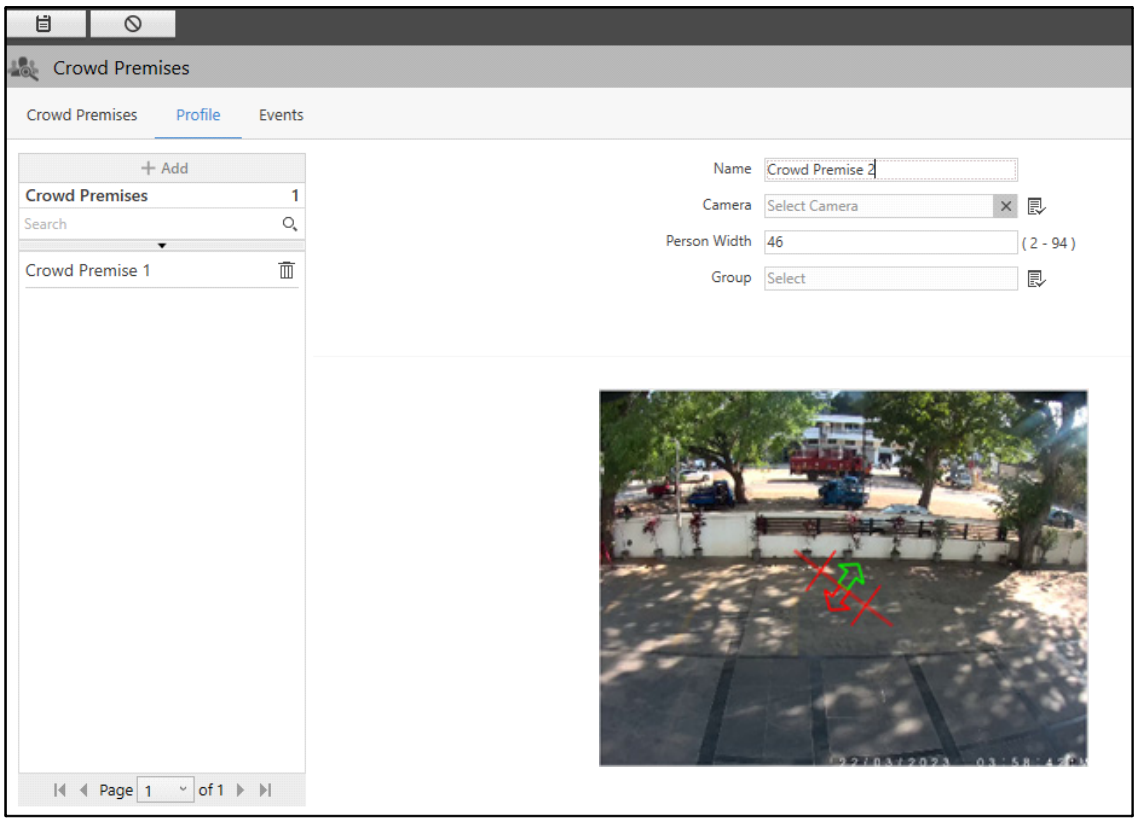
This tab enables you to configure Crowd Premises. All the Crowd Premises configured here appear under the **Crowd Premises** tab.

To configure Crowd Premises,

- Click the **Profile** tab.

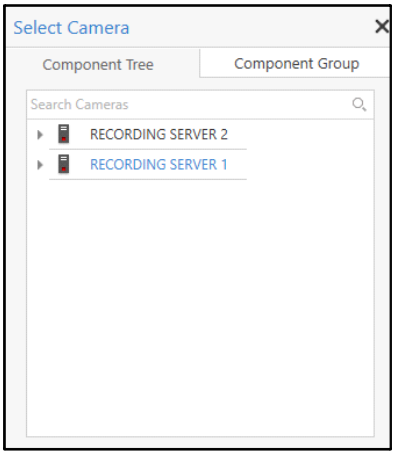


- Click **Add**.



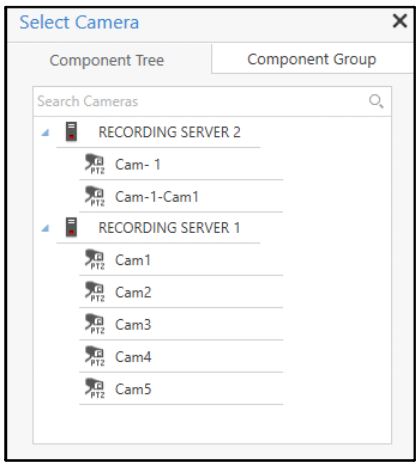
Configure the following parameters:

- **Name**: Specify a suitable name for the Crowd Premise.In Na me, you can enter upto 50 characters. Default: Blank.
- **Camera**: Select the desired camera which you wish to assign to the Crowd Premise using the **Camera** picklist.
  - Click **Camera** picklist. The **Select Camera** pop-up appears.



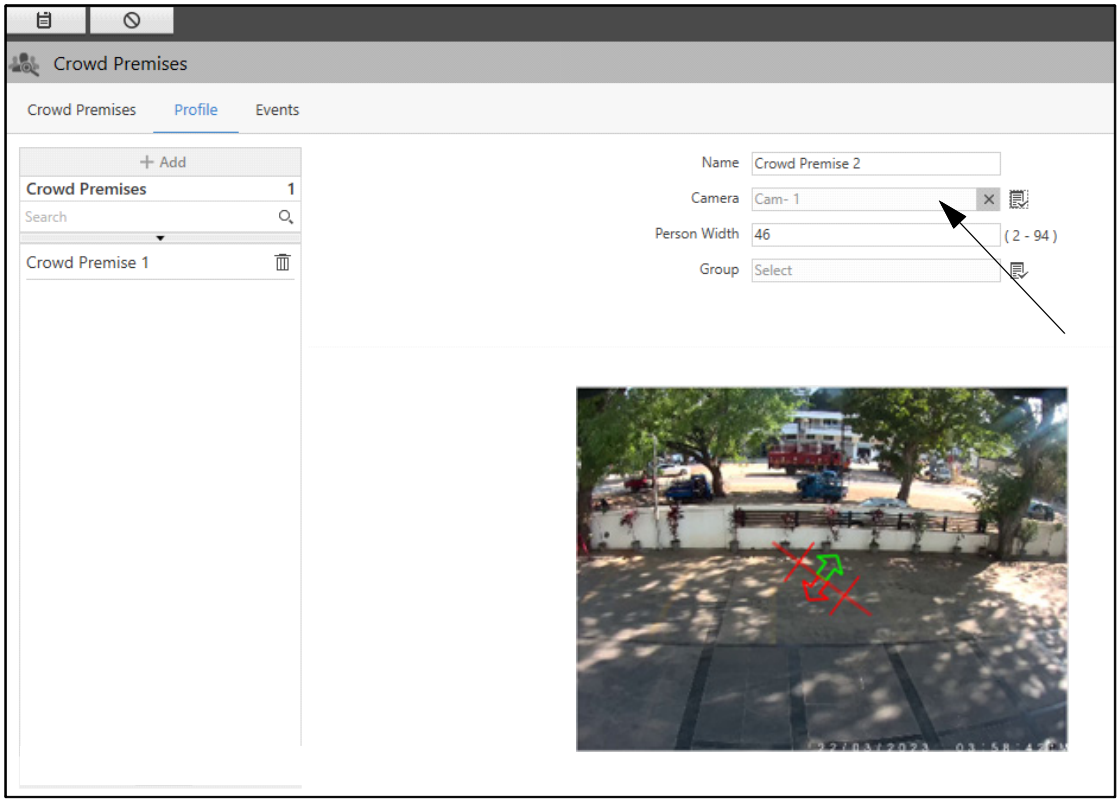
- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To

know more, refer to “Component Group”. Double-click the desired camera to assign it to the Crowd Premises. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click the desired option from the list.
  - Click **Go to selected position** to move the camera to the selected preset position.
- To remove the camera, click **Remove** .



Person Width will not be applicable if you select Object Type in any Event. For details, refer to "Events".

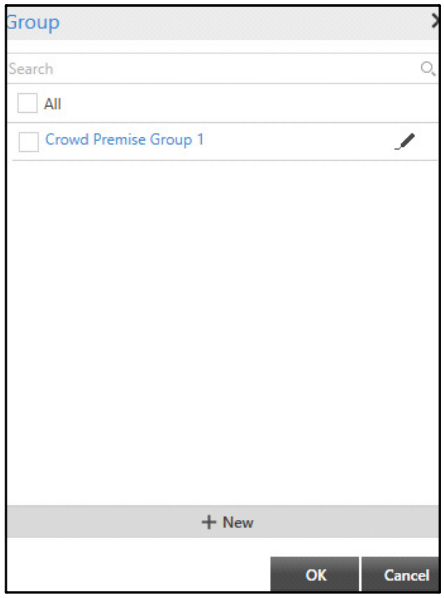
- **Person Width**: Specify the width of the person on the People Counting Line. According to the specified width, the pixels for the minimum and maximum width of the person will be set in the live view. The average shoulder-to-shoulder length of a person as captured in pixels is counted as the person width. Those pixels will be recognized as a single person in the image.

  The person width depends on the position of the camera with respect to the crowd premise. If the camera is far from the crowd premise, the person width will be small. Similarly, if the camera is near the crowd premise, the person width will be large.

  Default Range:2 to 492. Default: 46. Maximum Size will vary as per the line configured by you.

Make sure the Person Width calibration is done precisely for People Counting to work accurately.

- **Group**: Select the desired Crowd Premises Group which you wish to assign to the Crowd Premise using the **Groups** picklist.
  - Click **Groups** picklist. The **Group** pop-up appears.



  - Select the check box of the desired Crowd Premises from the list.

    You can edit an existing Crowd Premises Group by clicking on **Edit** . You can also configure a new Crowd Premises Group by clicking **New**. For more details, refer to "Crowd Premises Group".

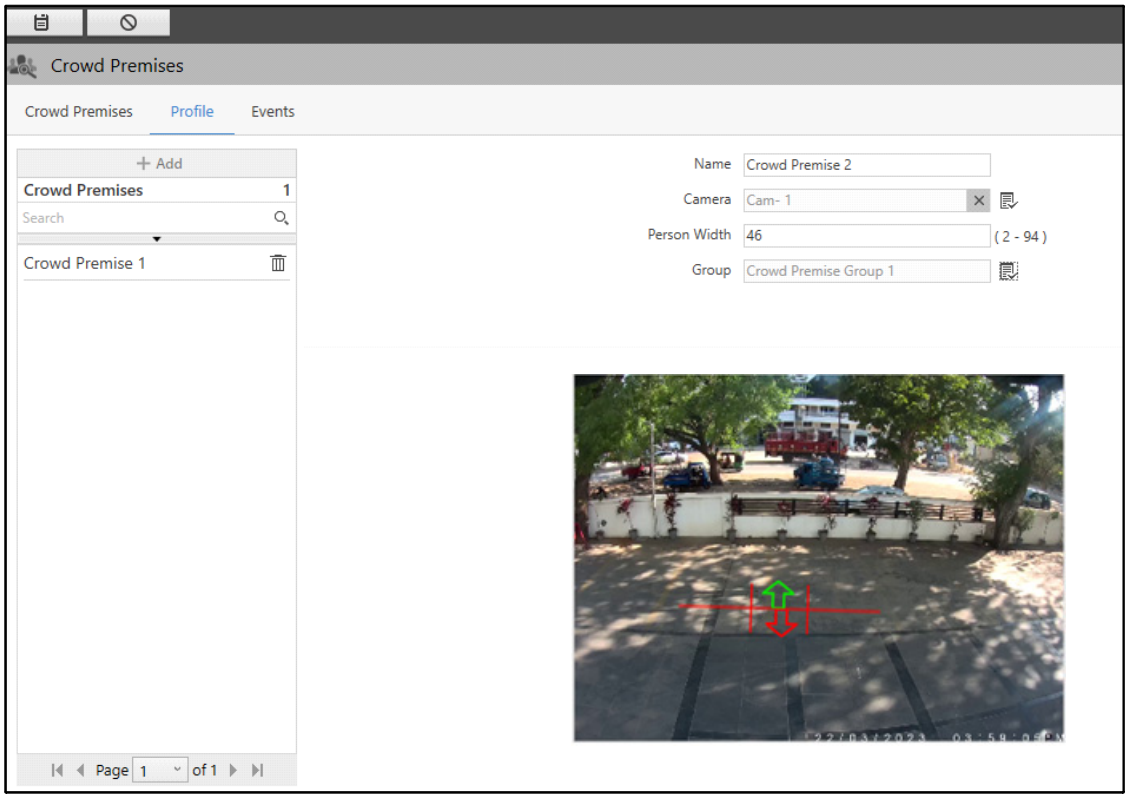
You can assign a particular line/premise to maximum 255 Groups.

  - Click **OK** to confirm or click **Cancel** to discard.

Once a camera is assigned, you can draw the Crowd Premises on the live view of the camera.

- Move the mouse pointer to any one end of the line, a four direction arrow appears. Drag the line to increase or decrease the length of the Security Line and set it as desired.

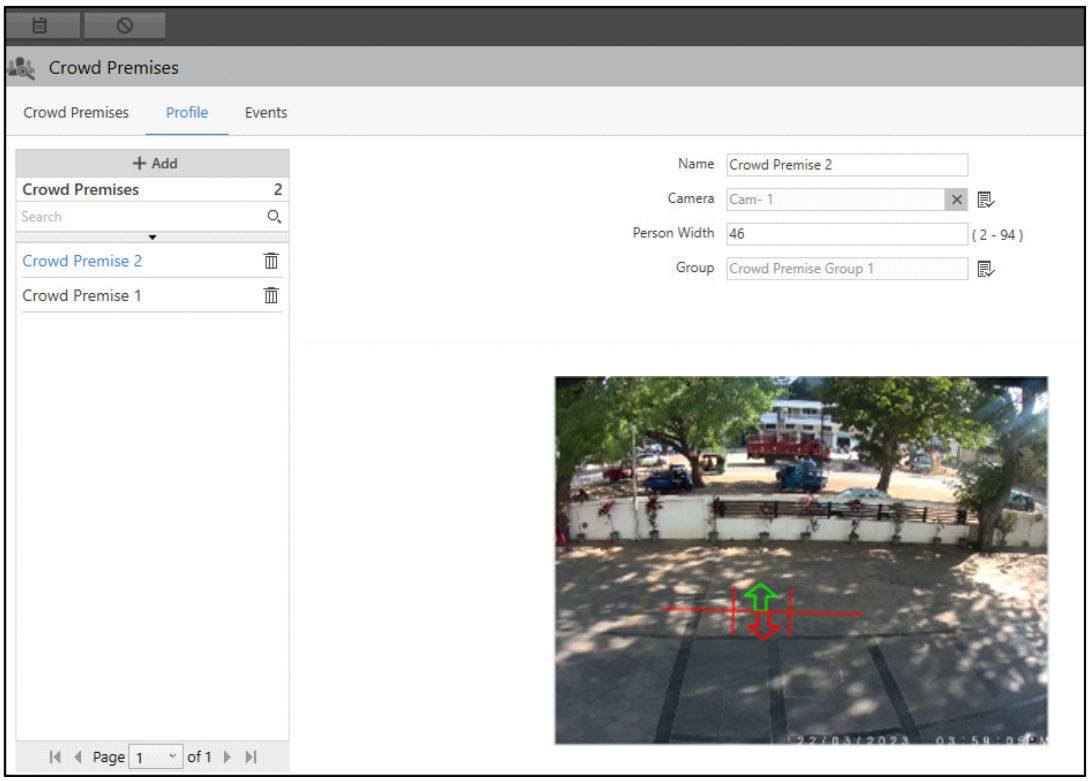
You can also drag it to change the Entry (Green arrow) and Exit (Red arrow) direction. To do so, Move the mouse pointer to any one end of the line, a four direction arrow appears.
Now, drag it in the desired direction.



- Click **Save** to save the settings or **Cancel** to discard.

The new Crowd Premise will appear in the list on the left hand side.

You can edit the configurations of the Crowd Premise or delete it.



- Select the desired Crowd Premise from the list and edit the details on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the Crowd Premise.

Similarly, you can configure the other Crowd Premises.

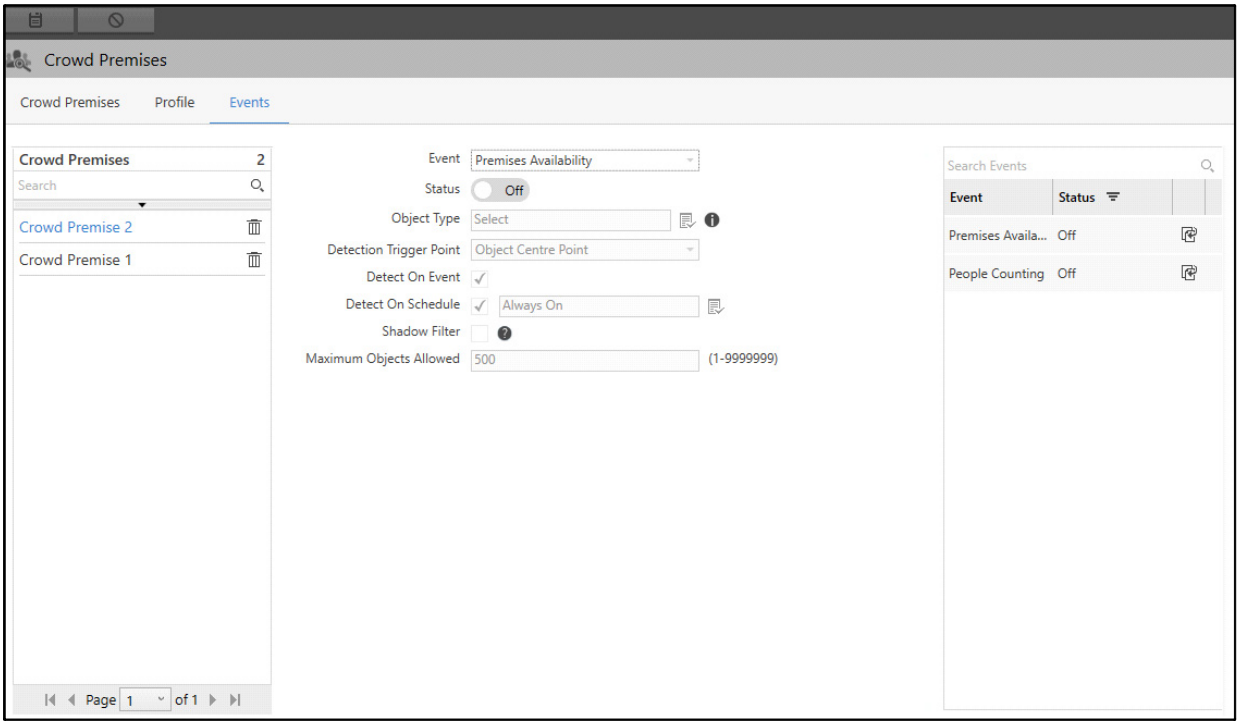
Events

This tab enables you to configure the Events for the Crowd Premises. All the configured Events appear under the **Crowd Premises** tab.

Person Width configured in any "Profile" will not be applicable if you select Object Type in any Event.

To configure an Event,

- Click the **Events** tab.



For Crowd Premises, you can configure two types of Events — “Premise Availability” and “People Counting”.

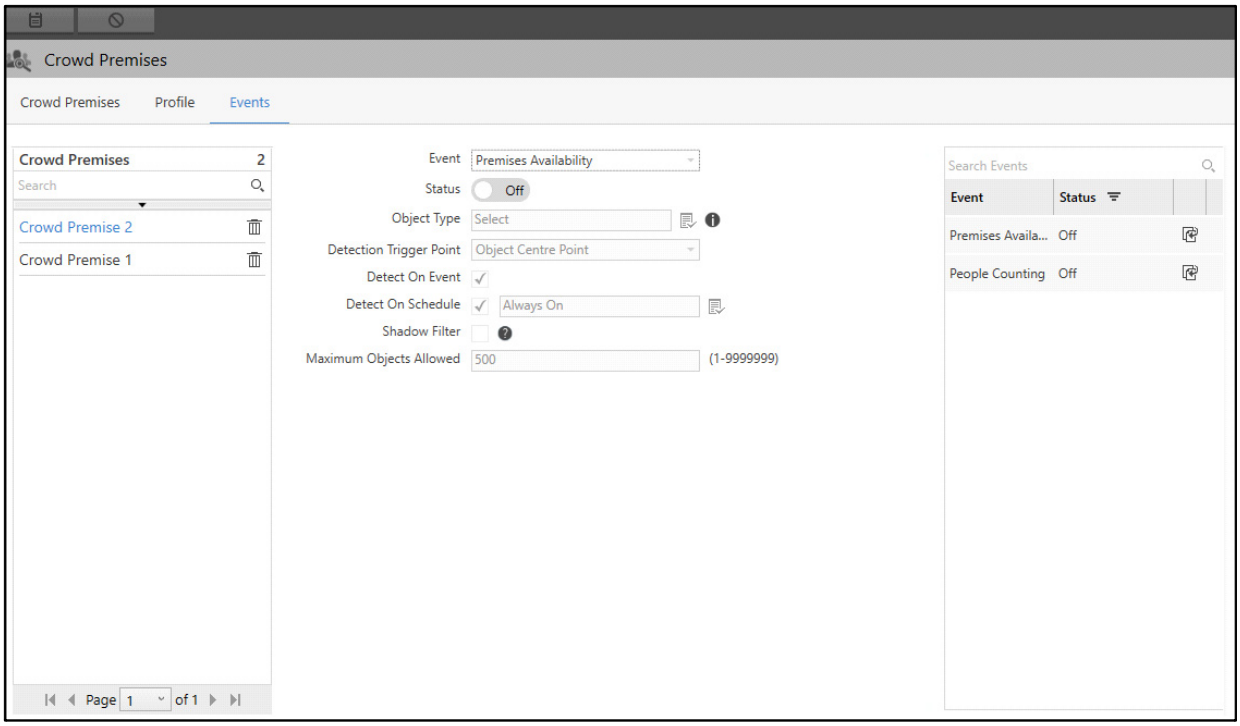
Premise Availability

The Premises Availability feature is used for keeping records of space availability at the premises to accommodate people efficiently. This helps you to know whether the configured premise is full or not and if not full then how much space is remaining in the premises. This is specially used in areas like schools, examination halls etc.

Based on the configured **Maximum Objects Allowed** count, if a person moves towards Red Arrow (Exit), then **Premise Availability** event will be generated, whereas if a person moves towards the Green Arrow (Entry), the **Premise Full** event will be generated.

To configure Premises Availability Event for Crowd Premises,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

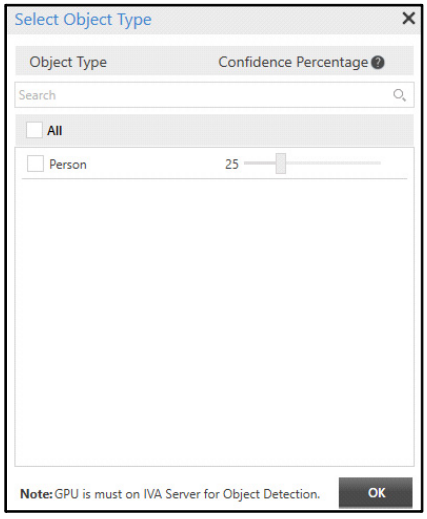


Configure the following parameters:

- **Event**: Select the Premises Availability Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

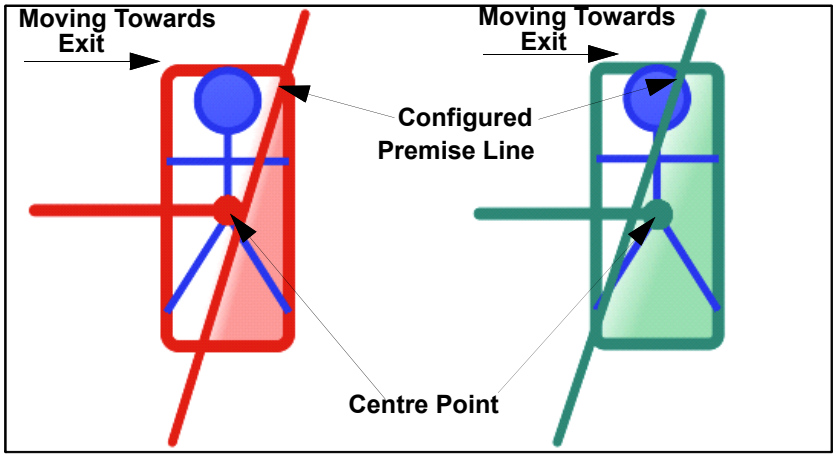


- Select the **Person** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point. Based on the selected option, the IVA engine will detect the selected Object Type.

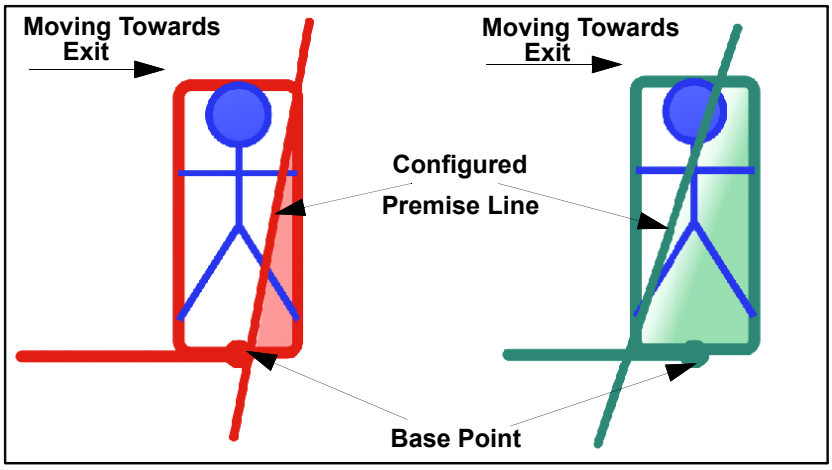
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured premise line.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point of the object crosses the configured premise line, an event will be generated if the object is moving away from the premise line. That is, the Premise will be said to be Available when the person moves away from the premise line in the direction of Red Arrow (Exit) on the configured premise line.

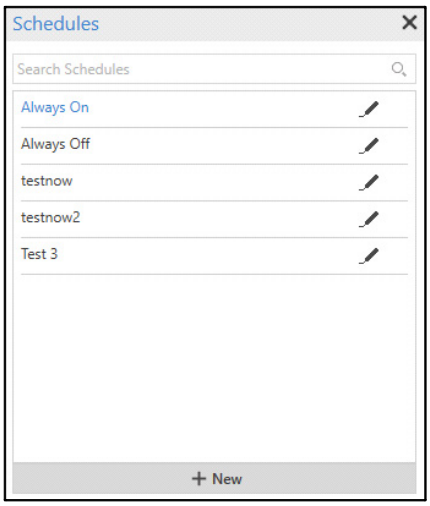


  If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured premise line.

  In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured premise line, an event will be generated if the object is moving away from the premise line. That is, the Premise will be said to be Available when the person moves away from the premise line in the direction of Red Arrow (Exit) on the configured premise line.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of the Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



    - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".
- **Shadow Filter**: Select the check box to ignore the shadow of the people/objects crossing the premises to reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Maximum Objects Allowed**: Specify the number of people/objects allowed in the Premises. Valid Range: 1 to 9999999. Default: 500.

- Click **Save** to save the settings or **Cancel** to discard.

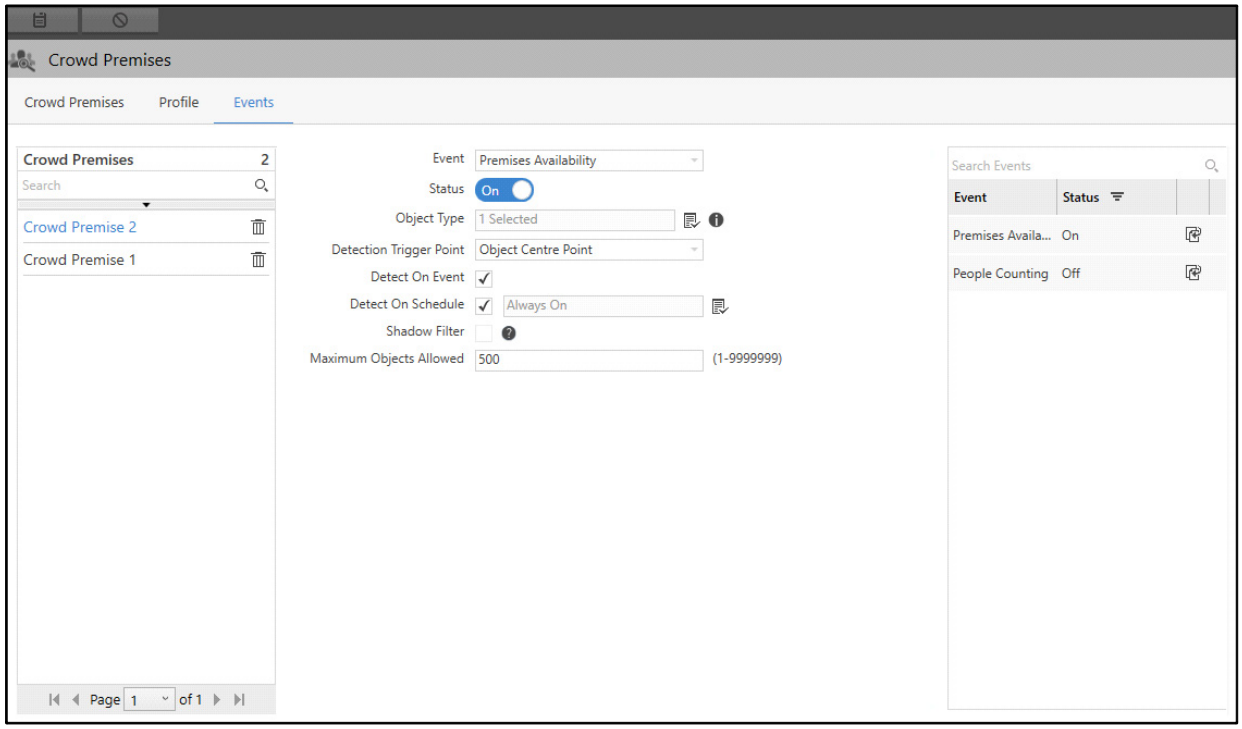
Once you have configured the Event, you can edit its configurations or disable it.

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

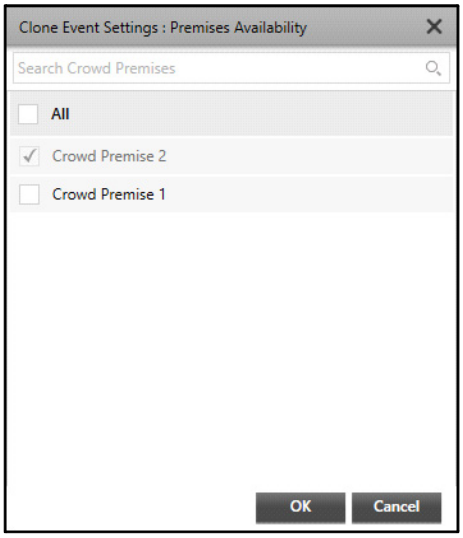
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Crowd Premises is created, the **Clone Event Settings** option is enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Premises Availability** pop-up appears.



- Select the desired crowd premises to which you wish to copy the configurations.

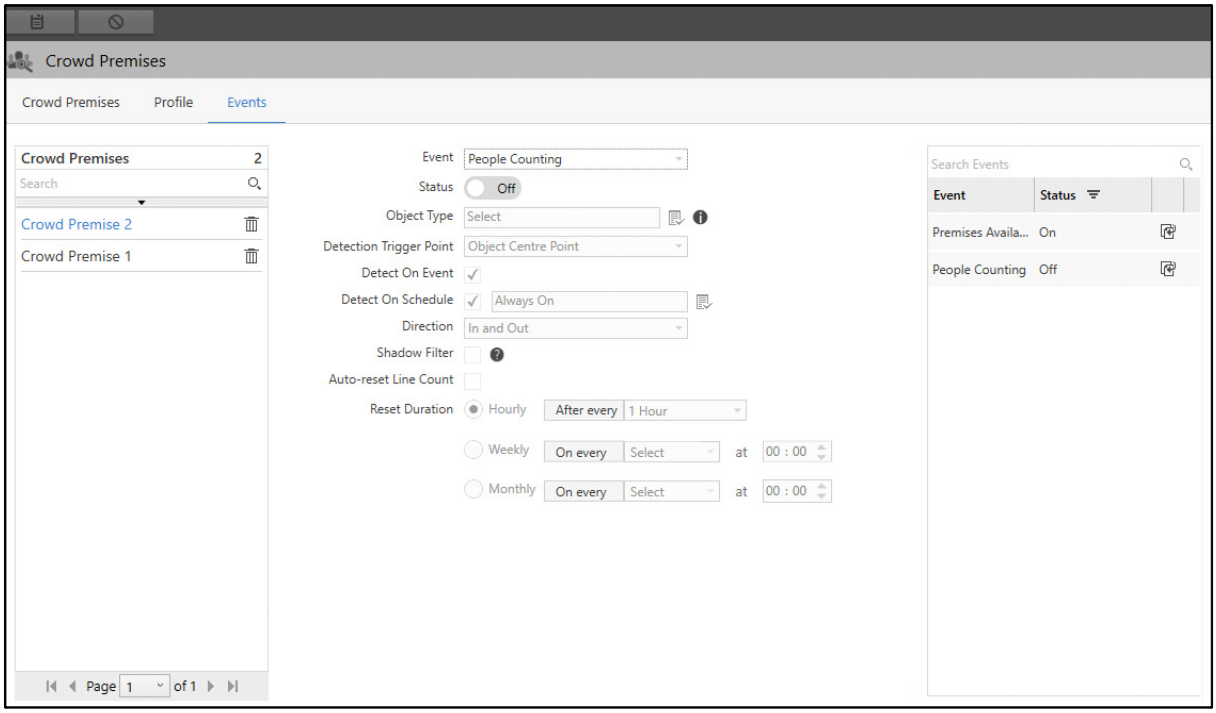
- Click **OK** to confirm or click **Cancel** to discard.

People Counting

The Premises Counting feature is used for keeping a record of the count of people at the premise.

To configure People Counting Event for Crowd Premises,

- Select the desired Profile from the left hand side for which you wish to configure the Event.

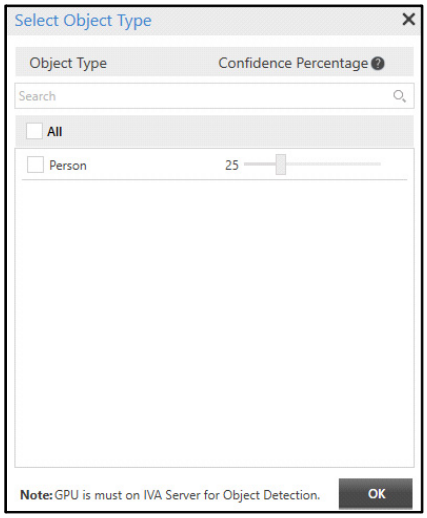


Configure the following parameters:

- **Event**: Select the People Counting Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

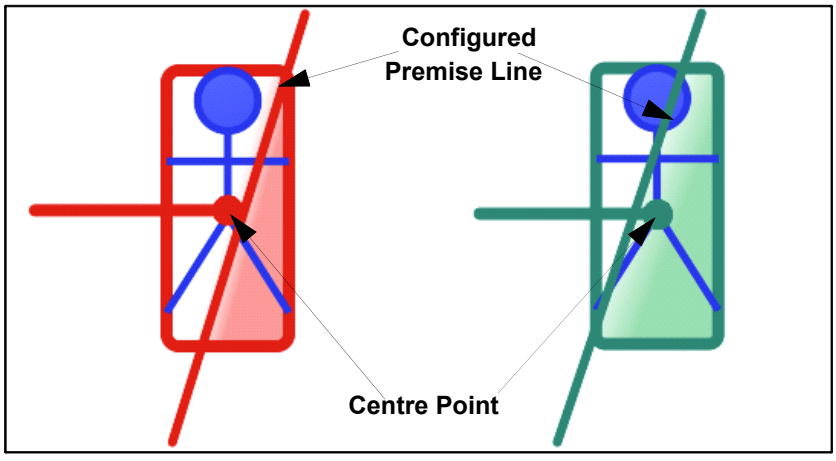


- Select the **Person** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Valid Range: 0-100%. Default: 25. Click **OK**.

- **Detection Trigger Point**: If you have selected **Object Type**, select the Detection Trigger Point from the drop-down list options — Object Centre Point, Object Base Point. Based on the selected option, the IVA engine will detect the selected Object Type.

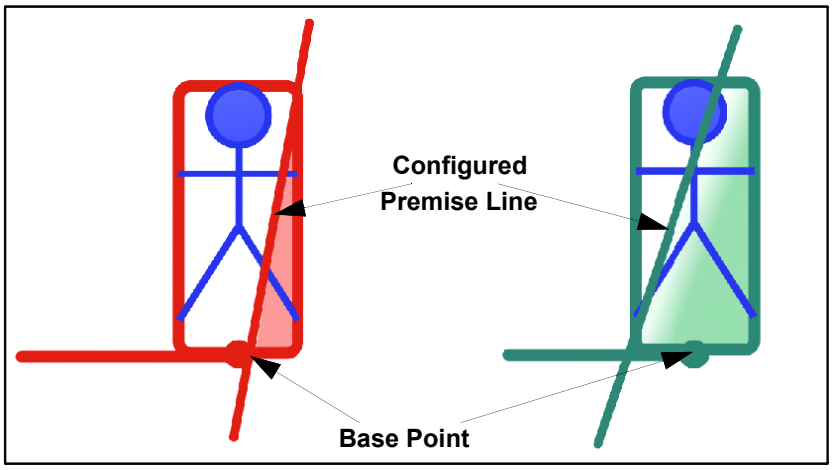
  If you select **Object Centre Point**, the IVA engine will detect the event based on the motion of the centre point of the detected object across the configured premise line.

  In the diagram below, the IVA engine tracks the motion of the centre point of the object. When the centre point of the object crosses the configured premise line in the direction of Red (Exit)/Green (Entry) Arrow, an event will be generated.

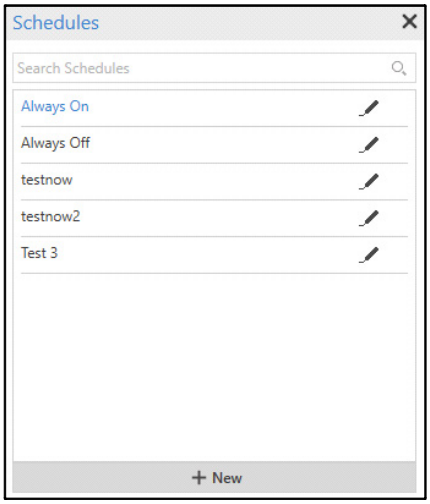


  If you select **Object Base Point**, the IVA engine will detect the event based on the motion of a point at the centre of the base of the detected object across the configured premise line.

  In the diagram below, the IVA engine tracks the motion of a point at the centre of the base of the object. When the point crosses the configured premise line in the direction of Red (Exit)/Green (Entry) Arrow, an event will be generated.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of the Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.
- **Direction**: Select the direction for people count from the drop-down list — In and Out, In or or Out.

  Select **In**, if the Event should occur only when a person enters the premises.

  Select **Out**, if the Event should occur only when a person moves out of the premises.

  Select **In and Out**, if the Event should occur when a person enters or moves out of the premises.
- **Shadow Filter**: Select the check box to ignore the shadow of the people/objects crossing the Premises to reduce false detection.

If you have selected Object Type, then Shadow Filter will be disabled.

- **Auto-reset Line Count**: Select the check box if you wish the People Counting Line counter to reset to zero. If you enable this option, you must configure the Reset Duration.

By default counter will not be reset till 99999999. You can reset the counter by selecting a value from the drop-down list.

- **Reset Duration**: Select the Reset Duration from the options — Hourly, Weekly or Monthly to auto-reset the Line counter.

  - **Hourly:** Select this option to auto-reset the Line counter hourly and select the desired interval from the drop-down list. The Line counter will reset automatically as per the selected interval.

    For example, if you select **1 Hour**, from the drop-down list, then Line counter will be reset automatically after every 1 Hour.
  - **Weekly:** Select this option to auto-reset the Line counter on a particular day of the week and at the chosen time. You can select multiple days of week. Select the desired day from the drop-down list and specify the desired time.

    For example, if you select **Monday** and **Wednesday** from the drop-down list and set the time as 18:00, the Line counter will reset on every Monday and Wednesday of the week at 6 PM.

  - **Monthly:** Select this option to auto-reset the Line counter on a particular date of the month and at the chosen time. You can select multiple dates of the month. Select the desired date from the drop-down list and specify the desired time.

    For example, if you select 1st and 25th date from the drop-down list and set the time as 18:00, the Line counter will reset on every 1st and 25th date of the month at 6 PM.

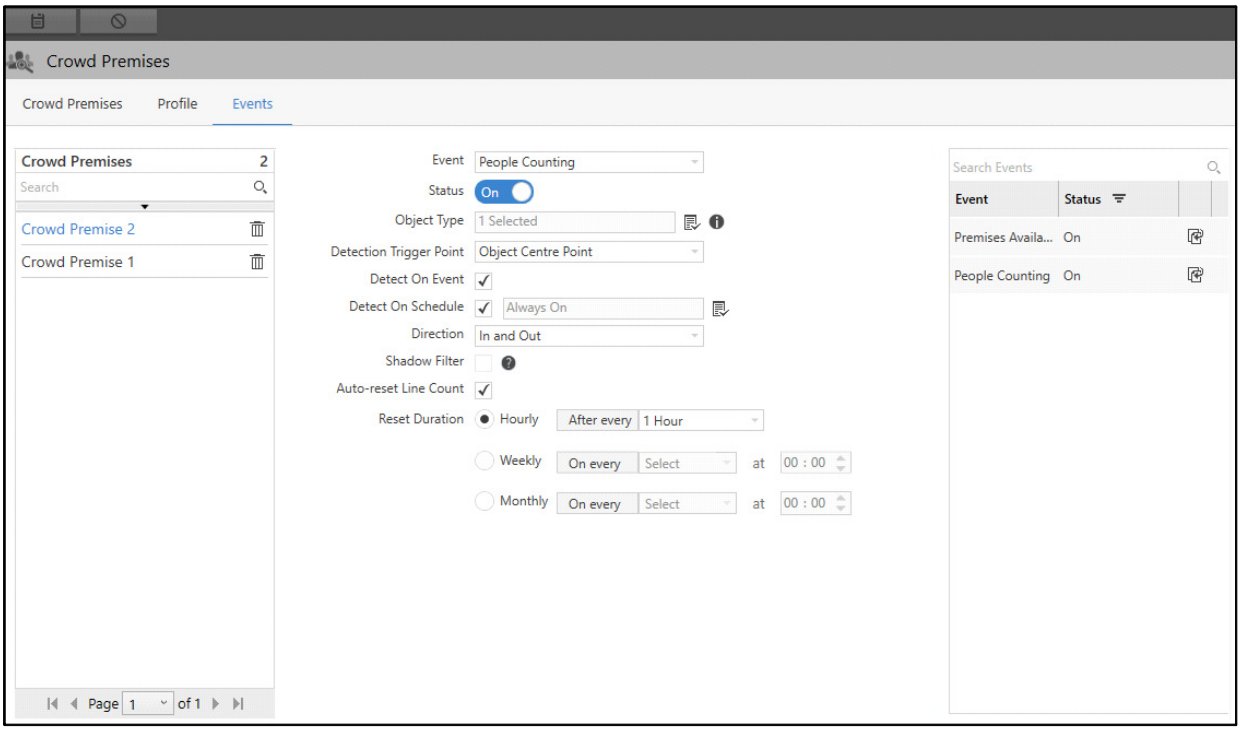
- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

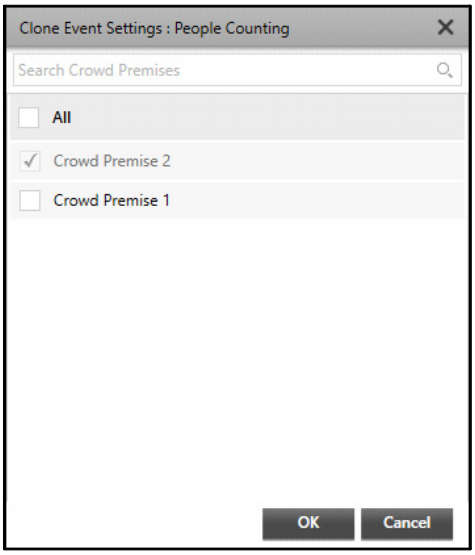
- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

Once the Event is configured, you can copy the Event configurations to other Events. To do so,

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: People Counting** pop-up appears.



- Select the desired crowd premises to which you wish to copy the Event configurations.

- Click **OK** to confirm or click **Cancel** to discard.

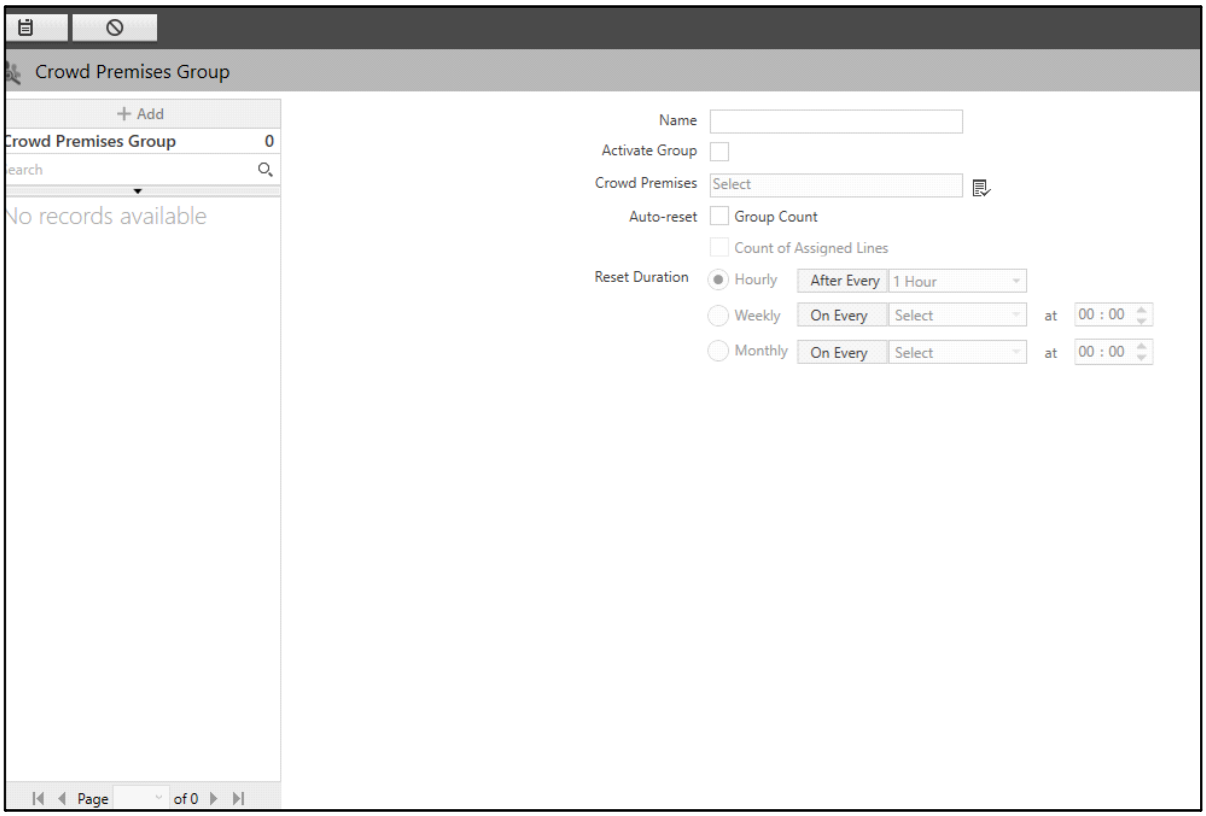
Crowd Premises Group

Crowd Premises Group are the logical groups of lines configured for the Crowd Premises Events. This feature is useful in a situation where a shop has multiple outlets located at different locations and the user needs a cumulative sum of the crowd visiting all the outlets. This helps the user to get a clear view of the number of people entering and exiting the premise.

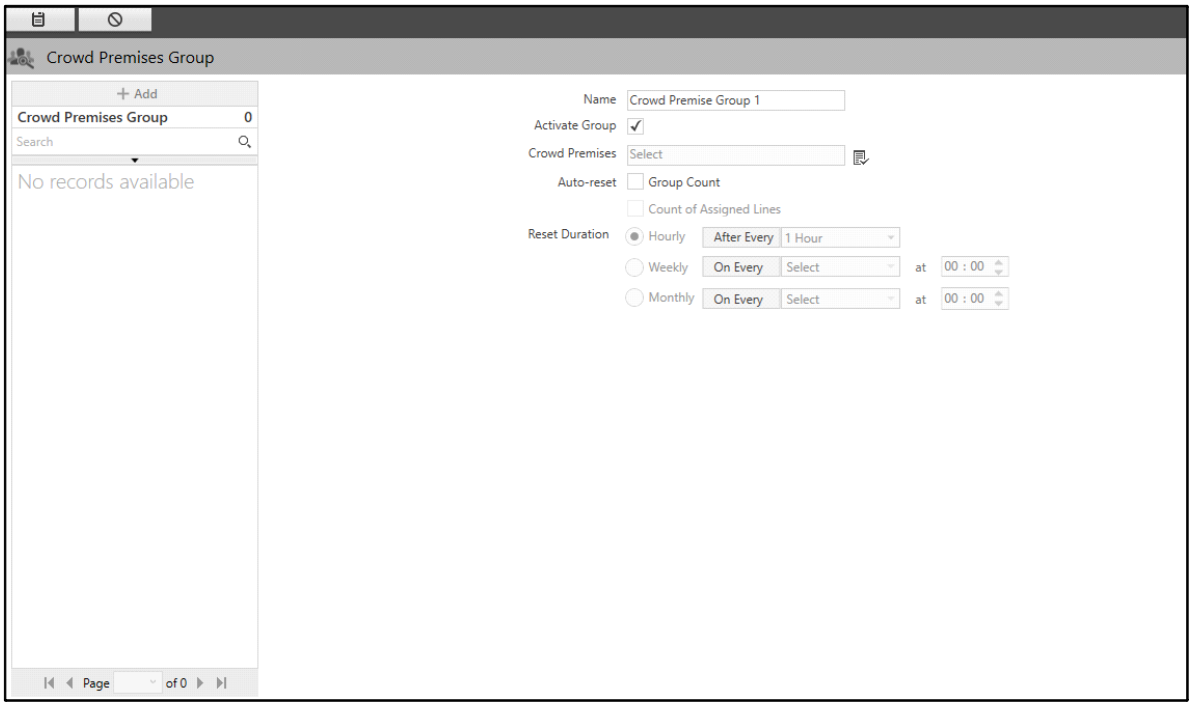
The Crowd Premises Group page displays all the configured Crowd Premises Groups. You can view and configure Crowd Premises Groups from this page.

To configure Crowd Premises Group,

- Click **Crowd Management > Security Sections > Crowd Premises Group**.

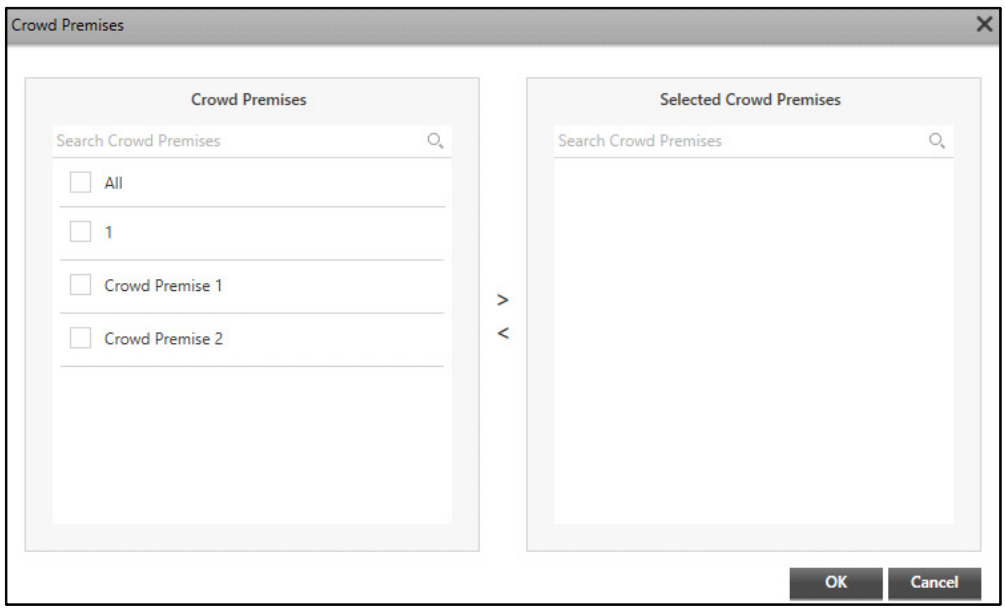


- Click **Add**.



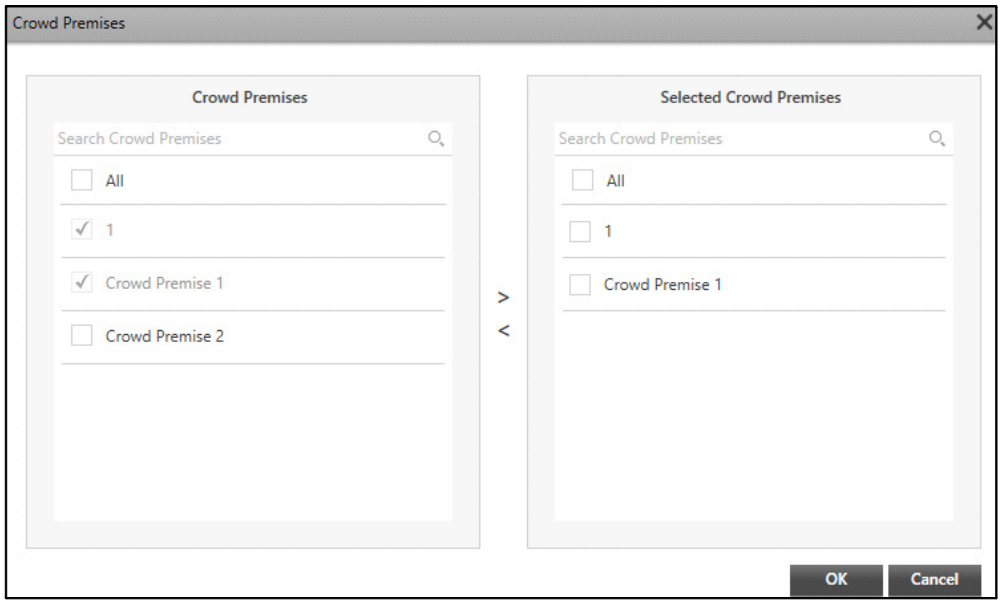
Configure the following parameters:

- **Name:** Specify a suitable name for the Crowd Premises Group. In Na me, you can enter upto 50 characters. Default: Blank.
- **Activate Group:** Select the check box to activate the group.
- **Crowd Premises**: Select the desired Crowd Premise which you wish to assign to the Crowd Premises Group using the **Select Crowd Premises** picklist.
  - Click **Select Crowd Premises** picklist. The **Crowd Premises** pop-up appears.



- All the configured Crowd Premises appear in the list. To configure Crowd Premises, refer to "Crowd Premises". Select the check boxes of the desired Crowd Premises you wish to select from the list. Click the right arrow button to add these Crowd Premises in the **Selected Crowd Premises** list. You can also search for the desired Crowd Premises using the **Search Crowd Premises** search bar.

  To remove Crowd Premises, select the check boxes of the desired Crowd Premises you wish to remove from the Selected Crowd Premises list. Click the left arrow button to remove the Crowd Premises from the Selected Crowd Premises list.



- Click **OK** to confirm or click **Cancel** to discard.

Auto-reset

- **Auto-reset Group Count**: Select the check box to automatically reset the Group Count of the Parking Premises Events. If this check box is enabled then the other parameters can be configured.

- **Count of Assigned Lines**: If Group Count is enabled, then only you can select this check box. Select the check box to automatically reset the count of the Lines assigned to the Group. If the same Lines are assigned to multiple groups, the Line count is reset for all the Groups.

If Auto-reset check box is not enabled, then the counter will not reset automatically. It can be reset either manually or when the counter reaches its limit, that is, till 999999999. Reset is done by the Management Server for selected Group.

- **Reset Duration**: Select the Reset Duration from the options — Hourly, Weekly or Monthly to auto-reset the Line counter.

  - **Hourly:** Select this option to auto-reset the Group/Line counter hourly and select the desired interval from the drop-down list. The Group/Line counter will reset automatically as per the selected interval.

    For example, if you select **1 Hour**, from the drop-down list, then Group/Line counter will be reset automatically after every 1 Hour.

- **Weekly:** Select this option to auto-reset the Group/Line counter on a particular day of the week and at the chosen time. You can select multiple days of week. Select the desired day from the drop-down list and specify the desired time.

  For example, if you select **Monday** and **Wednesday** from the drop-down list and set the time as 18:00, the Group/Line counter will reset on every Monday and Wednesday of the week at 6 PM.

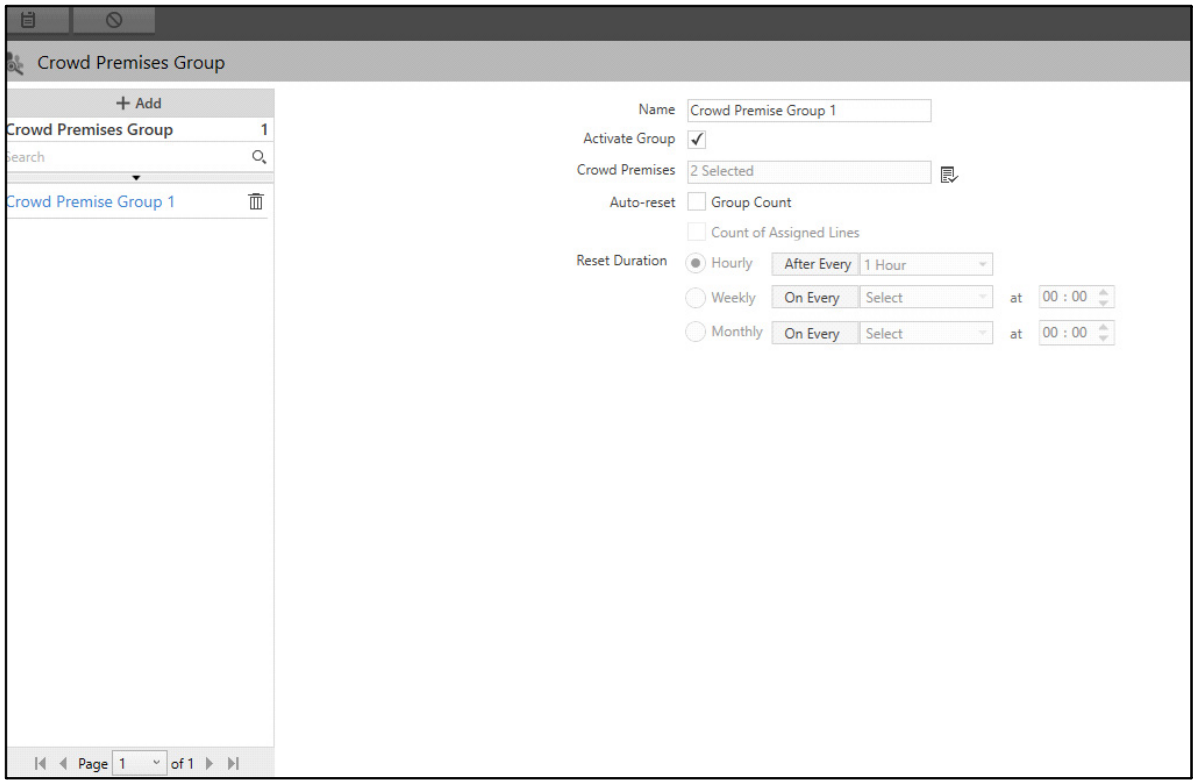
- **Monthly:** Select this option to auto-reset the Group/Line counter on a particular date of the month and at the chosen time. You can select multiple dates of the month. Select the desired date from the drop-down list and specify the desired time.

  For example, if you select 1st and 25th date from the drop-down list and set the time as 18:00, the Group/Line counter will reset on every 1st and 25th date of the month at 6 PM.

- Click **Save** to save the settings or **Cancel** to discard.

The Crowd Premises Group appears in the list on the left hand side.

You can edit the configurations of the Crowd Premises Group or delete it.



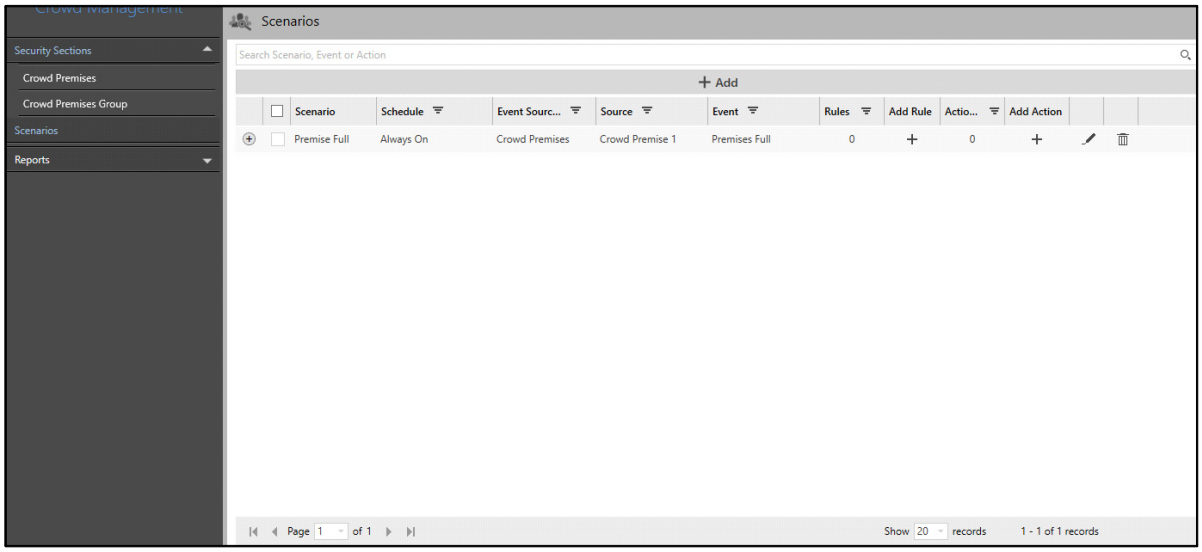
- Select the desired Crowd Premises Group from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the Crowd Premises Group.

Crowd Management-Scenarios

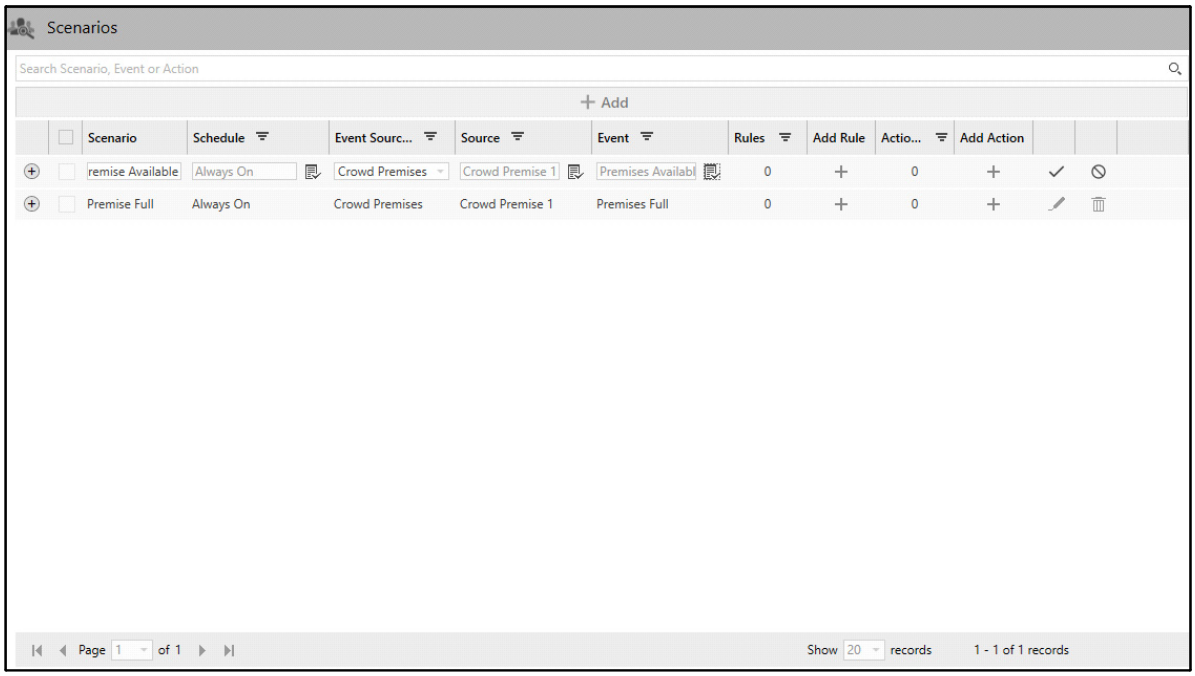
In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send SMS) on the occurrence of the Events at certain sources (For example, Premises Available). The Scenarios page displays all the Scenarios configured for Crowd Management. You can view and configure the Scenarios for all the configured Crowd Premises.

To configure Scenarios,

- Click **Crowd Management > Scenarios**.



- Click **Add.**



The configurations of Scenarios for Crowd Management are similar to that of the Basic Scenario. For details, refer to “Basic Scenario”.

People Counting Reports

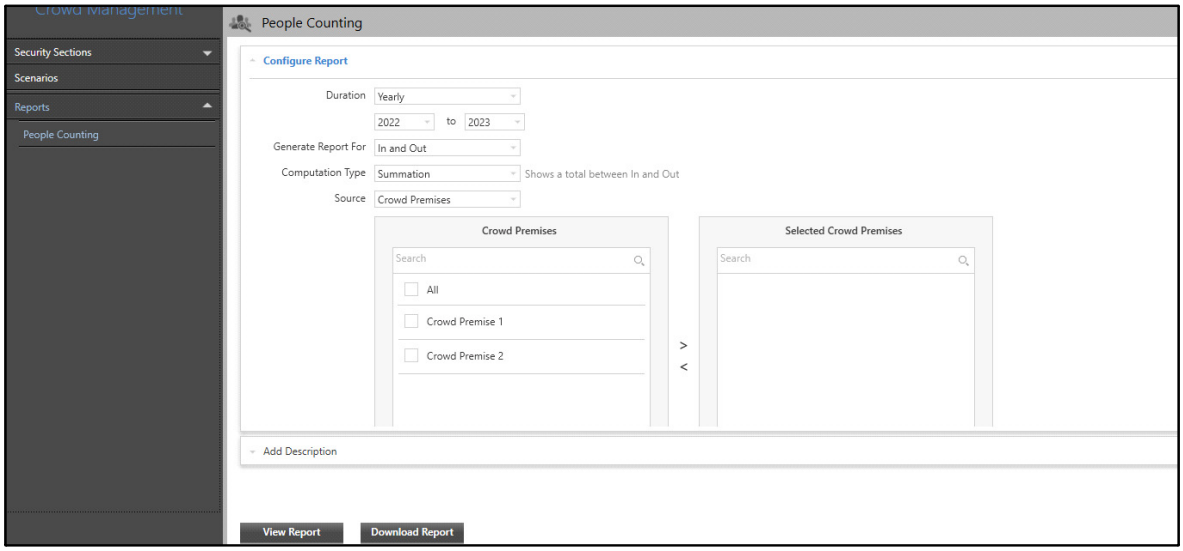
People Counting Report provides tabular as well as graphical statistics on crowd behavior. These statistics can be useful in managing the crowd at various locations from one place. It allows the user to track the number of persons passing-by within the defined duration at any place. The report includes the count of people across multiple entries/ exits.

For example, consider a shop having various outlets at different locations. Based on this report, the user can track the number of persons entering and exiting various outlets from a single location. If the crowd increases at a particular outlet, it can be managed by taking appropriate actions.

The People Counting page enables you to configure parameters for People Counting Reports. You can view and configure People Counting Reports on Yearly, Monthly, Weekly, Daily, Hourly and Peak Hour basis.

To configure People Counting Report,

- Click **Crowd Management > Report > People Counting**.



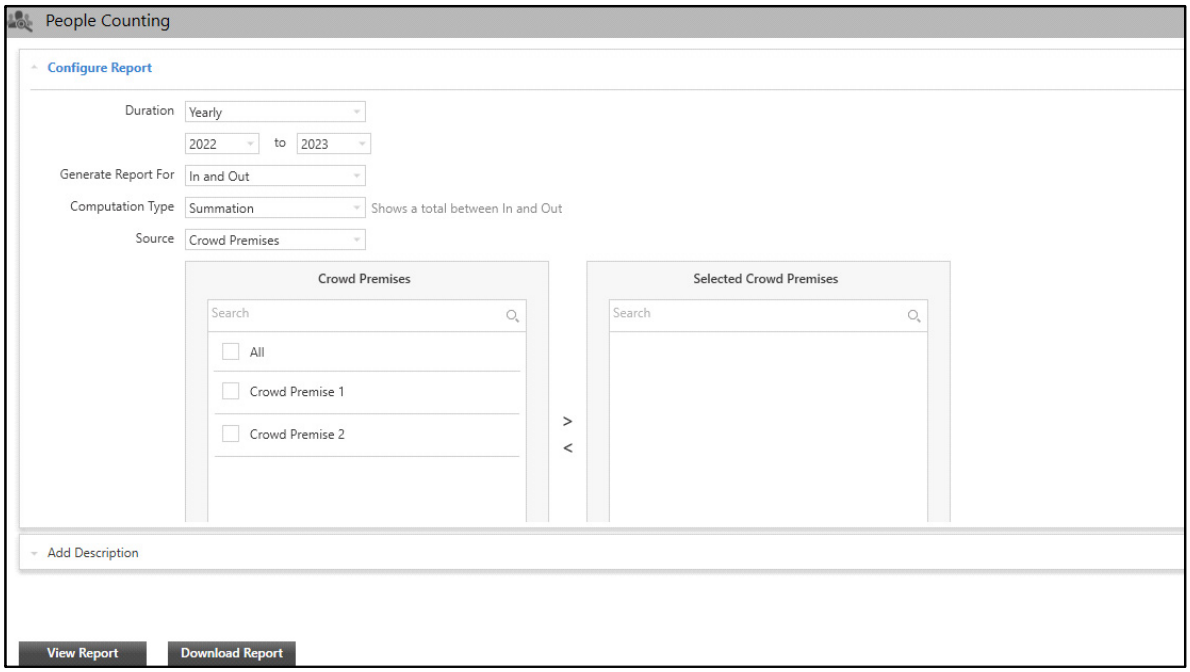
The People Counting page contains two collapsible panels — “Configure Report” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the People Counting Report from this collapsible panel.

To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

- **Duration**: Select the desired Duration from the drop-down list — Yearly, Monthly, Daily, Hourly, Weekly and Peak Hour Reports.
    - **Yearly**: Select this option to generate yearly reports. Select the desired From and To year from the drop-down lists.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
    - **Weekly**: Select this option to generate weekly reports. Select the desired From and To dates from the calendar. Select the day of the week from when you wish the weekly report from the **Start Week From** drop-down list.
    - **Peak Hour**: Select this option to generate reports for the peak hours. Select the period for which you wish the report from the **Period** drop-down list. Select the year, month or day to configure the peak period duration. Specify the **Peak Period** time.
- **Generate Report For**: Select the parameter for which you wish to generate the report from the drop-down list options — In, Out and In and Out.
    - If you select **In**, the report will include only **In** counts of the people from various locations.
    - If you select **Out**, the report will include only **Out** counts of the people from various locations.

- If you select **In and Out,** the report will include both **In** and **Out** counts of the people from various locations.

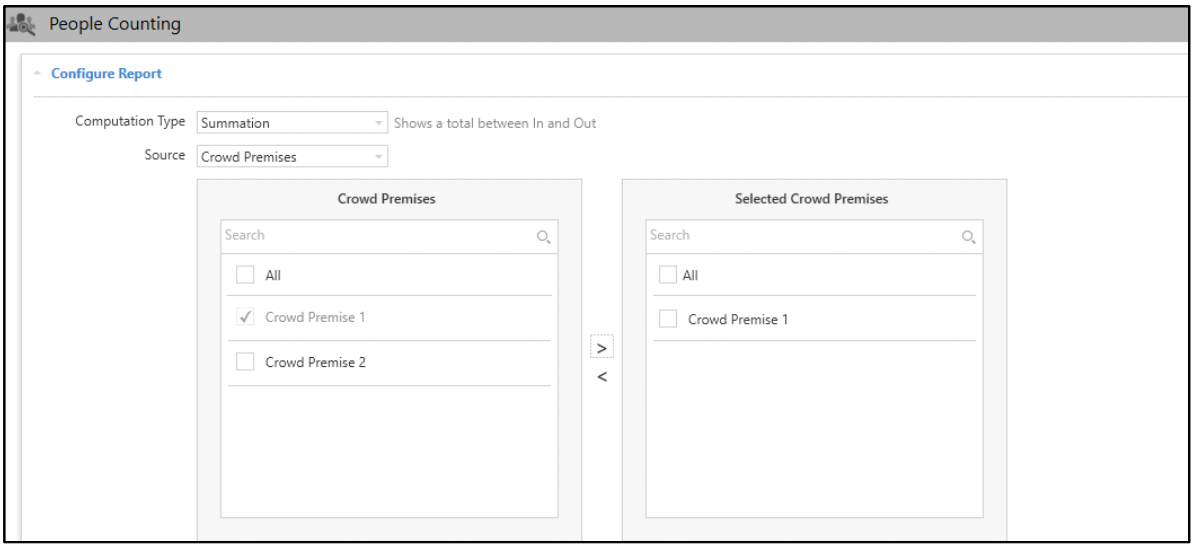
- **Computation Type**: Select the type of computation for the report from the drop-down list — Summation, Differentiation and Maximum Count. The data will be processed according to the selected computation type option.

  - **Summation**: This report will give you total counts between In and Out for the selected Crowd Premises or Crowd Premises Group.

  - **Differentiation**: This report will give you difference between In and Out count for the selected Crowd Premises or Crowd Premises Group.

  - **Maximum Count**: This report will give the maximum count of In or Out count for the selected Crowd Premises or Crowd Premises Group.

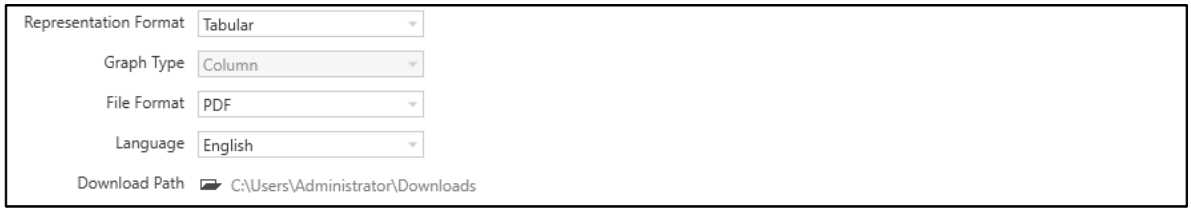
- **Source**: Select the source from the drop-down list — Crowd Premises or Crowd Premises Group.



  - Select the check boxes of the desired Crowd Premises or Crowd Premises Group you wish to select for the report from the **Crowd Premises** or **Crowd Premises Group** list. Click the right arrow button to add these Crowd Premises or Crowd Premises Group in the **Selected Crowd Premises** or **Selected Crowd Premises Group** list. You can also search for the desired Crowd Premises or Crowd Premises Group using the search bar.

    To remove Crowd Premises or Crowd Premises Group, select the check boxes of the desired Crowd Premises or Crowd Premises Group you wish to remove from the Selected Crowd Premises or Selected Crowd Premises Group list. Click the left arrow button to remove the Crowd Premises or Crowd Premises Group from the list.

- **Representation Format**: Select the format in which you wish the report to be generated from the drop-down list.



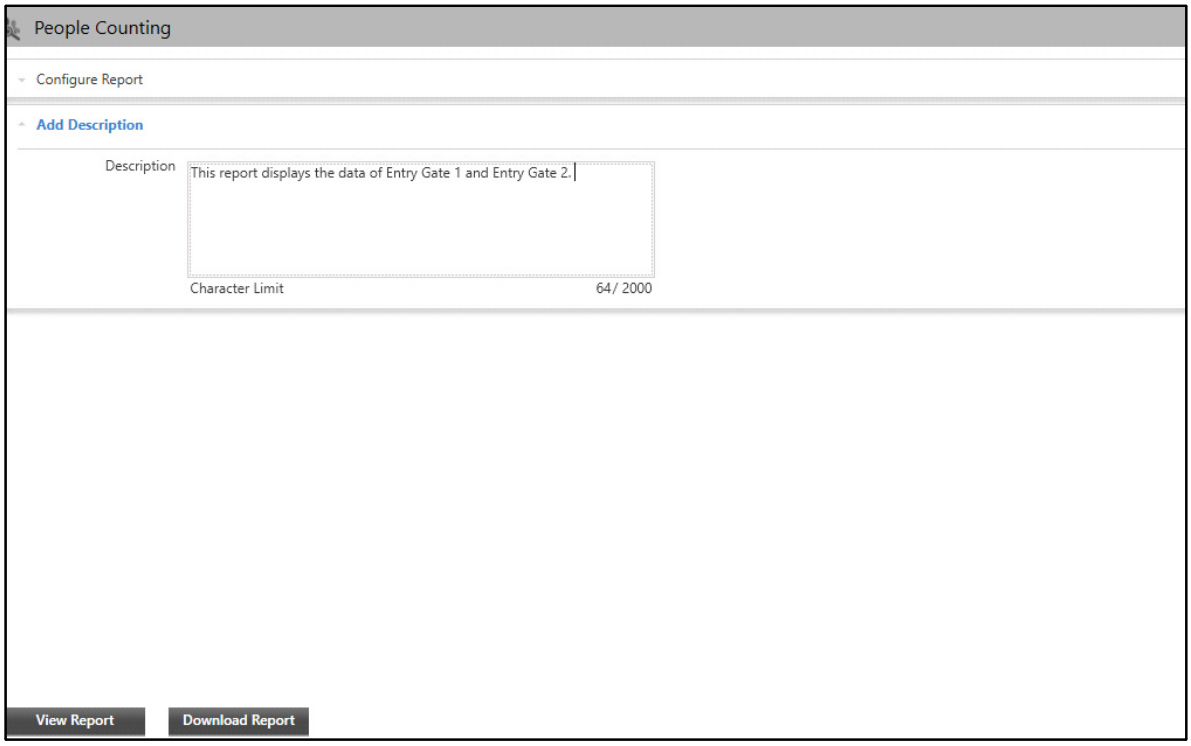
- **Graph Type**: Select the Graph Type from the drop-down list if you selected Graph as the Representation Format.
- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all the folders which are in the drive. Select the desired folder.

Add Description

This panel allows you to add a description for the People Counting Report once the report configurations are done. This description is visible in the generated report.

To configure the description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. The Description can be of upto 2000 characters only and it is displayed on the second page of the report.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

CHAPTER 12

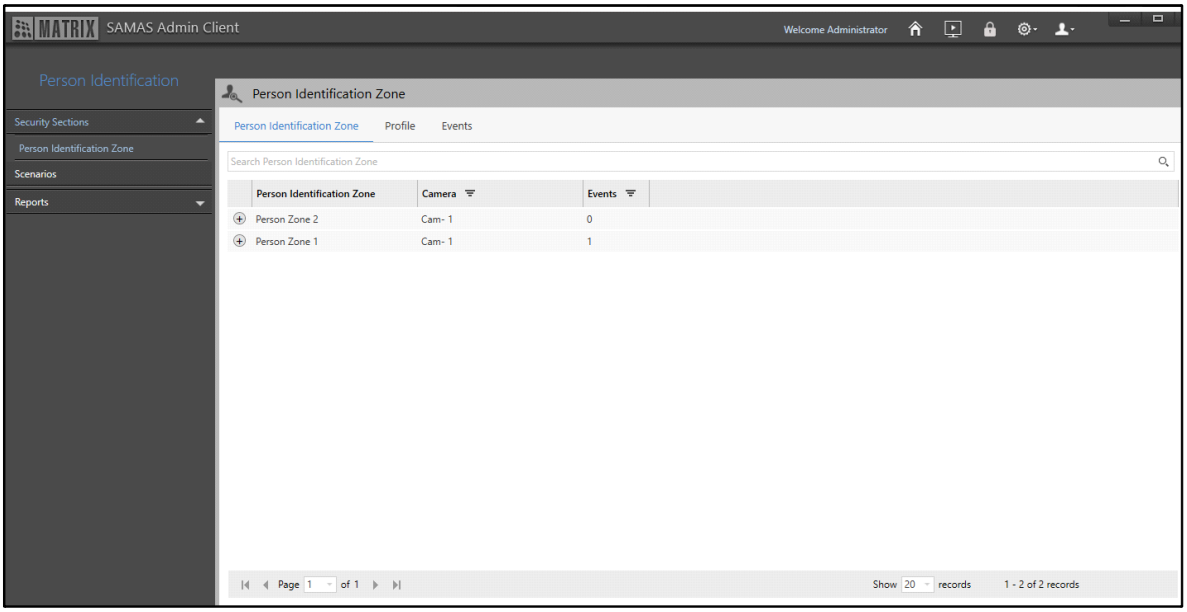
Person Identification

The Person Identification module enables you to configure various Person Identification zones and Events for them. Person Identification uses video content analysis which is effective in detecting Events such as Face Detection based on live stream of a camera. It also enables you to configure Scenarios based on the Events.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report— assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure Person Identification,

- Click **Person Identification**.



The Person Identification module contains these pages — "Person Identification Zone" and "Person Identification-Scenarios".

*The Face Recognition Camera[7] license will be consumed when Face Detection Event is configured. For detailed license information, refer to the **SATATYA SAMAS Installation Guide**.*

To ensure smooth functioning of the Face Detection Event, make sure the IVA Server and MS are upgraded to the latest and same version.

7. *This feature is not available in the current Software Release. It will be included in the upcoming release.*

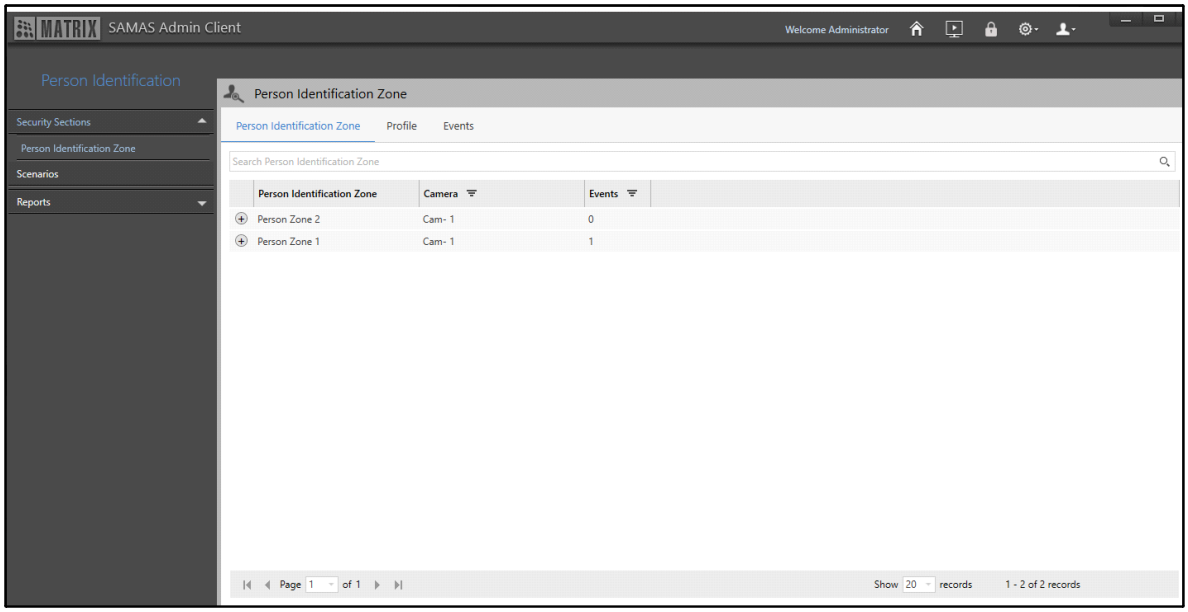
Person Identification-Zone

The Person Identification module allows to configure Person Identification Zones wherein human faces appearing on the live of the camera can be detected. The Person Identification Zone feature is useful at places like Banks, Offices, etc. to detect any Events (For example, Face Detection) in the premises. These Events can help security person or management to identify any suspicious person in case any unusual activity takes place. Events that can be configured against the configured Person Identification Zones is Face Detection.

The Person Identification Zone page displays all the configured Person Identification Zones. You can view and configure the Person Identification Zones from this page. For each zone, when faces are detected, the total count is displayed in the Event Log.

To configure Person Identification Zones,

- Click **Person Identification > Person Identification Zone**. The **Person Identification Zone** page appears by default.



The Person Identification Zone page consists of the following tabs:

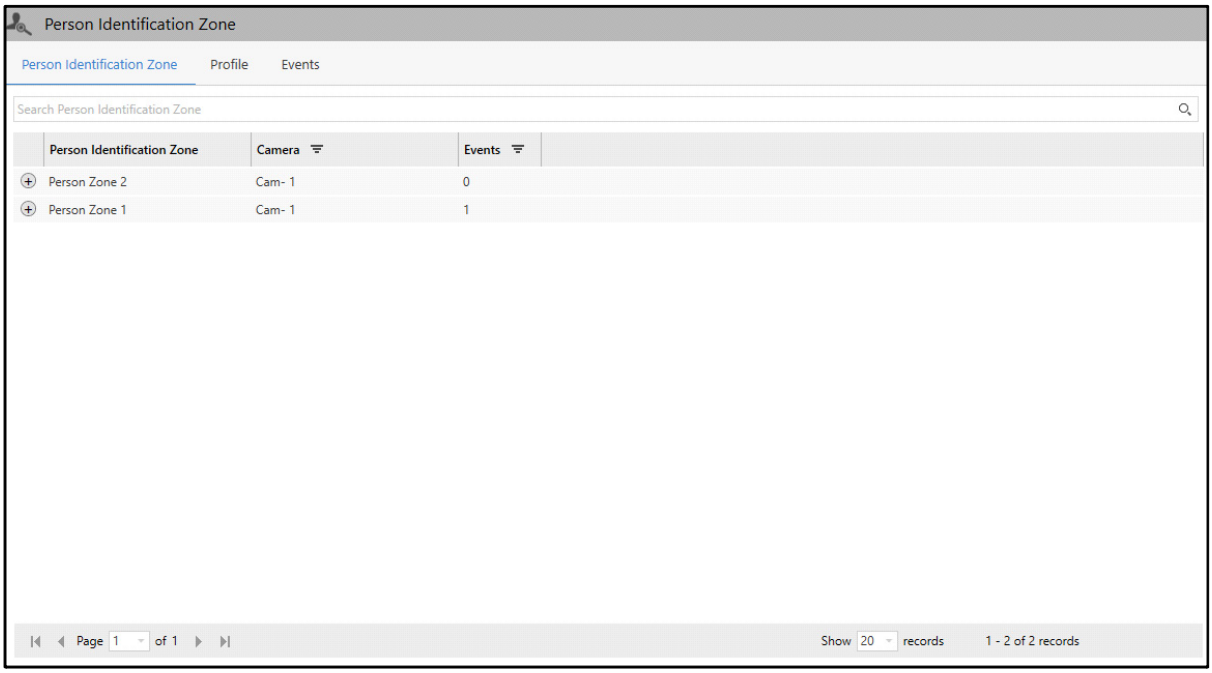
- “Person Identification Zone”
- “Profile”
- “Events”

Person Identification Zone

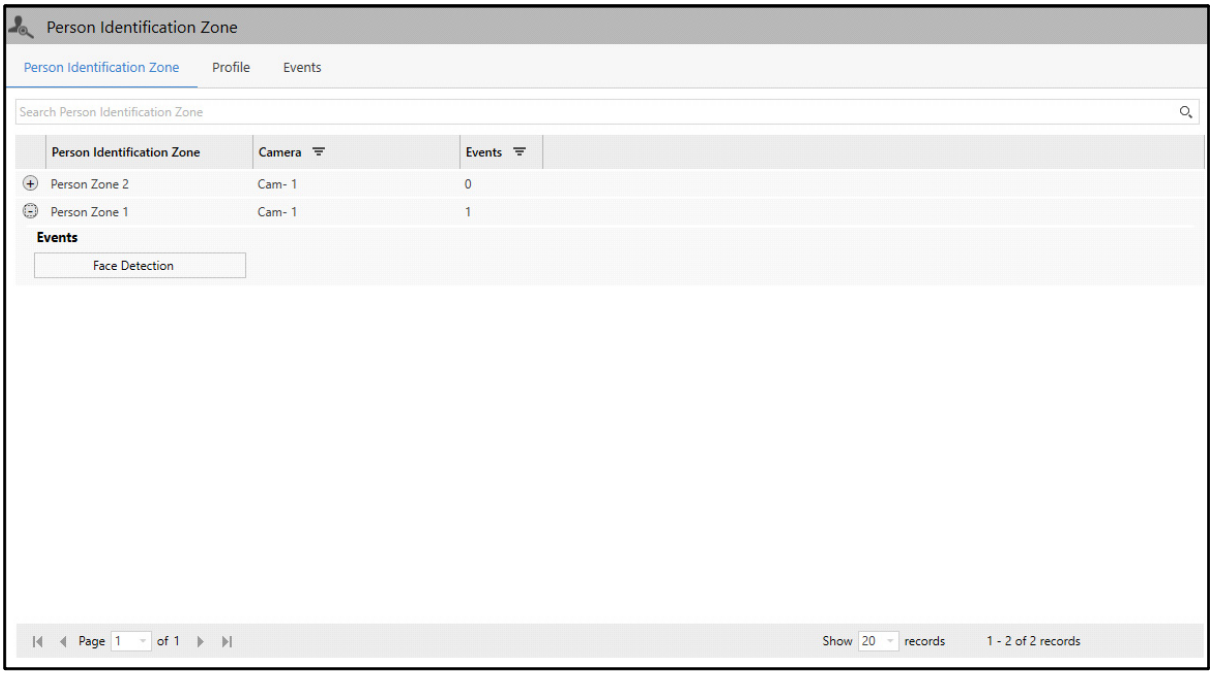
This tab enables you to view Person Identification Zones. You can configure the Person Identification Zones from “Profile”. All the Person Identification Zones and the Events configured for them appear under this tab. The Person Identification Zone details displayed are — Person Identification Zone, Camera and Events.

To view Person Identification Zone,

- Click the **Person Identification Zone** tab.



- Click **Show Events** to view the Events configured for the Person Identification Zone.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

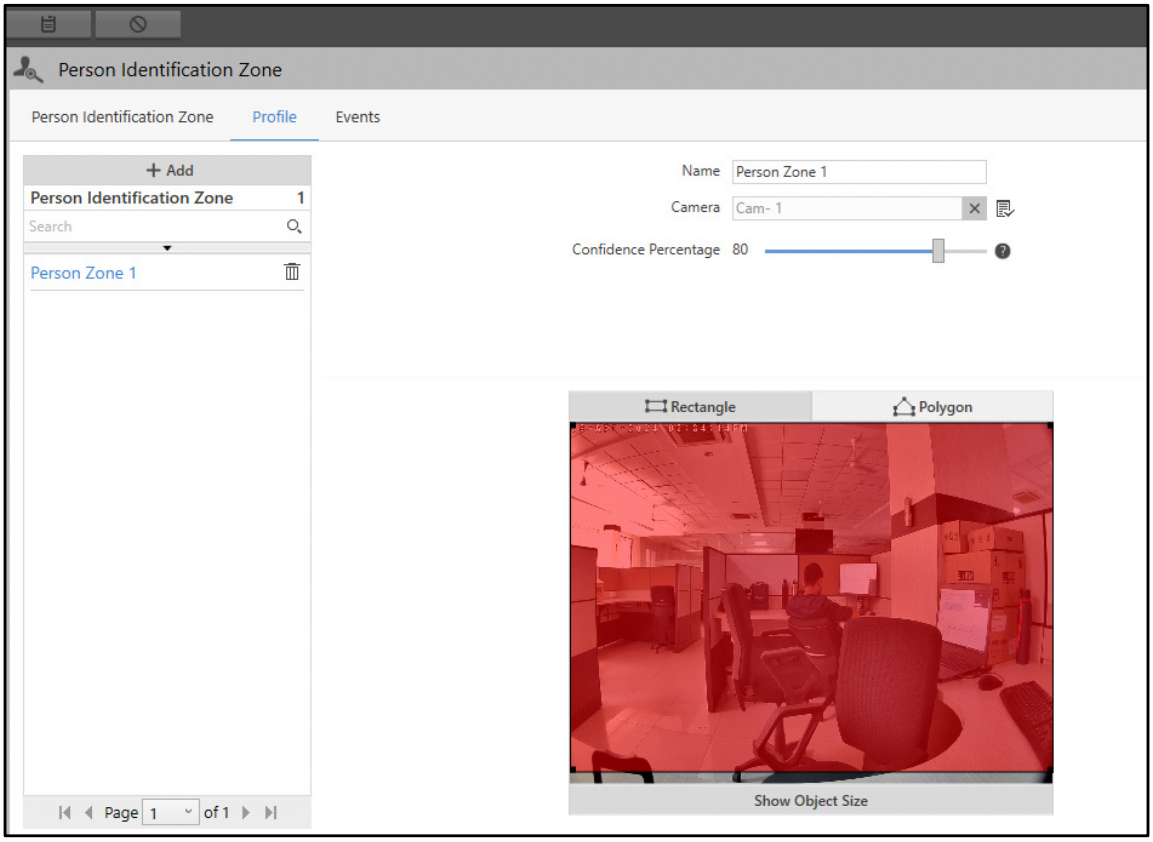
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

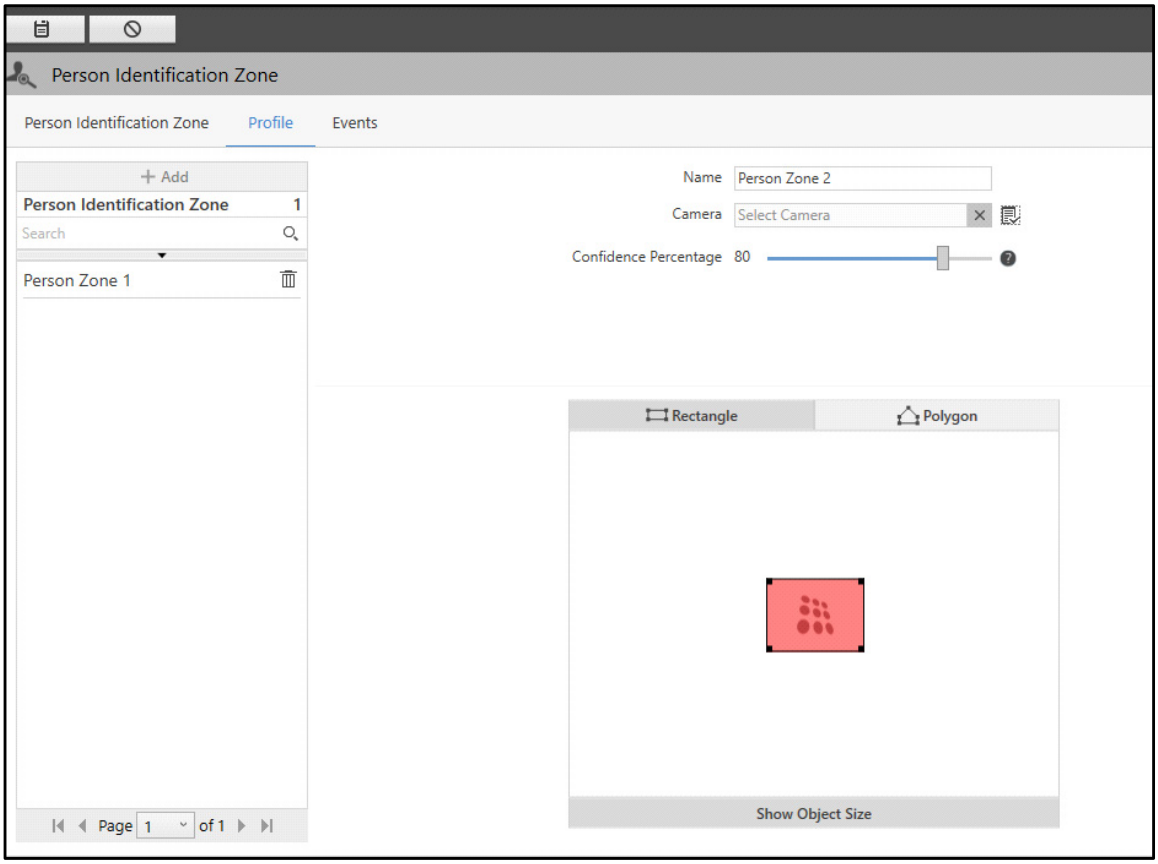
This tab enables you to configure Person Identification Zone. All the Person Identification Zones configured here appear under the **Person Identification Zone** tab.

To configure Person Identification Zones,

- Click the **Profile** tab.

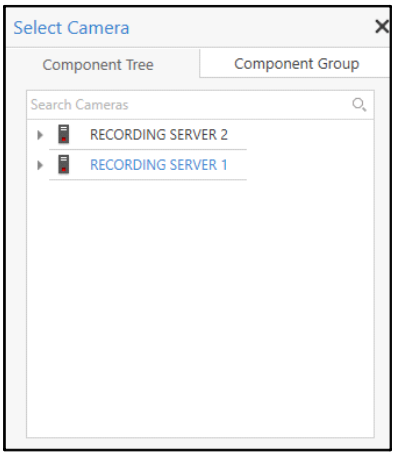


- Click **Add**.

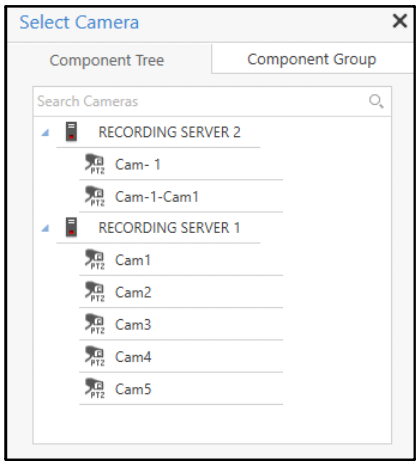


Configure the following parameters:

- **Name**: Specify a suitable name for the Person Identification Zone.In Na me, you can enter upto 50 characters. Default: Blank.
- **Camera**: Select the desired camera which you wish to assign to the Person Identification Zone using the **Camera** picklist.
  - Click **Camera** picklist. The **Select Camera** pop-up appears.

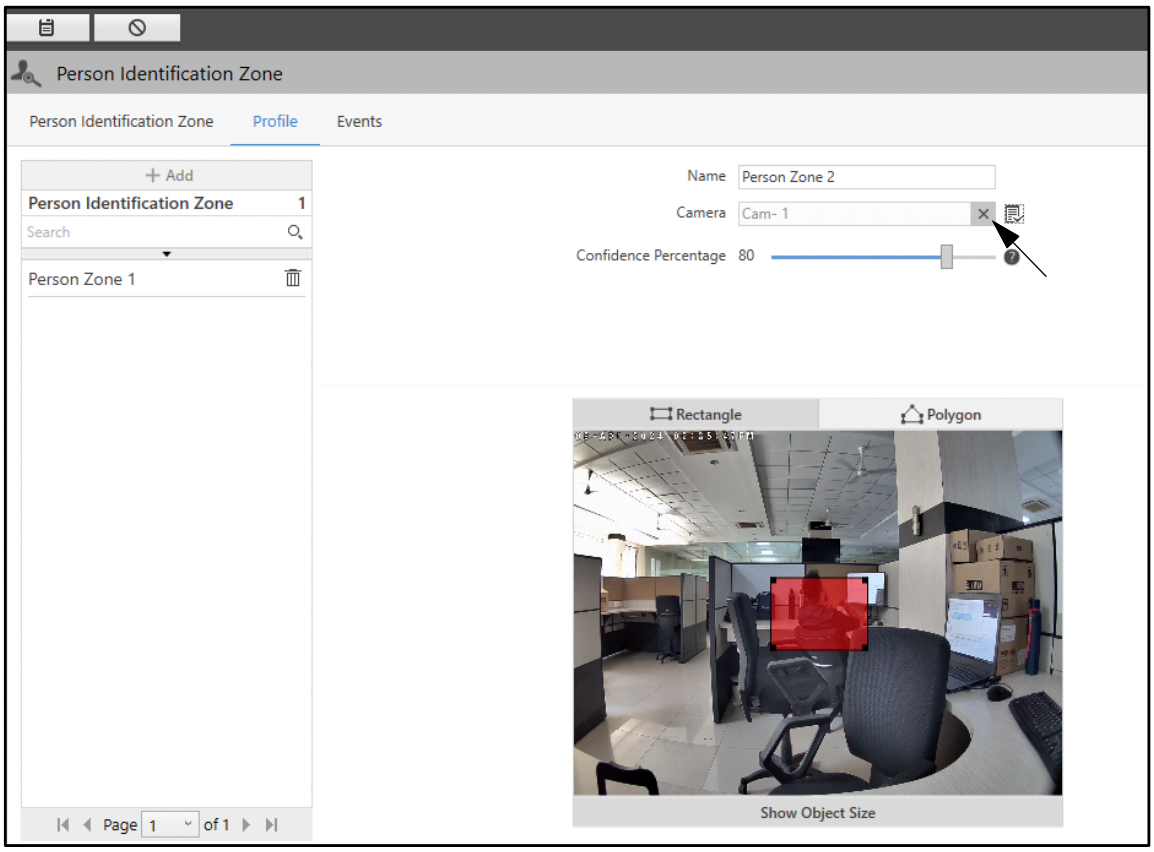


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to "Component Group". Double click the desired camera to assign it to the Person Identification Zone. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

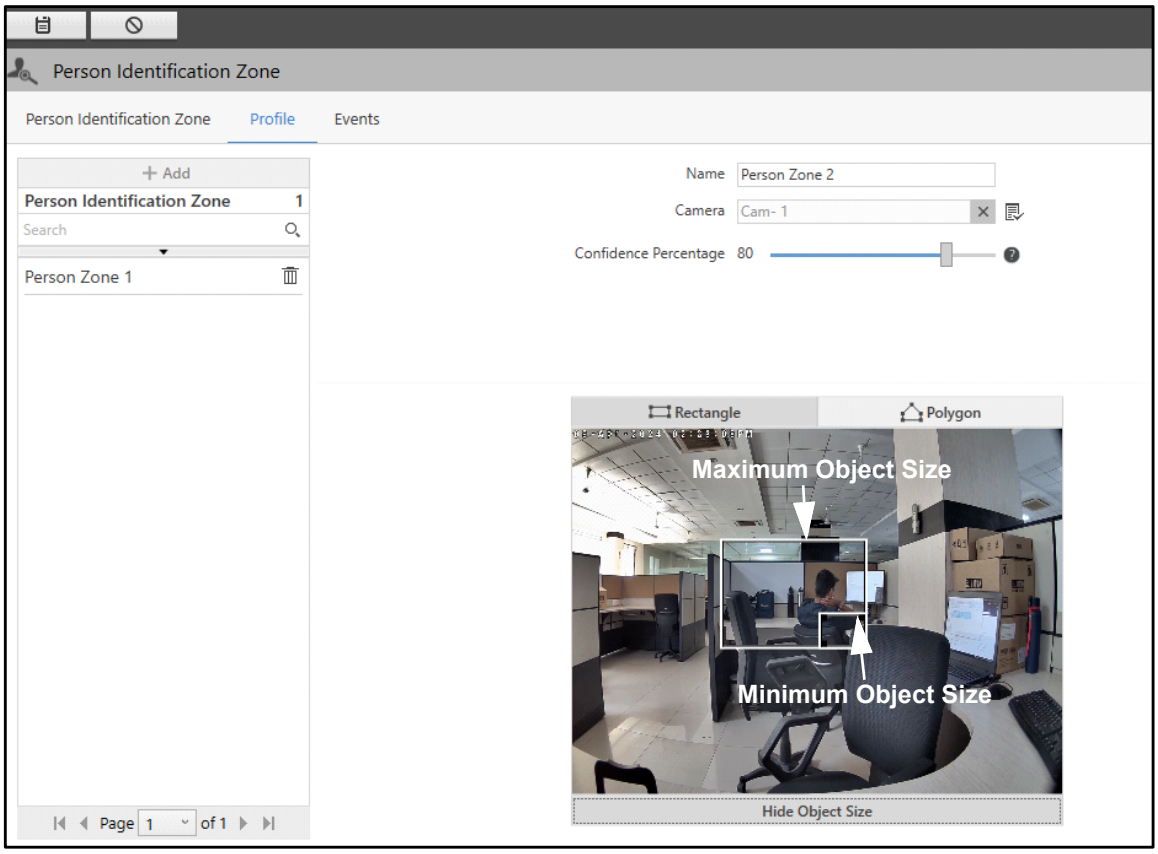
- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click the desired option from the list.
  - Click **Go to selected position** to move the camera to the selected preset position.
- To remove the camera, click **Remove** .



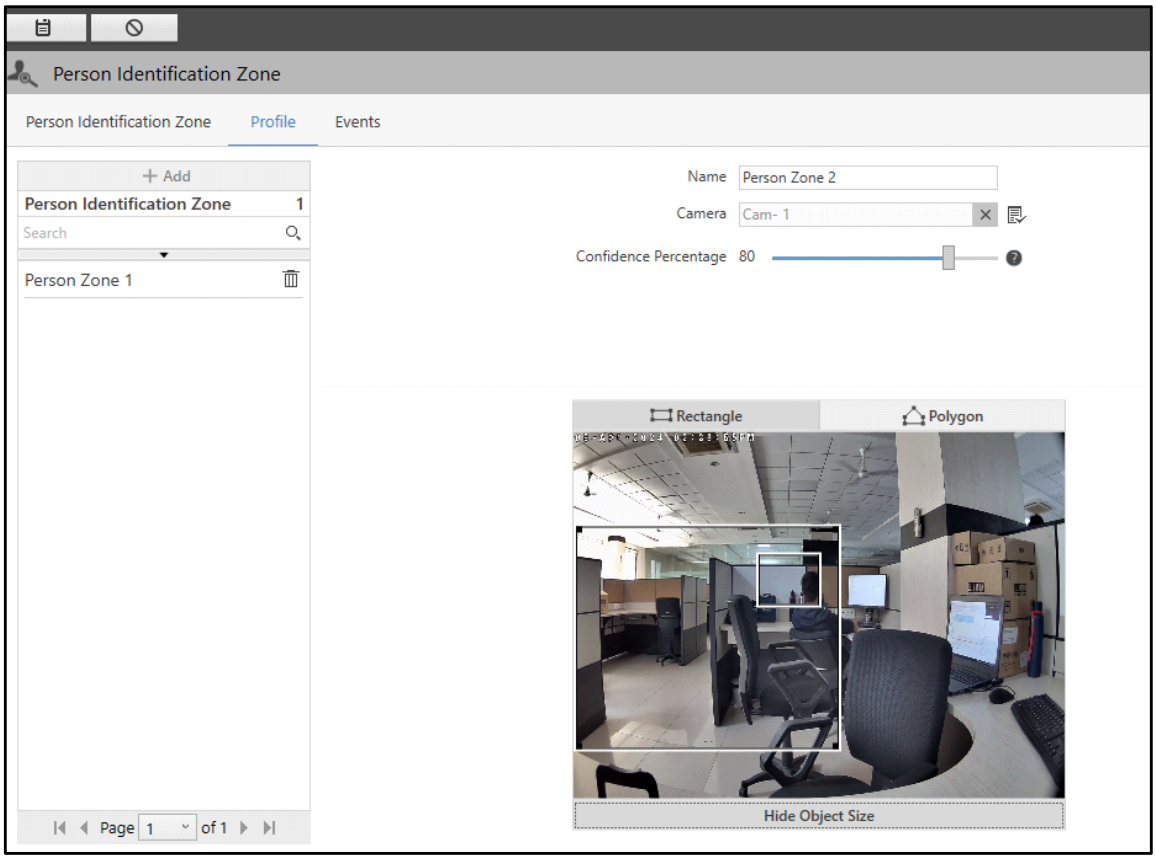
- **Confidence Percentage**: Set the Confidence Percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. A higher Confidence Percentage will ensure more accuracy in Face Detection. Valid Range: 0-100%. Default: 60.

Once a camera is assigned, you can draw a Person Identification Zone on the live view of the camera. You can also define the **Minimum** and **Maximum Object Size**. You can either draw a **Rectangle** or **Polygon** to define the Zone.

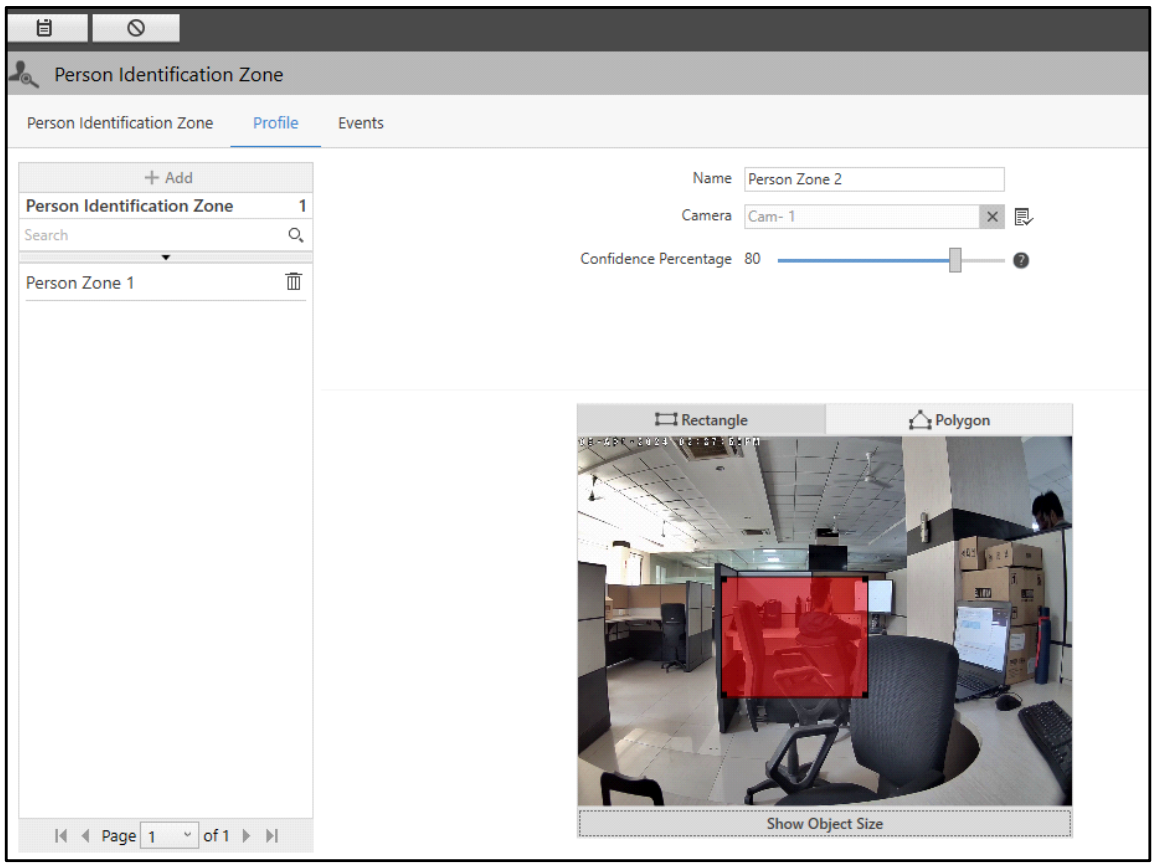
- Click **Show Object Size**. The default **Minimum** and **Maximum Object Size** appear.



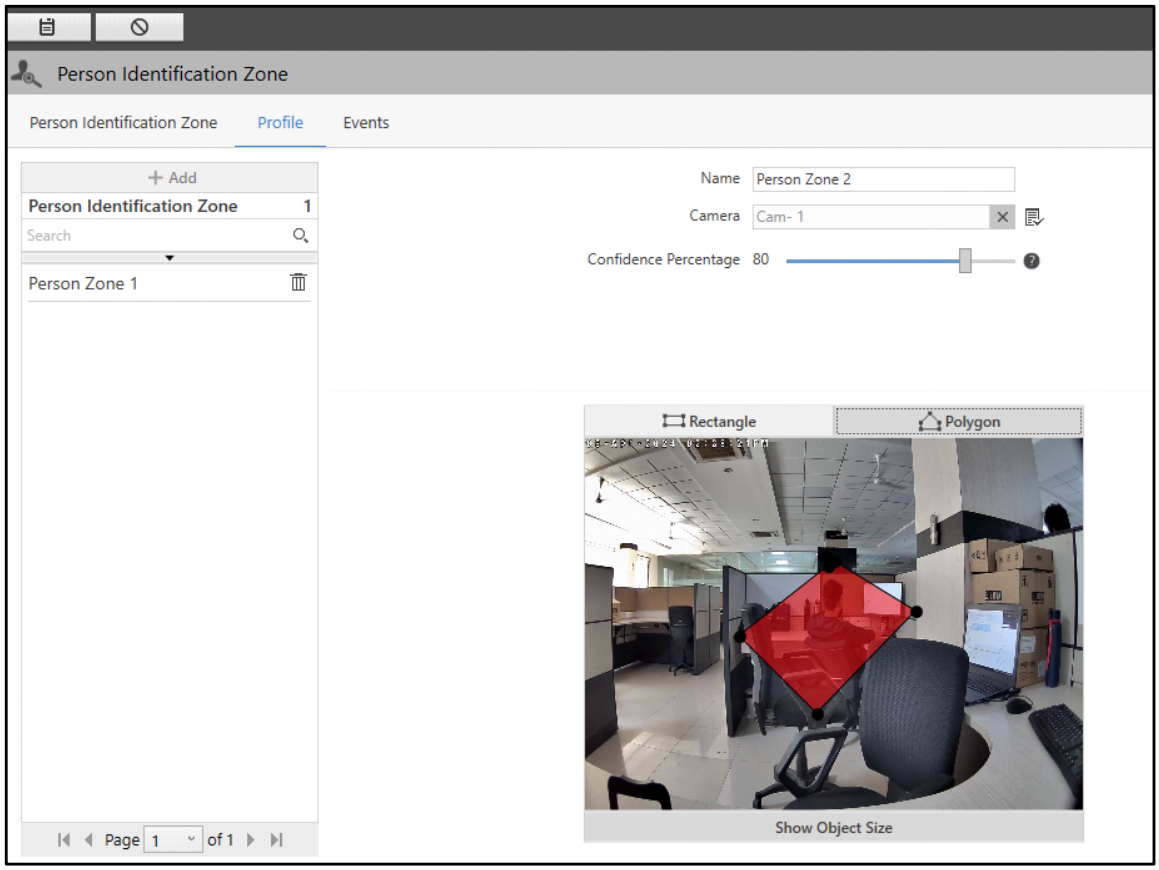
- Drag the corners of the rectangles to configure the minimum and maximum object size to be detected in the Event, if required. When the object size meant to be detected in the Event does not fit in the default Minimum and Maximum Object Size, you can configure it to match the desired object size.



- Click **Save** to save the settings or **Cancel** to discard.
- Click **Hide Object Size** to hide the size and draw the Zone.
  - Select either **Rectangle** or **Polygon** to draw the Zone.
  - If you select **Rectangle**, drag the corners and sides of the rectangle to configure the Zone.



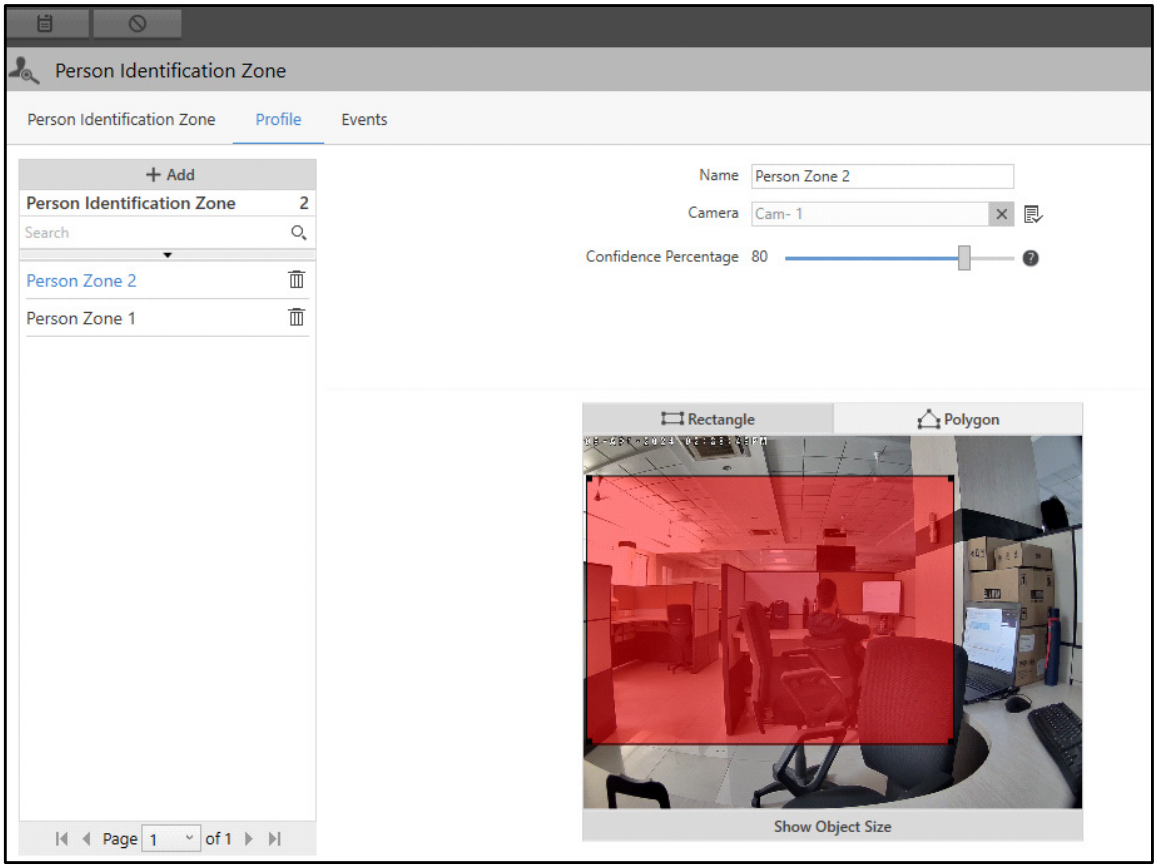
- If you select **Polygon**, click on the live view to place the vertex of the polygon. Click again on the desired place to join the previous vertex with a new vertex. Continue this process to complete the polygon.



- Click **Save** to save the settings or **Cancel** to discard.

The new Person Identification Zone will appear in the list on the left hand side.

You can edit the configurations of the Zone or delete it.



- Select the desired Person Identification Zone from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Person Identification Zone.

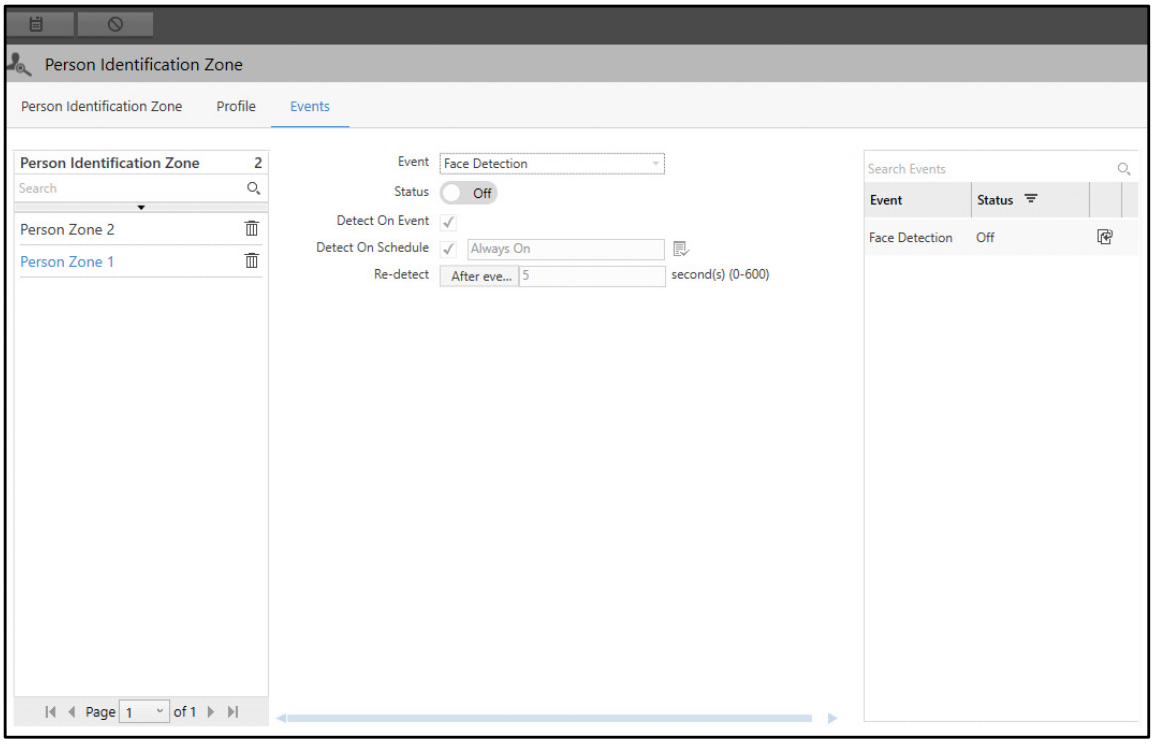
Similarly, you can configure the other Person Identification Zones.

Events

This tab enables you to configure the Face Detection Event for the Person Identification Zones. All the configured Events appear under the **Person Identification Zone** tab.

To configure the Face Detection Event,

- Click the **Events** tab.
- Select the desired Profile from the left hand side for which you wish to configure the Event.

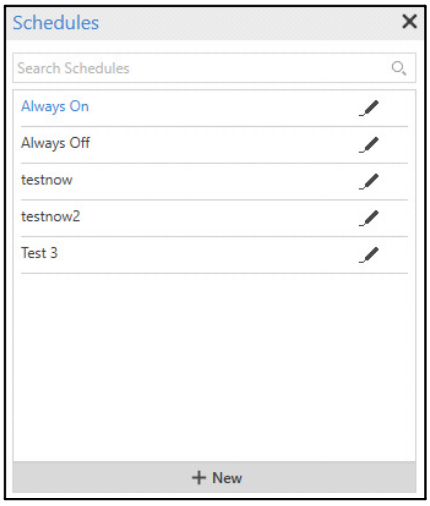


Configure the following parameters:

- **Event:** Select the Face Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Detect on Event**: Select the check box to detect Event only on the occurrence of the Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".

- **Re-detect After every**: Specify the Re-detect time after which the Face Detection Event should be detected again after the previous detection. Valid Range: 1- 600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

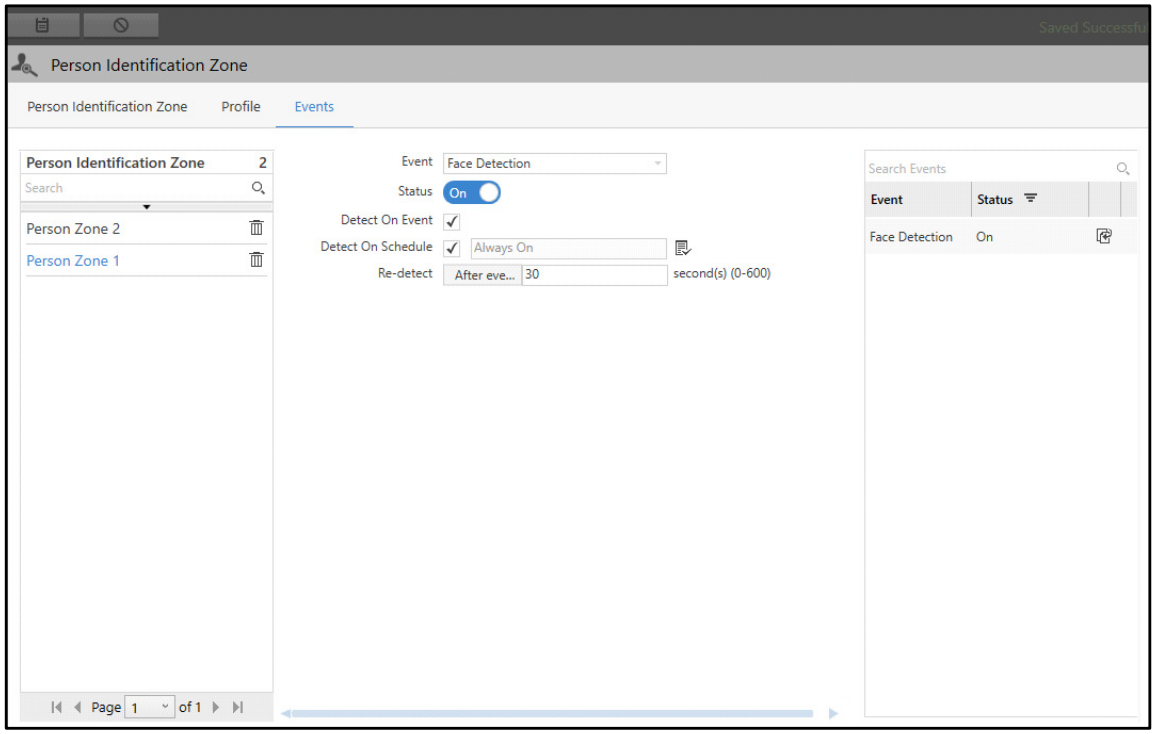
Once you have configured the Event, you can edit its configurations or disable it.

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

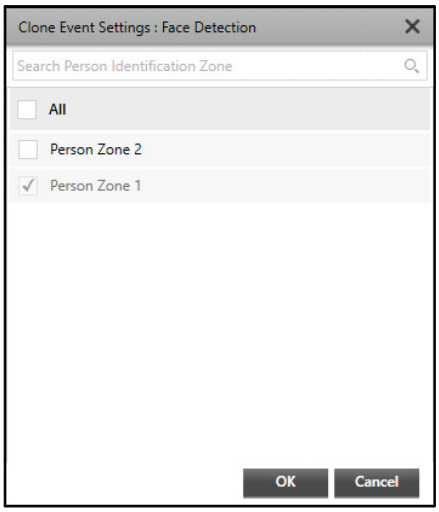
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Perimeter Zone is created, the **Clone Event Settings** option is enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Face Detection** pop-up appears.



- Select the desired Events to which you wish to copy the configurations.

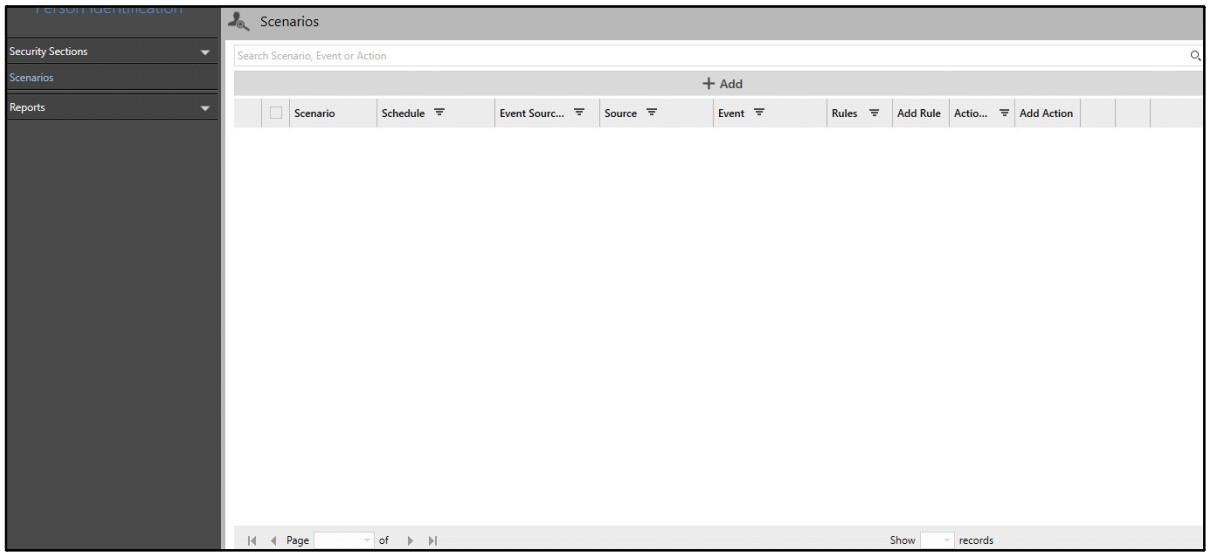
- Click **OK** to confirm or click **Cancel** to discard.

Person Identification-Scenarios

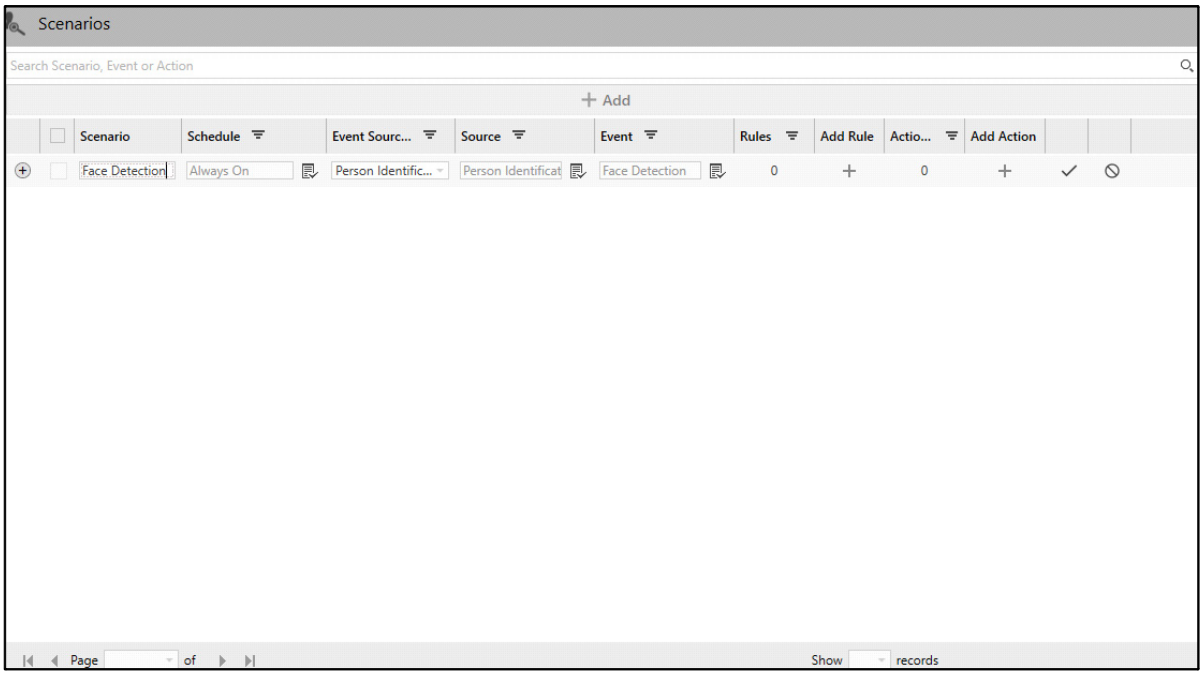
In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send SMS) on Events occuring at certain sources (For example, Face Detection). The Scenarios page displays all the Scenarios configured for Person Identification. You can view and configure the Scenarios for all the configured Person Identification Zones.

To view and configure Scenarios,

- Click **Person Identification > Scenarios**.



- Click **Add.**



The configurations of Scenarios for Person Identification are similar to the Basic Scenario. For details, refer to “Basic Scenario”.

Face Detection Report

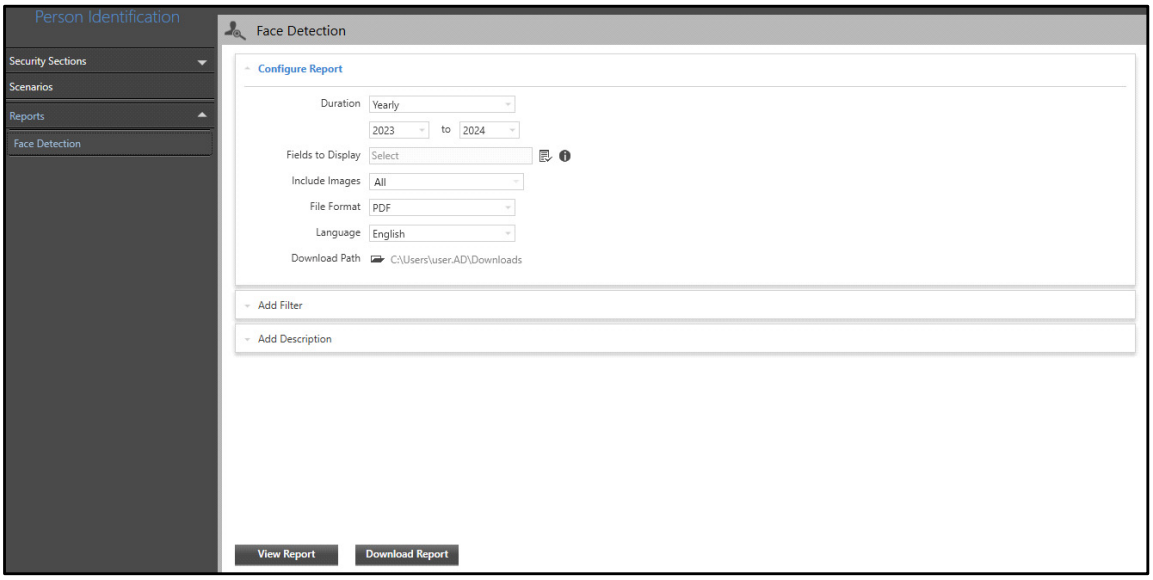
The Face Detection Report provides statistics of People Detection Event. These statistics can be useful in managing security at various locations from one place. It allows the user to detect each individual passing-by within the defined duration at any place. The report includes the detection records of people across multiple detection regions.

For example, consider a bank having various outlets at different locations. Based on this report, the user can track the persons entering and exiting various outlets by sitting at a place. If any unusual activity takes place and there are suspicious people present at the premises during that duration, they can be identified and appropriate actions can be taken.

The Face Detection page enables you to configure parameters for Face Detection Reports. You can view and configure Face Detection Reports on Yearly, Monthly, Daily and Hourly basis.

To configure Face Detection Report,

- Click **People Identification > Reports > Face Detection**.



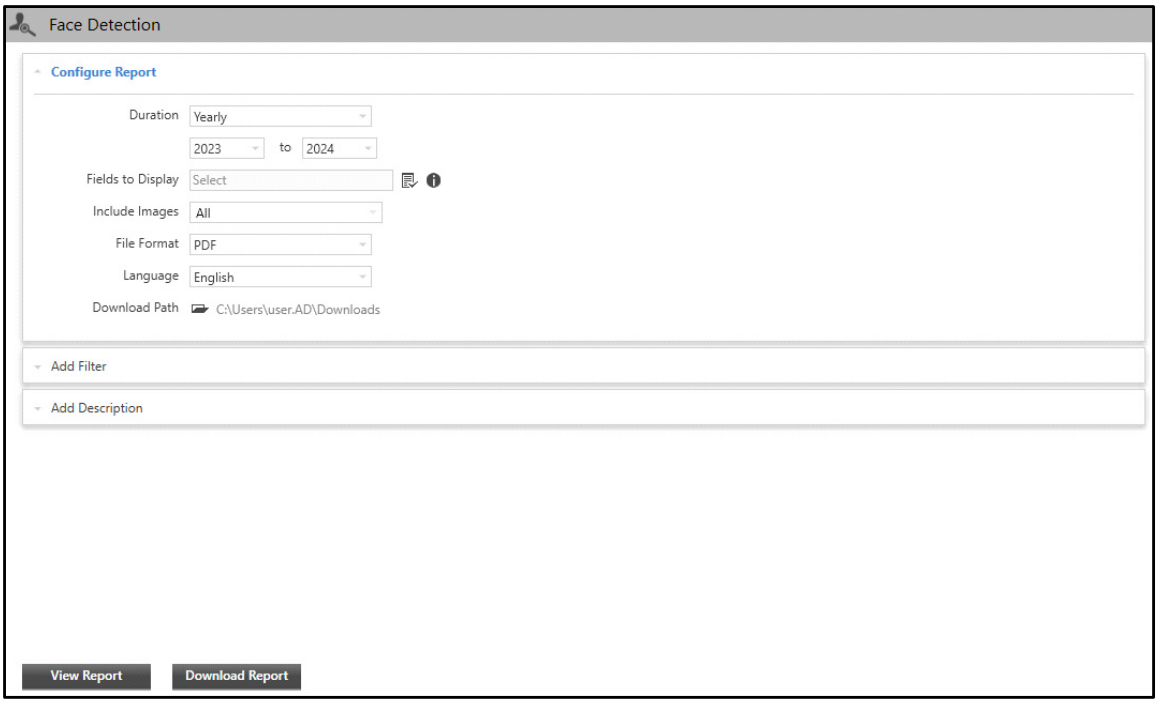
The Face Detection page contains three collapsible panels — “Configure Report”, “Add Filter” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Face Detection Report from this collapsible panel.

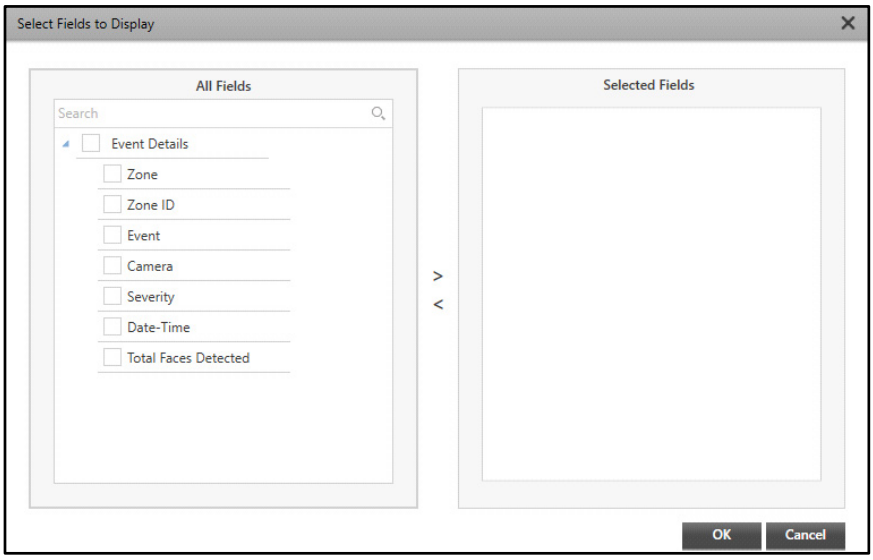
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

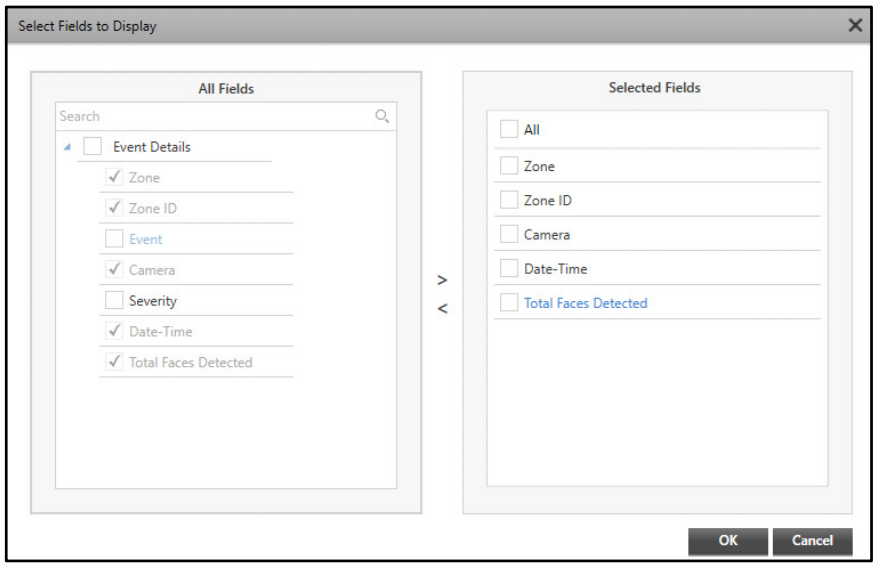
- **Duration**: Select the Duration from the drop-down list options — Yearly, Monthly, Daily and Hourly Reports.
    - **Yearly**: Select this option to generate yearly reports. Select the desired From and To year from the drop-down lists.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
- **Fields to Display**: Select the desired fields that you wish to display in the report using the **Fields to Display** picklist.
    - Click the **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



Select the check boxes of the desired fields you wish to include in the report from the **Event Fields**.

Click the right arrow button to move these fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

To remove fields, select the check boxes of the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields.



- Click **OK** to confirm or click **Cancel** to discard.
- **Include Images**: Select the check boxes of the desired images to be included in the report from the drop-down list.
- **File Format**: Select the File Format in which you wish to generate the report from the drop-down list.



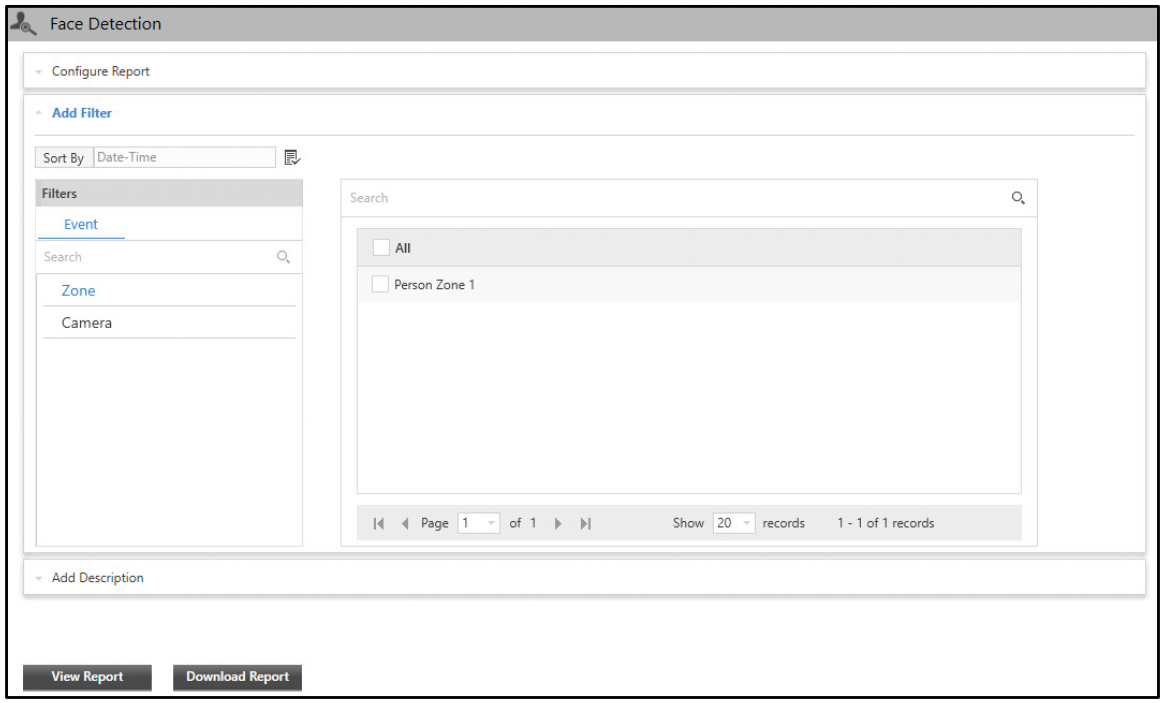
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click on **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Filter

This panel allows you to add filters for the Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters. You can view and edit the filters from this collapsible panel.

To set the filters,

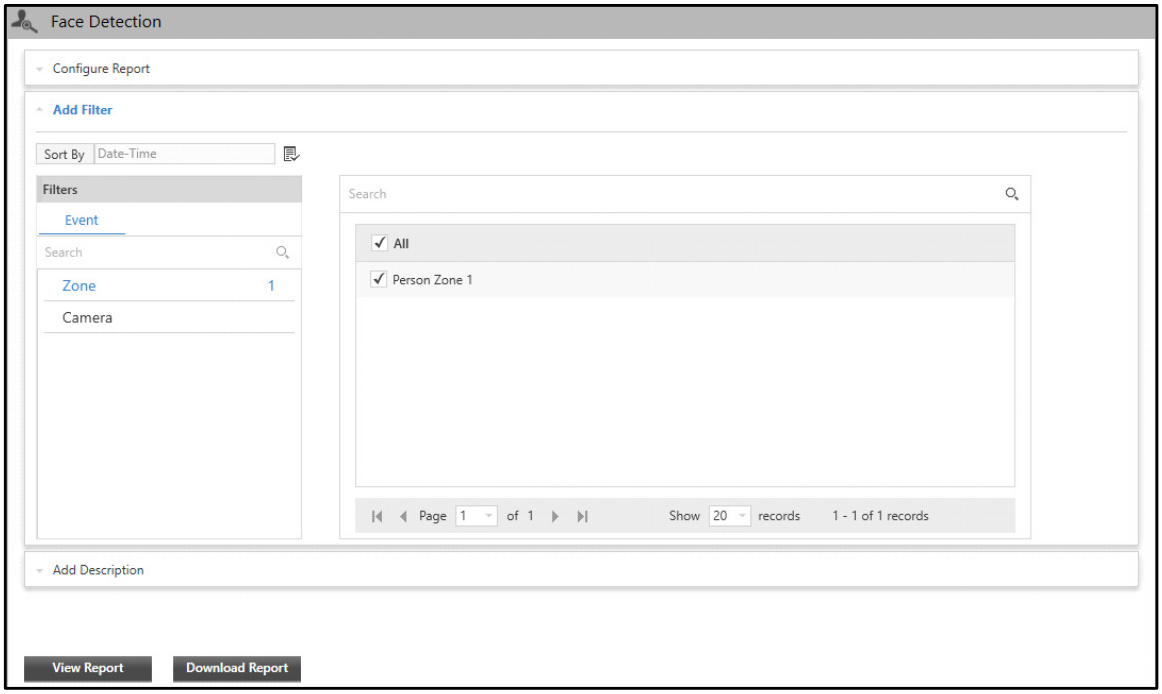
- Click the **Add Filter** collapsible panel.



Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data from Event Fields in the report using the **Sort By** picklist. Double-click to select the desired option. By default, the sorting is done as per the Date and Time of Event Occurrence.
- **Filters**: You can get the desired data for the report using Filters. The Filters section contains only one tab — Event. Select the tab to view the associated parameters.

- Click the desired parameter to view the associated entities with the selected Event. For example, if you select Camera, all the cameras associated with the selected Event are displayed on the right hand side. Select the desired entities to include in the report.

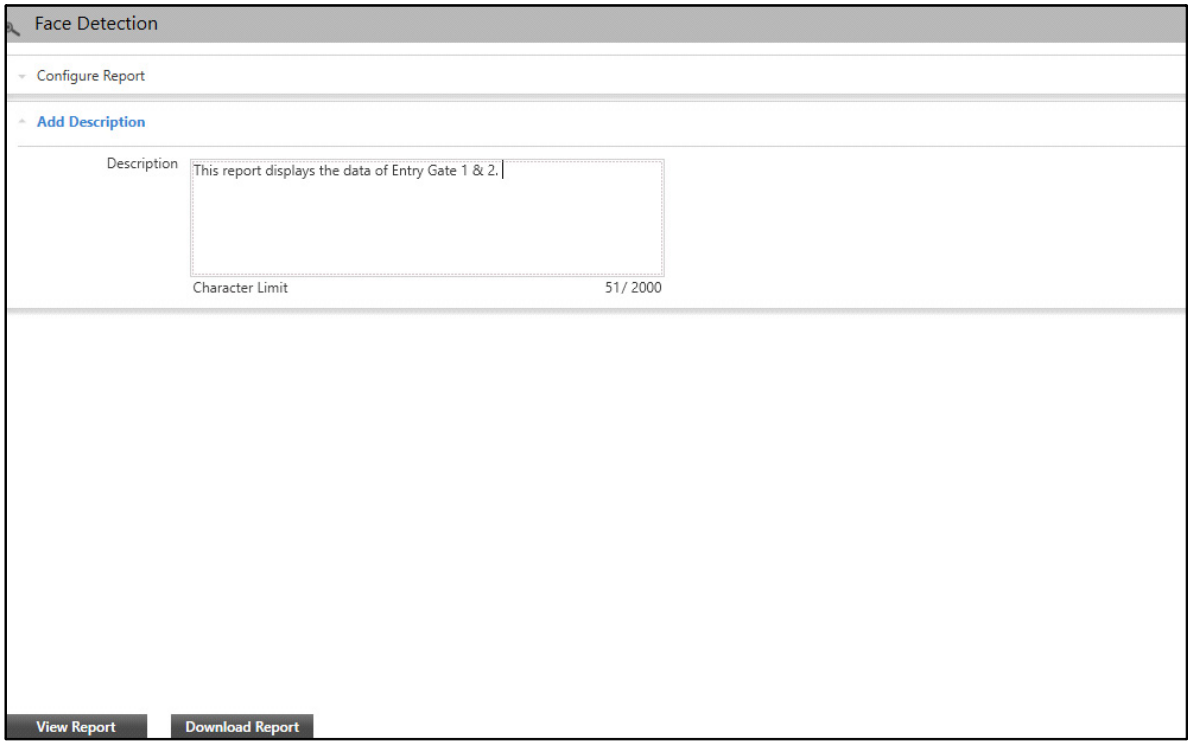


Add Description

This panel allows you to add a description for the Face Detection Report once the report configurations are done. This description is visible in the generated report.

To configure the description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

CHAPTER 13

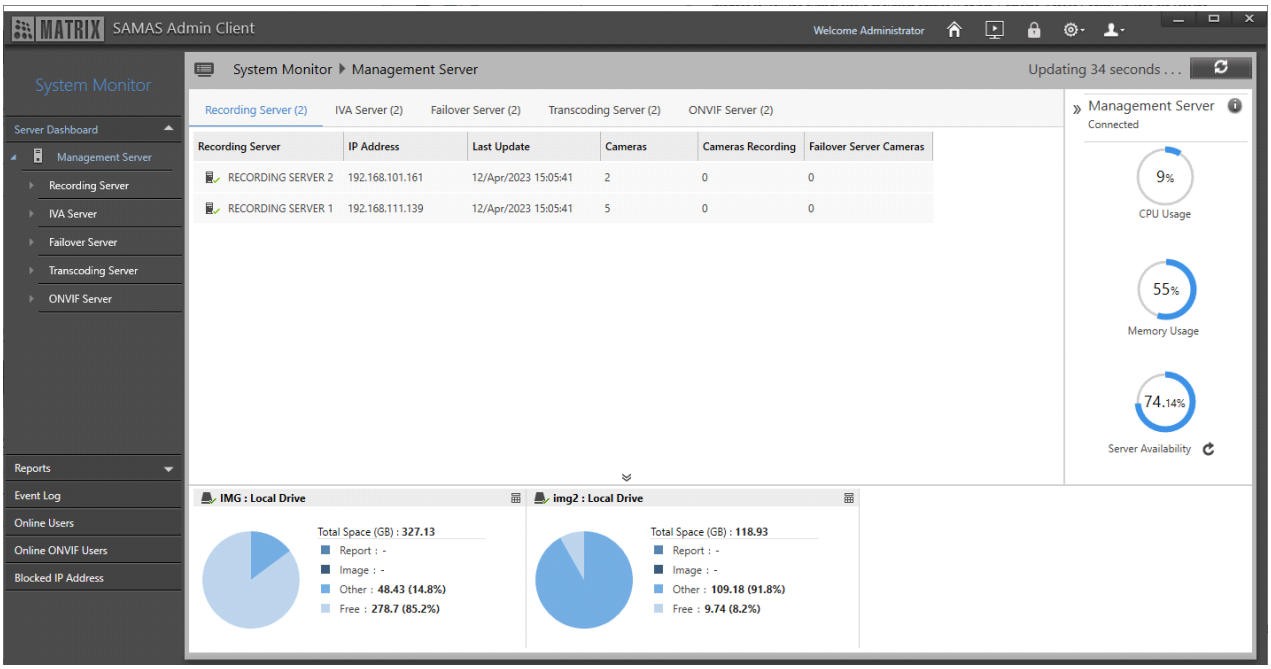
System Monitor

The System Monitor module enables you to view live information related to Servers, Camera availability, Server performance, Real-time storage details, System usage as well as Event logs. This vital feature provides you an interface to view the current status of system entities (Servers, Cameras, Access Control Devices etc.) for the purpose of administrative monitoring. If SATATYA SAMAS is integrated with COSEC Access Control Management Solution, you will also be able to view COSEC Monitor Events in the Event logs.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure System Monitor,

- Click **System Monitor**



The System Monitor module contains these sections and pages — "Server Dashboard", "Reports", "Event Log", "Online Users", "Online ONVIF Users" and "Blocked IP Address".

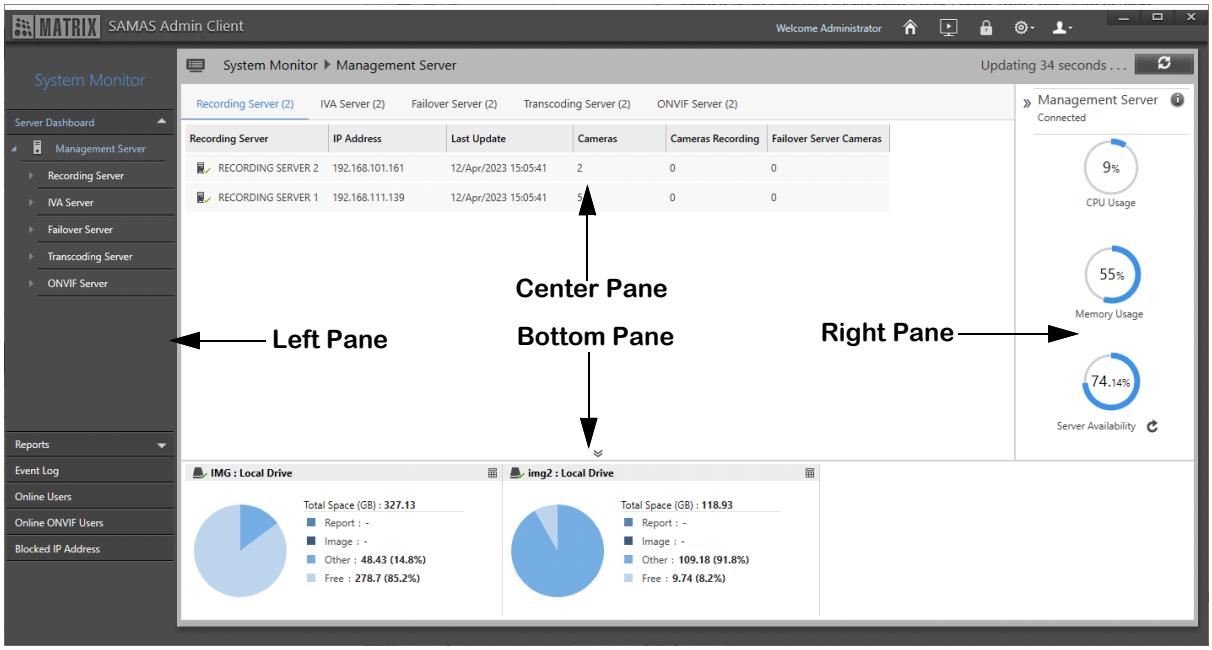
Server Dashboard

The Server Dashboard page displays the details and live status of the Servers. You can also view the storage and memory usage details from this page.

The IPv4/IPv6 Address of all the Servers/Cameras will be displayed under Server Dashboard as per the configurations done.

To view Server Dashboard,

- Click **System Monitor > Server Dashboard**.



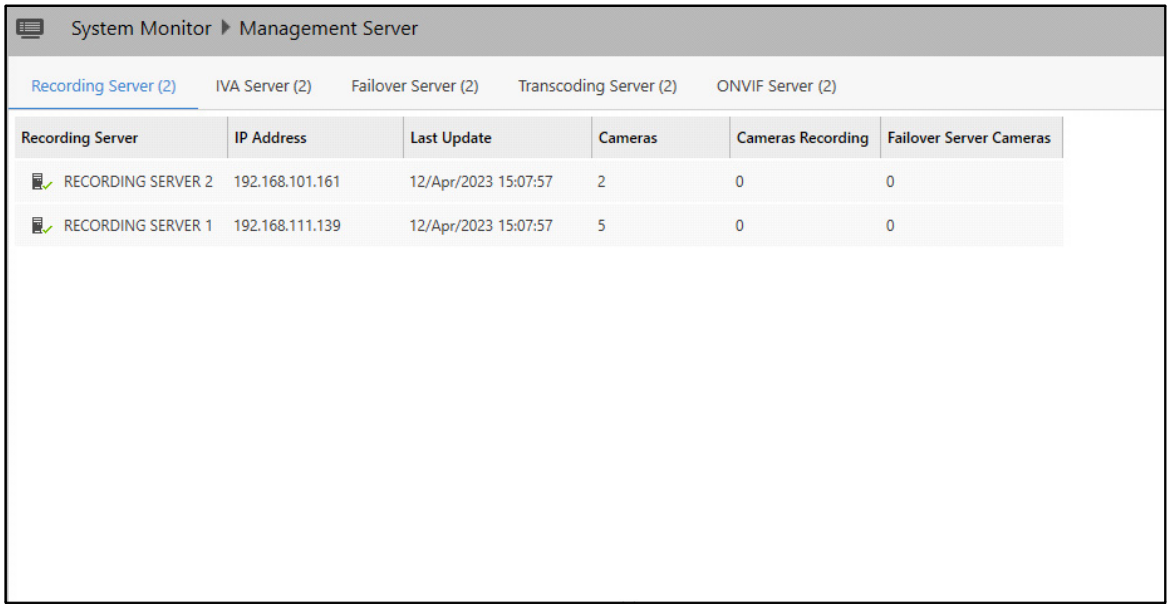
- The Server Dashboard displays the Management Server's details in different panes — Left Pane, Center Pane, Right Pane and Bottom Pane.
- Click **Refresh** to update the Management Server details.

Left Pane

The Left Pane displays all the pages of the System Monitor module.

Center Pane

The Center Pane displays all the Servers that are connected with the Management Server in different tabs.

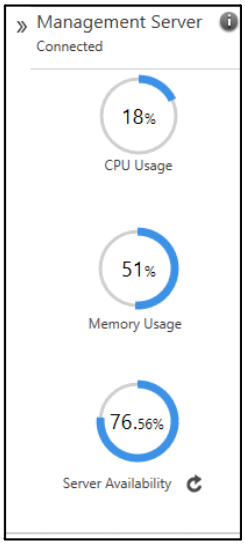


To view the details of each server, click the desired tab:

- "Recording Server"
- "IVA Server"
- "Failover Server"
- "Transcoding Server"
- "ONVIF Server"

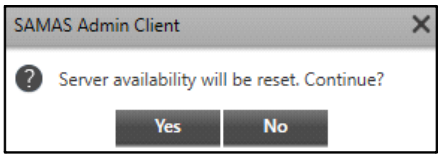
Right Pane

The Right Pane displays the Connection Details, CPU Usage, Memory Usage and Server Availability details of the Management Server.



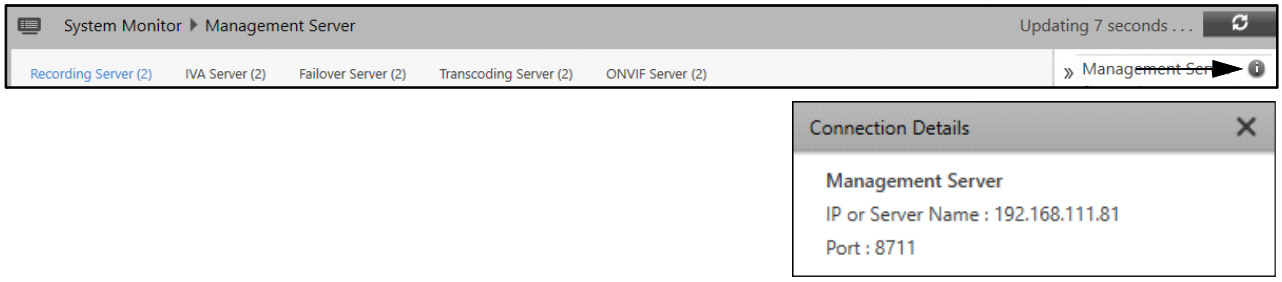
- Click **Reset Server Availability** to reset the Server Availability to 100%. Only a user with **Administrator** rights can reset the Server Availability.

  The following pop-up appears.



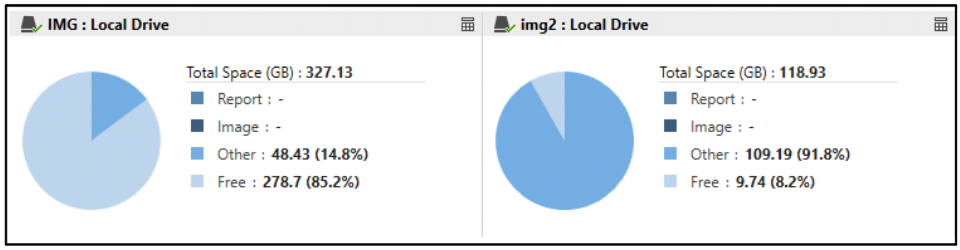
  - Click **Yes** to confirm or click **No** to discard.

- Click **Connection Details** at top right corner of the page, to view the connection details of the Management Server. It displays the Management Server Name, IP (IPv4/IPv6) or Server Name and Port.



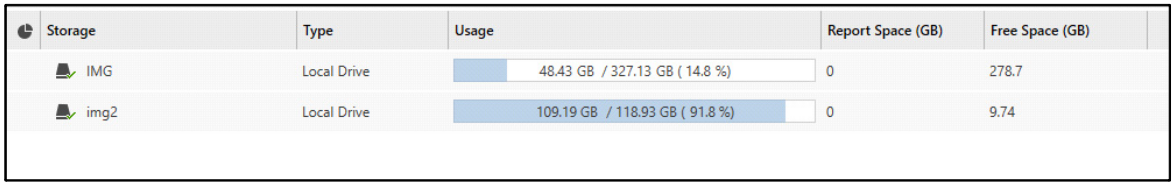
Bottom Pane

The Bottom Pane displays the Management Server's Storage Drive details.



The drive details displayed are — Drive Name, Drive Type, Total Storage Space (GB), Space occupied by Reports, Space occupied by Images, Space occupied by other files and Free Space.

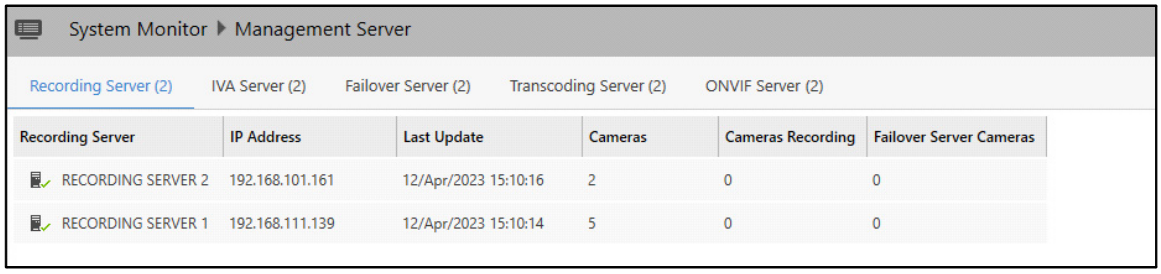
- Click **Tabular View** , if you wish to view the Drive details in a tabular format.



- Click **Graphical View** to view the Drive details in a graphical format again.

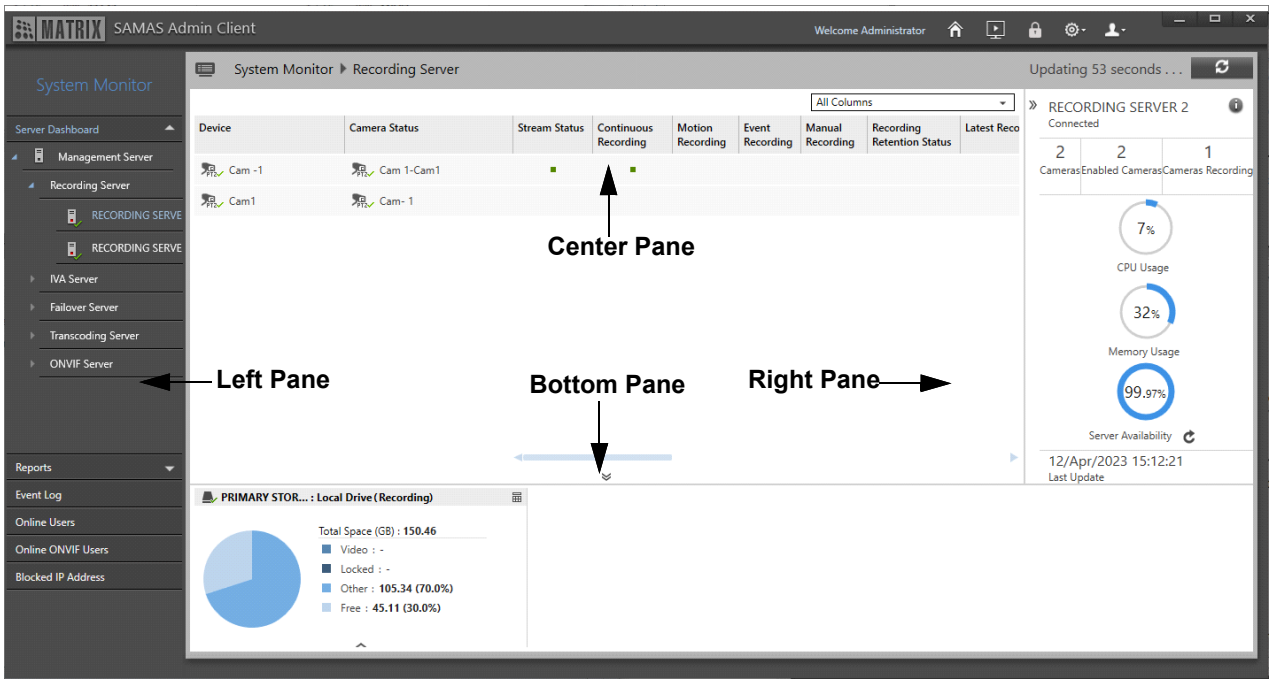
Recording Server

This tab enables you to view all the Recording Servers connected with the Management Server. You can also click on **Recording Server** from the Left Pane to view this tab.



The Server details displayed are — Recording Server Name, IPv4/IPv6 Address, Last Update, Cameras, Cameras Recording and Failover Server Cameras.

Double-click on a Recording Server to view its individual details.



The Recording Server's details are displayed in different panes — Left Pane, Center Pane, Right Pane and Bottom Pane.

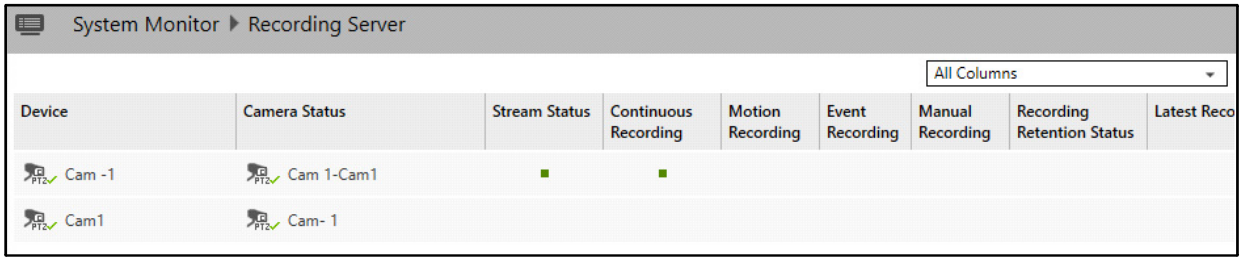
- Click **Refresh** to update the Recording Server details.

Left Pane

The Left Pane displays all the pages of the System Monitor module.

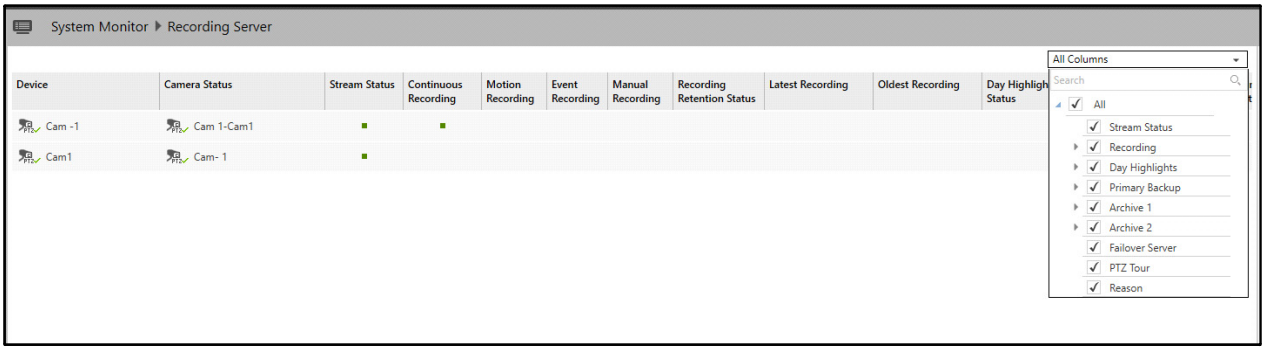
Center Pane

The Center Pane displays all the configuration details of the selected Recording Server.

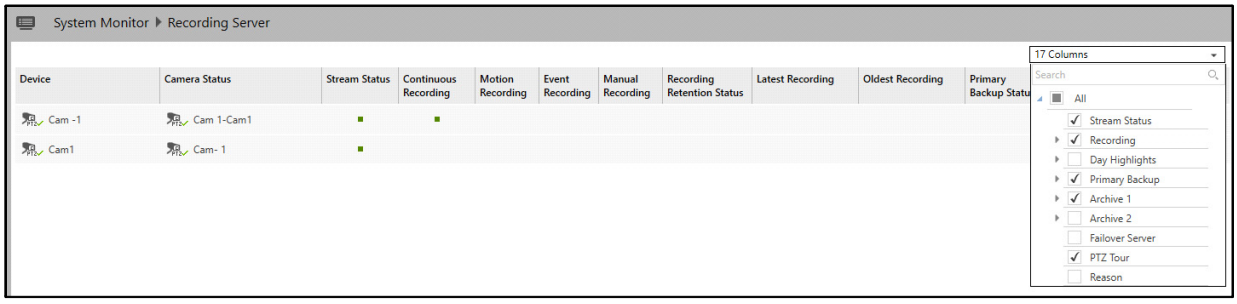


You can customize the configurations parameters that you wish to display in the Center Pane. To do so,

- Click the **Show or Hide Columns** drop-down list.



- Select the check boxes for the parameters that should be displayed in the Center Pane. Clear the check boxes for the parameters that should not be displayed in the Center Pane.



By default all the configuration parameters are displayed. The columns displayed in the Center Pane are:

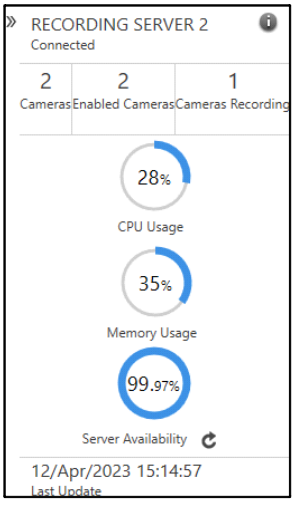
- **Stream Status:** Stream Status displays the status of the current stream under which the recording is running. If the camera is on, it is indicated in green color.
- **Recording:** There are different types of Recording — Continuous, Motion, Event and Manual. Each is displayed separately. The type of recording which is currently running for the camera is indicated in green color.
- **Recording Retention Status:** Recording Retention Status displays the status of retention of camera recording. If the retention is running, it is indicated in green color.
- **Latest & Oldest Recording:** Latest and Oldest Recording displays the date and time of the Latest and Oldest recorded file which are available in the configured Storage Drive.

- **Day Highlights**: Day Highlights displays the hours of recording in minutes for the clip/record.
- **Day Highlights Status:** Day Highlights Status displays the status of Day Highlights. If the Day Highlights is running, it is indicated in green color.
- **Day Highlights Retention Status:** Day Highlights Retention Status displays the status of retention of camera Day Highlights. If the retention is running, it is indicated in green color.
- **Primary Backup, Archive 1 & Archive 2:** Primary Backup, Archive 1 and Archive 2 displays the following details — Drive Status, Retention and Latest and Oldest Backup. If the Backup is currently in progress, it is indicated in green color.
- **Failover Server:** Failover Server displays the name of the Failover Server assigned to a particular camera.
- **PTZ tour:** PTZ Tour displays the status of the PTZ tour. Whenever the PTZ tour is running for a particular camera, it is indicated in green color.
- **Reason:** Reason displays the justification for a particular camera if it is under maintenance.

The columns configured for display will be set to default after every logout from the Admin Client.

Right Pane

The Right Pane displays the Connection Details, Camera details., CPU and Memory usage details as well as Server Availability of the Recording Server.

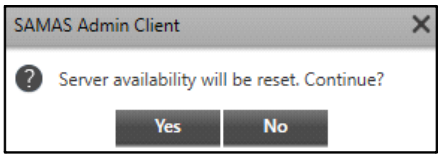


The details displayed are — Number of Cameras added, Number of Cameras Enabled, Number of Cameras with Recording Status as **On**, CPU Usage, Memory Usage and Server Availability. The date and time of last update is also displayed.

If Recording Server/Management Server are online, but CPU Usage and Memory are continuously displaying same values or 0 for Recording Server/Management Server, then it is possible that the system's performance counter may be corrupted.

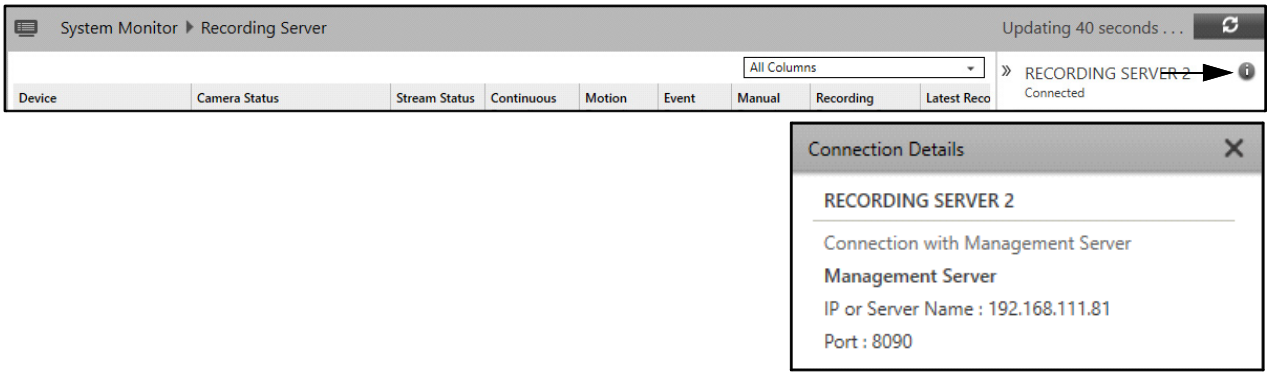
- Click **Reset Server Availability** to reset the Server Availability to 100%. Only a user with **Administrator** rights can reset the Server Availability.

  The following pop-up appears.



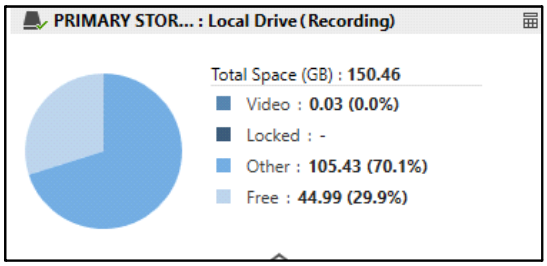
  - Click **Yes** to confirm or click **No** to discard.

- Click **Connection Details** at top right corner of the page, to view the connection details of the Recording Server. It displays the Management Server Name, IP (IPv4/IPv6) or Server Name and Port with which Recording Server is connected currently.



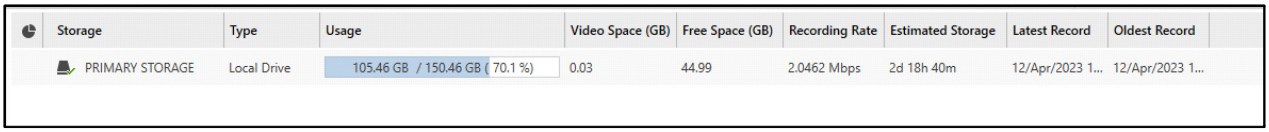
Bottom Pane

The Bottom Pane displays the Recording Server's Recording Storage Drive and Backup Drive details.



The drive details displayed are— Drive Name, Drive Type, Total Storage Space (GB), Space occupied by Videos, Locked Space, Space occupied by other files and Free Space.

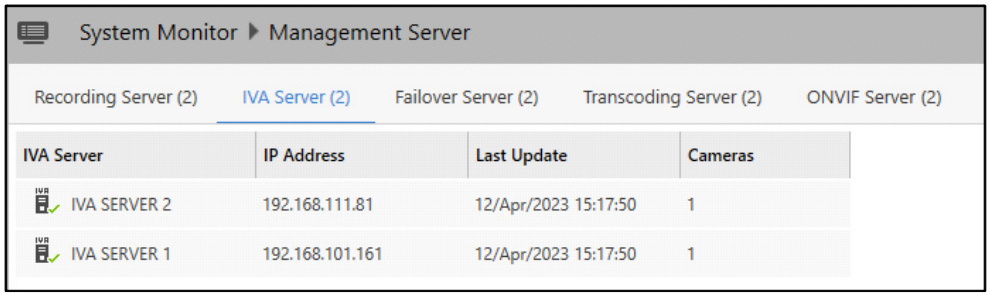
- Click **Tabular View** to view the Drive details in a tabular format. All the details displayed in Graphical format are also displayed in Tabular Format. The additional details displayed in Tabular Format are Latest and Oldest Record.



- Click **Graphical View** , to view the Drive details in a graphical format again.

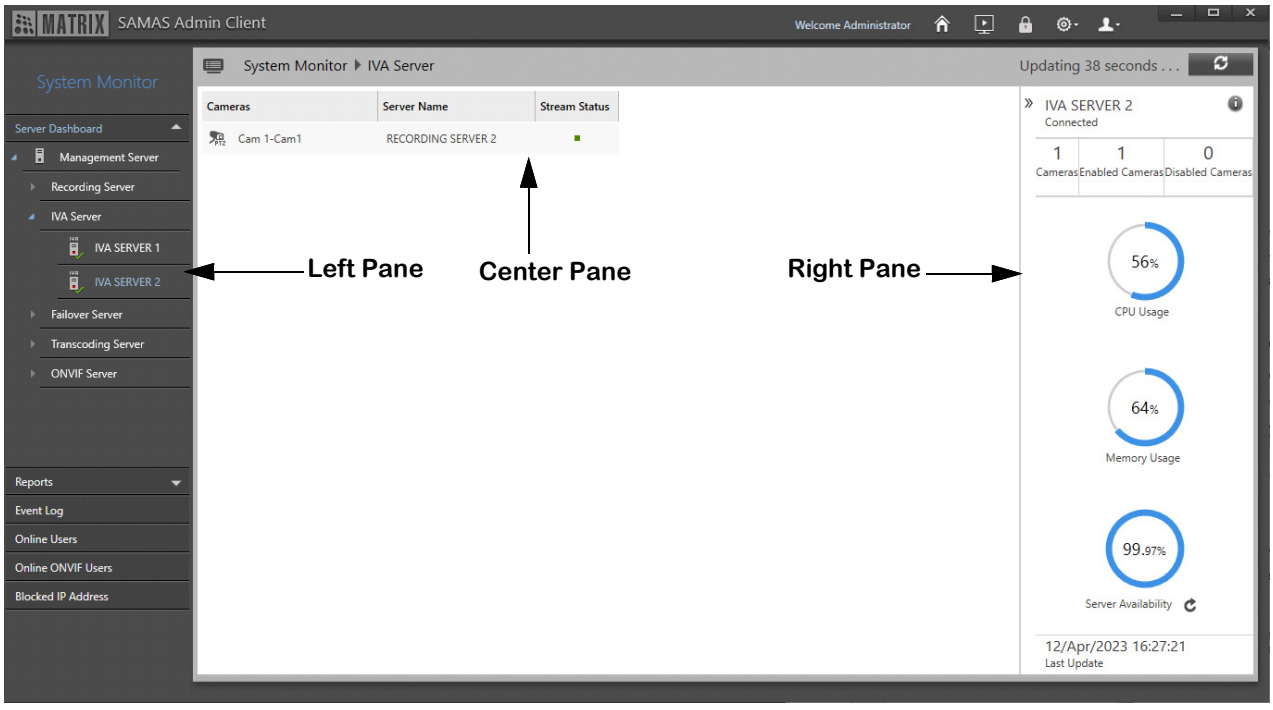
IVA Server

This tab enables you to view all the IVA Servers connected to the Management Server. You can also click on **IVA Server** from the Left Pane to view this tab.



The Server details displayed are — IVA Server Name, IPv4/IPv6 Address, Last Update and Cameras.

Double-click on a IVA Server to view its individual details.



The IVA Server's details are displayed in different panes — Left Pane, Center Pane and Right Pane.

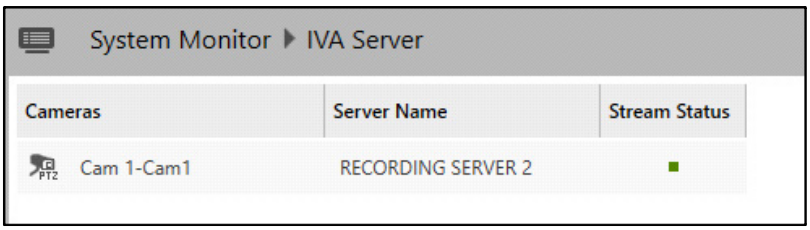
- Click **Refresh** to update the IVA Server details.

Left Pane

The Left Pane displays all the pages of the System Monitor module.

Center Pane

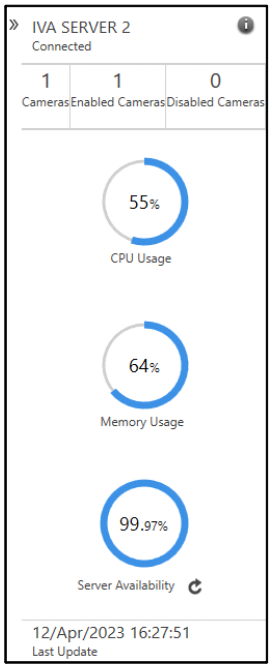
The Center Pane displays all the configuration details of the selected IVA Server.



The Server details displayed are — Cameras, Server Name and Stream Status. The camera for which IVA streaming is currently on is displayed in green color.

Right Pane

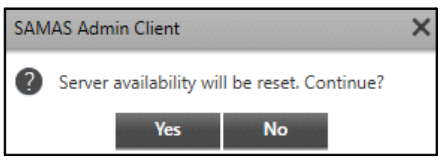
The Right Pane displays the Connection Details, CPU Usage, Memory Usage and Server Availability of the IVA Server along with Camera details.



The details displayed are — Number of Cameras added, Number of Cameras Enabled, Number of Cameras Disabled, CPU Usage, Memory Usage and Server Availability. The date and time of last update is also displayed.

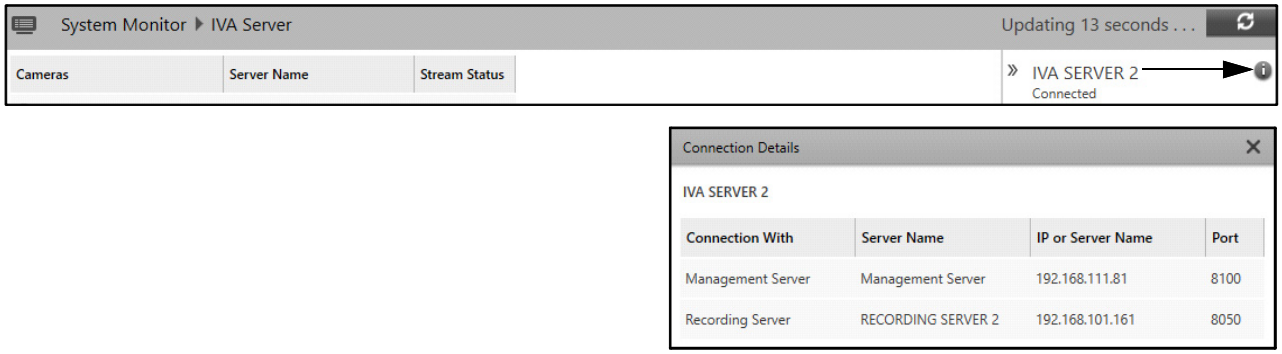
- Click **Reset Server Availability** to reset the Server Availability to 100%. Only a user with **Administrator** rights can reset the Server Availability.

  The following pop-up appears.



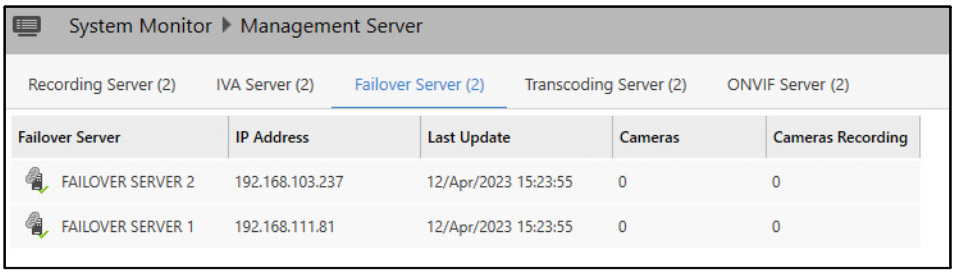
- Click **Yes** to confirm or click **No** to discard.

- Click **Connection Details** at top right corner of the page, to view the connection details of the IVA Server, It displays the connection details of the IVA Server with the Management Server and Recording Server. It displays the following details — Connection With, Server Name, IP (IPv4/IPv6) or Server Name and Port.



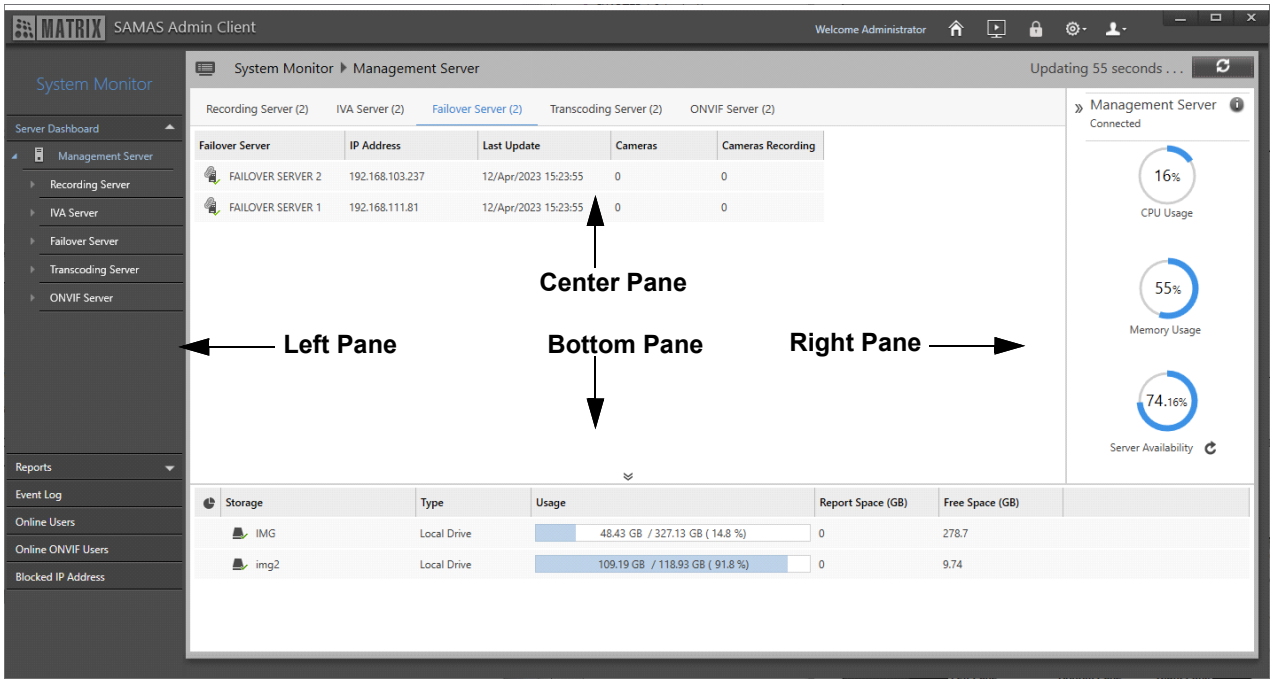
Failover Server

This tab enables you to view all the Failover Servers connected to the Management Server. You can also click on **Failover Server** from the Left Pane to view this tab.



The Server details displayed are — Failover Server Name, IPv4/IPv6 Address, Last Update, Cameras and Cameras Recording.

Double-click on a Failover Server to view its individual details.



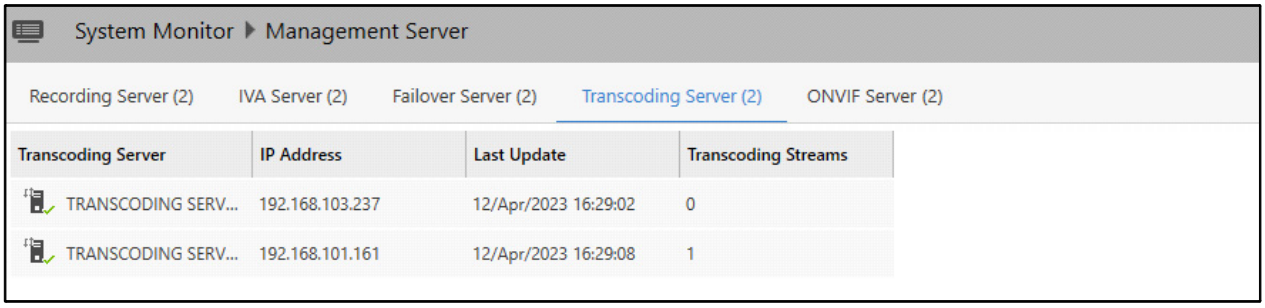
The Failover Server's details are displayed in different panes — Left Pane, Center Pane, Right Pane and Bottom Pane.

- Click **Refresh** to update the IVA Server details.

The details displayed for Failover Server are similar to that of the Recording Server. For more details, refer to "Recording Server".

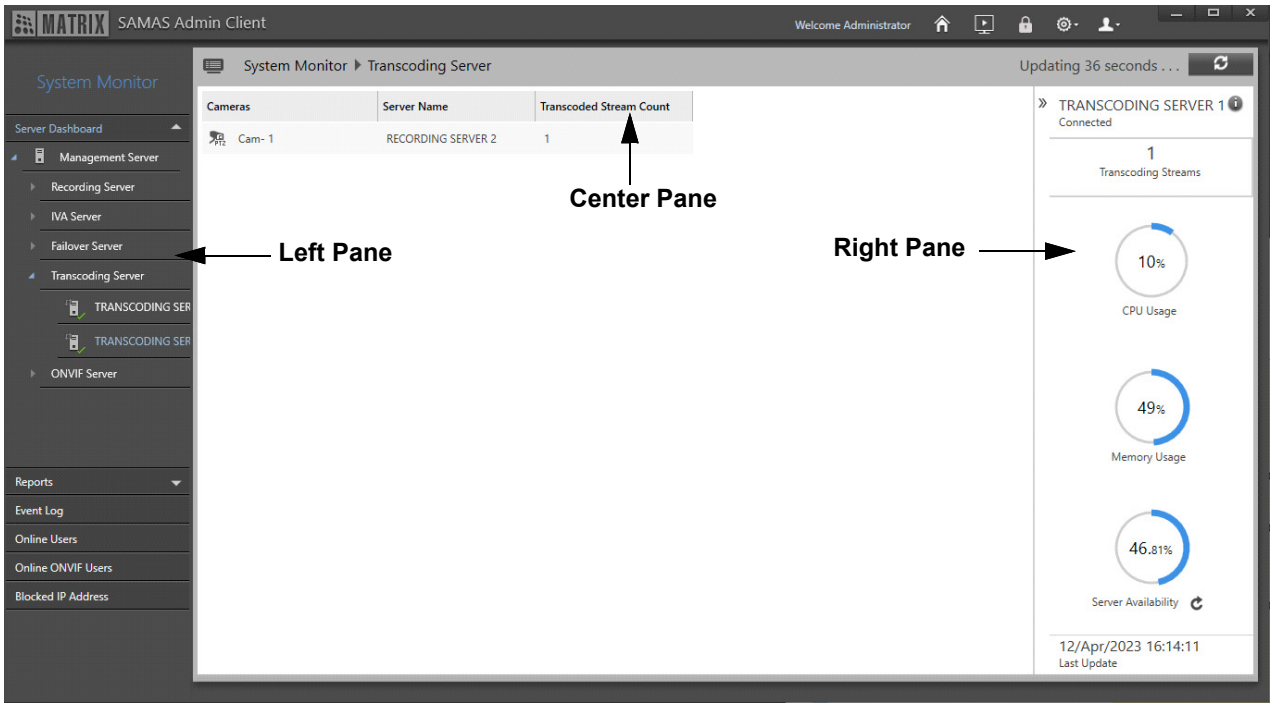
Transcoding Server

This tab enables you to view all the Transcoding Servers connected to the Management Server. You can also click on **Transcoding Server** from the Left Pane to view this tab.



The Server details displayed are — Transcoding Server Name, IPv4/IPv6 Address, Last Update and Transcoding Streams.

Double-click on a Transcoding Server to view its individual details.



The Transcoding Server's details are displayed in different panes — Left Pane, Center Pane and Right Pane.

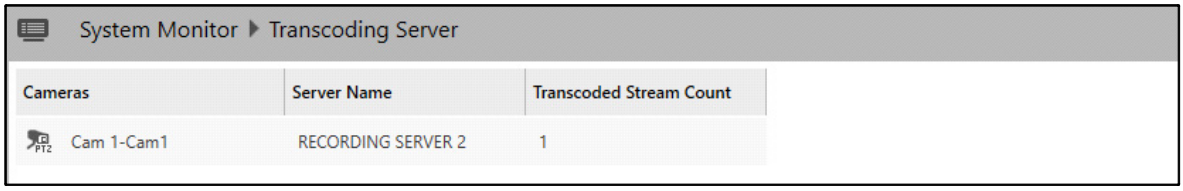
- Click **Refresh** to update the Transcoding Server details.

Left Pane

The Left Pane displays all the pages of the System Monitor module.

Center Pane

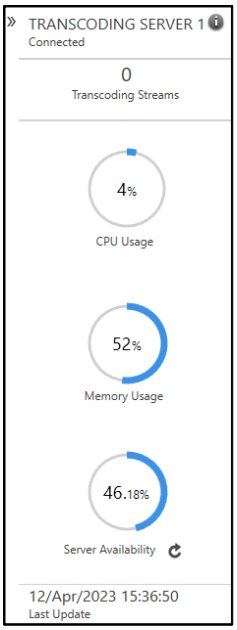
The Center Pane displays all the configuration details of the selected Transcoding Server.



These Server details are displayed — Cameras, Server Name and Transcoded Stream Count.

Right Pane

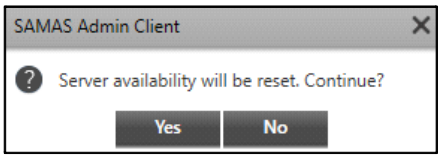
The Right Pane displays the Connection Details, CPU Usage, Memory Usage and Server Availability of the Transcoding Server along with stream details.



The details displayed are — Number of Transcoding Streams, CPU Usage, Memory Usage and Server Availability. The date and time of last update is also displayed.

- Click **Reset Server Availability** to reset the Server Availability to 100%. Only a user with **Administrator** rights can reset the Server Availability.

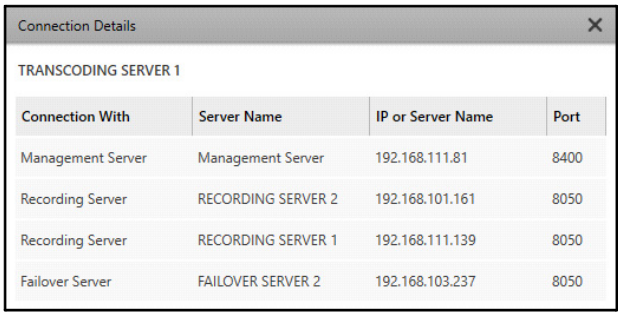
  The following pop-up appears.



  - Click **Yes** to confirm or click **No** to discard.

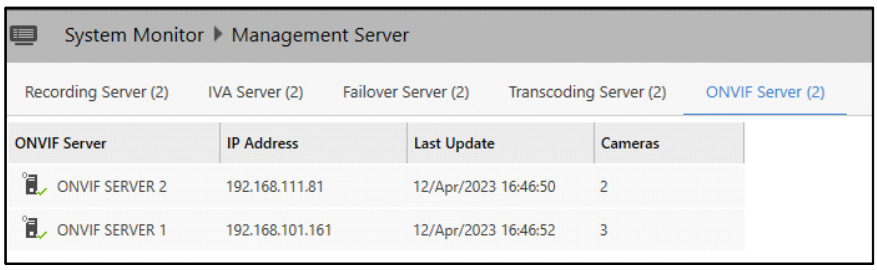
- Click **Connection Details** at top right corner of the page, to view the connection details of the Transcoding Server. It displays the connection details of the Transcoding Server with the Management Server, Recording Server and Failover Server. It displays the following details — Connection With, Server Name, IP (IPv4/IPv6) or Server Name and Port.





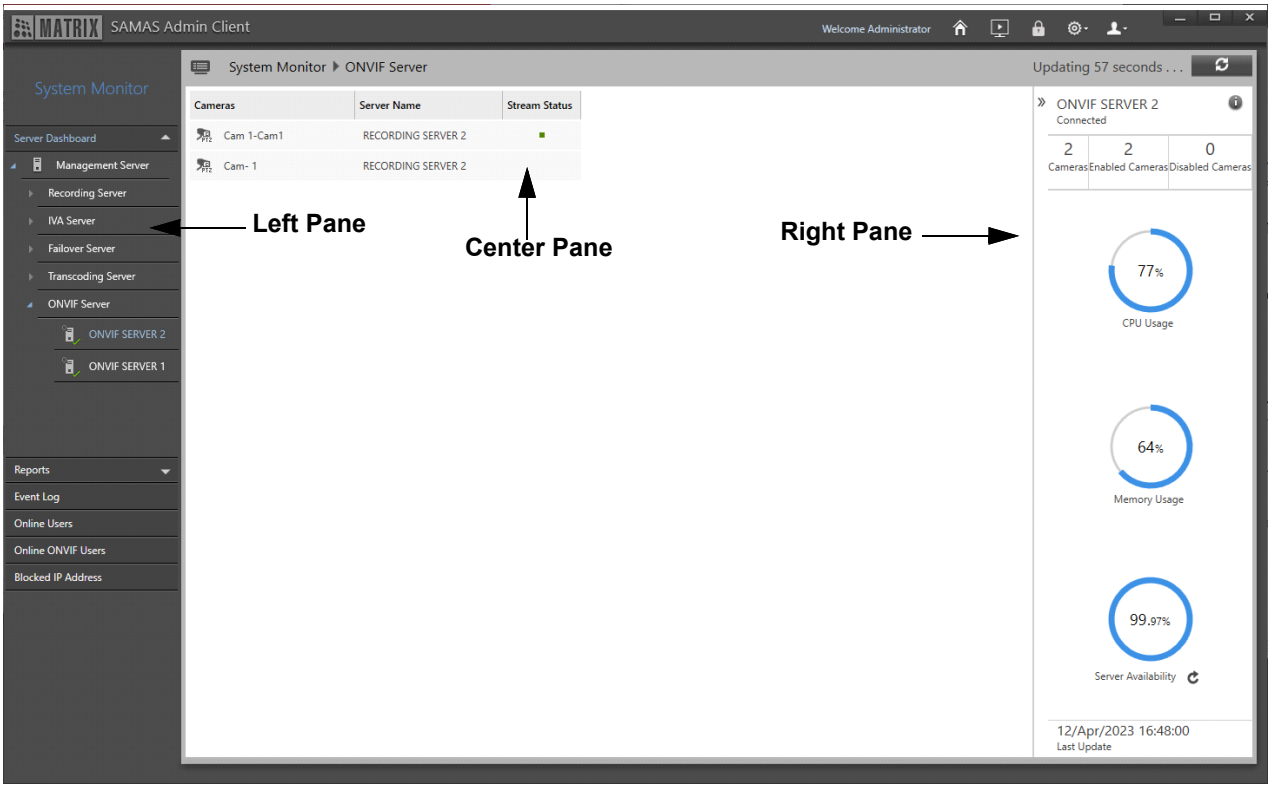
ONVIF Server

This tab enables you to view all the ONVIF Servers connected to the Management Server. You can also click on **ONVIF Server** from the Left Pane to view this tab.



The Server details displayed are — ONVIF Server Name, IPv4/IPv6 Address, Last Update and Cameras.

Double-click on a ONVIF Server to view its individual details.



The ONVIF Server's details are displayed in different panes — Left Pane, Center Pane and Right Pane.

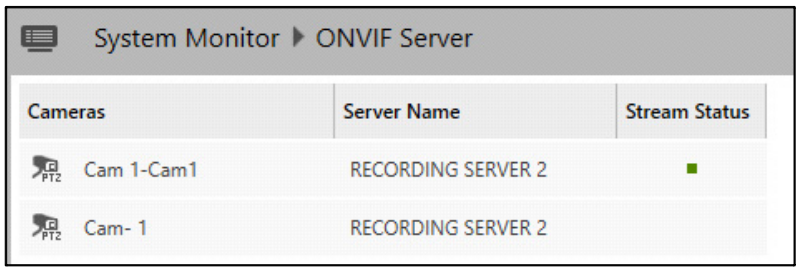
- Click **Refresh** to update the ONVIF Server details.

Left Pane

The Left Pane displays all the pages of the System Monitor module

Center Pane

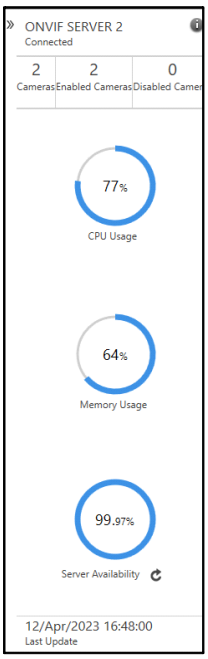
The Center Pane displays all the configuration details of the selected ONVIF Server.



The Server details displayed are — Cameras, Server Name and Stream Status. The camera for which ONVIF streaming is currently on is displayed by green color.

Right Pane

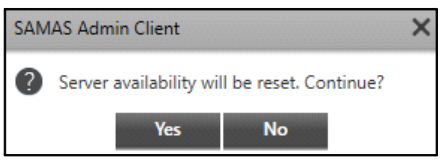
The Right Pane displays the Connection Details, the CPU Usage, Memory Usage and Server Availability of the ONVIF Server along with Camera details.



The details displayed are — Number of Cameras added, Number of Cameras Enabled, Number of Cameras Disabled, CPU Usage, Memory Usage and Server Availability. The date and time of last update is also displayed.

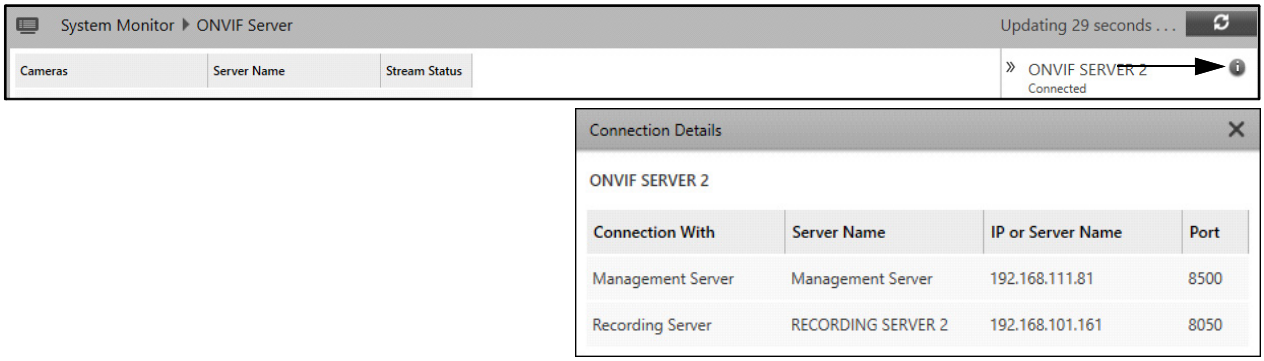
- Click **Reset Server Availability** to reset the Server Availability to 100%. Only a user with **Administrator** rights can reset the Server Availability.

  The following pop-up appears.



  - Click **Yes** to confirm or click **No** to discard.

- Click **Connection Details** at top right corner of the page, to view the connection details of the ONVIF Server. It displays the connection details of the ONVIF Server with the Management Server and Recording Server. It displays the following details — Connection With, Server Name, IP (IPv4/IPv6) or Server Name and Port.

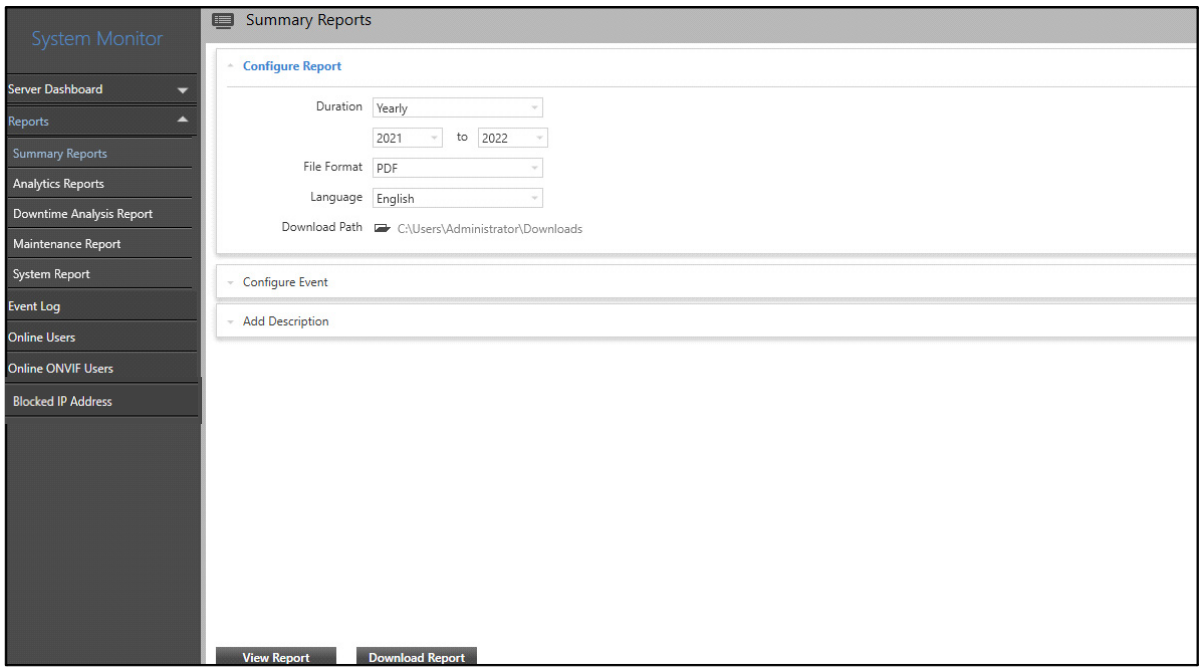


Reports

The Reports page enables you to generate, view and download different types of System Module reports, such as Summary, Analytics, Downtime Analysis, Maintenance and System Report.

To configure Reports,

- Click **System Monitor > Reports**.



Click the desired link for the configuration details of various reports.

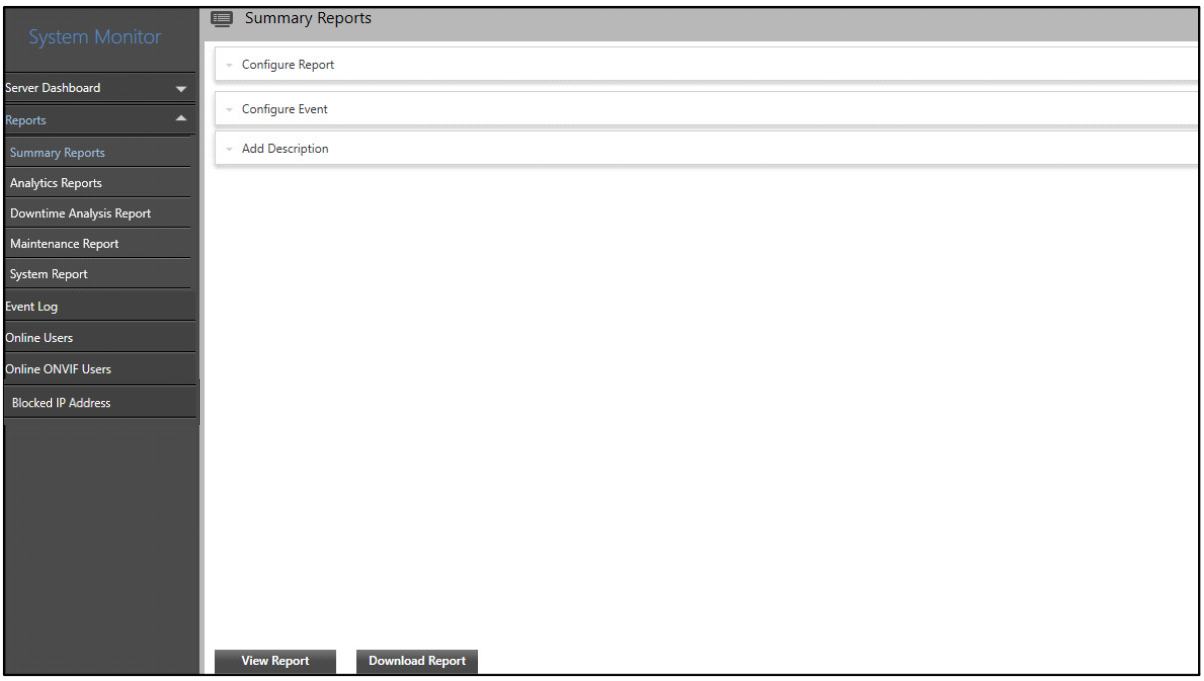
- “Summary Reports”
- “Analytics Reports”
- “Downtime Analysis Report”
- “Maintenance Report”
- “System Report”

Summary Reports

The Summary Reports page enables you to configure parameters for Summary Reports. You can view and configure Summary Reports on Yearly, Monthly, Daily, and Hourly basis.

To configure Summary Report,

- Click **System Monitor > Reports > Summary Reports**.



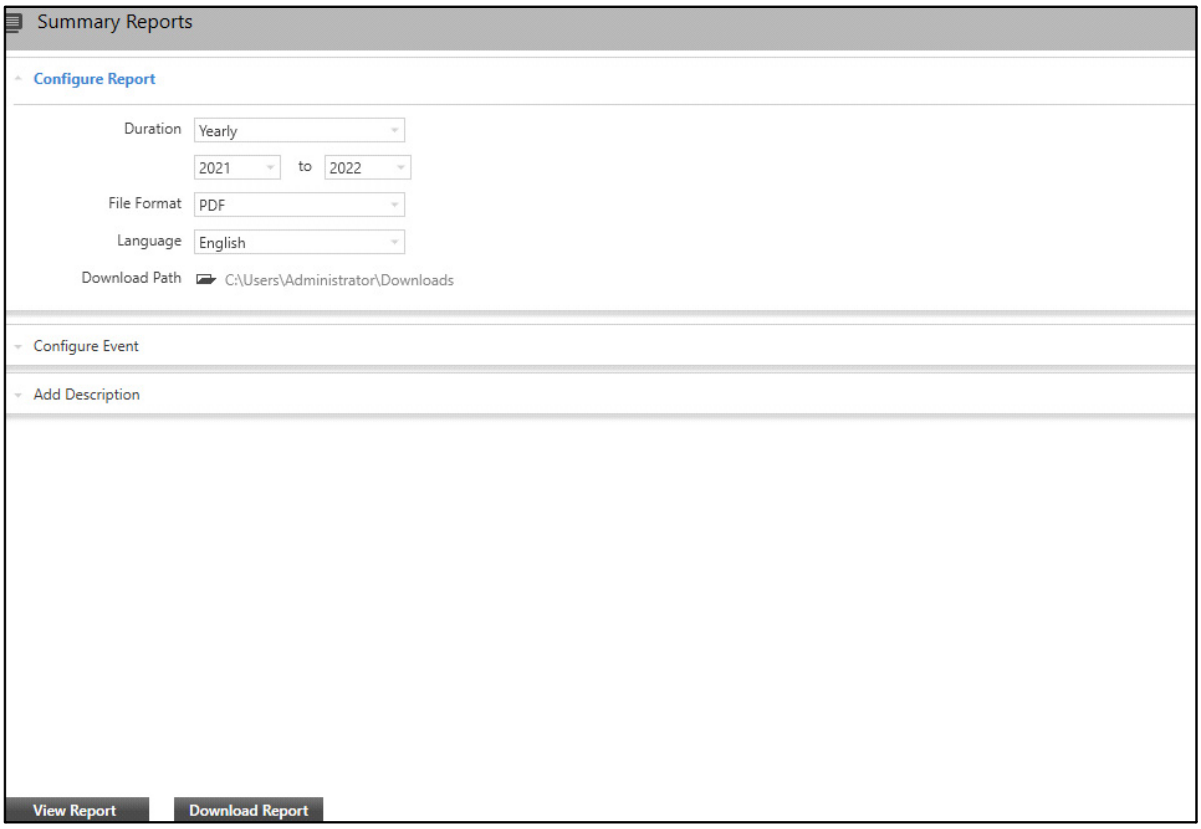
The Summary Reports page contains three collapsible panels — “Configure Report”, “Configure Event” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Summary Report from this collapsible panel.

To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

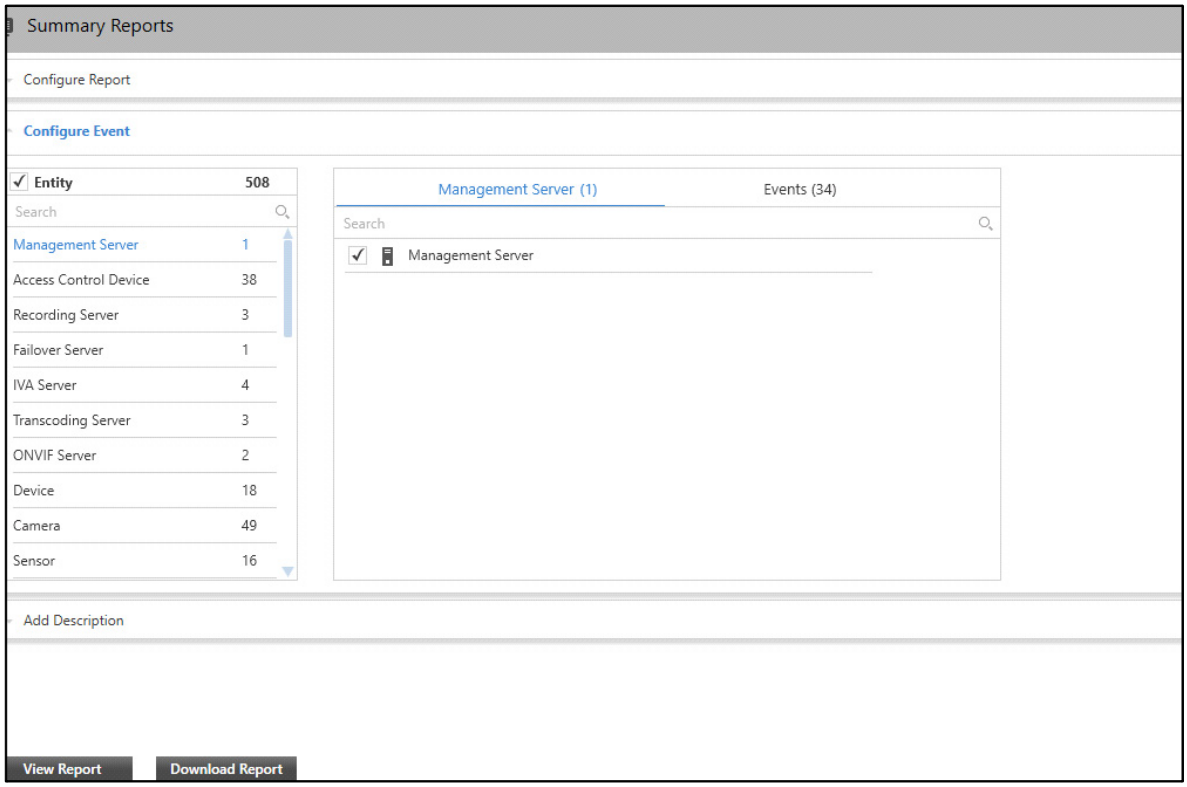
- **Duration**: Select the Duration from the drop-down list — Yearly, Monthly, Daily, Hourly, Weekly and Peak Hour Reports.
    - **Yearly**: Select this option to generate yearly reports. Select the desired From and To year from the drop-down lists.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the desired Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Configure Event

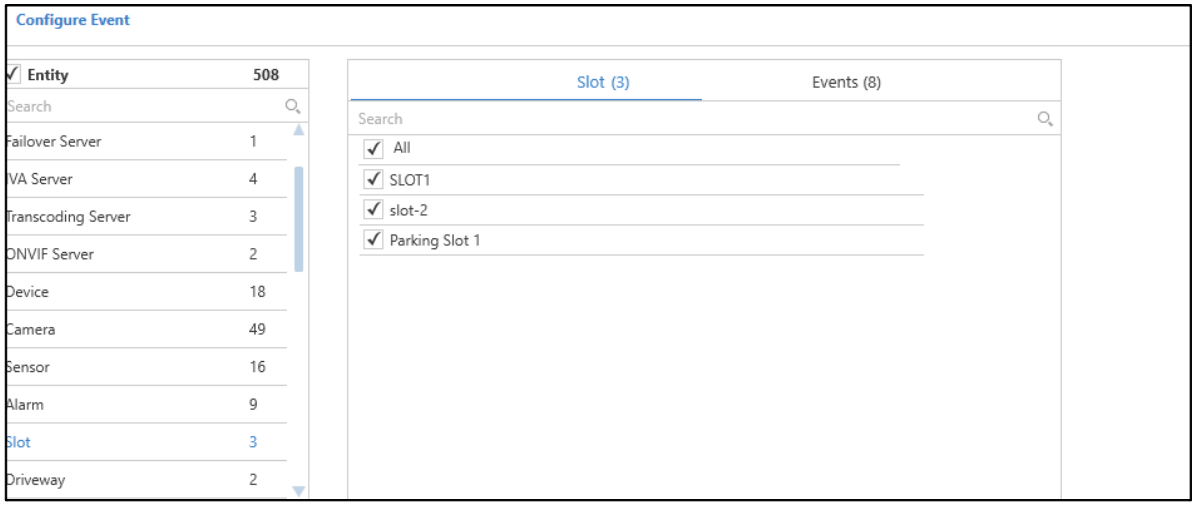
This panel allows you to configure Events for the Report once the report configurations are done. You can select the various configured entities and Events for them to generate the Summary Report.

To configure Events,

- Click the **Configure Event** collapsible panel.



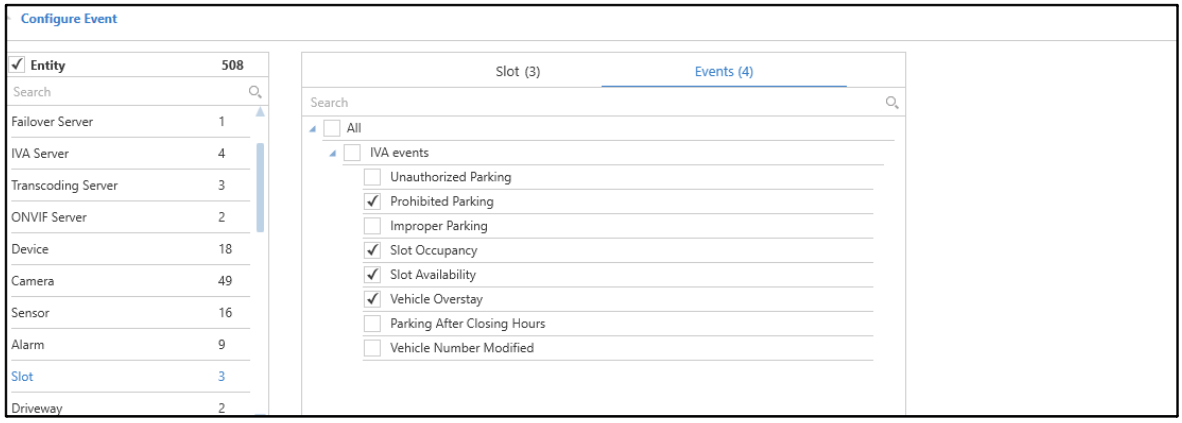
- Select the desired Entity for which you wish to generate the Summary Report from the list. The list of all configured entities for the selected Entity appears in a list on the right hand side. For example, if you select Slot, all the configured slots appear in a list under the **Slot** tab on the right hand side.



- Select the check boxes for the entities you wish to select from the Entity tab. The name of this tab changes as per the Entity selected from the list.



- The **Events** tab displays all the Events related to the selected Entity. Select the check boxes of the desired Events from the Events tab.



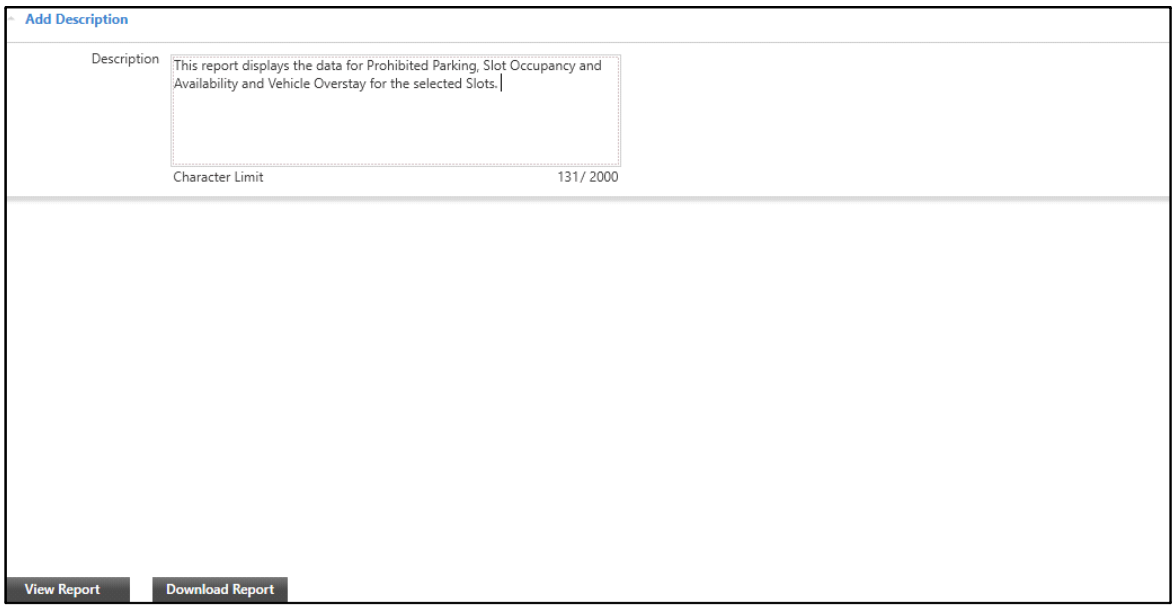
The Summary Report will be generated for the selected Entities and Events.

Add Description

This panel allows you to add a description for the Summary Report once the report configurations are done. This description is visible in the generated report.

To configure the Description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

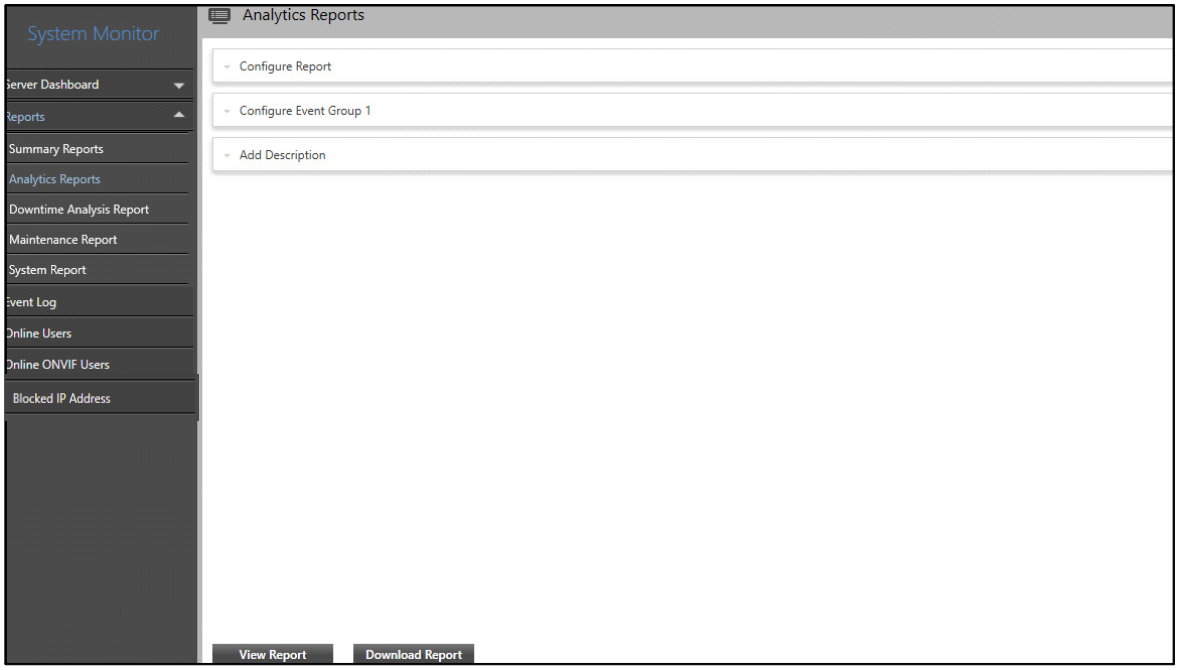
Analytics Reports

Analytics Report enables you to relate two Events occurring on the same or different Sources and analyze the time difference between their occurrences (For example, Motion Started and Motion Stopped, Trip Wire In and Trip Wire Out, etc.). These statistics can be useful in management of certain sectors like Logistics, Hospitality, Transportation, etc. where there is a dependency between two Events or where time required for certain activities needs to be analyzed.

The Analytics Reports page enables you to configure parameters for Analytics Reports. You can view and configure Analytics Reports on Monthly and Daily basis.

To configure Analytics Report,

- Click **System Monitor > Reports > Analytics Reports**.



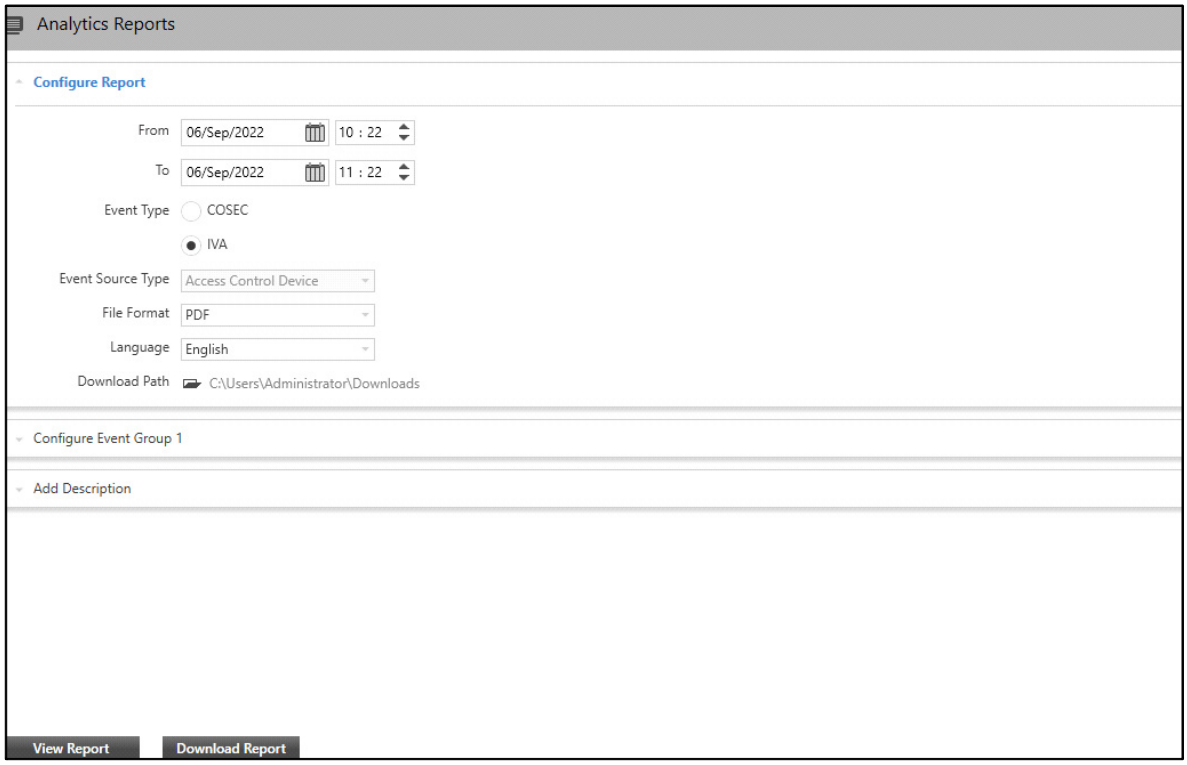
The Analytics Reports page contains three collapsible panels — “Configure Report”, “Configure Event Group 1” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Analytics Report from this collapsible panel.

To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

- **From**: Select the date from which you wish to generate the report from the calendar and specify the time.
- **To**: Select the date till which you wish to generate the report from the calendar and specify the time.
- **Event Type**: Select the Event type from the options — COSEC or IVA. You can select Events for the report based on the selected Event type.

  If you select **COSEC** as the Event Source Type, configure the following parameter:

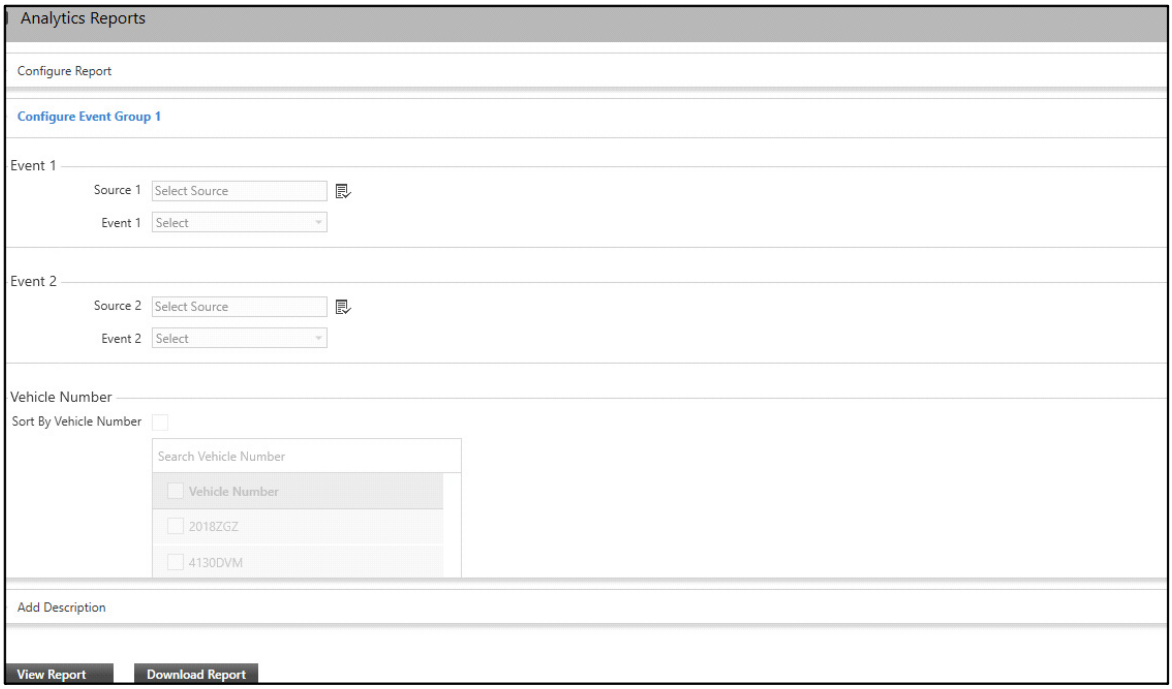
- **Event Source Type**: Select the Event Source Type for which you wish to generate the report from the drop-down list.
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the desired Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It will display all folders which are in the drive. Select the desired folder.

Configure Event Group 1

This panel allows you to configure Event Group for the Report once the report configurations are done. You can select the various configured Sources and Events for them to generate the Analytics Report.

To configure the Event Group 1,

- Click the **Configure Event Group 1** collapsible panel.



Configure the following parameters:

Event 1

- **Source 1**: Select the Source for which you wish to generate the report using the **Source** picklist. The **Source** pop-up appears. Double-click to select the desired option.
- **Event 1**: Select the Event for which you wish to generate the report from the drop-down list.

Event 2

- **Source 2**: Select the Source for which you wish to generate the report using the **Source** picklist. The **Source** pop-up appears. Double-click to select the desired option.
- **Event 2**: Select the Event for which you wish to generate the report from the drop-down list.

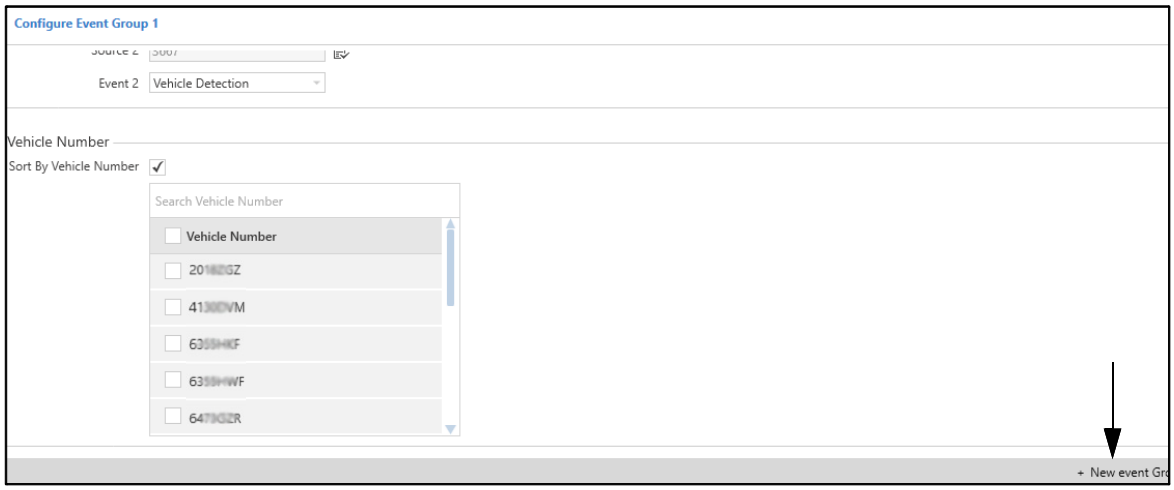
Vehicle Number

Vehicle Number is configurable only if both the selected Events can be detected using Vehicle Number Plate.

- **Sort By Vehicle Number**: Select the check box to enable the selection of vehicle numbers. Select the check boxes for the desired vehicle numbers according to which you wish to sort the data.

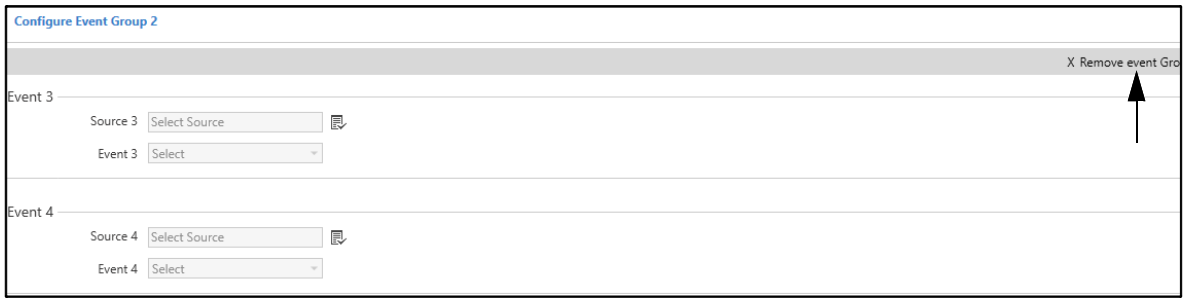
You can also configure an additional Event Group, if required. However, you can configure only one Event Group for License Plate Registration.

- Click **New Event Group** to configure an additional Event Group.



The parameters for Event 3 and Event 4 appear in a new collapsible panel — **Configure Event Group 2**.

- Click the **Configure Event Group 2** collapsible panel.



Configure the following parameters:

Event 3

- **Source 3**: Select the Source for which you wish to generate the report using the **Source** picklist. The **Source** pop-up appears. Double-click to select the desired option.
- **Event 3**: Select the Event for which you wish to generate the report from the drop-down list.

Event 4

- **Source 4**: Select the Source for which you wish to generate the report using the **Source** picklist. The **Source** pop-up appears. Double-click to select the desired option.
- **Event 4**: Select the Event for which you wish to generate the report from the drop-down list.

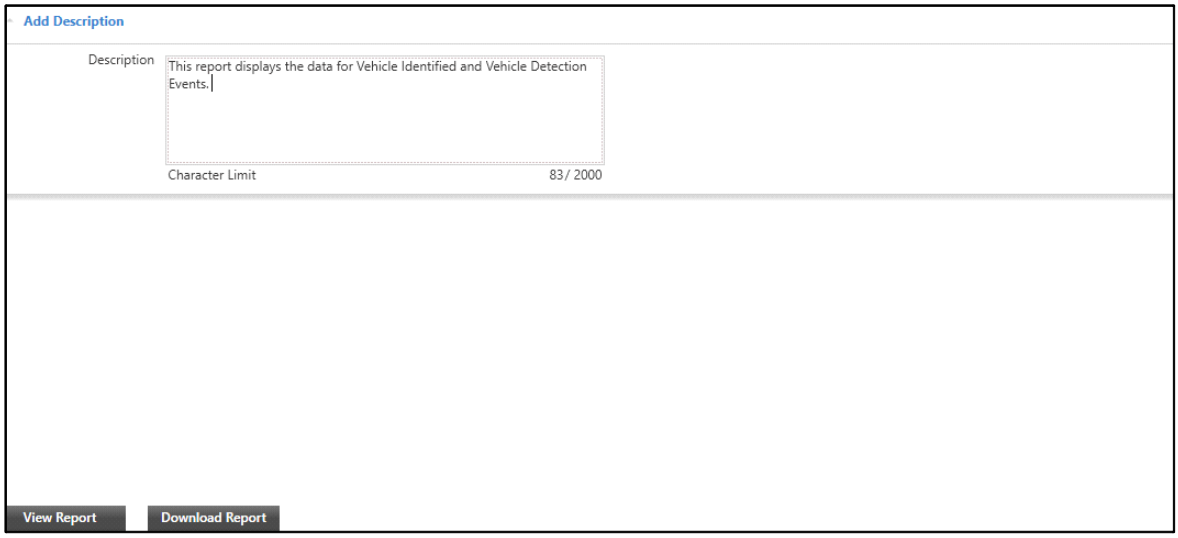
- To remove the Event Group, click **Remove event Group**.

Add Description

This panel allows you to add a description for the Analytics Report once the report configurations are done. This description is visible in the generated report.

To configure the Description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

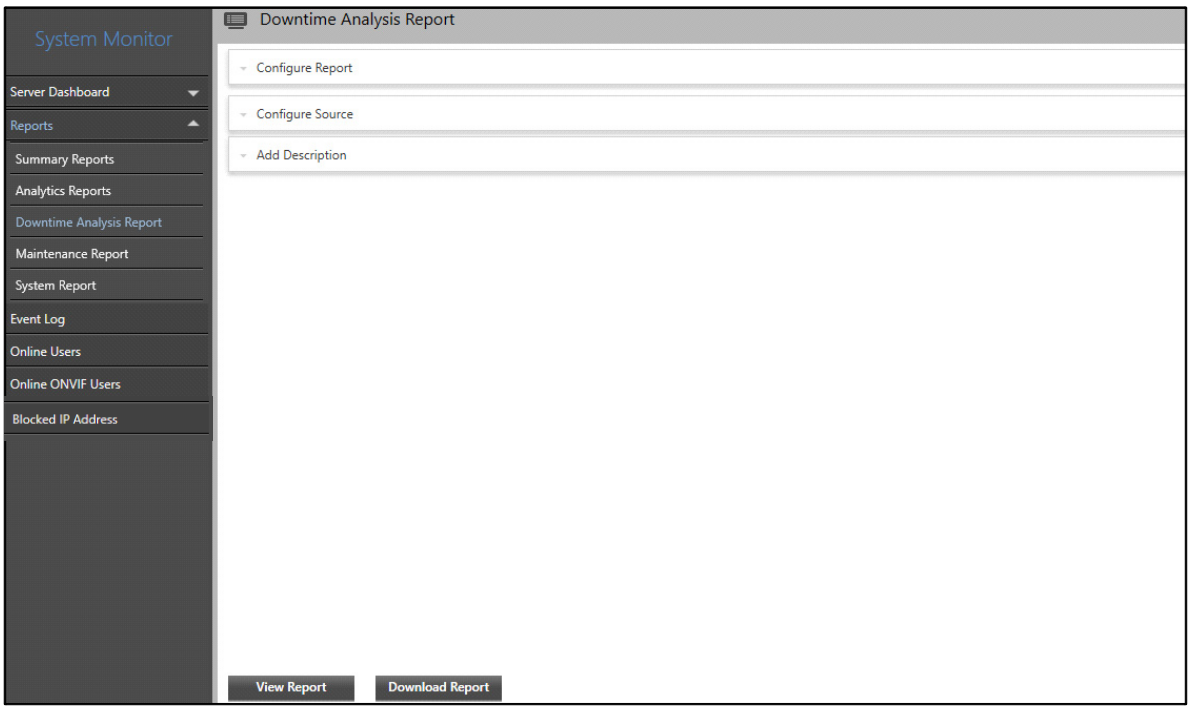
Downtime Analysis Report

Downtime Analysis Report enables you to analyze the performance of Servers and Devices. It displays data regarding the connection and disconnection duration of Servers and Devices. The Servers and Devices may get disconnected due to certain reasons such as network failure or hardware error. These statistics are useful to monitor the health status of the Servers and Devices.

The Downtime Analysis Report page enables you to configure parameters for Downtime Analysis Reports. You can view and configure Downtime Analysis Reports on Monthly and Daily basis.

To configure Downtime Analysis Report,

- Click **System Monitor > Reports > Downtime Analysis Report**.



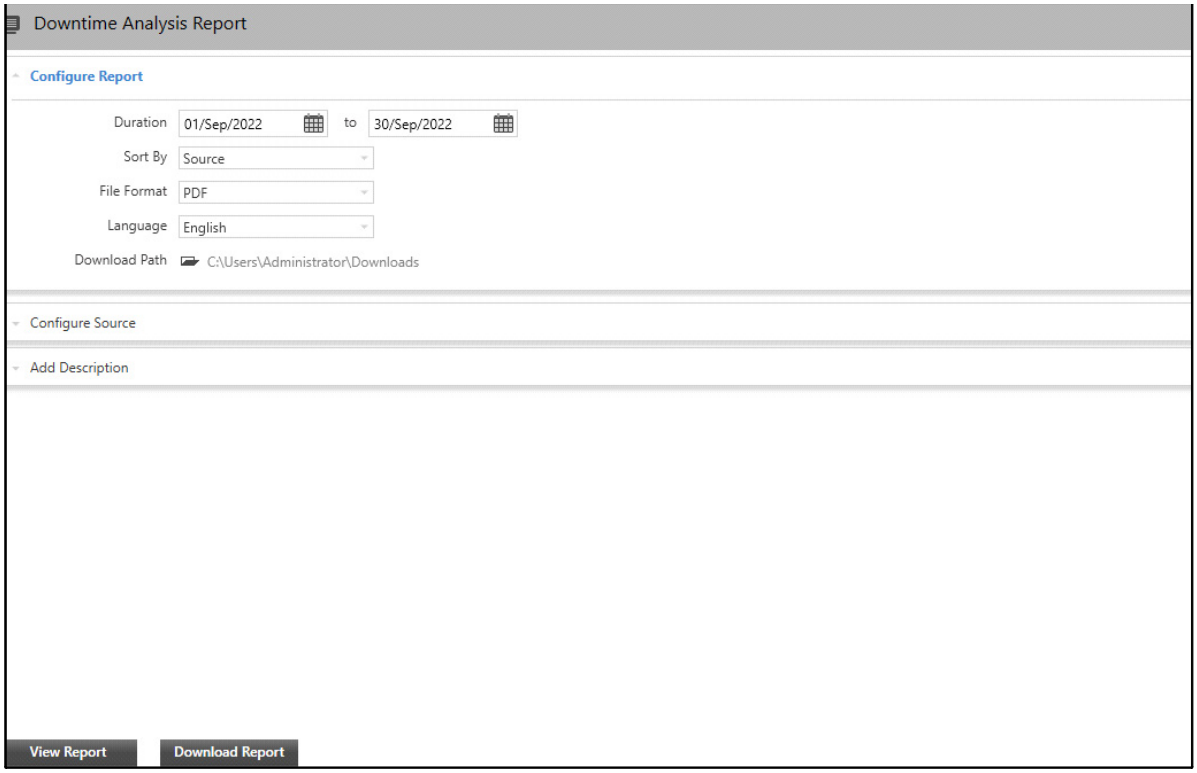
The Downtime Analysis Report page contains three collapsible panels — “Configure Report”, “Configure Source” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Downtime Analysis Report from this collapsible panel.

To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

- **Duration**: Select the From and To date for which you wish to generate the report from the calendar.
- **Sort By**: Select the option by which you wish to sort the report data from the drop-down list options — Time or Source.

  If you select **Time**, the report data will be sorted on the basis of disconnection time of the selected entities.

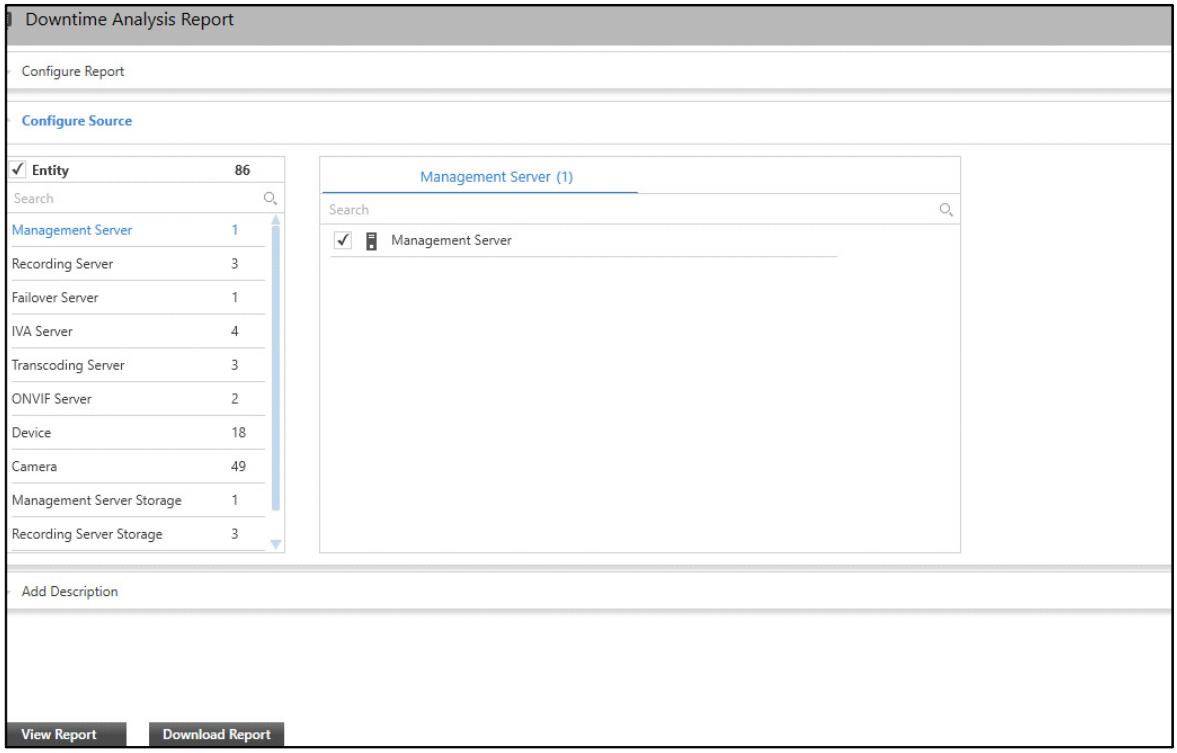
  If you select **Source**, the report data will be sorted on the basis of Source IDs of the selected entities.
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Configure Source

This panel allows you to configure the Source for the Report once the report configurations are done. You can select the various configured Sources and Events for them to generate the Downtime Analysis Report.

To configure the Source parameters,

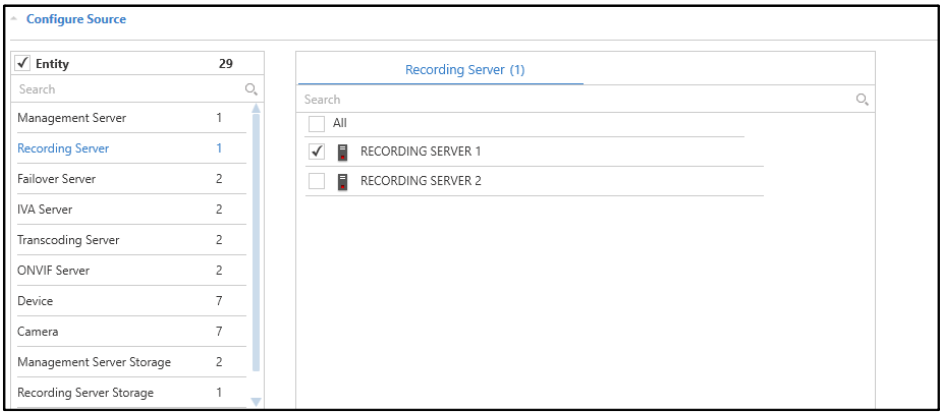
- Click the **Configure Source** collapsible panel.



- Select the desired Entity for which you wish to generate the Downtime Analysis Report from the list. The list of all configured entities for the selected Entity appears in a list on the right hand side. For example, if you select Recording Server, all the configured Recording Servers appear in a list under the **Recording Server** tab on the right hand side.



- Select the check boxes for the entities you wish to select from the Entity tab. The name of this tab varies as per the Entity selected from the list.



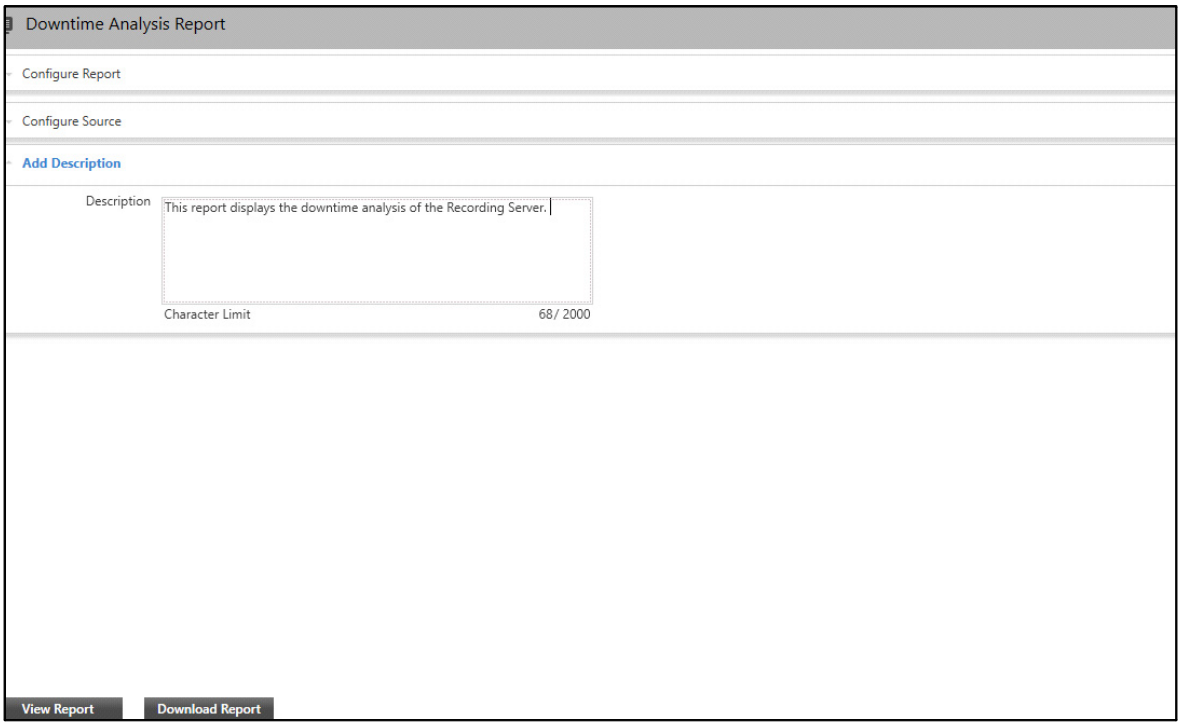
The Downtime Analysis Report will be generated for the selected Entities.

Add Description

This panel allows you to add a description for the Downtime Analysis Report once the report configurations are done. This description is visible in the generated report.

To configure the Description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. The Description can be of upto 2000 characters only and it is displayed on the second page of the report.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

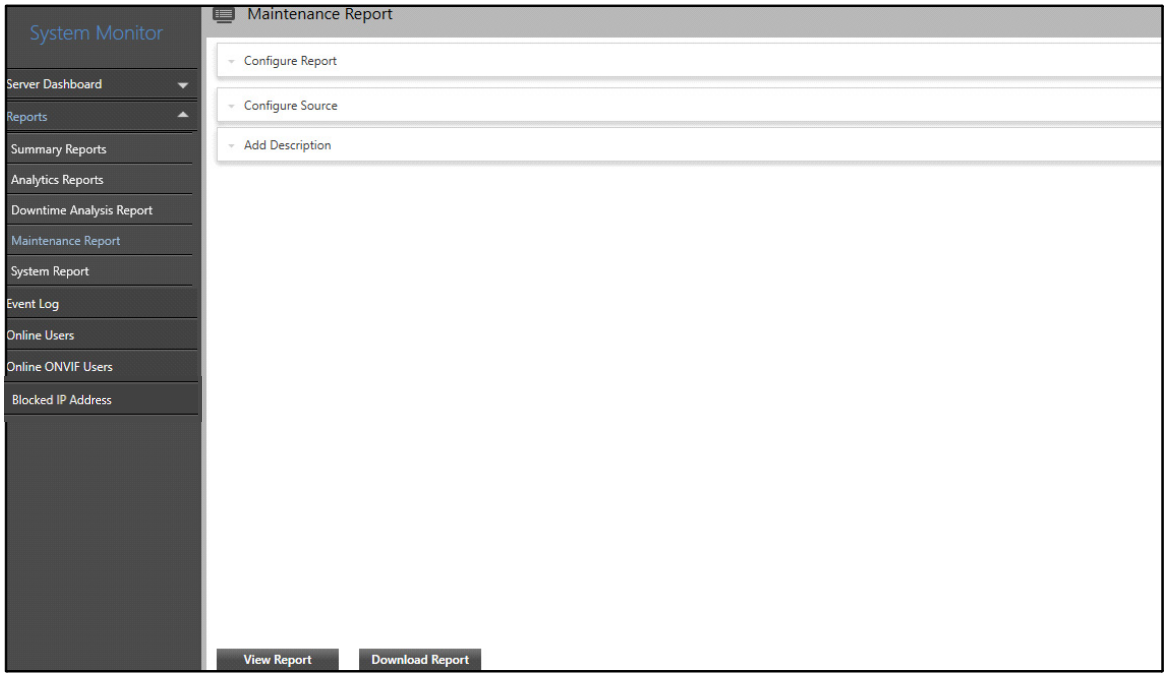
Maintenance Report

Maintenance Report enables you to analyze the Product Life Cycle of Devices as per its performance. It displays data regarding how much duration and for how many times a device was under maintenance. More the duration of device being under maintenance, less will be the efficiency of the device.

The Maintenance Report page enables you to configure parameters for Maintenance Reports. You can view and configure Maintenance Reports on Monthly and Daily basis.

To configure the Maintenance Report parameters,

- Click **System Monitor > Reports > Maintenance Report**.



The configurations of Maintenance Report are similar to that of the Downtime Analysis Report. For details, refer to “Downtime Analysis Report”.

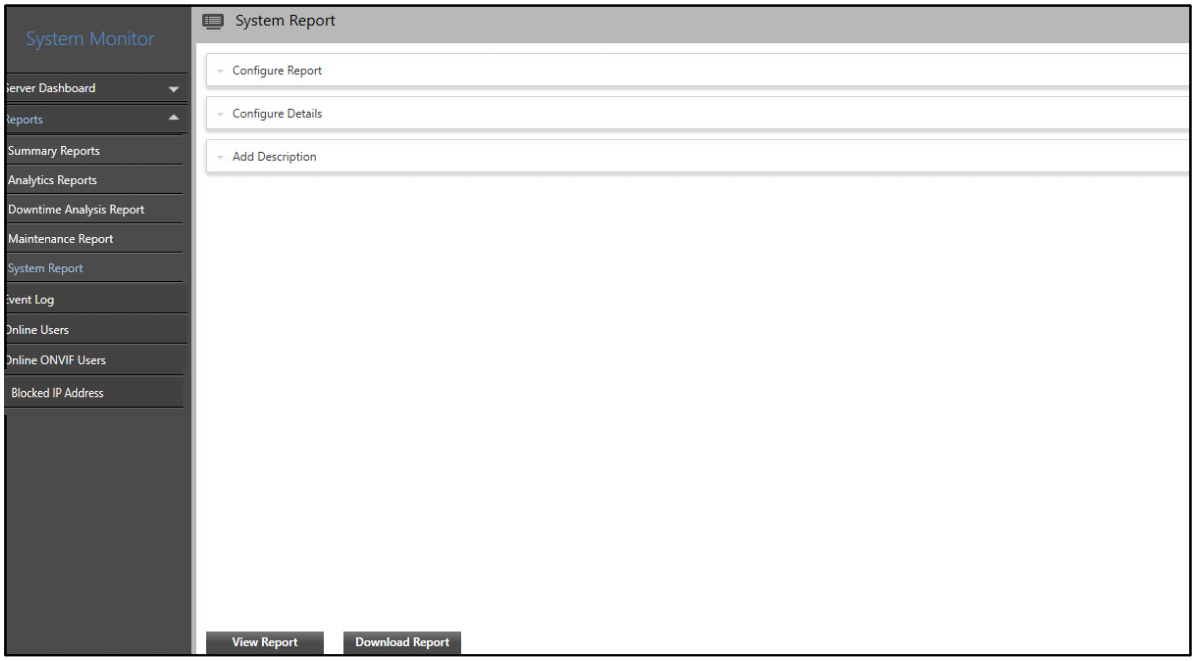
System Report

System Report enables you to generate reports with the details of the various Servers and their parameters, the various Devices connected and their network parameters, Sensors, Alarms, etc. This information is useful to analyze the configuration of these entities so as to optimize the system. The System Report can also be used as an Audit Report for the regular security audits where the Devices and IP Cameras are audited.

The System Report page enables you to configure parameters for System Reports. You can view and configure System Reports on Monthly and Daily basis.

To configure the System Report parameters,

- Click **System Monitor > Reports > System Report**.



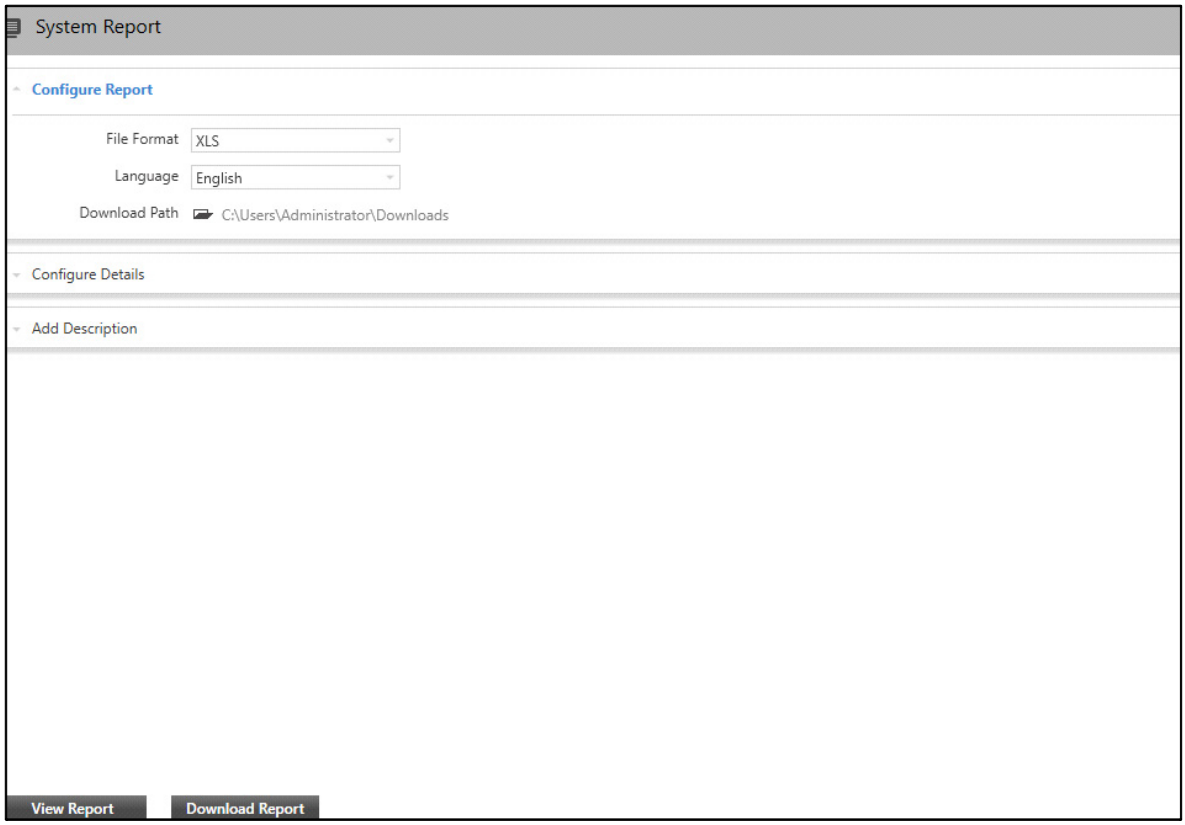
The System Report page contains three collapsible panels — “Configure Report”, “Configure Details” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the System Report from this collapsible panel.

To configure the report parameters,

- Click the **Configure Report** collapsible panel.



Configure the following parameters:

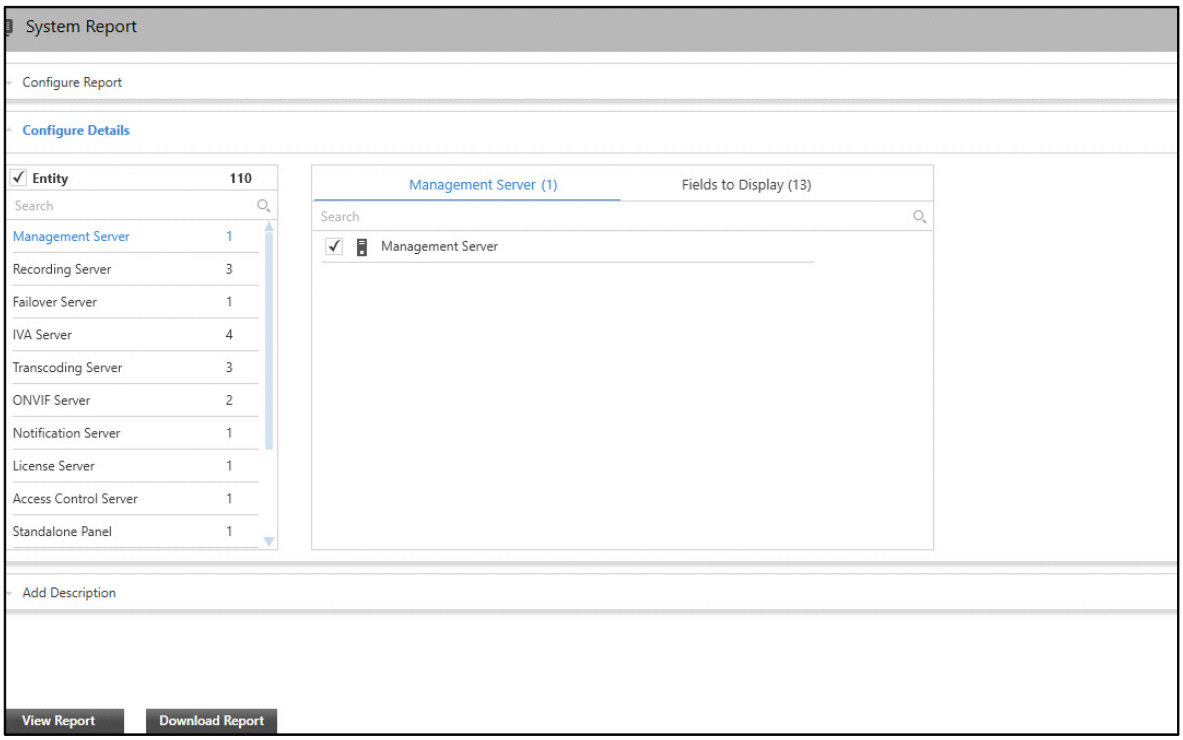
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the desired Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Configure Details

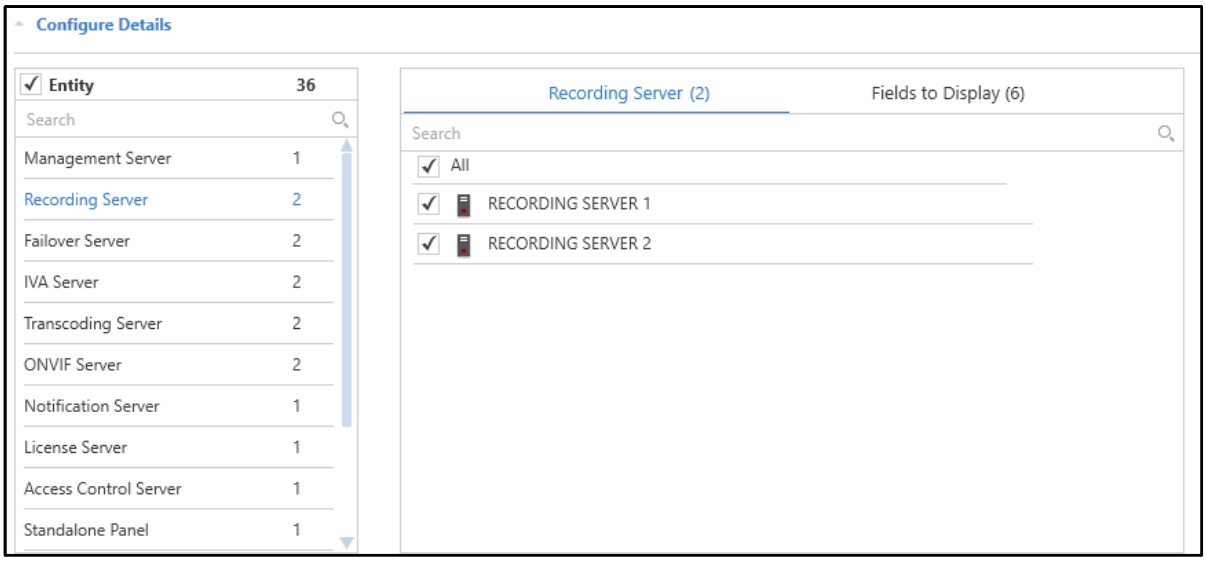
This panel allows you to configure Details for the Report once the report configurations are done. You can select the various configured Entities and Fields to be displayed in the generated System Report.

To configure the Details,

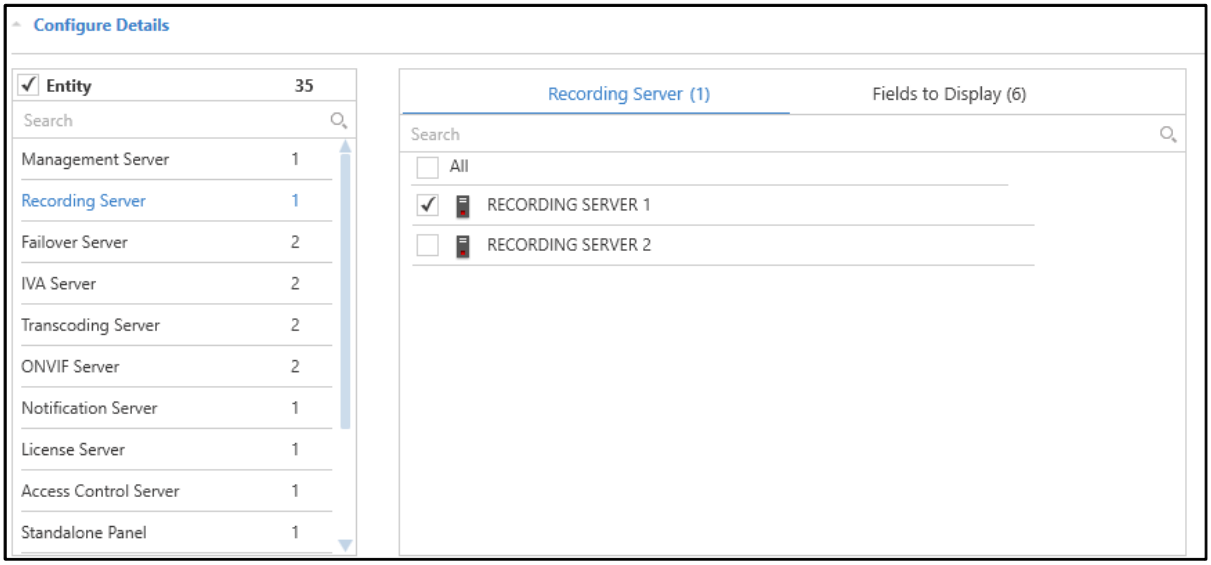
- Click the **Configure Details** collapsible panel.



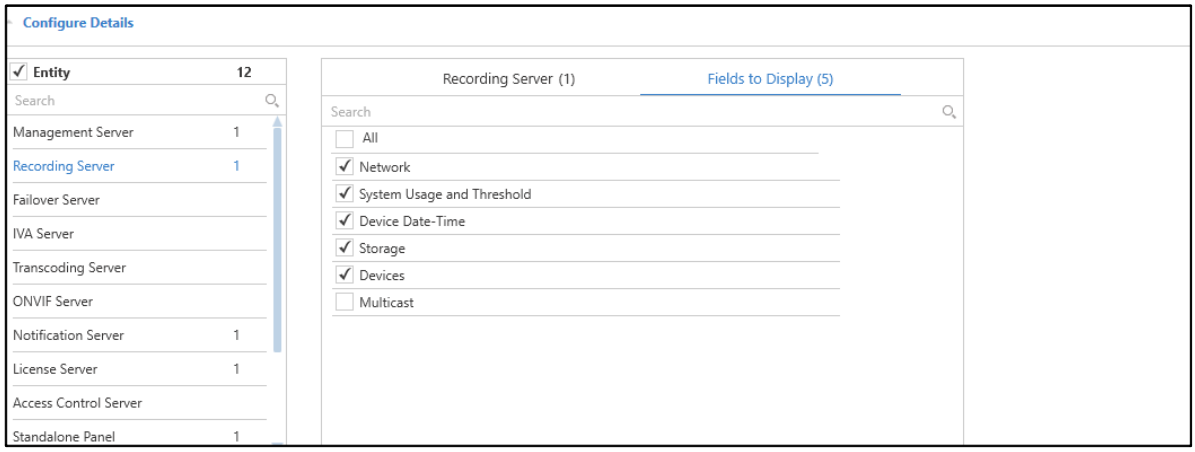
- Select the desired Entity for which you wish to generate the System Report from the list. The list of all configured entities for the selected Entity appears in a list on the right hand side. For example, if you select Recording Server, all the configured Recording Servers appear in a list under the **Recording Server** tab on the right hand side.



- Select the check boxes for the entities you wish to select from the Entity tab. The name of this tab varies as per the Entity selected from the list.



- The **Fields to Display** tab displays all the Fields related to the selected Entity. Select the check boxes of the desired Fields you wish to display for the selected entity from the Fields to Display tab.



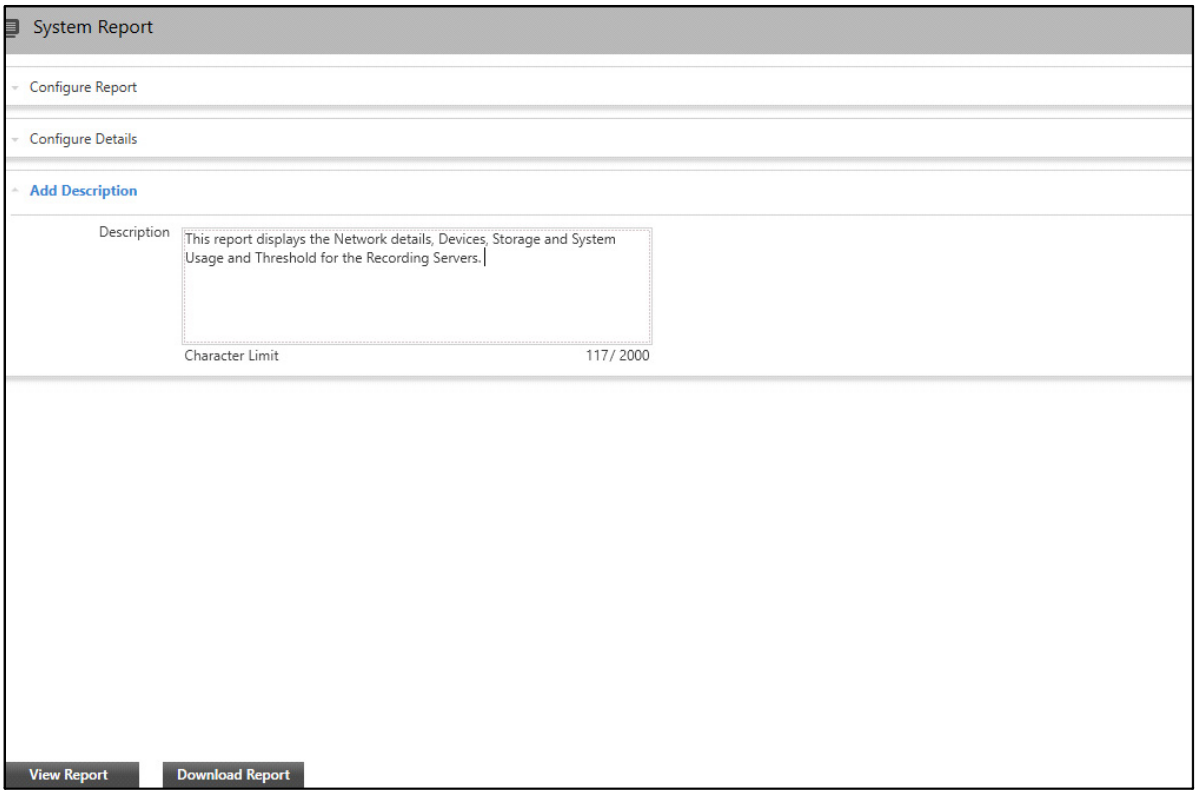
The System Report will be generated for the selected Entities and Fields.

Add Description

This panel allows you to add a description for the System Report once the report configurations are done. This description is visible in the generated report.

To configure the Description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

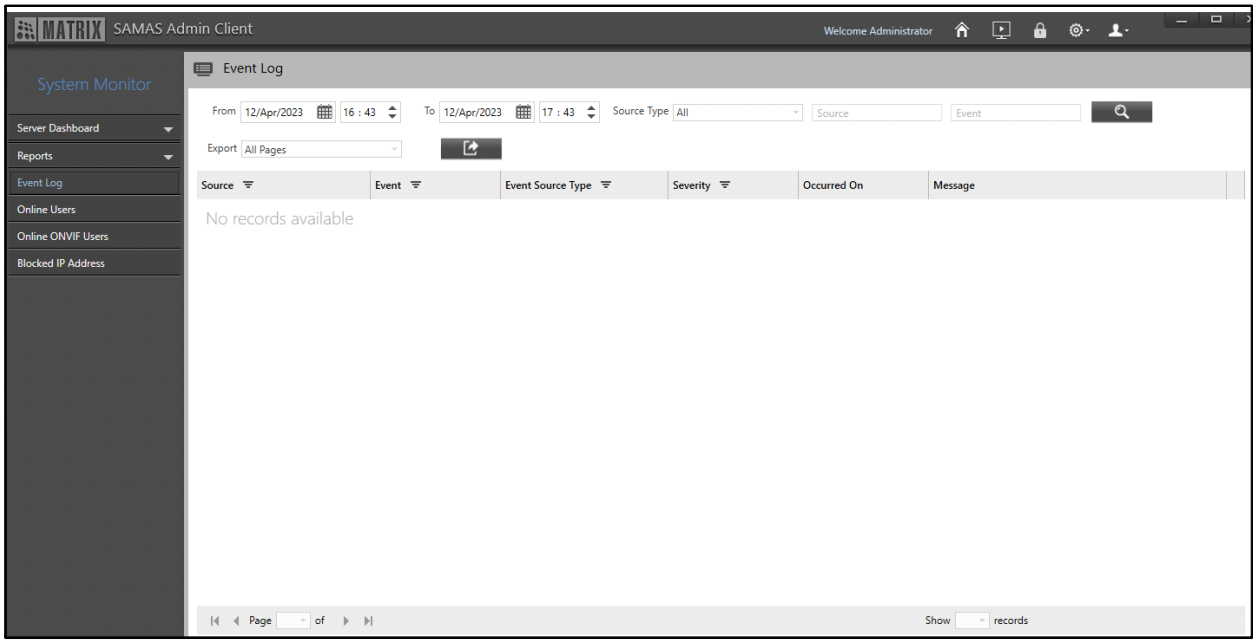
Event Log

The Event Log page enables you to view the Event logs for all the Events and Event Source Types for which "Event Monitoring Rights" have been assigned to your User Group. You can search and filter different Event logs from this page.

For the list of all events, refer to "Scenario Events With Actions". If you have enabled SSL and if the certificate expires/unavailable, then the system switches to the SAMAS Default Certificate. Hence, such events will also be logged under Event Logs.

To configure Event Log,

- Click **System Monitor > Event Log**.



Configure the following parameters:

- **From**: Select the date from which you wish to view the Event Log from the calendar and specify the time.
- **To**: Select the date till which you wish to view the Event Log from the calendar and specify the time.
- **Source Type**: Select the Source Type for which you wish to view the Event Log from the drop-down list.
- **Source**: Specify the name of the Source/keyword of the Source according to the selected Source Type. In Source, you can enter upto 80 characters. Default: Blank.
- **Event**: Specify the name of the Event/keyword of the Event of the Source Type for which you wish to view the Event Log.
- **Event Details**: If you have selected Source Type as Access Control Device, you can filter the Event Logs based on User Name and User ID. Type the desired User Name/ID in the text box. When you

click Search, all the Events for the configured duration containing the entered User Name/ID will appear. In Event Details, you can enter upto 45 characters. Default: Blank.

- Click **Search** . The list of all the Event Logs for the configured duration appear in a list.

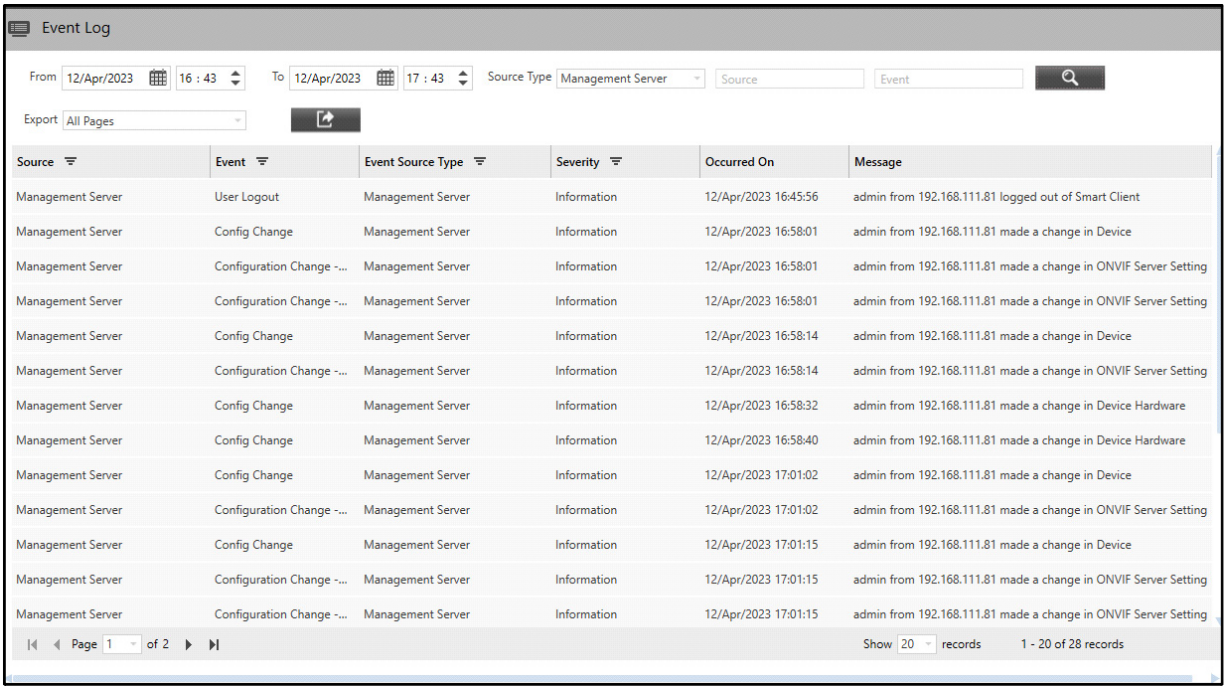
The Event Log details displayed are — Source, Event, Event Source Type, Severity, Occurred On and Message. You can also export the Event logs to your system.

- Click **Filter** of the respective parameter in the header row.

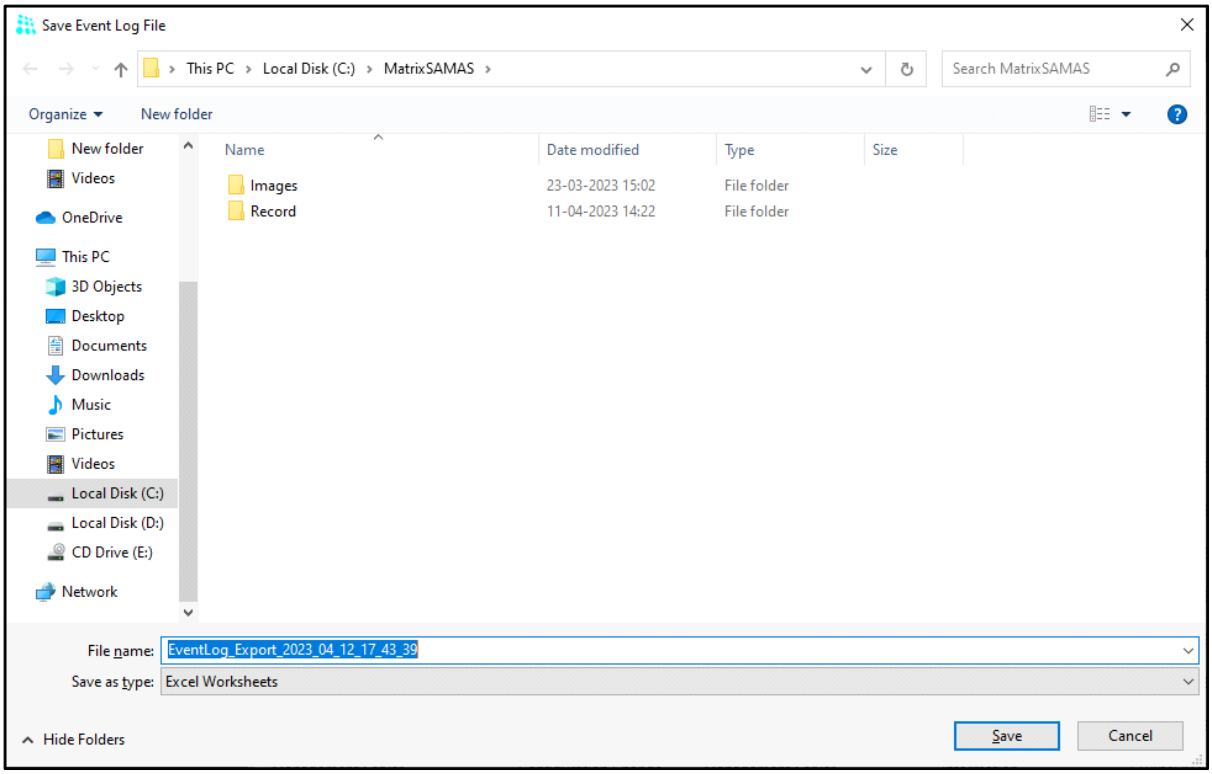
  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.



- Select the pages that you wish to export from the **Export** drop-down list.
- Click **Export** . The **Save Event Log File** pop-up appears.



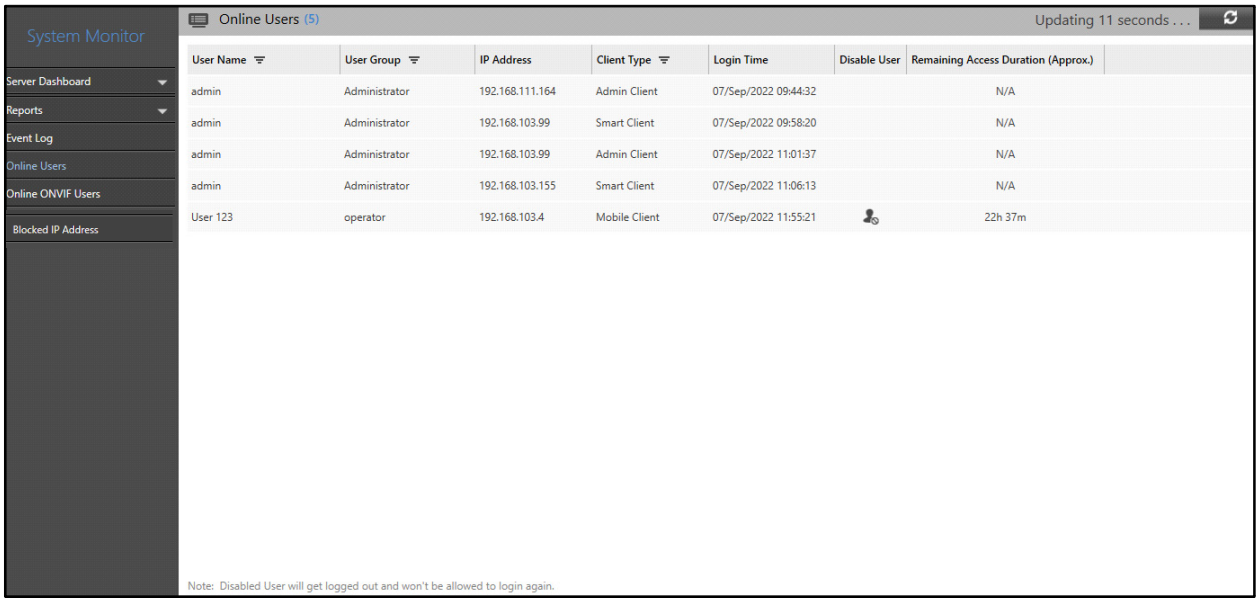
- Select the desired folder where you wish to save the Event Log file and specify the file name.
- Click **Save** to save the file or click **Cancel** to discard.

Online Users

The Online Users page enables you to view the users that are currently using the SATATYA SAMAS components (Admin Client, Smart Client and Mobile Client).

To view Online Users,

- Click **System Monitor > Online Users**.



The following User Details are displayed — User Name, User Group, IPv4/IPv6 Address, Client Type, Login Time, Disable User and Remaining Access Duration (Approx.).

You can filter the User records according to User Name, User Group or Client Type. You can also sort the data by clicking on the respective fields — User Name, User Group, IP Address, Client Type, Login Time, Disable User and Remaining Access Duration (Approx.).

- Click **Filter** of the respective parameter in the header row.

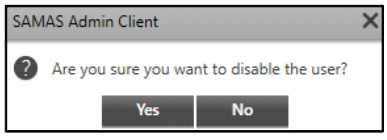
  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

You can disable User's to prevent them from logging in.

- Click **Disable User** . The following pop-up appears.



- Click **Yes** to disable the User or click **No** to cancel.

The disabled User's active session will be terminated within one minute. To enable the User, select the **Enable User** check box from **General Settings > System Account > Users** for the disabled user.



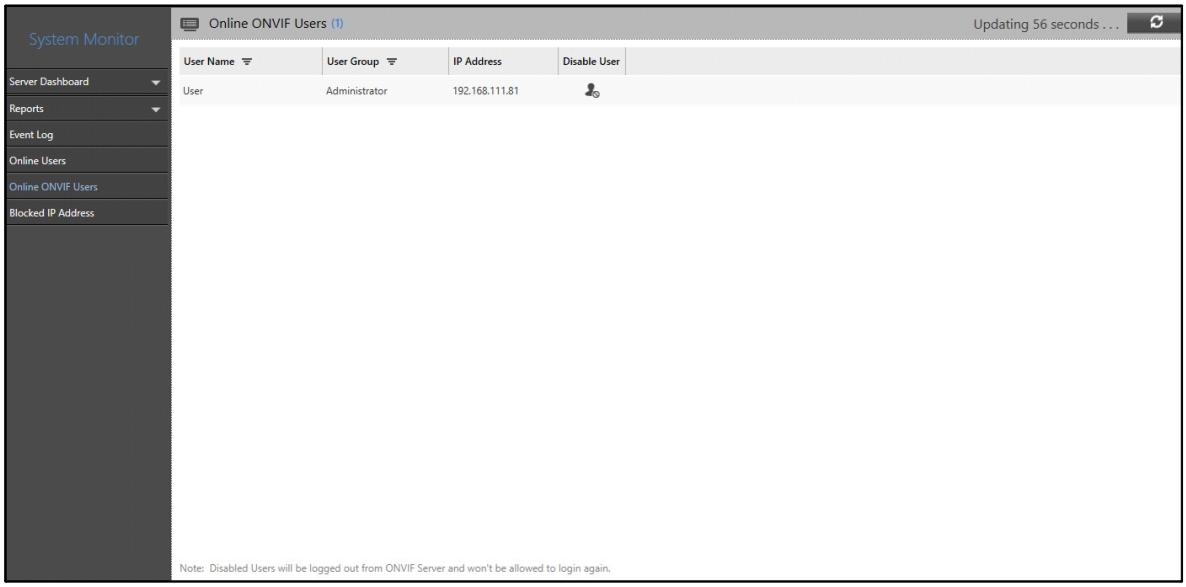
Admin User cannot be disabled.

Online ONVIF Users

The Online ONVIF Users page enables you to view the RTSP Clients that are currently active.

To view Online ONVIF Users,

- Click **System Monitor > Online ONVIF Users**.



The following User Details are displayed — User Name, User Group, IPv4/IPv6 Address and Disable User.

You can filter the User records according to User Name or User Group. You can also sort the data by clicking on the respective fields — User Name, User Group, IP Address and Disable User.

- Click **Filter** of the respective parameter in the header row.

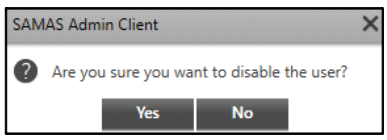
  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

You can disable User's to prevent them from logging in.

- Click **Disable User** . The following pop-up appears.



- Click **Yes** to disable the user or click **No** to cancel.

The disabled User’s active session will be terminated within one minute.

To enable the User, select the **Enable User** check box from **General Settings > System Account > ONVIF Users** for the disabled user.



Admin User cannot be disabled.

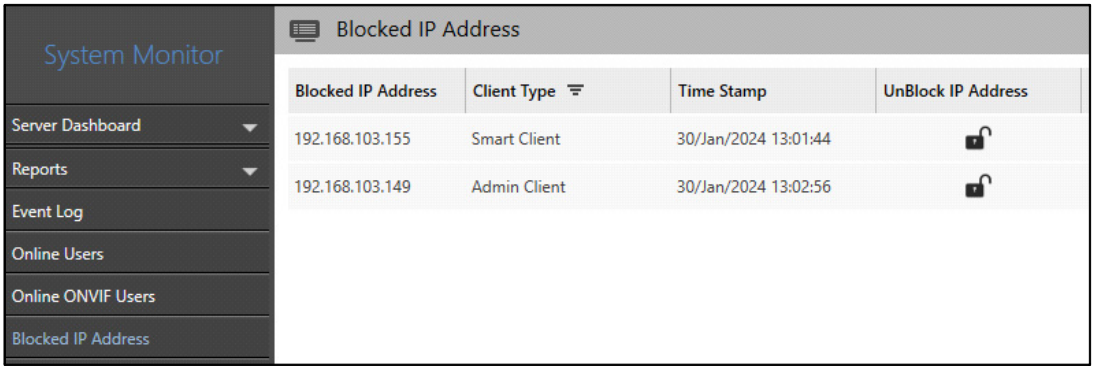
Blocked IP Address

The Blocked IP Address page enables you to view the list of IP addresses blocked under the IP Blocking Policy. You can unblock the IP addresses from this page. When any user's login fails due to blocked IP Address, then the reason for Login Failed Event will be displayed as IP Address Blocked in the Event Log.

To ensure smooth functioning of this feature, make sure the Admin Client and MS are upgraded to the same version.

To view Blocked IP Addresses,

- Click **System Monitor > Blocked IP Address**.

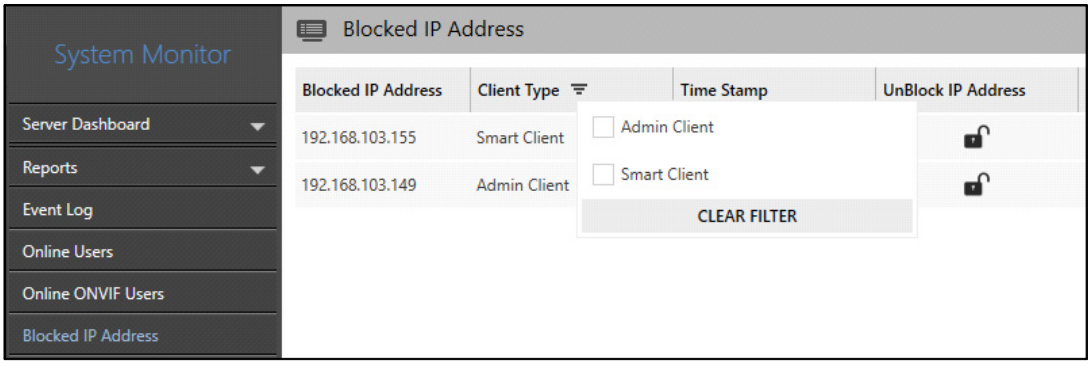


The following details are displayed —Blocked IPv4/IPv6 Address, Client Type, Time Stamp and Unblock IP Address.

You can also sort or filter the data.

- To sort, click on the Blocked IP Address/Time Stamp in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

- To filter according to the **Client Type**, click **Filter** .



- Select the desired check boxes from the **Client Type** filter list. The IP Addresses are sorted as per the set filters.

- Click **Clear Filter** to clear all the filters.

You can unblock the desired IP Address.

- Click **Unblock**  against the desired IP address. The IP address gets cleared from the list.

CHAPTER 14

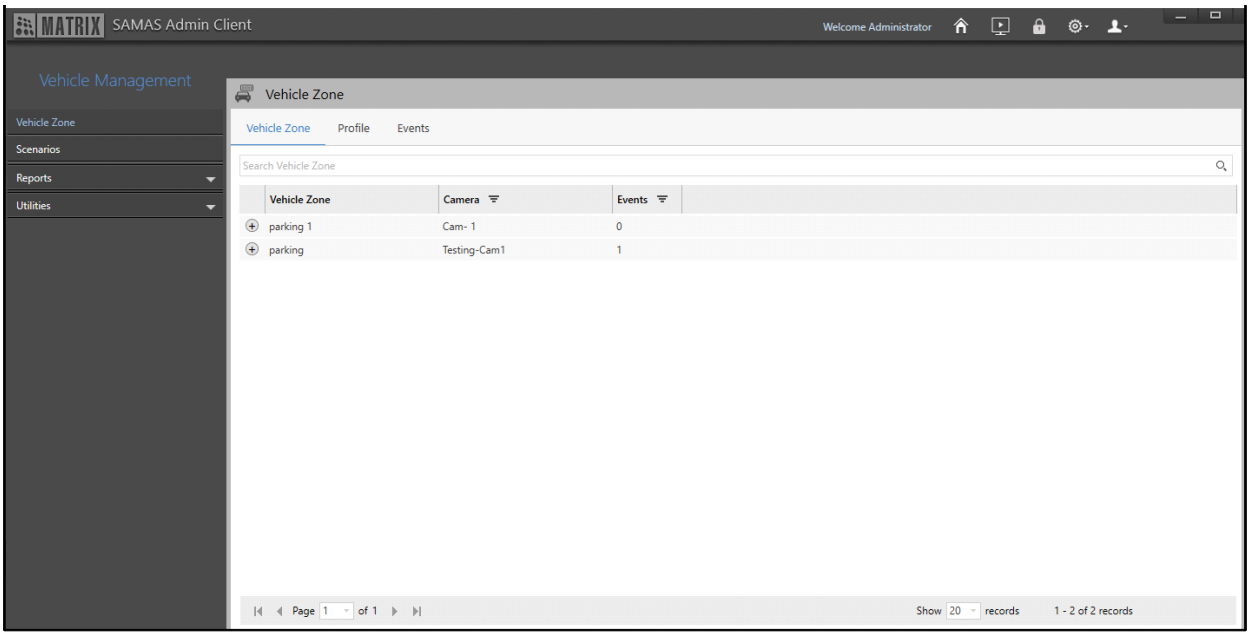
Vehicle Management

The Vehicle Management module enables you to configure various Vehicle Zones and Events for them. Vehicle Management uses Video Content Analysis which is effective in detecting Events such as Vehicle Detection based on live stream of a camera. It also enables you to configure Scenarios based on Events.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure Vehicle Management,

- Click **Vehicle Management**.



The Vehicle Management module contains these pages — "Vehicle Zone", "Vehicle Management Scenario", "Vehicle Management - Reports" and "Utilities".

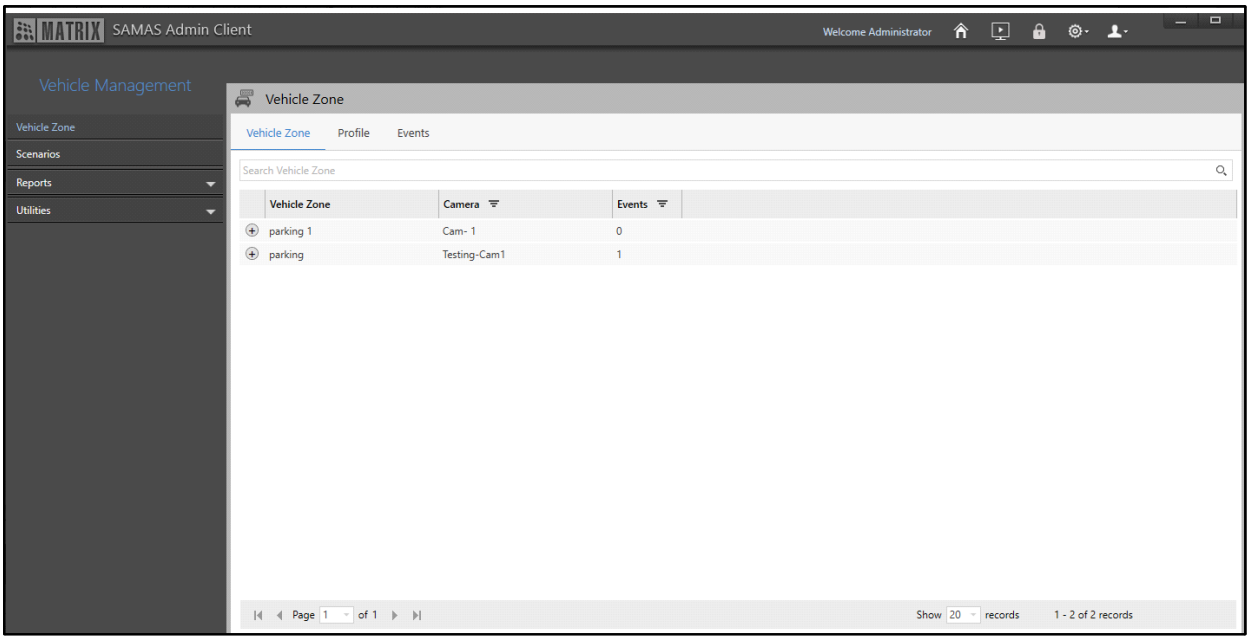
Vehicle Management-Zone

The Vehicle Management module allows you to configure Vehicle Zones to detect the vehicle number. The Vehicle Zone feature is useful in places like Offices, Toll plaza, etc. to detect any Events (For example, Vehicle Detection) in the premises. These Events can help security person or management to detect suspicious or blacklisted vehicles. Event that can be configured against the configured Vehicle Zones is Vehicle Detection.

The Vehicle Zone page displays all the configured Vehicle Zones. You can view and configure the Vehicle Zones from this page.

To configure Vehicle Zones,

- Click **Vehicle Management**. The **Vehicle Zone** page appears by default.



The entity name (Vehicle Zone) can also be changed from the Rename Entity section, for more details, refer to "Rename Entities" The reflection will be applicable everywhere in the Admin Client.

The Vehicle Zone page consists of the following tabs:

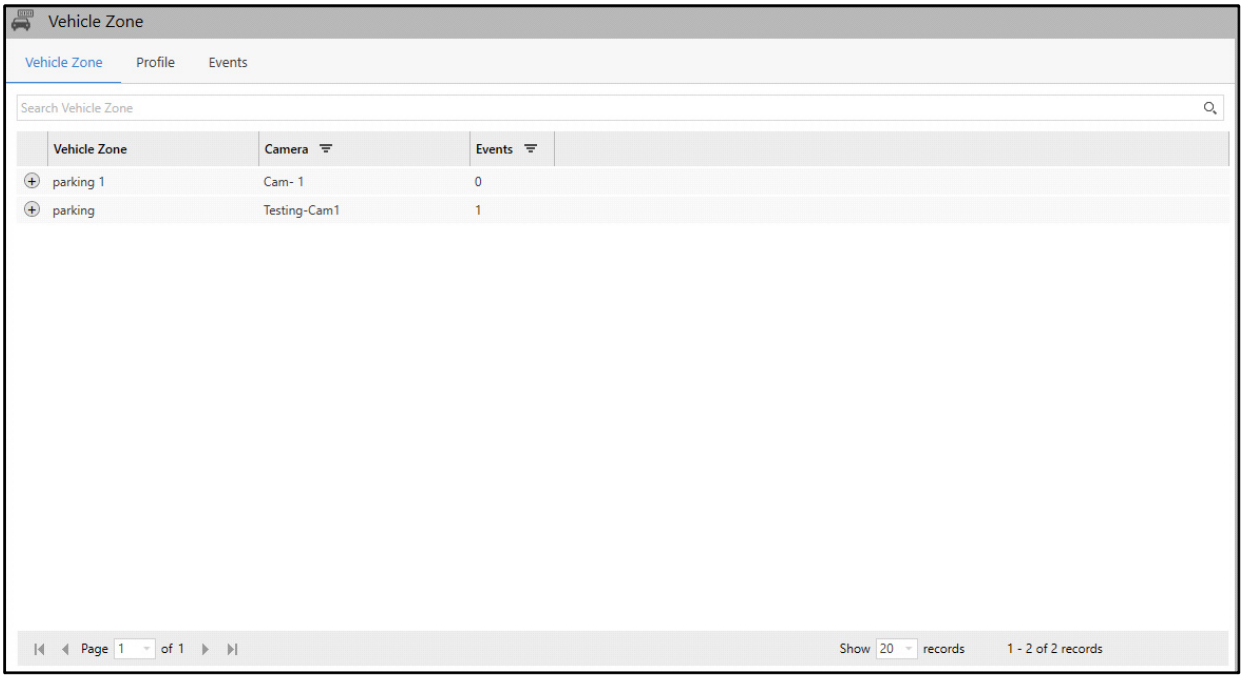
- "Vehicle Zone"
- "Profile"
- "Events"

Vehicle Zone

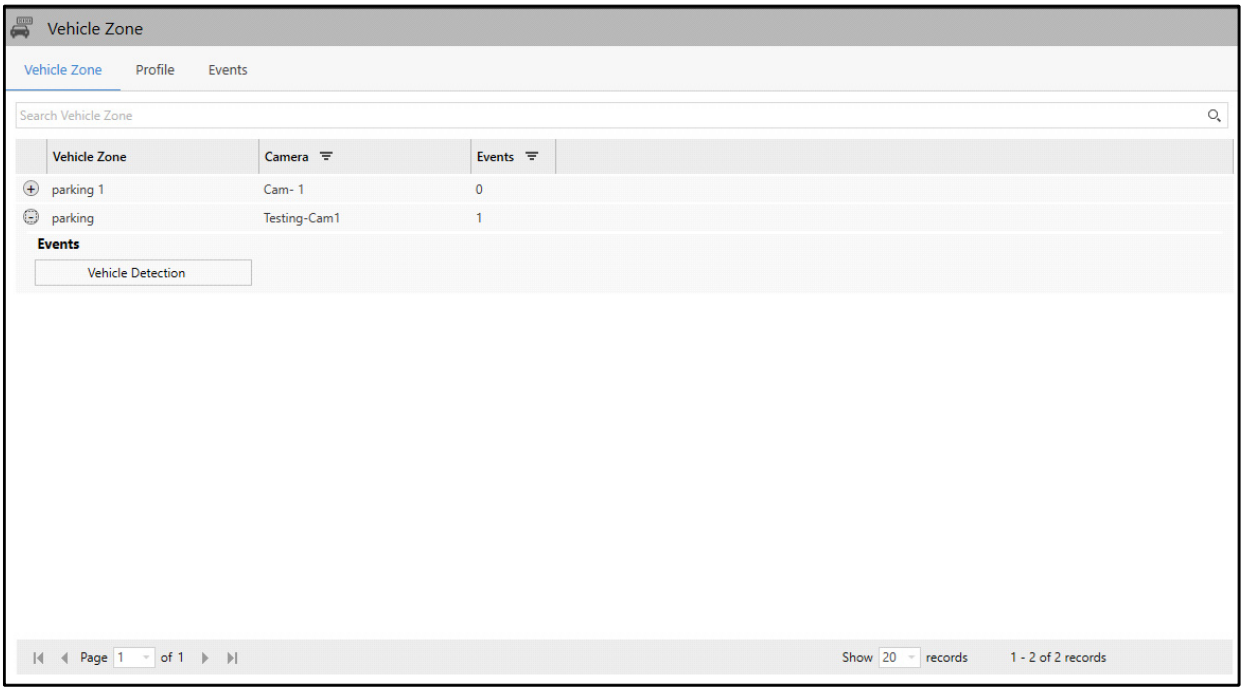
This tab enables you to view Vehicle Zones. You can configure the Vehicle Zones from "Profile". All the Vehicle Zones and the Events configured for them appear under this tab. The Vehicle Zone details displayed are — Vehicle Zone, Camera and Events.

To configure Vehicle Zone,

- Click the **Vehicle Zone** tab.



- Click **Show Events** to view the Events configured for the Vehicle Zone.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

To clear the filter, click **Filter** and then click **CLEAR FILTER**.

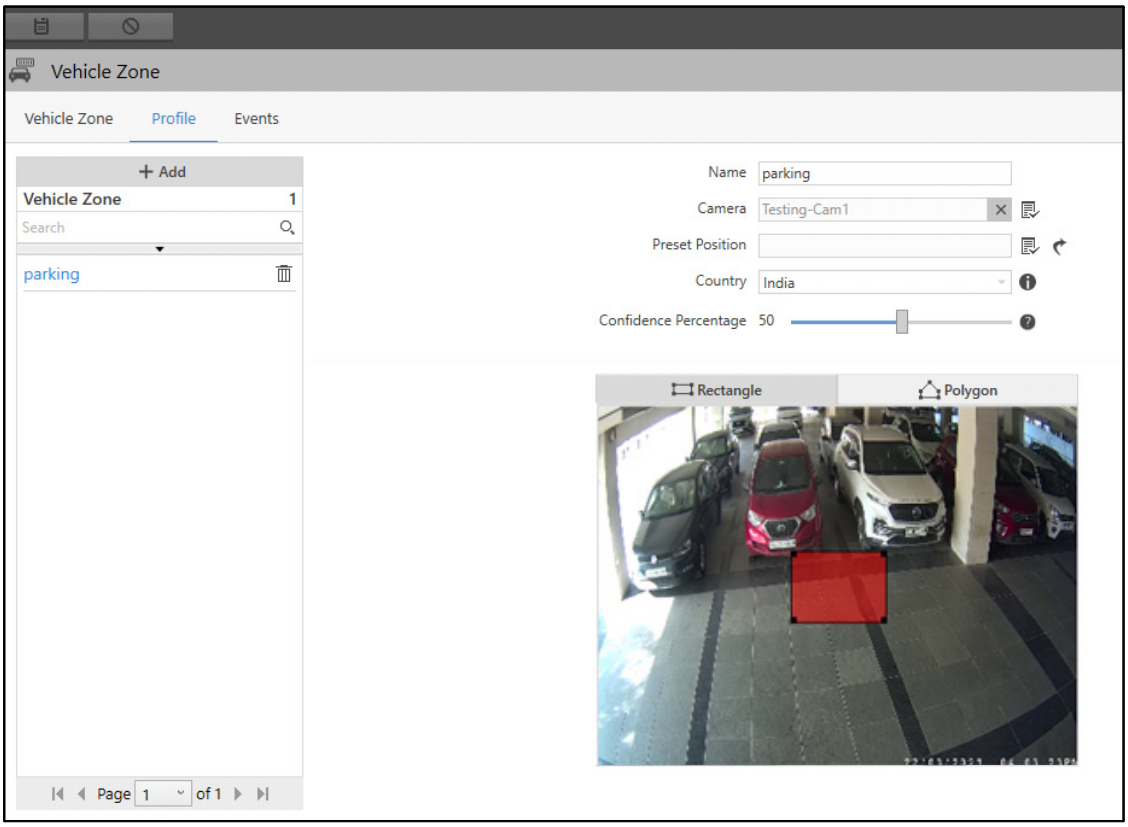
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

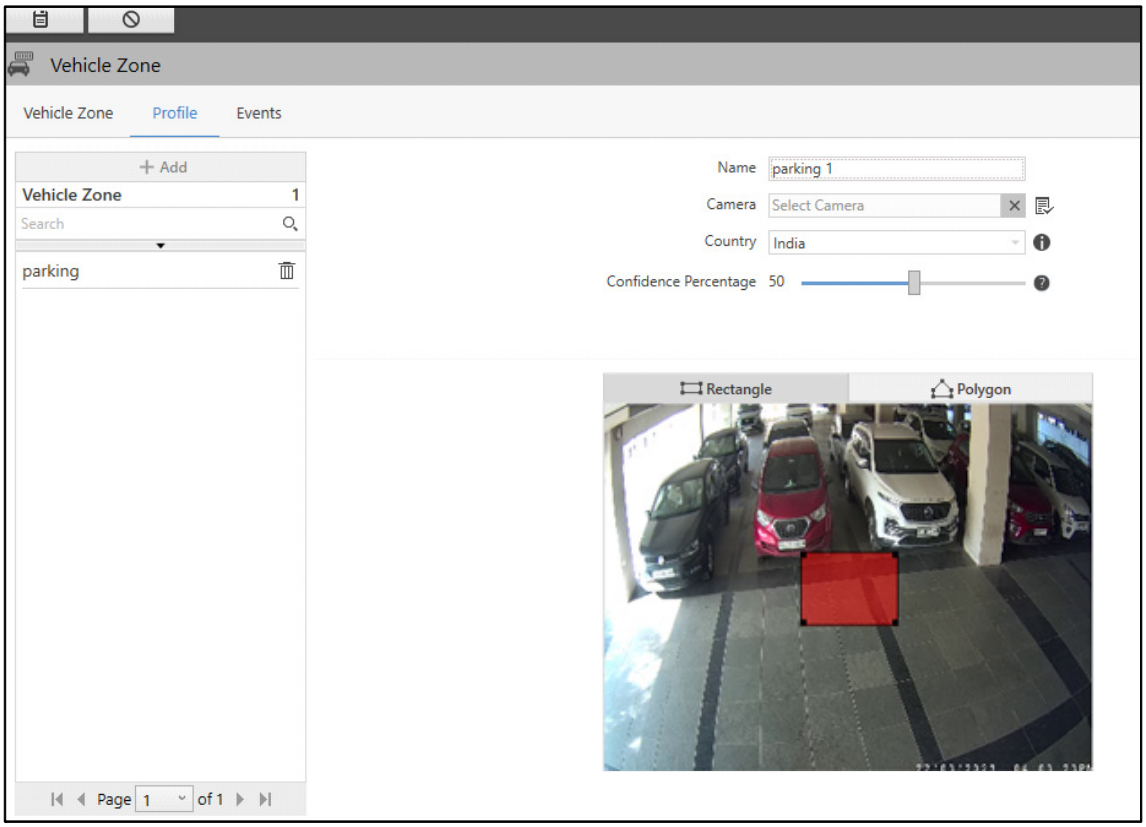
This tab enables you to configure Vehicle Zone. All the Vehicle Zones configured here appear under the **Vehicle Zone** tab.

To configure Vehicle Zones,

- Click the **Profile** tab.

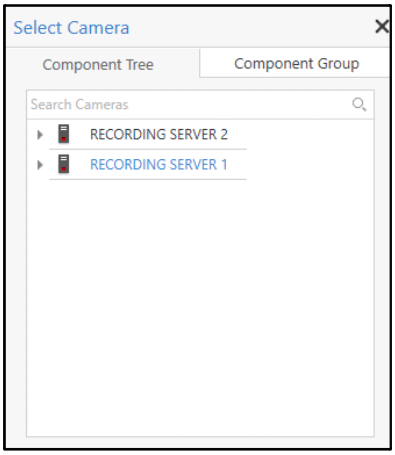


- Click **Add**.



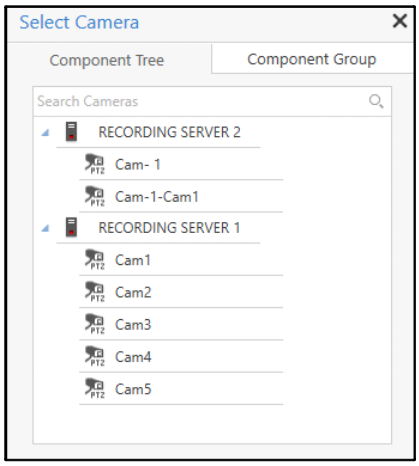
Configure the following parameters:

- **Name**: Specify a suitable name for the Vehicle Zone. In Name, you can enter upto 50 characters. Default: Blank.
- **Camera**: Select the desired camera which you wish to assign to the Vehicle Zone using the **Camera** picklist.
  - Click **Camera** picklist. The **Select Camera** pop-up appears.



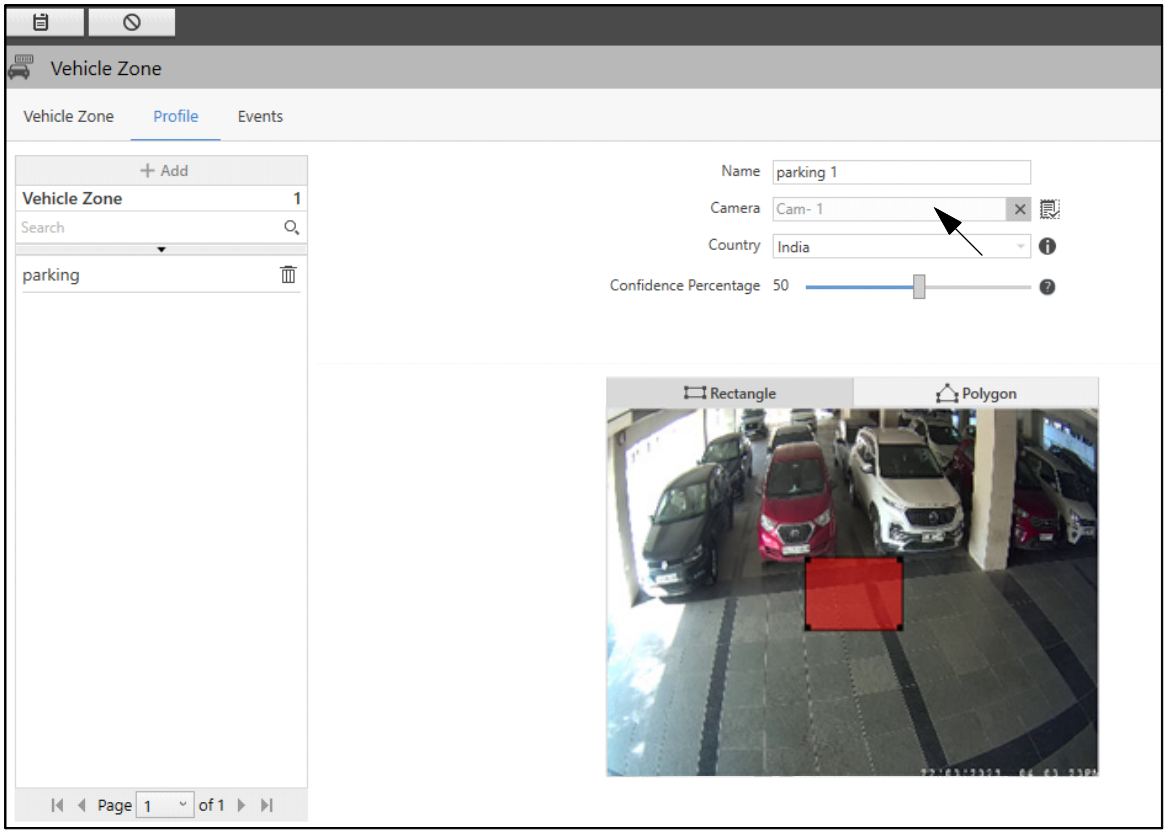
- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To

know more, refer to “Component Group”. Double-click the desired camera to assign it to the Vehicle Zone. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click to select the desired option.
  - Click **Go to selected position** , to move the camera as per the selected preset position.
- To remove the camera, click **Remove** .



- **Country**: Select the country from the drop-down list where the camera is installed. This option is helpful in increasing the efficiency of vehicle recognition.

*The **Country** option will be applicable only when Number Plate Detection is done using Native ANPR.*

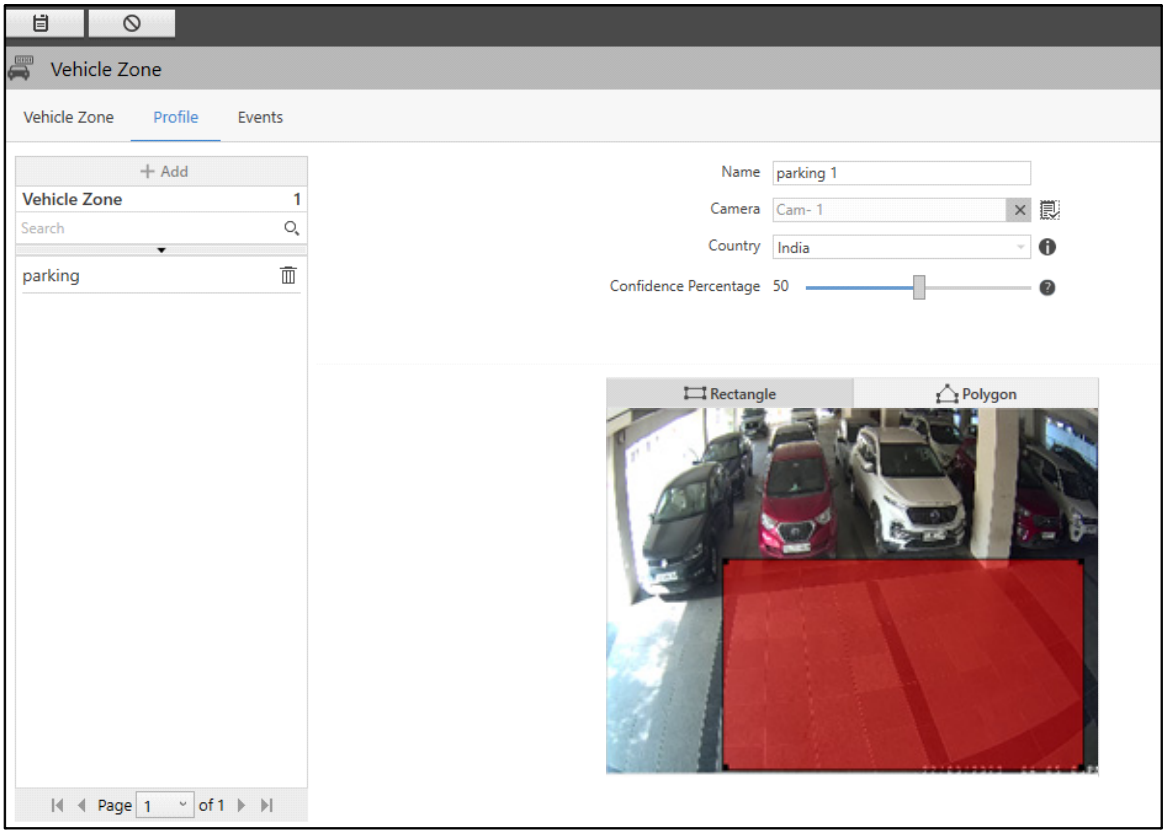
- **Confidence Percentage**: Set the Confidence Percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the percentage of success between image plate recognized and the text which is recognized from the image plate. This will be the minimal percentage allowed for successful vehicle detection. Valid Range: 0-100%. Default: 50.

- Click **Save** to save the settings or **Cancel** to discard.

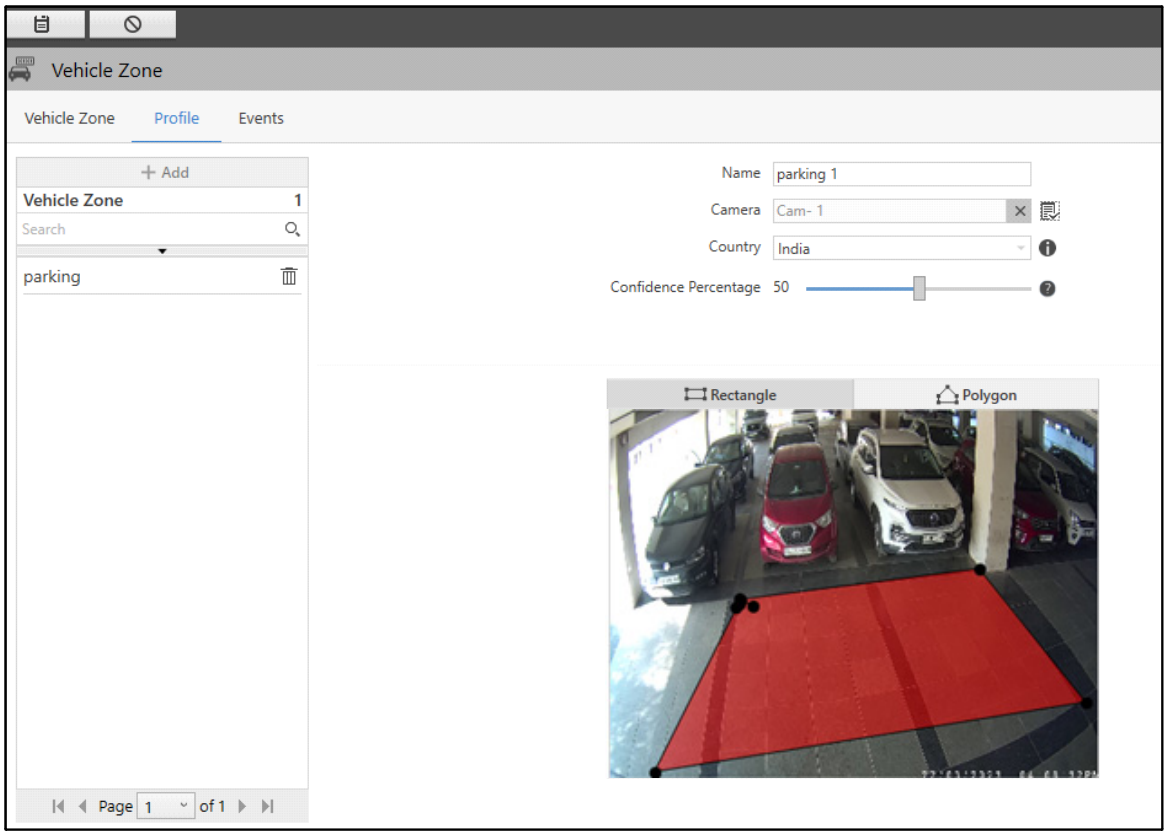
Once a camera is assigned, you can draw a Vehicle Zone on the live view of the camera. You can either draw a **Rectangle** or **Polygon** to define the Zone.

- Select either **Rectangle** or **Polygon** to draw the Zone.

- If you select **Rectangle**, drag the corners and sides of the rectangle to configure the Zone.



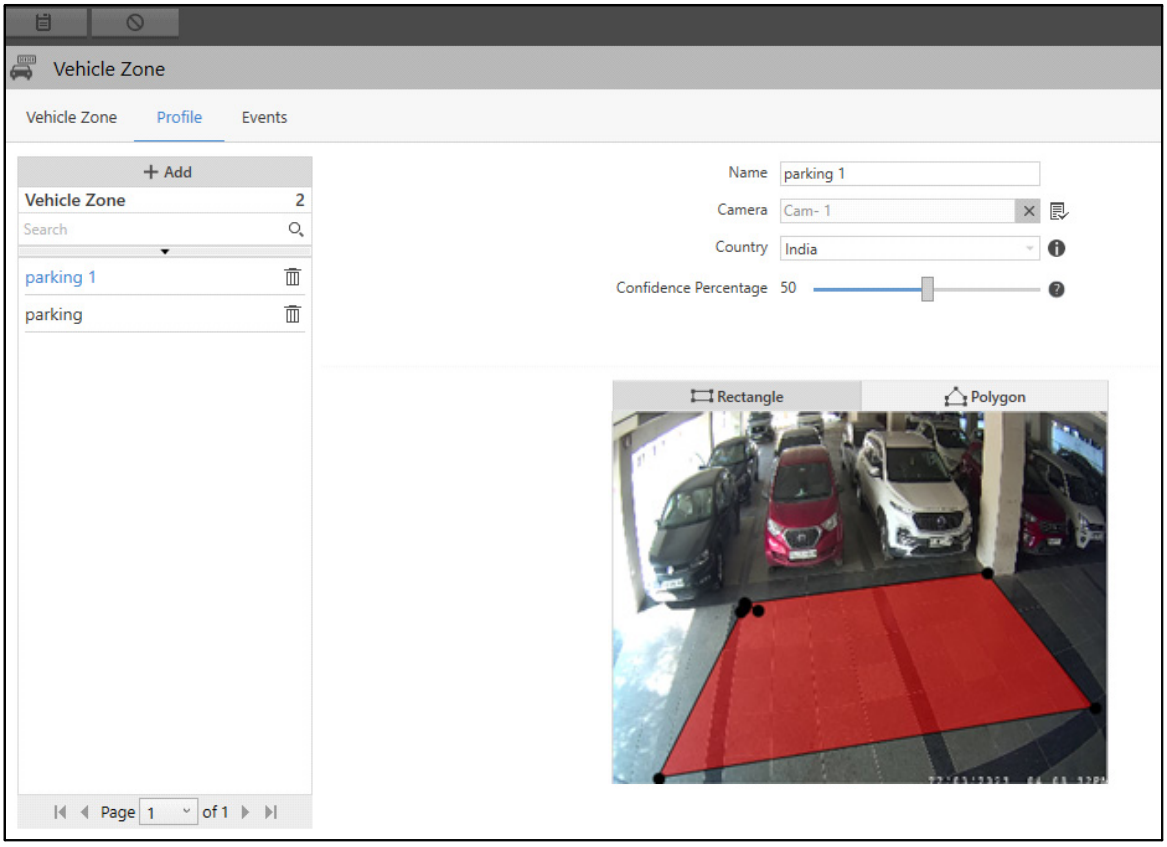
- If you select **Polygon**, click on the live view to place the vertex of the polygon. Click again on the desired place to join the previous vertex with a new vertex. Continue this process to complete the polygon.



- Click **Save** to save the settings or **Cancel** to discard.

The new Vehicle Zone will appear in the list on the left hand side.

You can edit the configurations of the Zone or delete it.



- Select the desired Vehicle Zone from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Vehicle Zone.

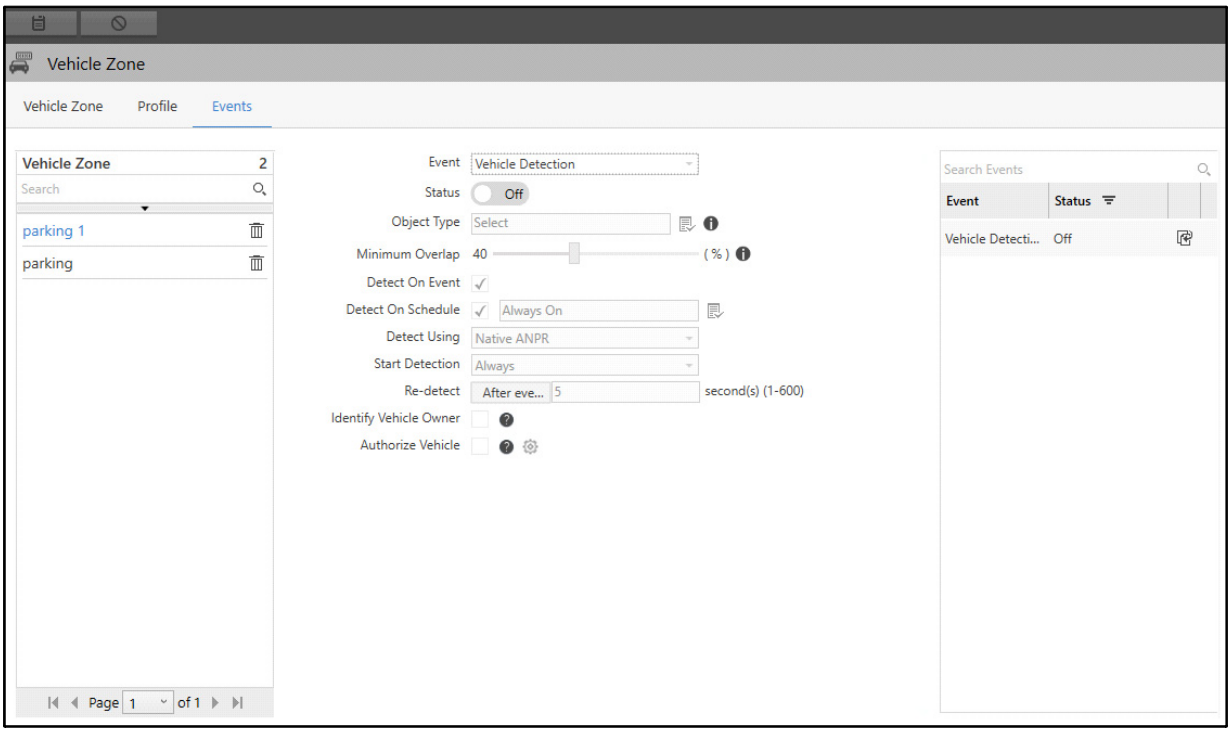
Similarly, you can configure the other Vehicle Zones.

Events

This tab enables you to configure the Vehicle Detection Event for the Vehicle Zones. All the configured Events appear under the **Vehicle Zone** tab.

To configure the Vehicle Detection Event,

- Click the **Events** tab.
- Select the desired Profile from the left hand side for which you wish to configure the Event.

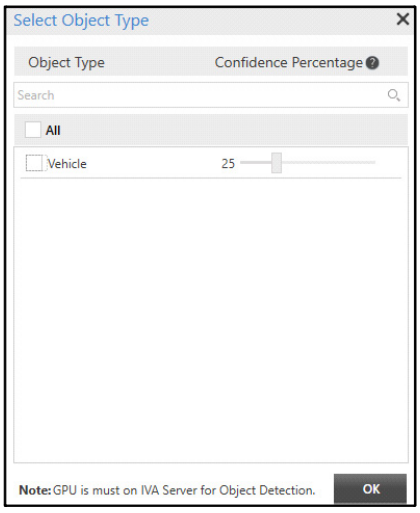


Configure the following parameters:

- **Event:** Select the Vehicle Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Object Type**: Select the desired Object Type which should be detected in the Event using the **Object Type** picklist.
  - Click **Object Type** picklist. The **Select Object Type** pop-up appears.

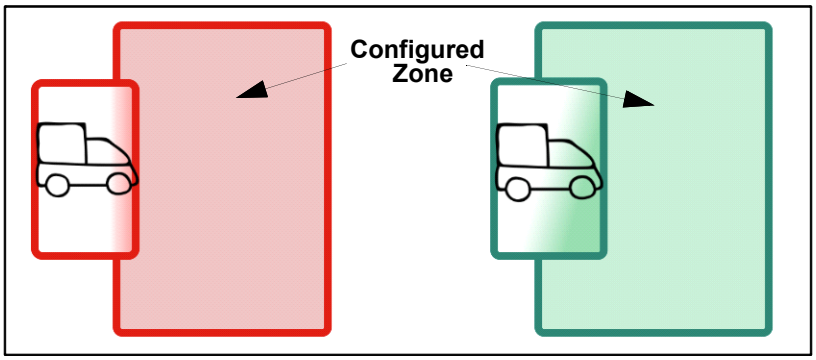


- Select the **Vehicle** check box and set the **Confidence Percentage** by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the accuracy with which the selected Object Type is detected. A higher Confidence Percentage will enable more precise detection. Click **OK**. Valid Range: 0-100%. Default: 25.

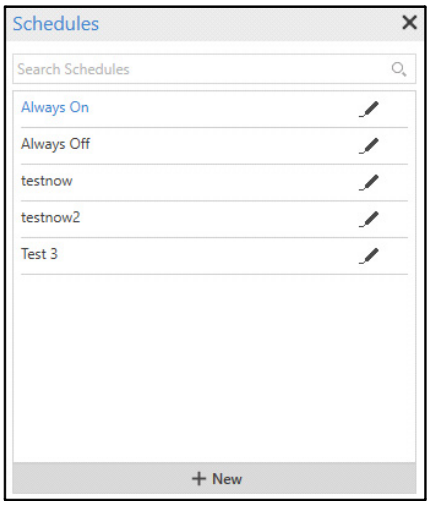
- **Minimum Overlap**: If you have selected **Object Type**, set the Minimum Overlap percentage by dragging the slider. Drag the slider to the left to decrease the percentage or to the right to increase. This indicates the minimum percentage of overlap of detected Object Type in the zone to trigger the event.

  If the Minimum Overlap Percentage is lower, then only a small percentage of the object overlapping the zone will trigger the event. Whereas, if the percentage is higher, then a high percentage of the object overlapping the zone will trigger the event. Valid Range: 0-100%. Default: 40.

  For example, if you have configured Minimum Overlap as 30%, then as per the Green Zone, the event will be triggered as 30% of the object is overlapping the configured zone. Whereas, in the Red Zone, the event will not be triggered as only 10% of the object is overlapping the configured zone.



- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Detect Using**: Select the detection method from the drop-down list — Native ANPR or CARMEN ARH.

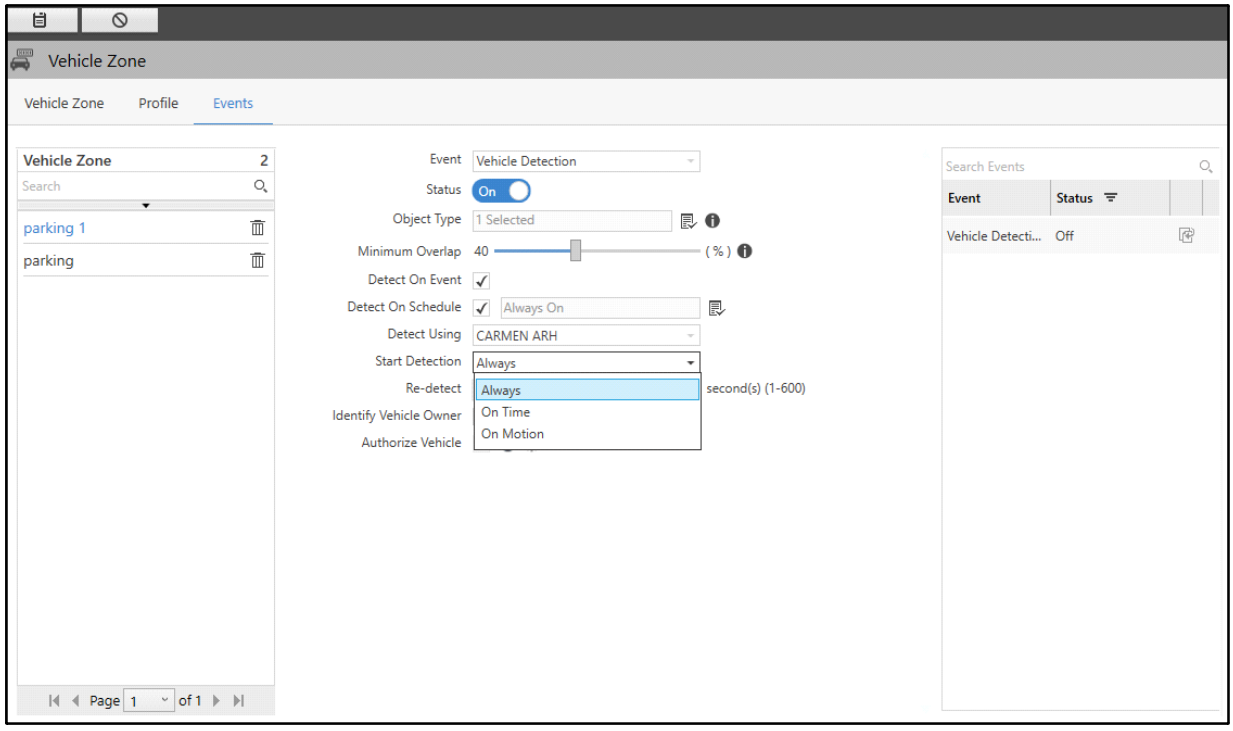
  Native ANPR algorithm is used for License Plate Recognition which has limitations in terms of speed and accuracy. You have to manually select countries from the available options in the Vehicle Profile. It does not support License Plate Recognition of various countries, namely; UAE, Middle-East Regions, Southern Asia-Pacific Region, Europe, GCC Countries, etc.

  CARMEN ARH is a fast and highly accurate License Plate Recognition technology. It can be used in traffic surveillance, toll collection, traffic management and many other applications. It is capable of reading the License Plates of multiple countries.

  If you select the detection method as **CARMEN ARH**, configure the following parameters:

There will be a delay of 10 seconds to check for the License (dongle), if it is not found (or removed in-between) during the process of Event generation for all Vehicle based Events where the CARMEN ARH has been used.

- **Start Detection**: Select the start detection method from the drop-down list — Always, On Time or On Motion.



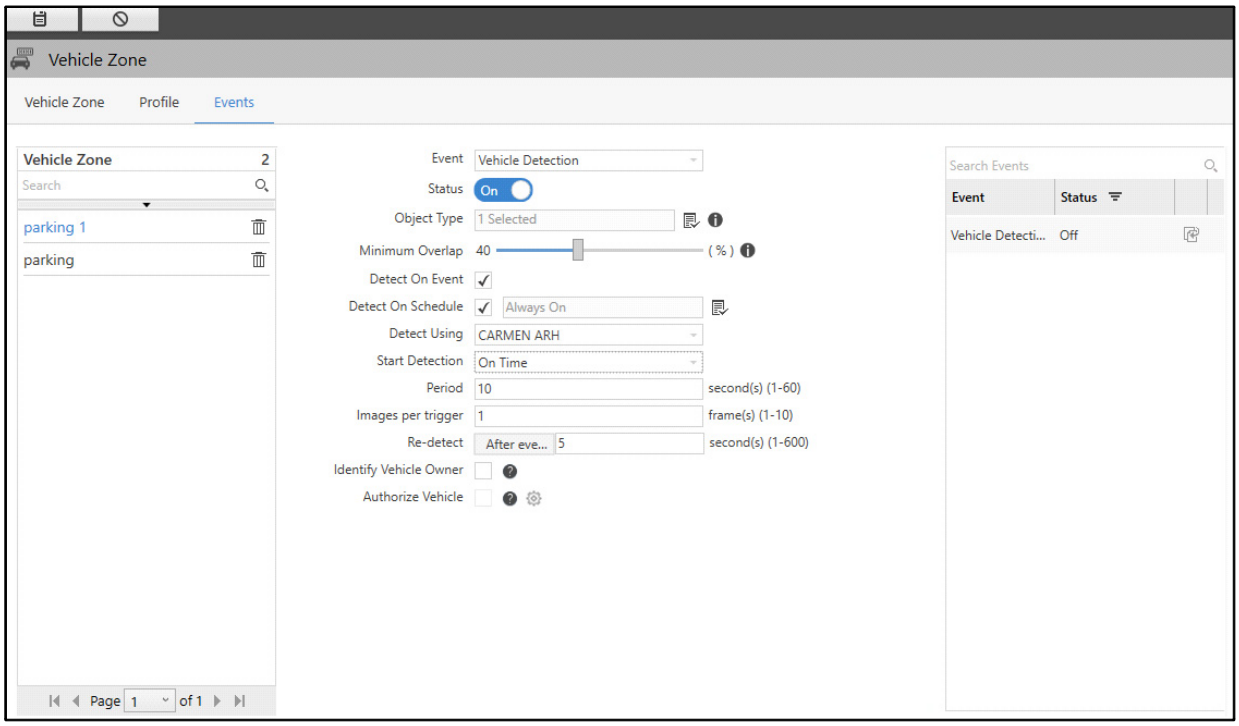
If you select **Always**, the IVA Server will process all the incoming image frames of the vehicle number plate and pass to ARH Engine for number plate detection.

If you select **On Time**, the IVA Server will process the number plate image frames and pass to ARH Engine as per set frequency of images per trigger and time period. In case, if the configured Images per Trigger is higher than frames received in the configured period, the maximum FPS is sent to ARH.

For example, Period = 1 sec and Images per Trigger = 10, but frames received in 1 sec = 5, then 5 Images per Trigger are sent to ARH Engine.

If you select the start detection as **On Time**, configure the following parameters:

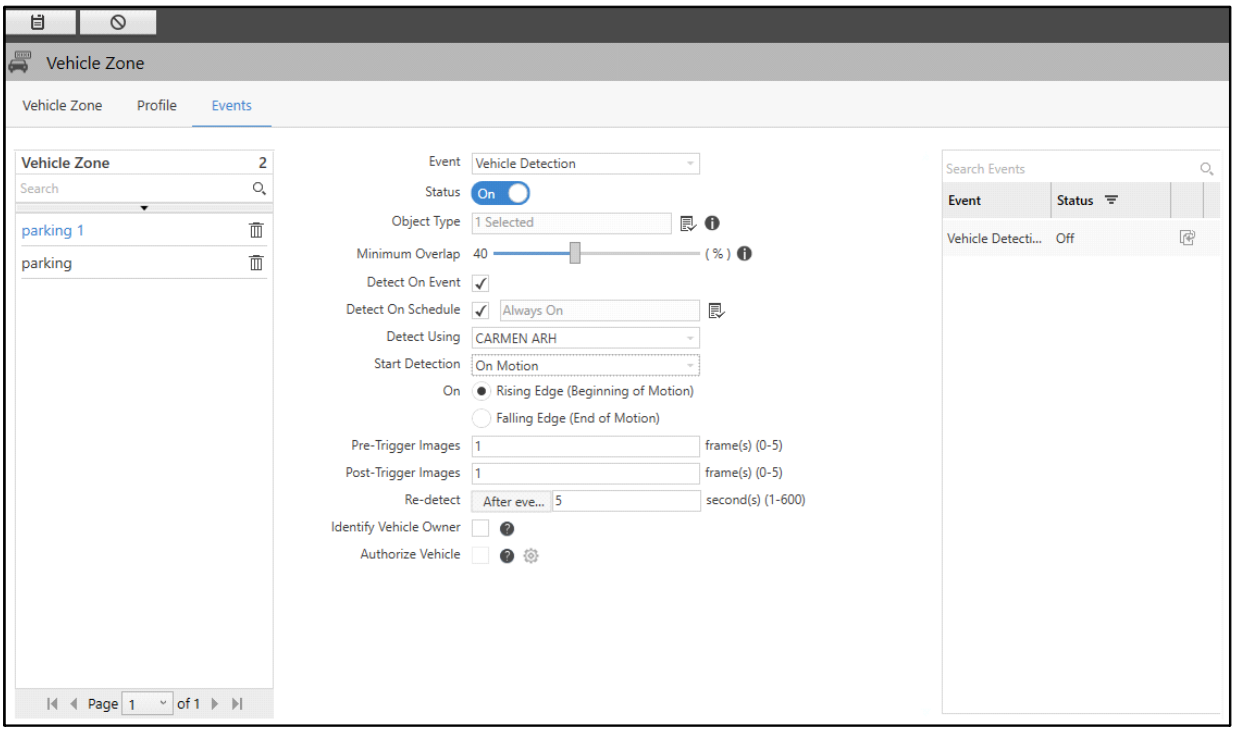
- **Period**: Specify the time period at which the images will be sent to the ARH Engine. Valid Range: 0-60 seconds. Default: 10.
- **Images per Trigger**: Specify the number of Images per Trigger that will be passed to the ARH Engine. Valid Range: 1- 10 frames. Default: 1.



If you select **On Motion**, the IVA Server will process the number plate images and pass to ARH Engine on Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).

If you select the start detection as **On Motion**, configure the following parameters:

- **On**: Select the desired option as per which you wish the images to be passed to the ARH Engine — Rising Edge (Beginning of Motion) or Falling Edge (End of Motion).
- **Pre-Trigger Images**: Specify the number of images to be passed to the ARH Engine before the motion. Valid Range: 0 - 5 frames. Default: 1.
- **Post-Trigger Images**: Specify the number of images to be passed to the ARH Engine after the motion. Valid Range: 0 - 5 frames. Default: 1.

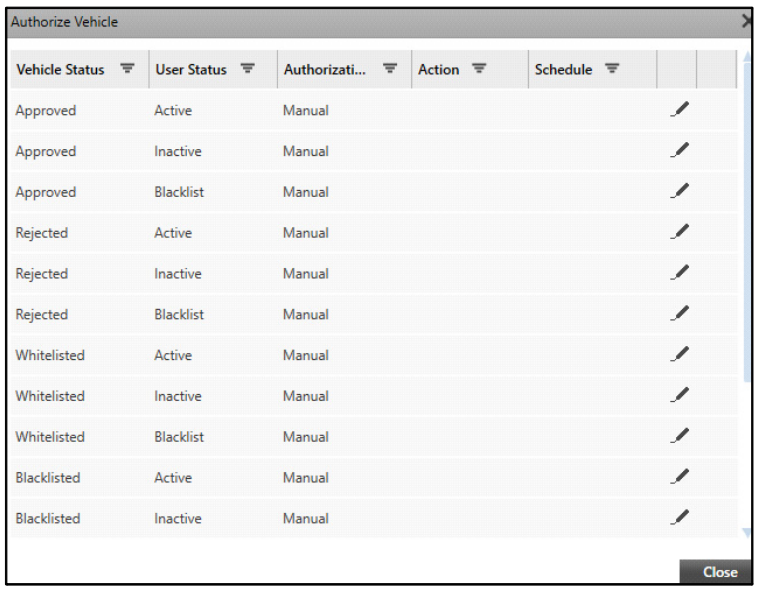


- **Re-detect After every:** Specify the time after which the Vehicle Detection Event will be detected again after the previous detection. Valid Range: 1- 600 seconds. Default: 5.

- **Identify Vehicle Owner**: Select the check box to detect the vehicle owner of the detected license plate. This will generate Events with user and vehicle details.

- **Authorize Vehicle**: Select this check box to authorize or unauthorize a vehicle number.

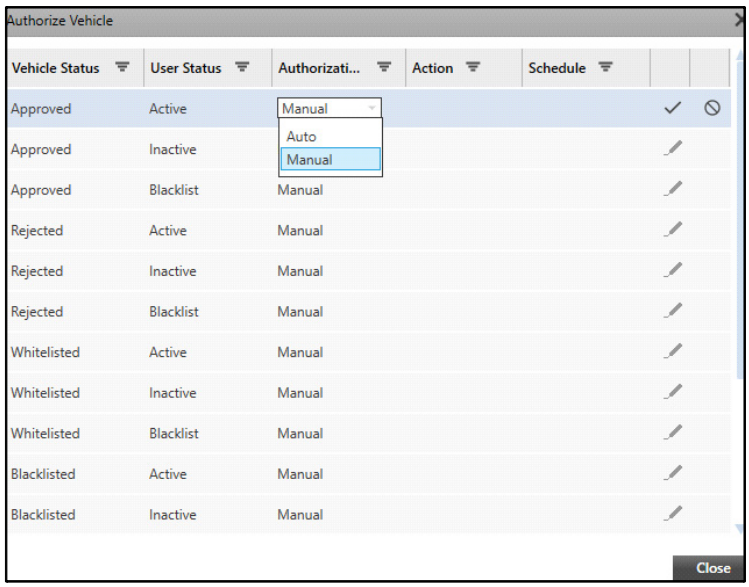
  - Click **Choose how to Authorize Vehicle** . The **Authorize Vehicle** pop-up appears.



The pop-up displays various combinations of Vehicle Status, User Status and Authorization Mode. By default, the Authorization Mode is set as **Manual**. You can configure Action and Schedule for Vehicle Status when the Authorization Mode is **Auto**.

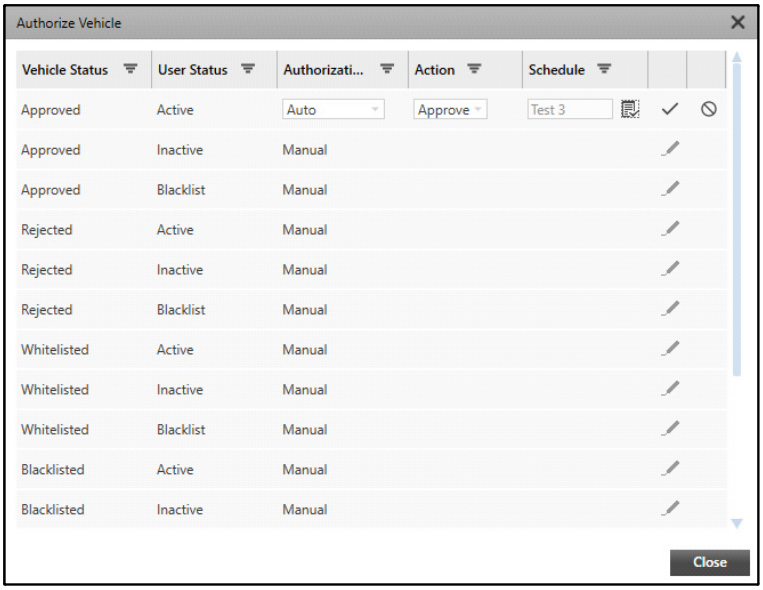
*The User Status can be set as **Active**, **Inactive** or **Blacklist** from **General Settings > User Profile**.*

- Click **Edit** to edit the **Authorization Mode**.



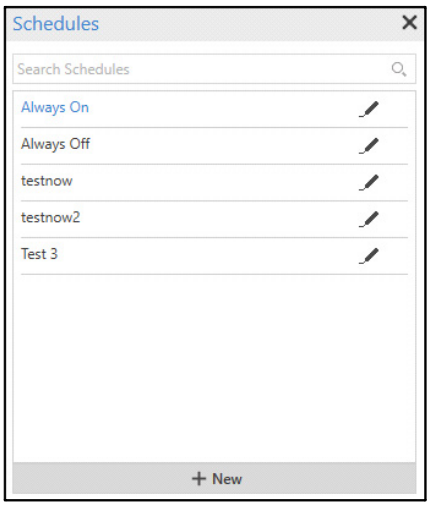
- Select the Authorization Mode as **Auto** from the drop-down list.

Once the Authorization Mode is selected as Auto, you can configure the Action and Schedule.



- **Action**: Select the desired **Action** from the drop-down list — Approve or Reject.
- **Schedule**: Select the desired schedule which you wish to assign to the Vehicle Status using the **Schedule** picklist.

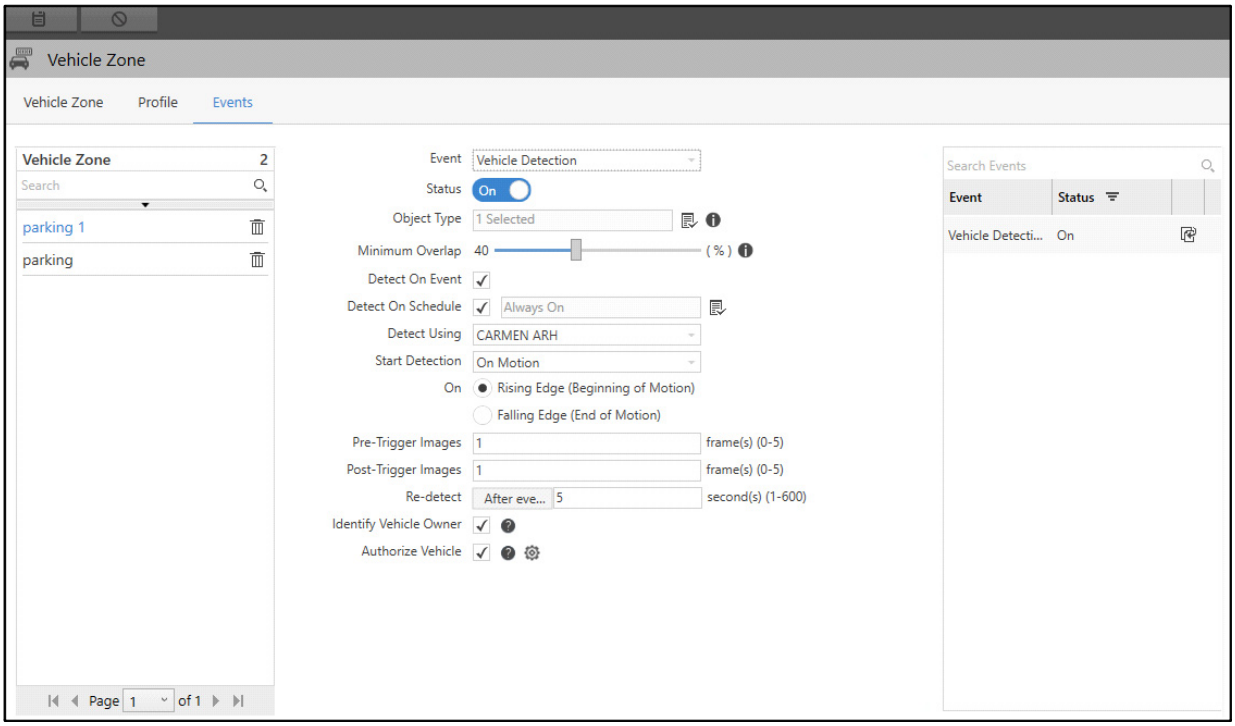
- Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Close**.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.

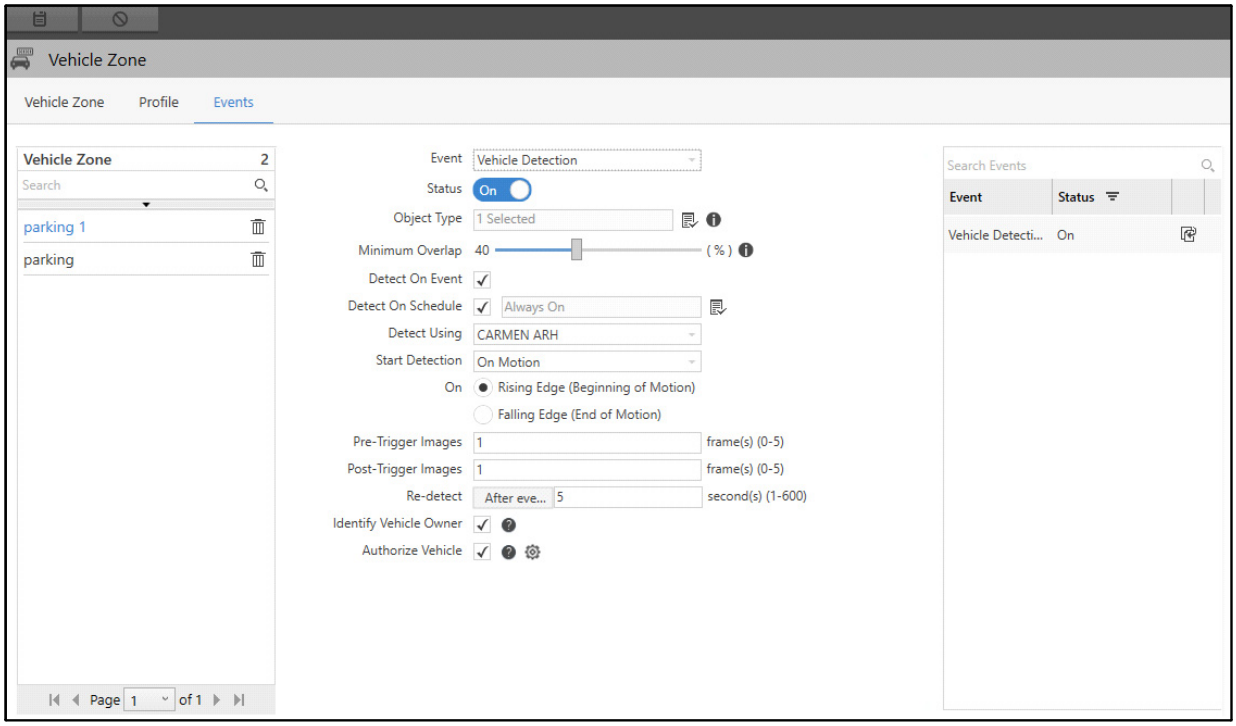


- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

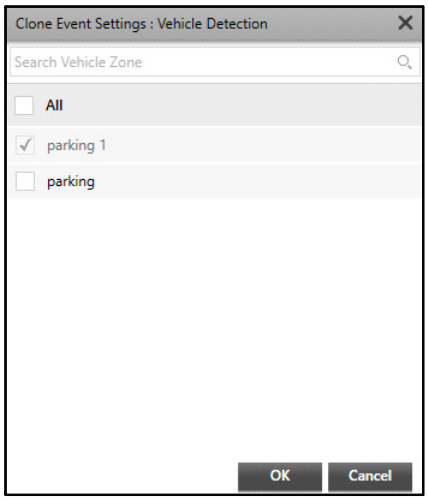
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Intrusion Detection is created, the **Clone Event Settings** option gets enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Vehicle Detection** pop-up appears.



- Select the desired Events to which you wish to copy these configurations.

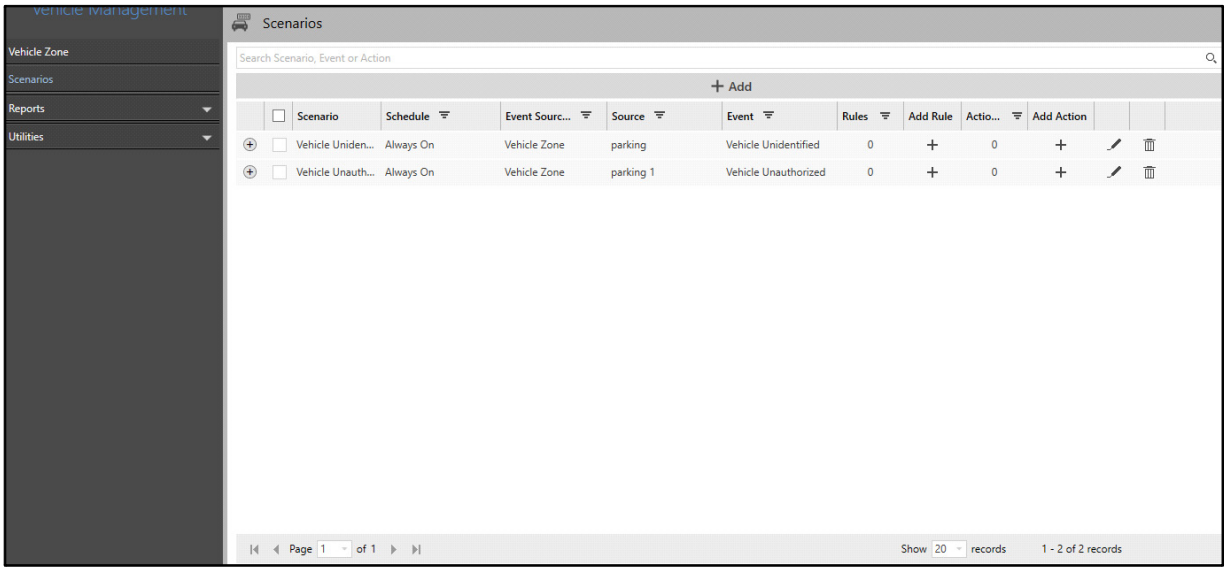
- Click **OK** to confirm or click **Cancel** to discard.

Vehicle Management Scenario

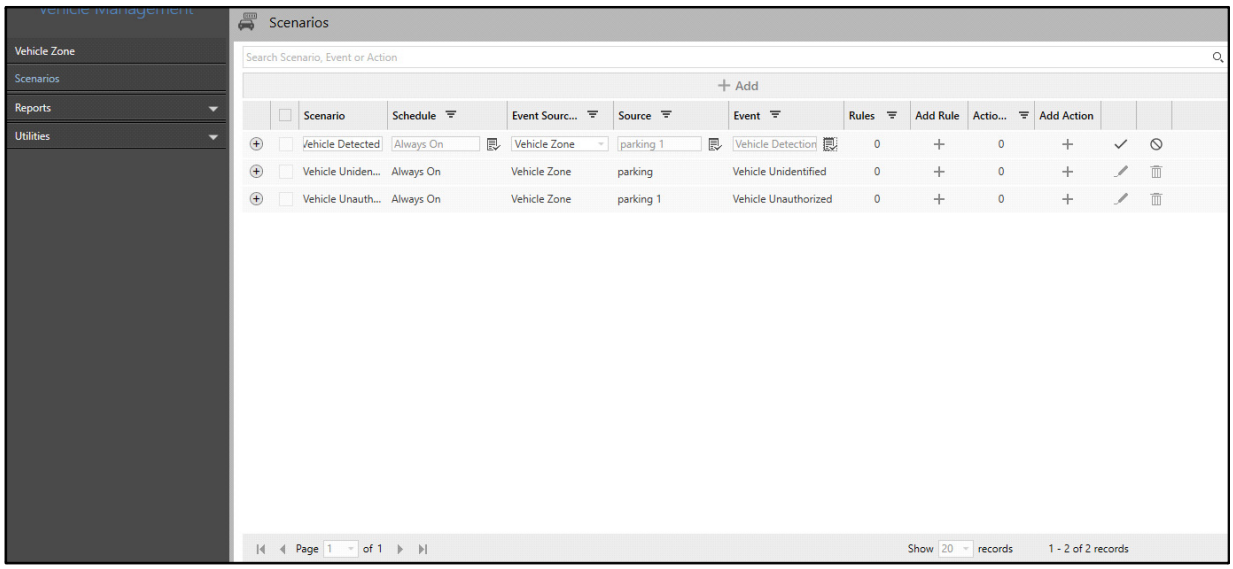
In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send SMS) on Events occurring at certain sources (For example, Vehicle Detection). The Scenarios page displays all the Scenarios configured for Vehicle Management. You can view and configure the Scenarios for all the configured Vehicle Zones.

To configure Scenarios,

- Click **Vehicle Management > Scenarios**.



- Click **Add.**



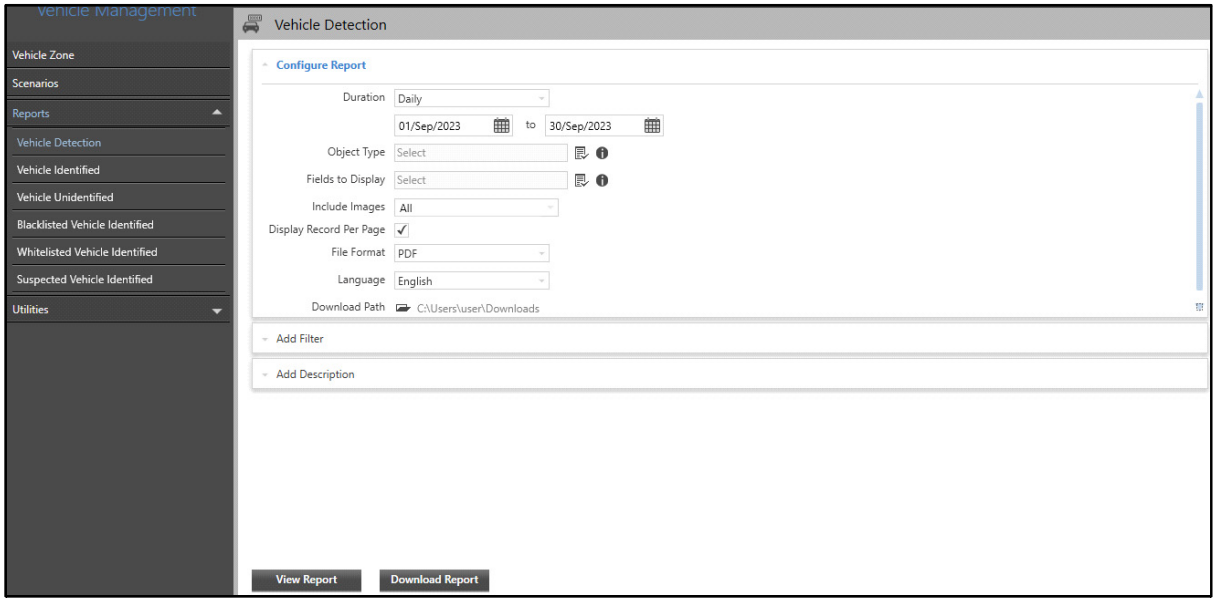
The configurations of Scenarios for Vehicle Management are similar to that of the Basic Scenario. For details, refer to “Basic Scenario”.

Vehicle Management - Reports

The Reports page enables you to generate, view and download different types of Vehicle Management reports, such as Vehicle Detection, Vehicle Identified, Vehicle Unidentified, Blacklisted Vehicle Identified, Whitelisted Vehicle Identified and Suspected Vehicle Identified.

To configure Report parameters,

- Click **Vehicle Management > Reports**.



Refer to the following links for the configuration details of each type of report.

- “Vehicle Detection Report”
- “Vehicle Identified Report”
- “Vehicle Unidentified Report”
- “Blacklisted Vehicle Identified Report”
- “Whitelisted Vehicle Identified Report”
- “Suspected Vehicle Identified Report”

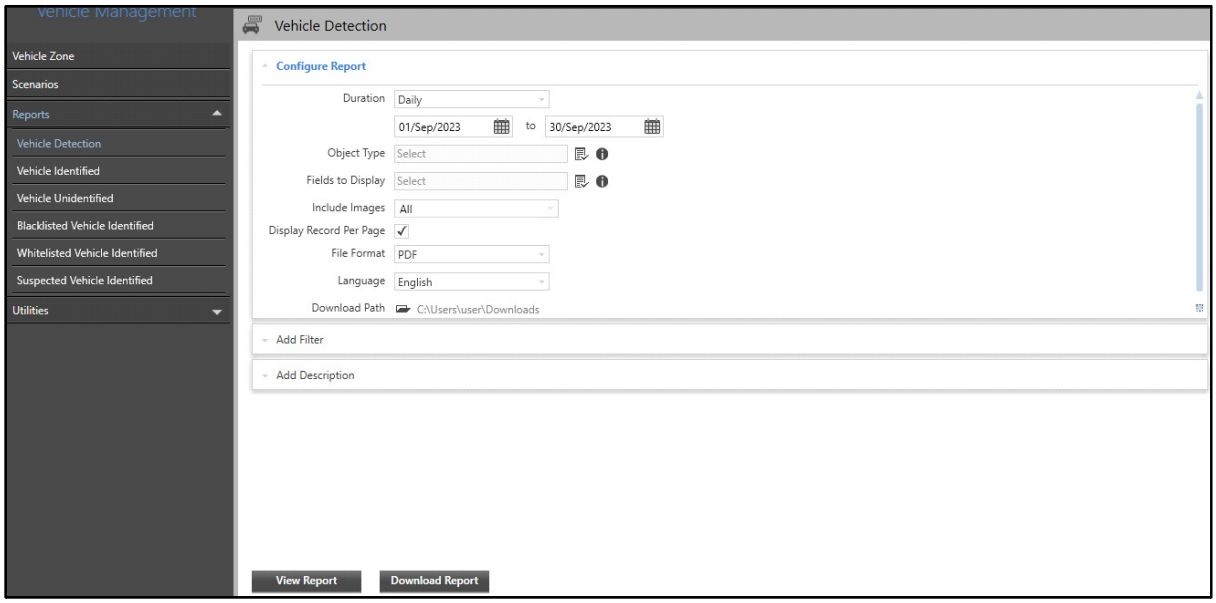
Vehicle Detection Report

The Vehicle Detection Report provides statistics on Vehicle Detection Event. These statistics can be useful in managing parking or toll plazas from one place. It allows user to detect each individual vehicle passing by within the defined duration at any place.

The Vehicle Detection page enables you to configure parameters for Vehicle Detection Reports. You can view and configure Vehicle Detection Reports on Monthly, Daily and Hourly basis.

To configure Vehicle Detection Report,

- Click **Vehicle Management > Reports > Vehicle Detection**.



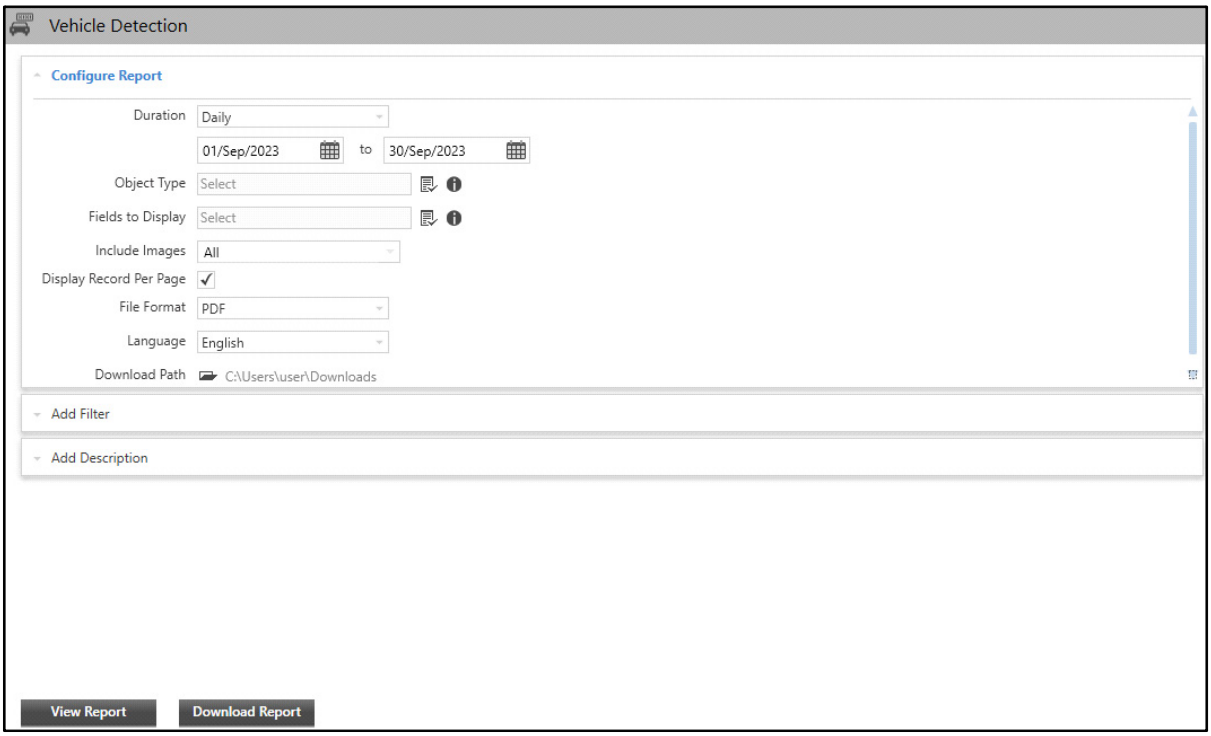
The Vehicle Detection page contains three collapsible panels —"Configure Report", "Add Filter" and "Add Description".

Configure Report

This panel displays the report configurations. You can edit and configure the Vehicle Detection Report from this collapsible panel.

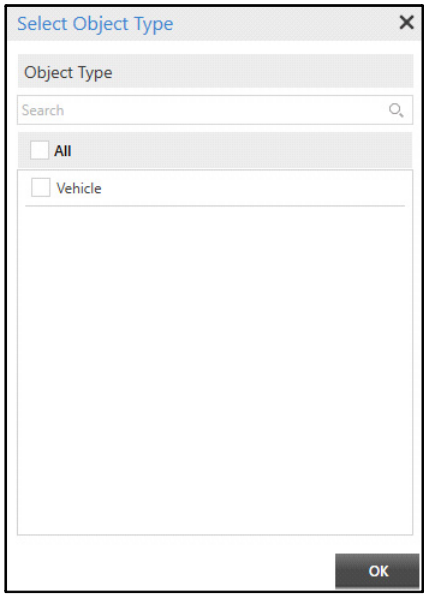
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



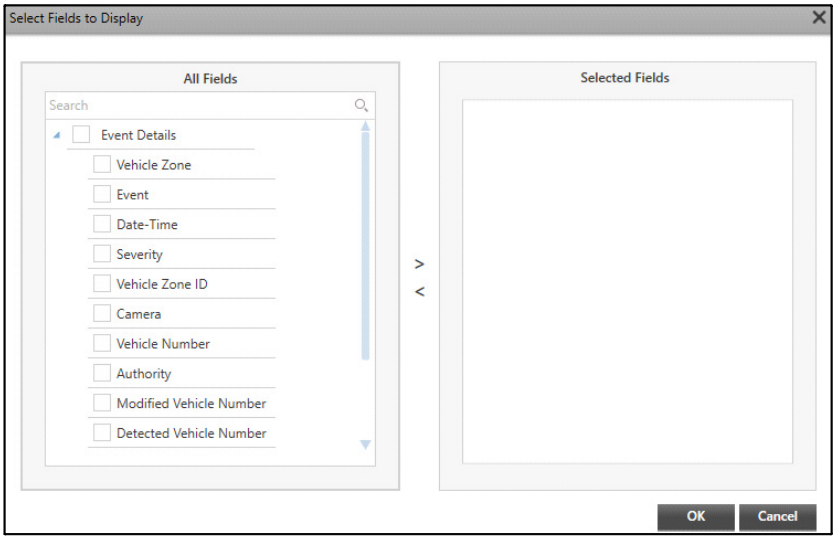
Configure the following parameters:

- **Duration**: Select the desired Duration from the drop-down list — Monthly, Daily or Hourly.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
- **Object Type**: Select the desired Object Type for which you wish to generate reports using the **Object Type** picklist.
    - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



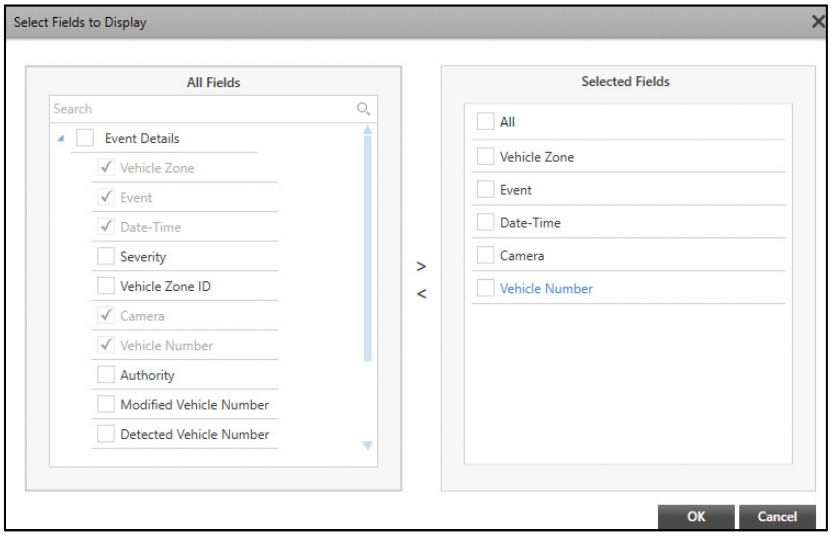
- Select the **Vehicle** check box. Click **OK**.

- **Fields to Display**: Select the desired fields which you wish to include in the report using the **Fields to Display** picklist.
  - Click **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



- Select the check boxes for the desired fields you wish to add from the **All Fields** list. Click the right arrow button to add these fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

  To remove fields, select the check boxes for the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields from the Selected Fields list.



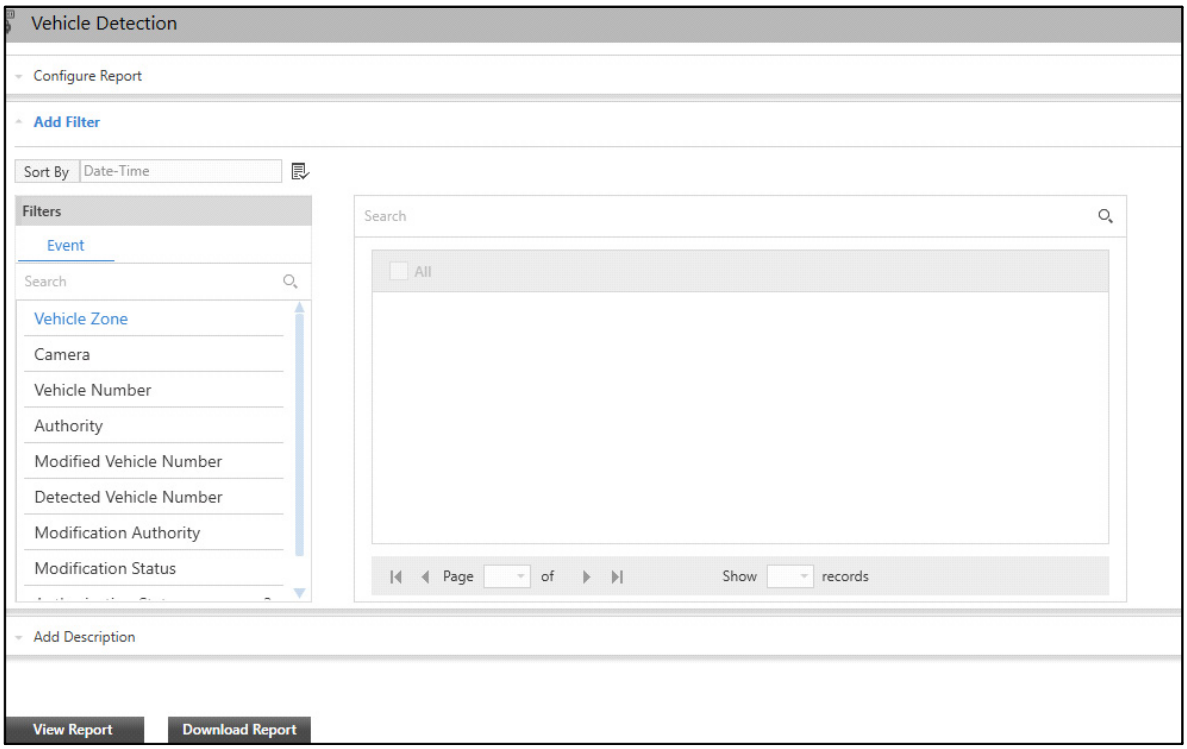
- Click **OK** to confirm or click **Cancel** to discard.
- **Include Images**: Select the type of images that you wish to include in the report using the drop-down list.
- **Display Record Per Page**: Select the check box to display each record for the selected fields on a new page.
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Filter

This panel allows you to add filters for the Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters.

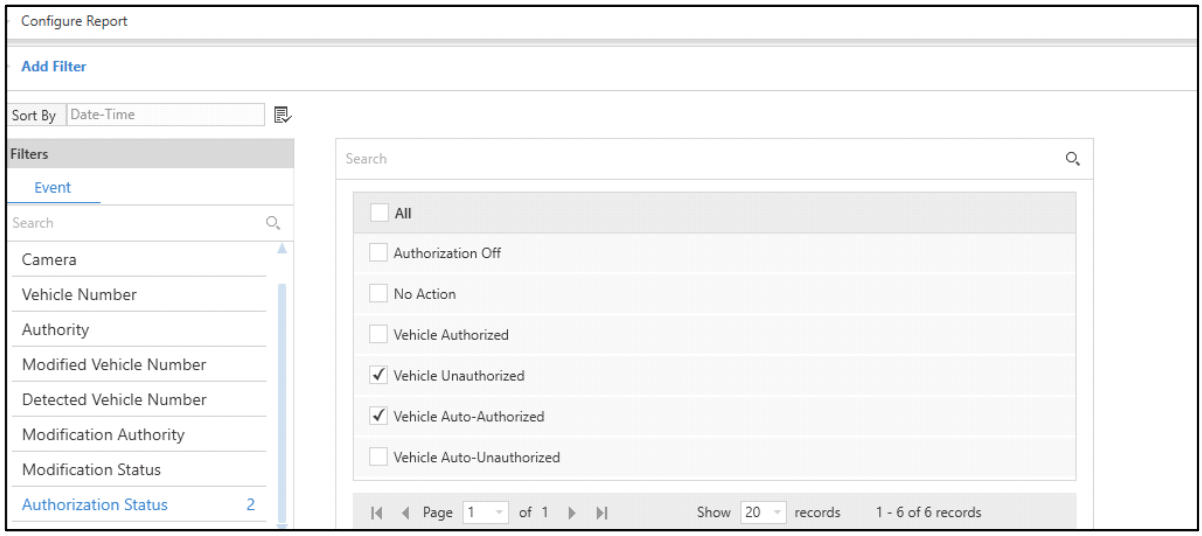
To configure the Filters,

- Click the **Add Filter** collapsible panel.



Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data from the Event Details in the report using the **Sort By** picklist. Double-click to select the desired option. By default, the sorting is done as per the Date and Time of the Event Occurrence.
- **Filters**: You can get the desired data for the report using Filters. The Filters section displays all the Event Details. Select the tab to view the associated parameters.
    - Click the desired parameter to view the associated entities with the selected Event. For example, if you select Authorization Status, all the Status associated with the selected Event are displayed on the right hand side. Select the check boxes of the desired entities to include in the report.

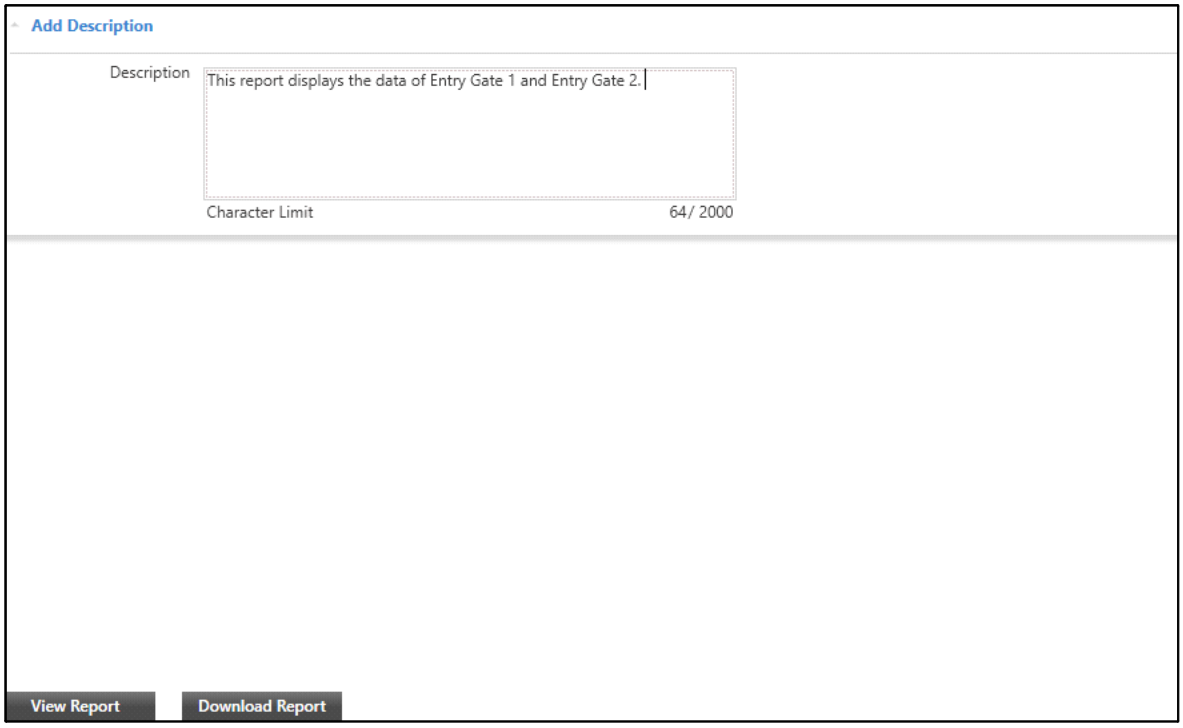


Add Description

This panel allows you to add a description for the Vehicle Detection Report once the report configurations are done. This description is visible in the generated report.

To configure the Description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

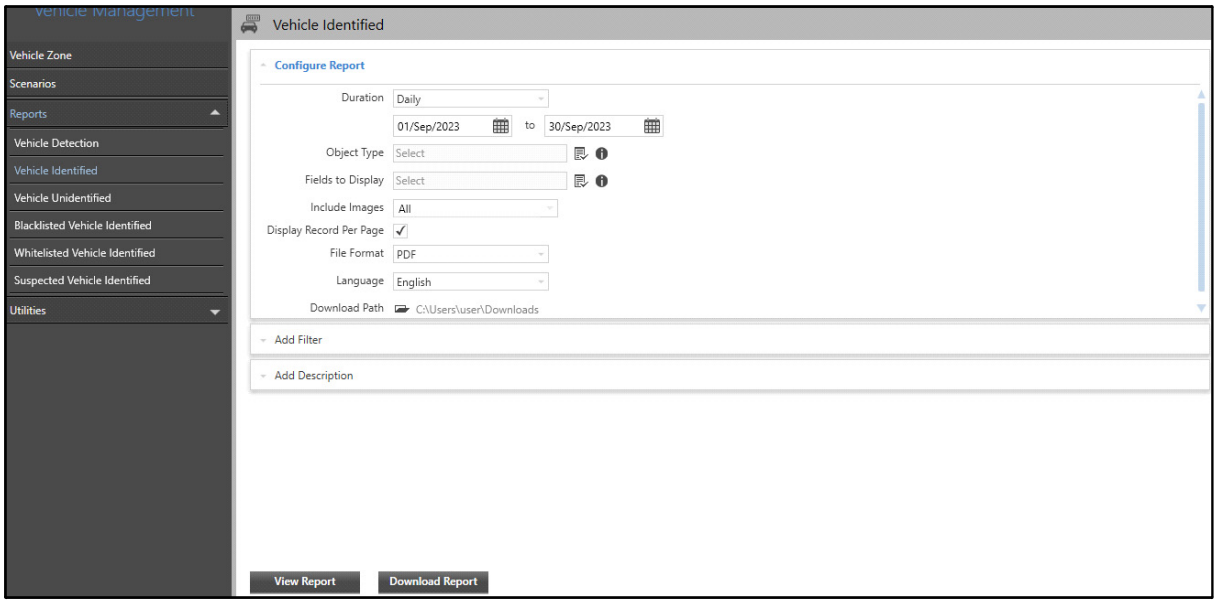
Vehicle Identified Report

The Vehicle Identified Report provides statistics on vehicles identified by the Admin Client database. These statistics can be useful in managing places such as Office or Residential parking. Based on this report, Vehicle and User details of vehicles whose Vehicle Number has been detected can be tracked easily.

The Vehicle Identified page enables you to configure parameters for Vehicle Identified Reports. You can view and configure Vehicle Identified Reports on Monthly, Daily and Hourly basis.

To configure Vehicle Identified Report,

- Click **Vehicle Management > Reports > Vehicle Identified**.



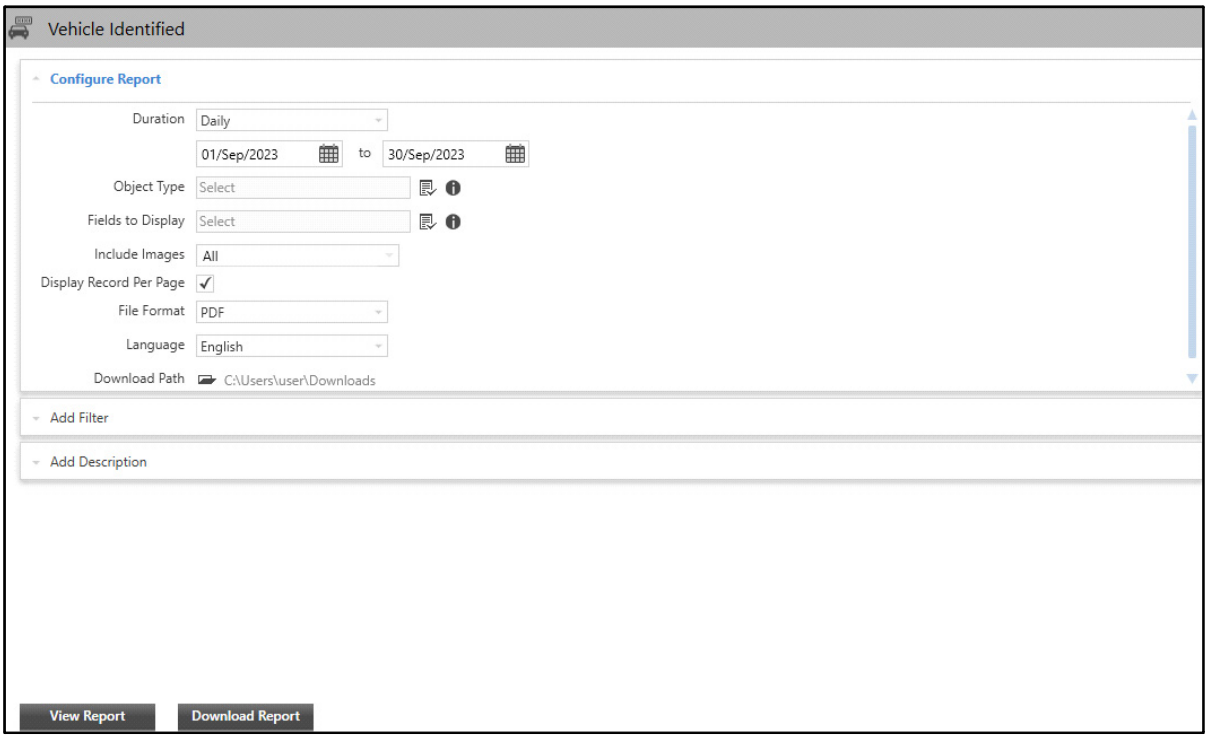
The Vehicle Identified page contains three collapsible panels — “Configure Report”, “Add Filter” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Vehicle Identified Report from this collapsible panel.

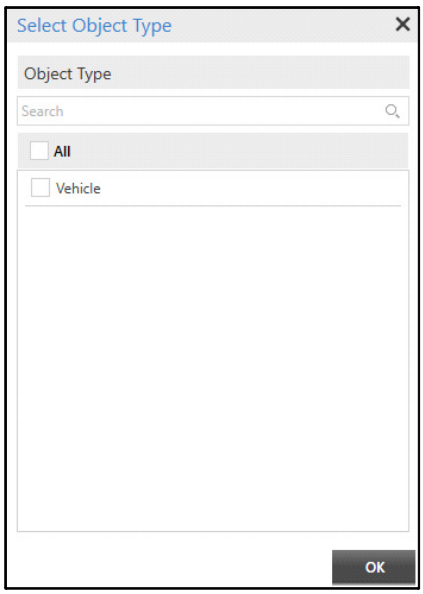
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



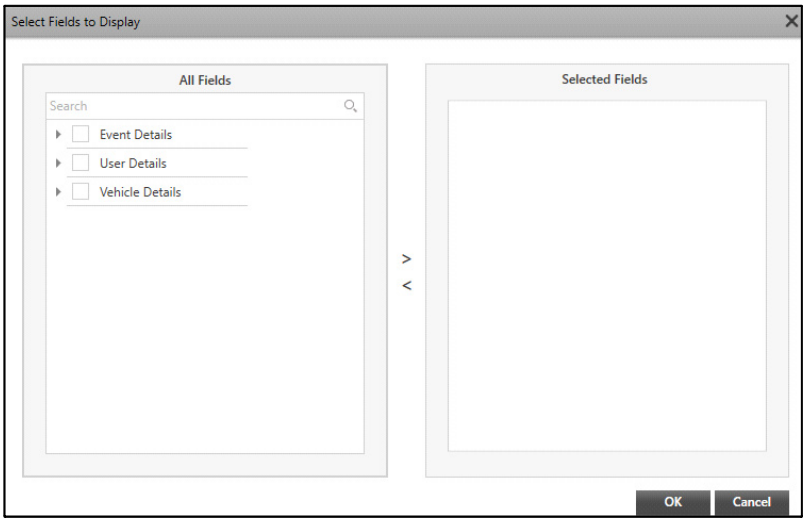
Configure the following parameters:

- **Duration**: Select the Duration from the drop-down list options — Monthly, Daily or Hourly.
    - **Monthly**: Select this option to generate monthly reports. Select the desired From and To month and year from the drop-down lists.
    - **Daily**: Select this option to generate daily reports. Select the desired From and To dates from the calendar.
    - **Hourly**: Select this option to generate hourly reports. Select the desired From and To date from the calendar and specify the time.
- **Object Type**: Select the desired Object Type for which you wish to generate reports using the **Object Type** picklist.
    - Click **Object Type** picklist. The **Select Object Type** pop-up appears.



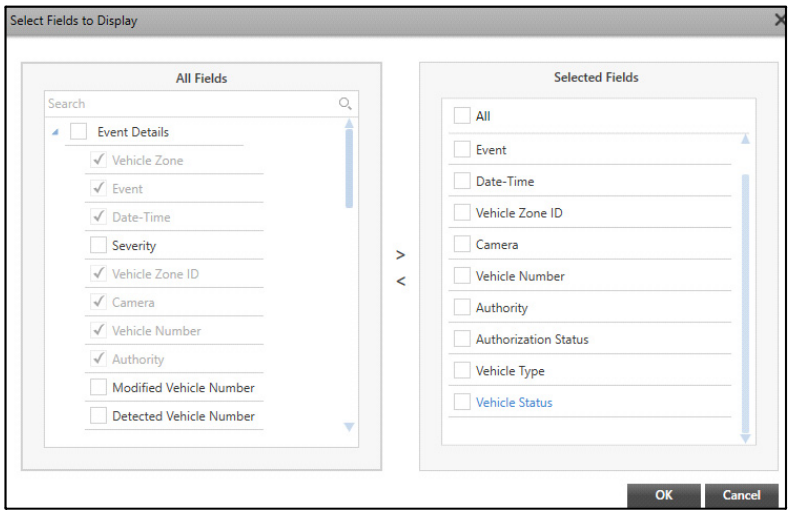
- Select the **Vehicle** check box. Click **OK**.

- **Fields to Display**: Select the desired fields which you wish to include in the report using the **Fields to Display** picklist.
  - Click **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



- Select the check boxes for the desired fields you wish to add from the **All Fields** list. Click the right arrow button to add these fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

  To remove fields, select the check boxes for the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields from the Selected Fields list.



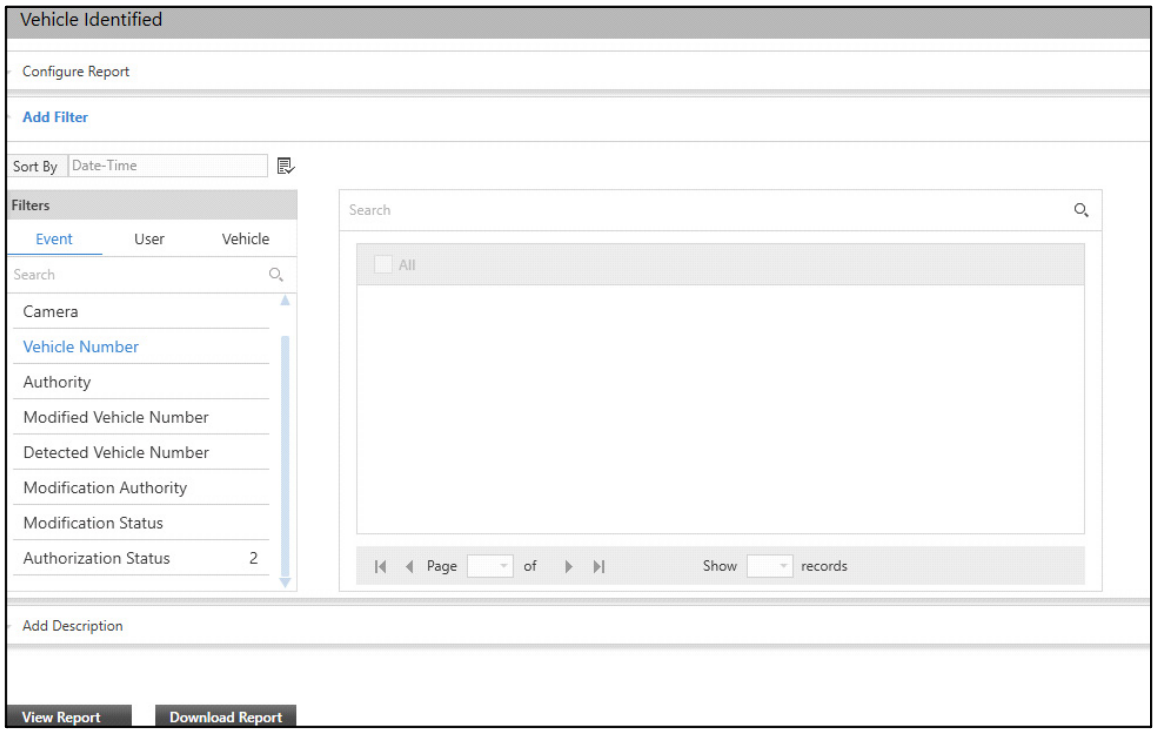
- Click **OK** to confirm or click **Cancel** to discard.
- **Include Images**: Select the type of images that you wish to include in the report using the drop-down list.
- **Display Record per Page**: Select the check box to display each record for the selected fields on a new page.
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.
- **Language**: Select the desired Language in which you wish to generate the report from the drop-down list.
- **Download Path**: Browse a storage path in the selected drive where you wish to store the downloaded reports. Click **Browse** . It displays all folders which are in the drive. Select the desired folder.

Add Filter

This panel allows you to add filters for the Vehicle Identified Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters.

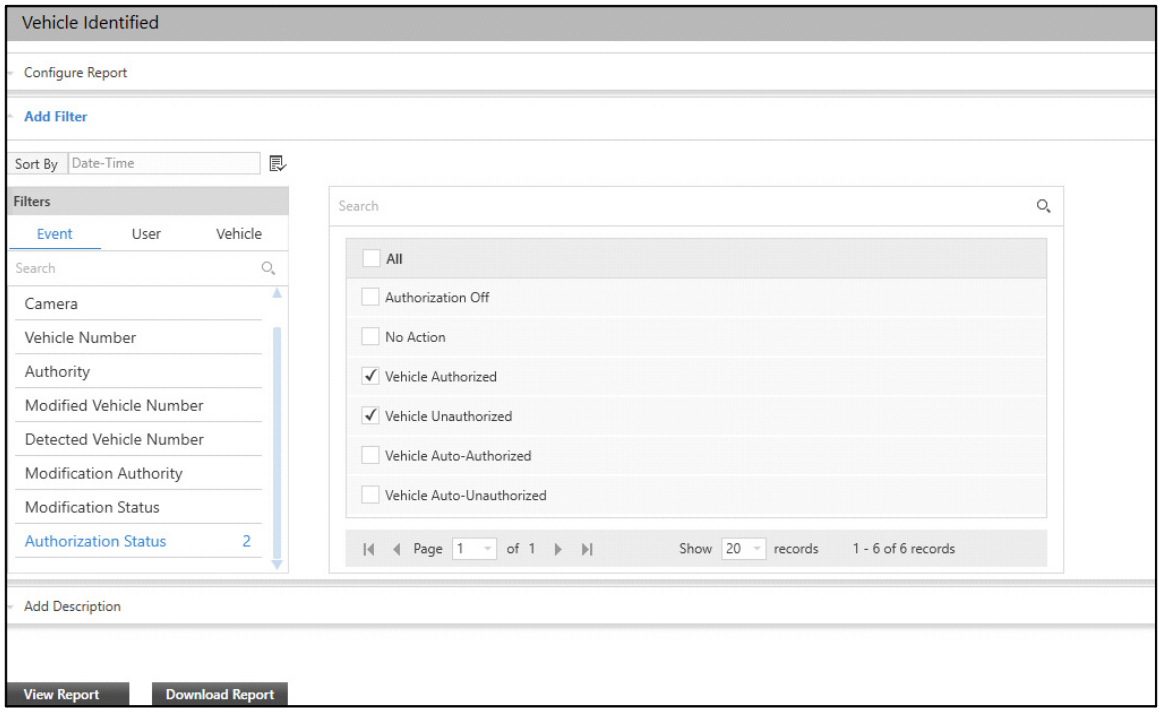
To configure the Filters,

- Click the **Add Filter** collapsible panel.



Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data from Event Details, User Details or Vehicle Details in the report using the **Sort By** picklist. By default, the sorting is done as per the Date and Time of the Event Occurrence.
- **Filters**: You can get the desired data for the report using Filters. The Filters section contains three tabs — Event, User and Vehicle. Select the tab to view the associated parameters.
    - Click the desired parameter to view the associated entities with the selected Event. For example, if you select Authorization Status, all the Status associated with the selected Event are displayed on the right hand side. Select the check boxes of the desired entities to include in the report.



Add Description

This panel allows you to add a description for the Vehicle Identified Report once the report configurations are done. This description is visible in the generated report.

To configure the Description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

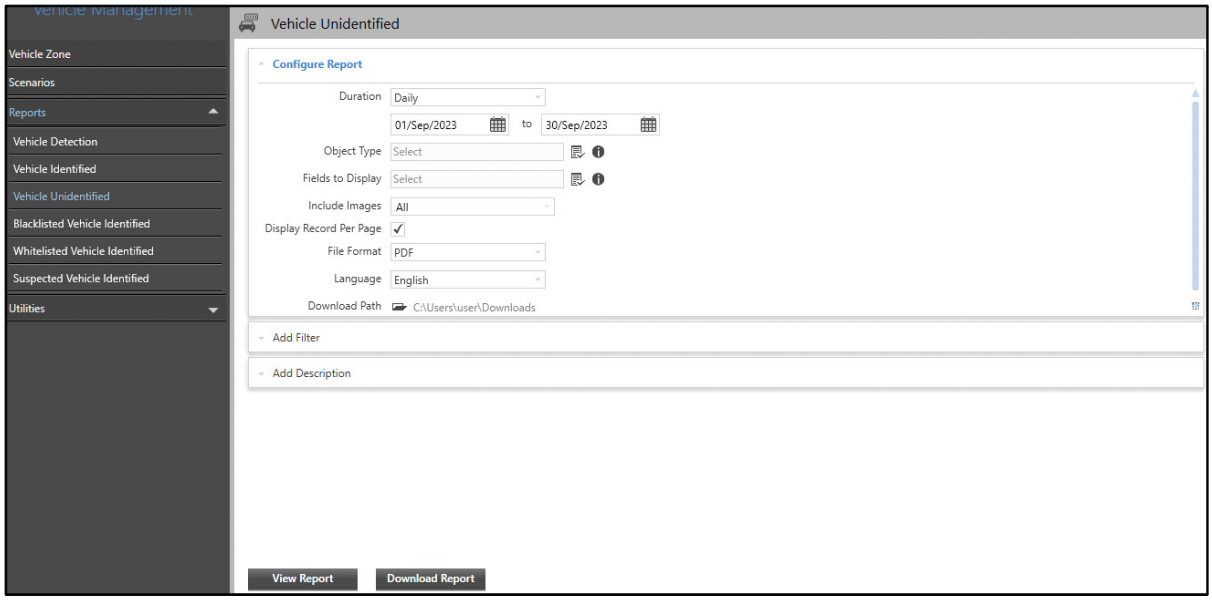
Vehicle Unidentified Report

The Vehicle Unidentified Report provides statistics on vehicles undetected by the Admin Client database. These statistics can be useful in managing places such as Office or Residential parking. Based on this report, Vehicle and User details of vehicles whose Vehicle Number that have not been detected can be tracked easily.

The Vehicle Unidentified page enables you to configure parameters for Vehicle Unidentified Reports. You can view and configure Vehicle Unidentified Reports on Monthly, Daily and Hourly basis.

To configure Vehicle Unidentified Report,

- Click **Vehicle Management > Reports > Vehicle Unidentified**.



The Vehicle Unidentified page contains three collapsible panels — Configure Report, Add Filter and Add Description. The configurations of Vehicle Unidentified Report are similar to that of the Vehicle Detection Report. For details, refer to “Vehicle Detection Report”.

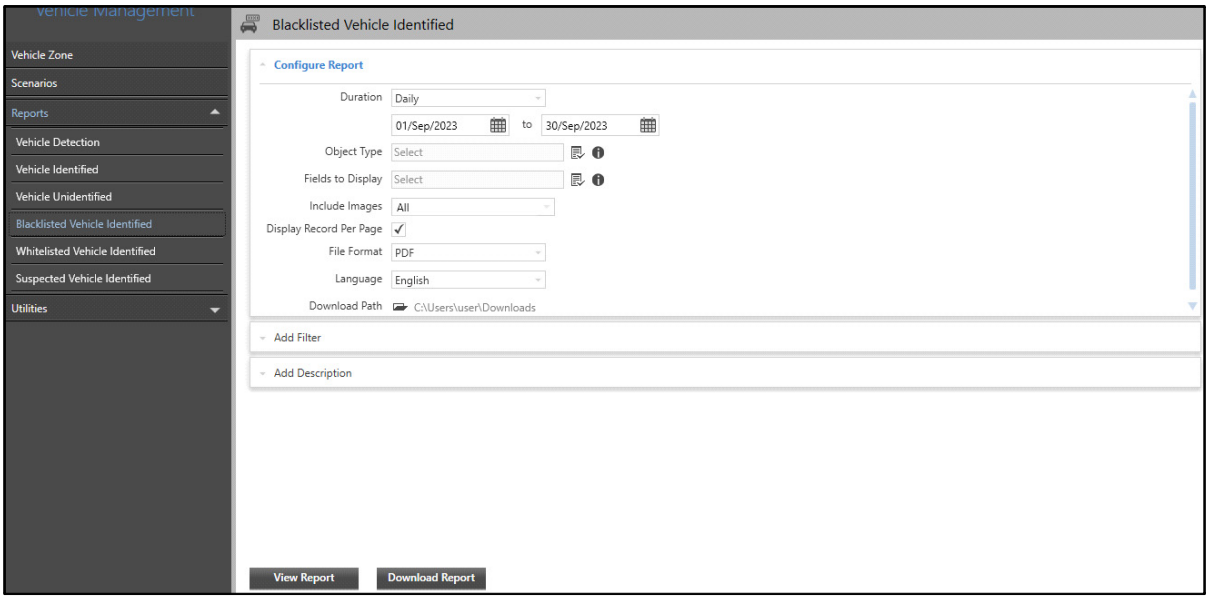
Blacklisted Vehicle Identified Report

The Blacklisted Vehicle Identified Report provides statistics on Blacklisted vehicles detected by the Admin Client database. These statistics can be useful in managing places such as Office or Residential parking. Based on this report, Vehicle and User details of vehicles whose Vehicle Number has been detected and the Vehicle Status is Blacklisted can be tracked easily.

The Blacklisted Vehicle Identified page enables you to configure parameters for Blacklisted Vehicle Identified Reports. You can view and configure Blacklisted Vehicle Identified Reports on Monthly, Daily and Hourly basis.

To configure Blacklisted Vehicle Identified Report,

- Click **Vehicle Management > Reports > Blacklisted Vehicle Identified**.



The Blacklisted Vehicle Identified page contains three collapsible panels — Configure Report, Add Filter and Add Description. The configurations of Blacklisted Vehicle Identified Report are similar to that of the Vehicle Identified Report. For details, refer to “Vehicle Identified Report”.

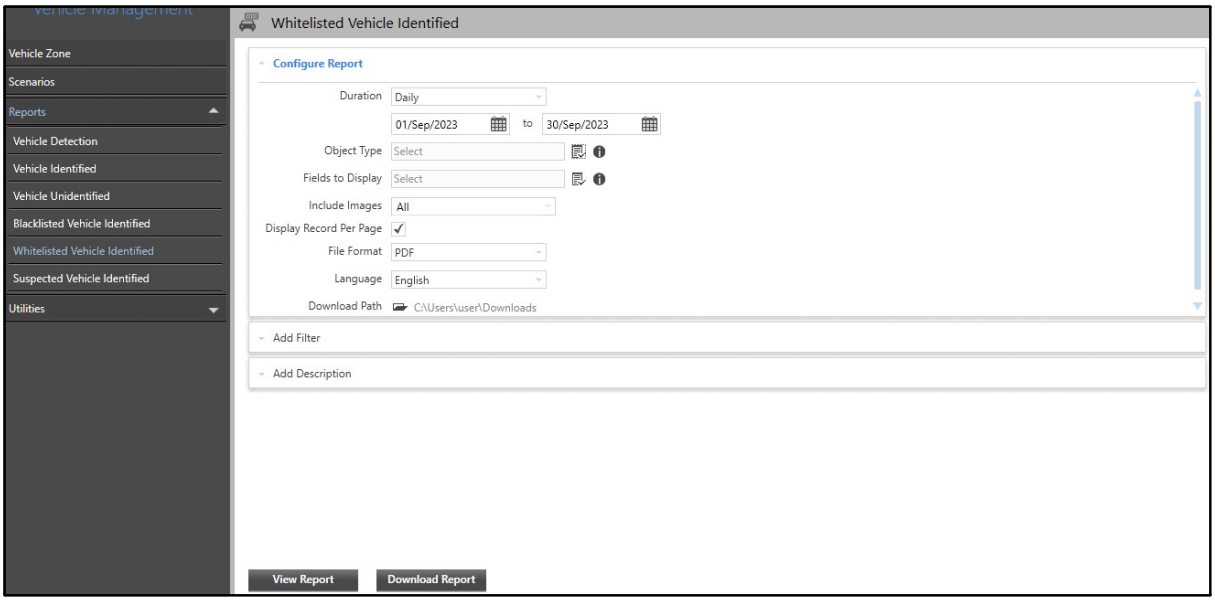
Whitelisted Vehicle Identified Report

The Whitelisted Vehicle Identified Report provides statistics on Whitelisted vehicles detected by the Admin Client database. These statistics can be useful in managing places such as Office or Residential parking. Based on this report, Vehicle and User details of vehicles whose Vehicle Number has been detected and the Vehicle Status is Whitelisted can be tracked easily.

The Whitelisted Vehicle Identified page enables you to configure parameters for Whitelisted Vehicle Identified Reports. You can view and configure Whitelisted Vehicle Identified Reports on Monthly, Daily and Hourly basis.

To configure Whitelisted Vehicle Identified Report,

- Click **Vehicle Management > Reports > Whitelisted Vehicle Identified**.



The Whitelisted Vehicle Identified page contains three collapsible panels — Configure Report, Add Filter and Add Description. The configurations of Whitelisted Vehicle Identified Report are similar to that of the Vehicle Identified Report. For details, refer to “Vehicle Identified Report”.

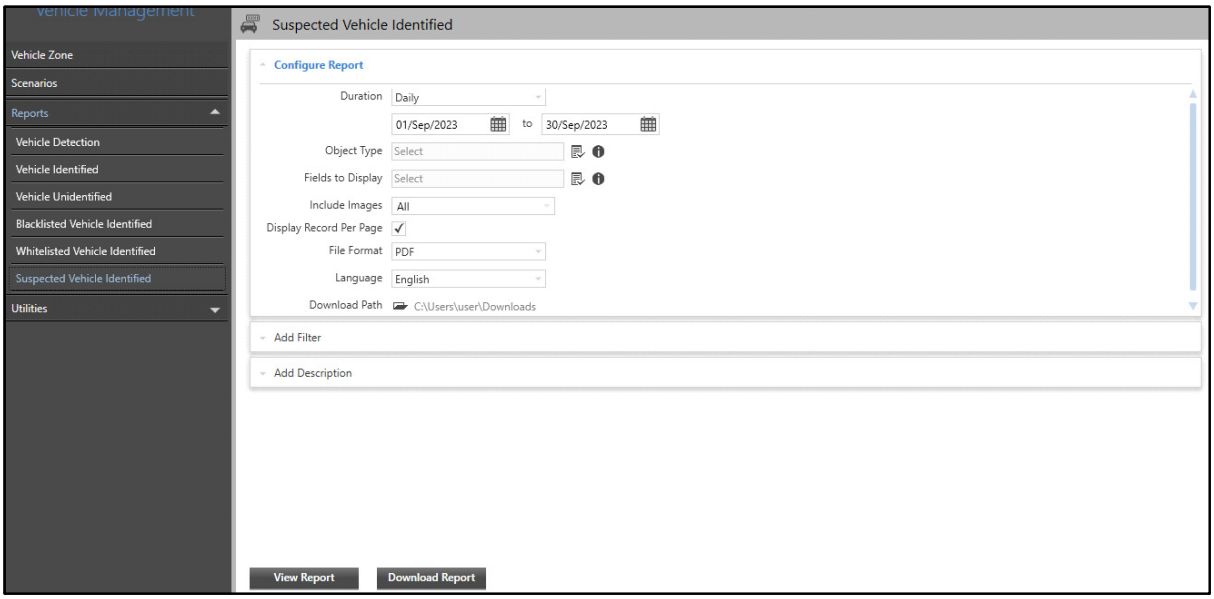
Suspected Vehicle Identified Report

The Suspected Vehicle Identified Report provides statistics on suspected vehicles detected by the Admin Client database. These statistics can be useful in managing places such as Office or Residential parking. Based on this report, Vehicle and User details of vehicles whose Vehicle Number has been detected and the Vehicle Status is Suspected can be tracked easily.

The Suspected Vehicle Identified page enables you to configure parameters for Suspected Vehicle Identified Reports. You can view and configure Suspected Vehicle Identified Reports on Monthly, Daily and Hourly basis.

To configure Suspected Vehicle Identified Report,

- Click **Vehicle Management > Reports > Suspected Vehicle Identified**.



The Suspected Vehicle Identified page contains three collapsible panels — Configure Report, Add Filter and Add Description. The configurations of Suspected Vehicle Identified Report are similar to that of the Vehicle Identified Report. For details, refer to “Vehicle Identified Report”.

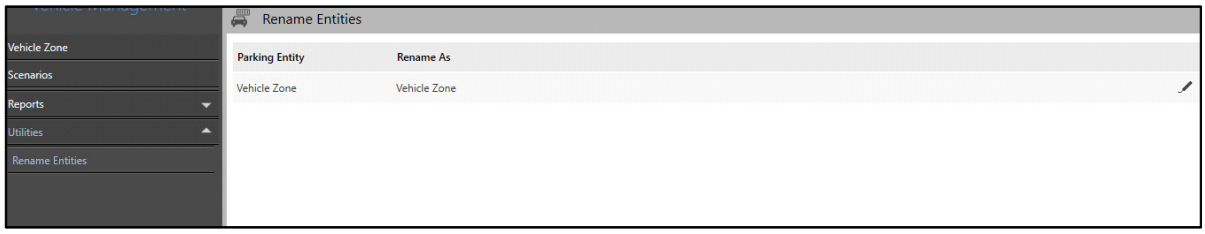
Utilities

Rename Entities

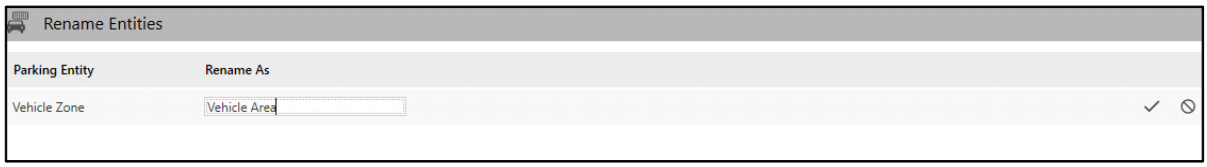
The Vehicle Management module allows you to change the names of the various Vehicle Entities. Rename Entities provides the user a flexibility to change the names of Vehicle Entities as required. The changed names are reflected wherever applicable in the Admin Client.

To view and edit Entities,

- Click **Vehicle Management > Utilities**. The **Rename Entities** page appears by default.



- Click **Edit** corresponding to the Entity you wish to rename.



- Specify the desired name. In Rename As, you can enter upto 30 characters.
- Click **Save** to save the details or click **Cancel** to discard.

CHAPTER 15

Weighbridge Application

Weighbridge Application is introduced to provide transparent business approach by making the loading & unloading process of Goods easy and dispute-free. It provides visual evidence of incidence when Tare/Gross/Net Weight was inserted/calculated and helps to track the records of any manipulation done by the operator while generating the Weight Transaction Receipt.

It generates the weight transaction receipt with the necessary snapshots of loaded/unloaded Vehicle, Weighbridge terminal display which displays Tare/Net/Gross Weight.

Usually the Weighbridge are installed in a premise where the weight of loaded or unloaded vehicle is to be measured. The weight which is measured by Weighbridge is displayed on weighing terminal display screen.

In terms of Weighbridge Application, consider each Weighbridge as a **Terminal** and a Premise transaction as a **Station**. One Premise or Station can have multiple Terminals.

The Weighbridge Application can be used in following scenarios for the weight detection of goods:

Scenario1: Premise having one Weighbridge at Entry gate and another Weighbridge at Exit gate.

Configuration Required: 1 Station, 2 terminals (1 Entry and 1 Exit)

- The loaded truck enters the premise through the Entry terminal, it will arrive on the Weighing machine. When the truck gets stable, the operator can initiate the Entry transaction by triggering entry transaction initiator. The Weighbridge application will fetch the full weight from weighing terminal through the monitoring camera.

- Operator will get the Entry Transaction Receipt in the Smart Client and also he/she can allow or reject the truck to enter inside the premise for unloading the goods.

- Now after delivering the goods when truck reaches to exit terminal, the Exit gate operator will give the exit trigger from Smart Client in the similar way to the Exit gate. Then again the empty weight will be read by the Terminal camera from the Weighbridge display.

- Once the transaction is completed the Exit Transaction Receipt will be generated in the Smart Client. The Exit gate operator will verify the receipt and can Allow/Reject the vehicle to leave the premise.

Scenario2: Premise having one Weighbridge for Entry-Exit gate.

Configuration Required: 1 Station, 1 terminal (Common for Entry and Exit)

- Consider a same Weighbridge or Terminal installed for Entry-Exit Transactions. The entry and exit process will be initiated by different Entry and Exit triggers.

Scenario3: Premise having Two Weighbridge at 2 Entry Gates and one Weighbridge at Exit Gate.

Configuration Required: 2 Station, 3 terminals (2 Entry and 1 Exit)

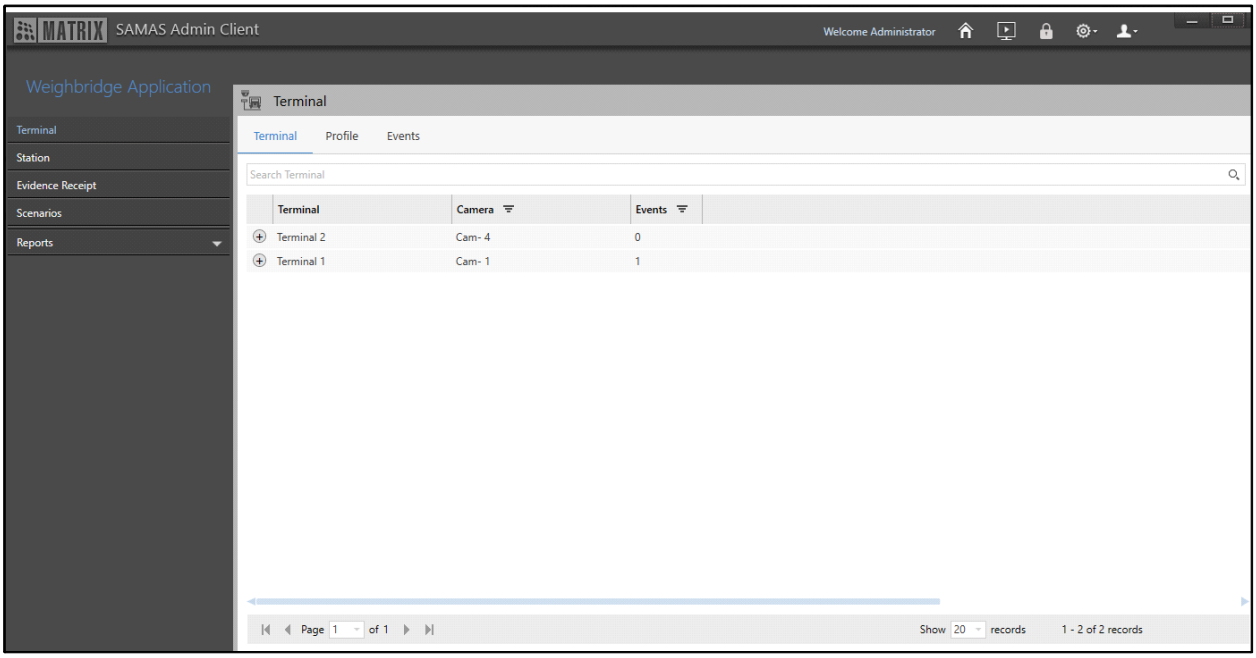
- Consider three Weighbridge installed at the Entry-1, Entry-2 and Exit gate each. The entry and exit process will be similar to Scenario 1.

The Weighbridge Application module enables you to configure various Terminals and Stations and Events for them. Weighbridge Application uses Video Content Analysis which is effective in detecting Events such as Wrong Weight Detected based on live stream of a camera. It also enables you to configure Scenarios based on Events.

The user's accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to "User Groups".

To configure Weighbridge Application,

- Click **Weighbridge Application**.



The Weighbridge Application module contains these sections and pages — "Terminals", "Station", "Evidence Receipt", "Scenarios" and "Reports".

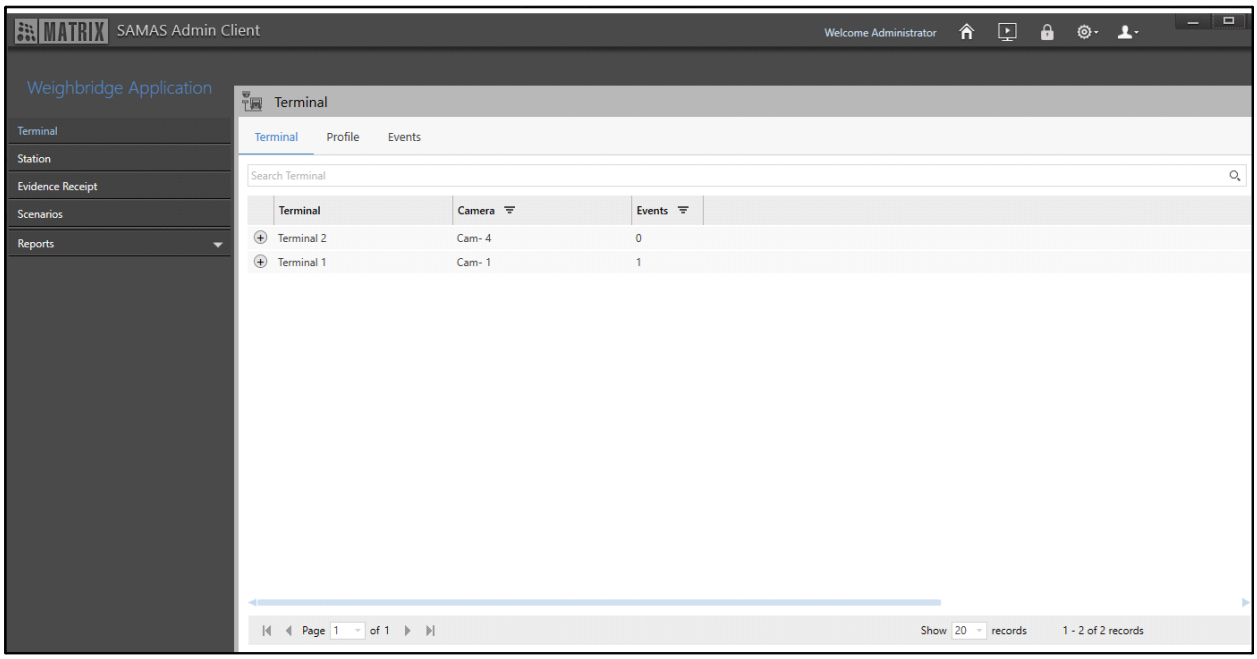
Terminals

The Weighbridge Application allows you to configure Terminals which can be defined as weighbridges installed in a premise to detect and calculate the vehicle weight. The Terminal feature is useful to detect any Events (For example, Weight Detection) in the premises. These Events can help weighbridge operator to initiate Entry or Exit transaction. Event that can be configured against the configured Terminals is Weight Detection.

The Terminal page displays all the configured Terminals. You can view and configure the Terminals from this page.

To configure Terminals,

- Click **Weighbridge Application**. The **Terminal** page appears by default.



The Terminal page consists of the following tabs.

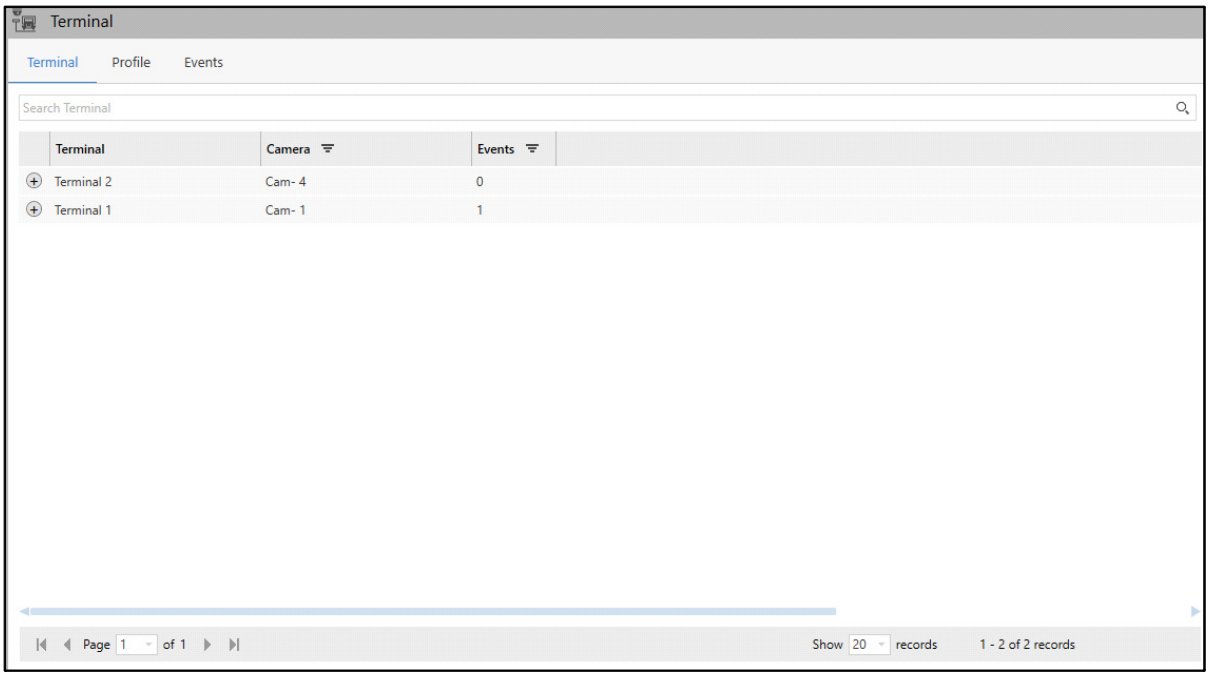
- “Terminal”
- “Profile”
- “Events”

Terminal

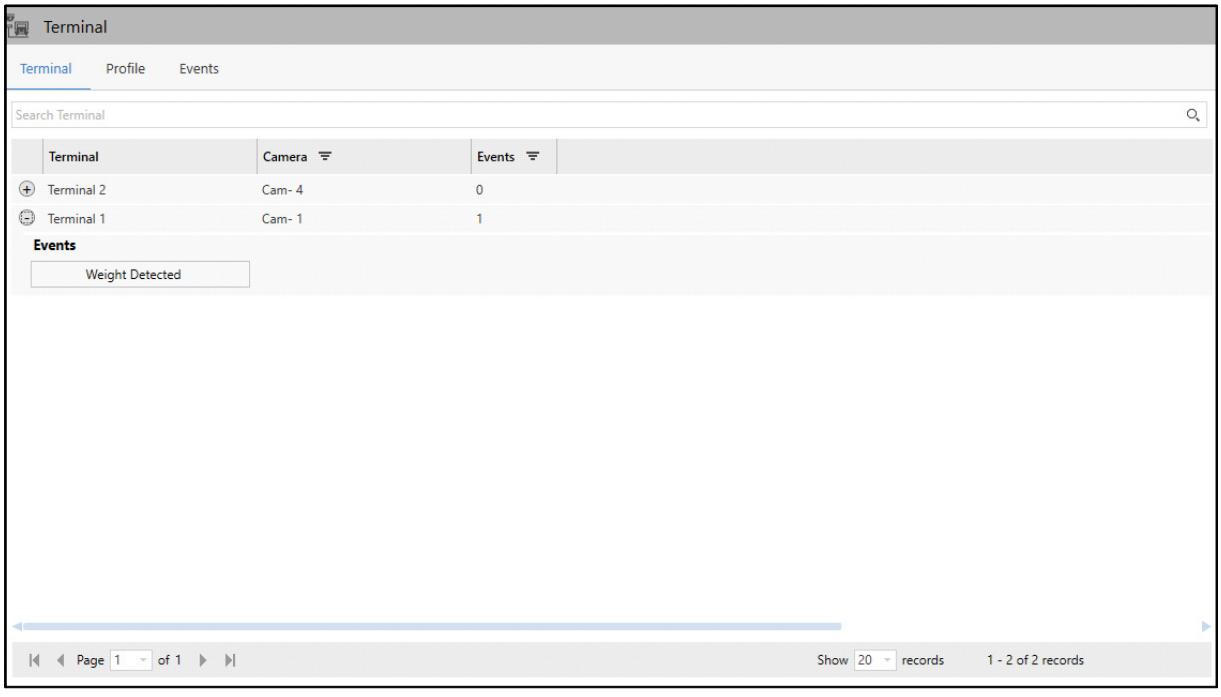
This tab enables you to view Terminals. You can configure the Terminals from “Profile”. All the Terminals and the Events configured for them appear under this tab. The Terminal details displayed are — Terminal, Camera and Events.

To view Terminal,

- Click the **Terminal** tab.



- Click **Show Events** to view the Events configured for the Terminal.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

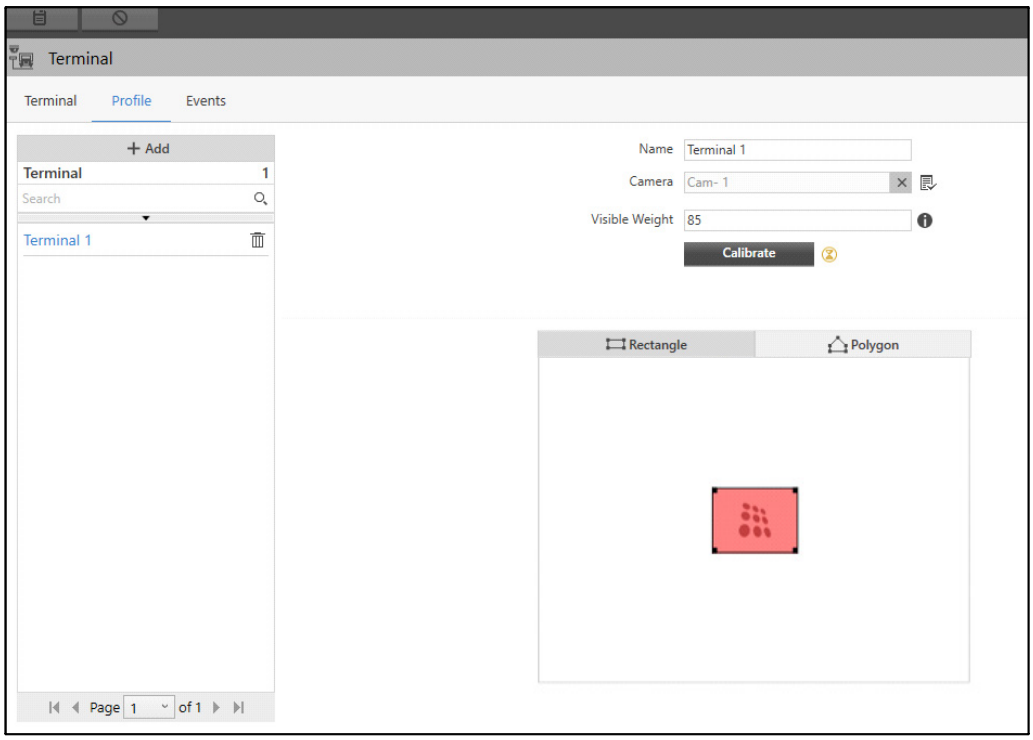
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow ▲ icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

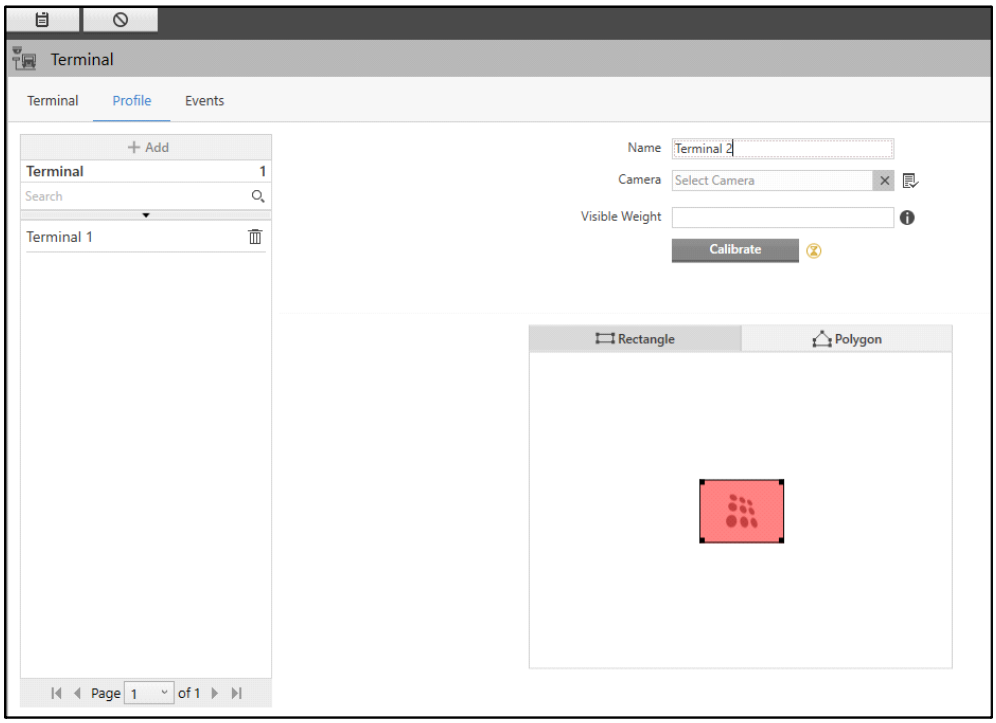
This tab enables you to configure Terminal. All the Terminals configured here appear under the **Terminal** tab.

To configure Terminals,

- Click the **Profile** tab.



- Click **Add**.

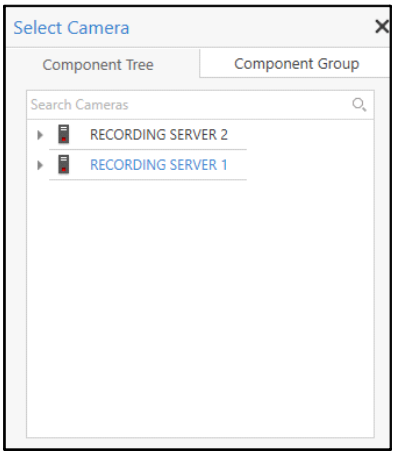


Configure the following parameters:

- **Name**: Specify a suitable name for the Terminal. In Name, you can enter upto 50 characters. Default: Blank.
- **Camera**: Select the desired camera which you wish to assign to the Terminal using the **Camera** picklist.

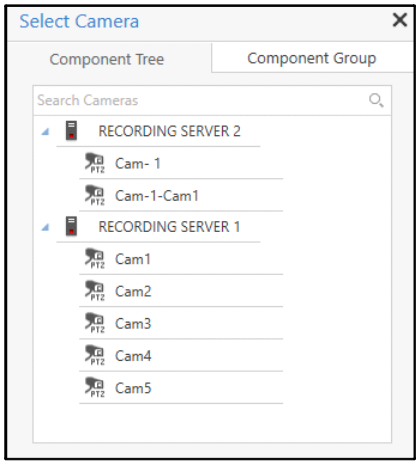
Make sure the selected camera is turned on and assigned to the IVA Server to enable calibration.

- Click **Camera** picklist. The **Select Camera** pop-up appears.



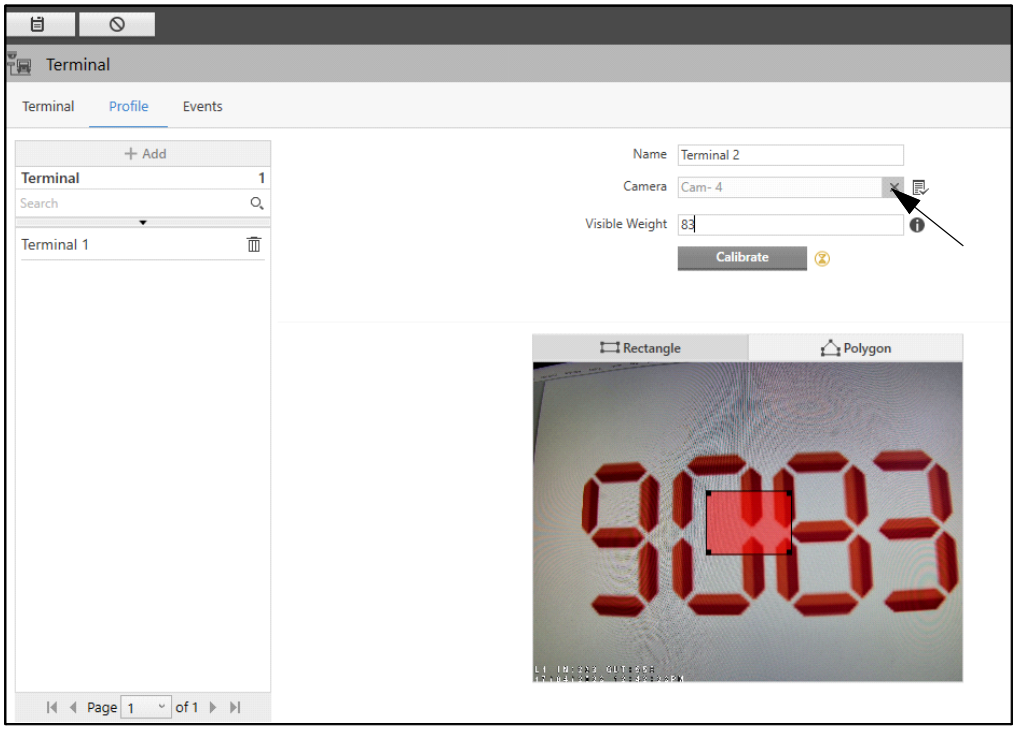
- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To

know more, refer to “Component Group”. Double click the desired camera to assign it to the Terminal. You can also search for the desired cameras using the **Search Cameras** search bar.



If you select a PTZ camera, you need to select the preset positions for it.

- **Preset Position**: Select the desired preset position for the selected camera using the **Preset Position** picklist. Double-click the desired option from the list.
  - Click **Go to selected position** to move the camera to the selected preset position.
- To remove the camera, click **Remove** .



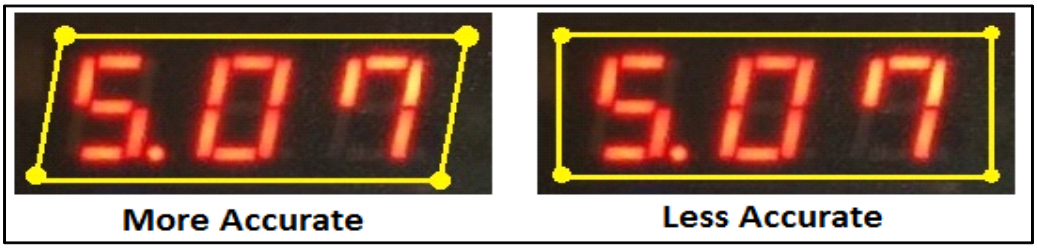
- **Visible Weight**: Specify the visible weight from live view of the camera which is currently displayed on weighbridge display. In Visible Weight, you can enter upto 50 characters. Default: Blank.

- Click **Save** to save the settings or **Cancel** to discard.

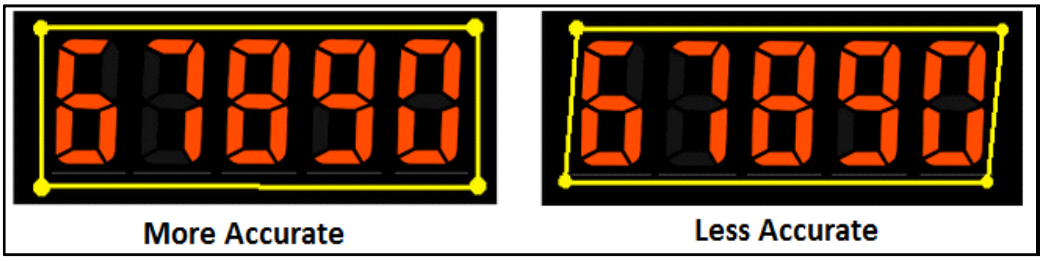
Once a camera is assigned, you can draw a Terminal on the live view of the camera to cover the weighbridge display. You can either draw a **Rectangle** or **Polygon** to define the Terminal.

Draw the detection region according to the slope of the digits of seven segment display to get more accuracy in weight detection. Consider the following examples.

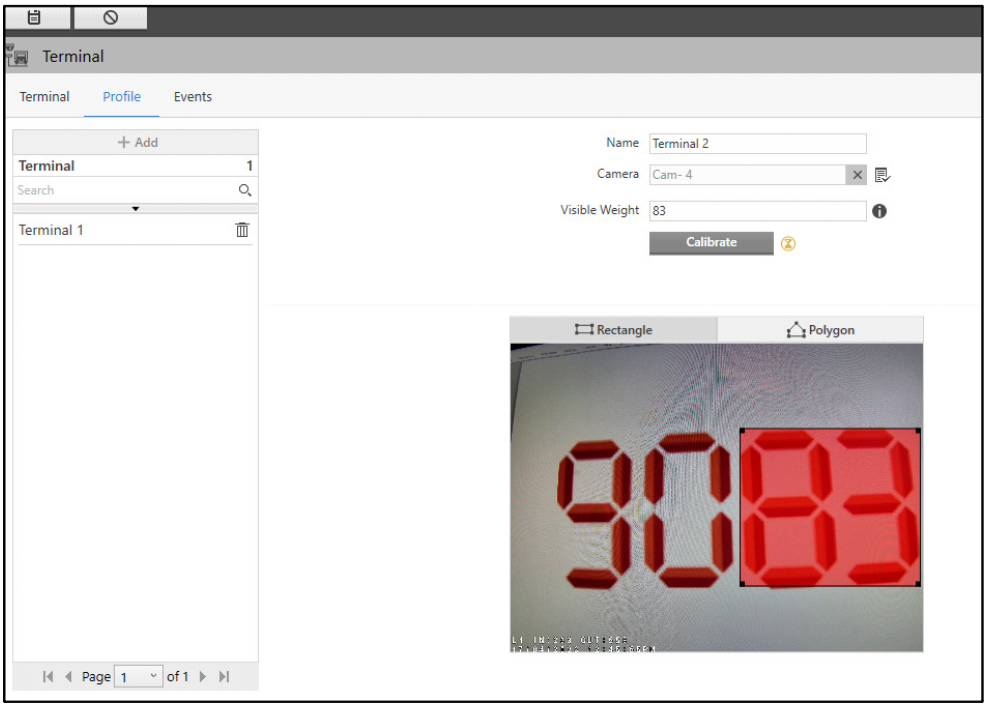
- *Example 1*



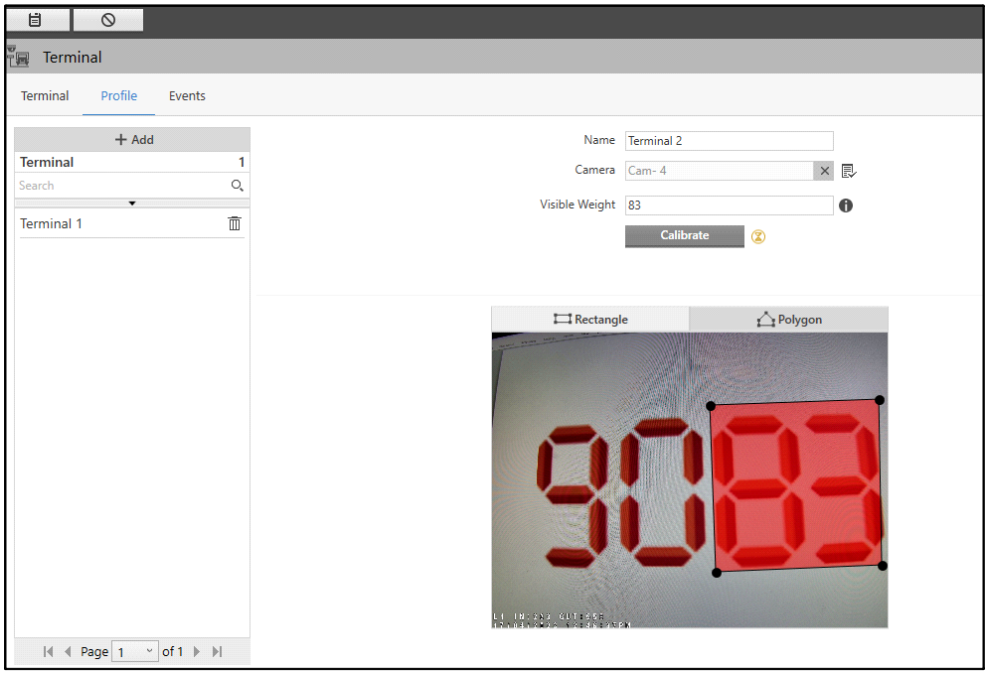
- *Example 2*



- Select either **Rectangle** or **Polygon** to draw the Terminal.
- If you select **Rectangle**, drag the corners and sides of the rectangle to configure the Terminal.



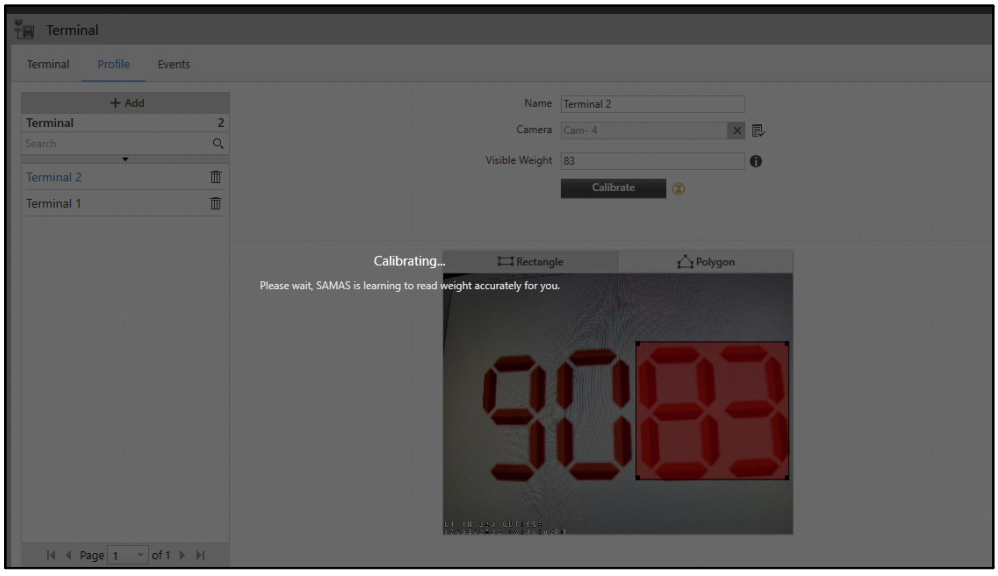
- If you select **Polygon**, click on the live view to place the vertex of the polygon. Click again on the desired place to join the previous vertex with a new vertex. Continue this process to complete the polygon.



- Click **Save** to save the settings or **Cancel** to discard.

Once the Terminal profile is created, you need to do the calibration.

- Click **Calibrate**.

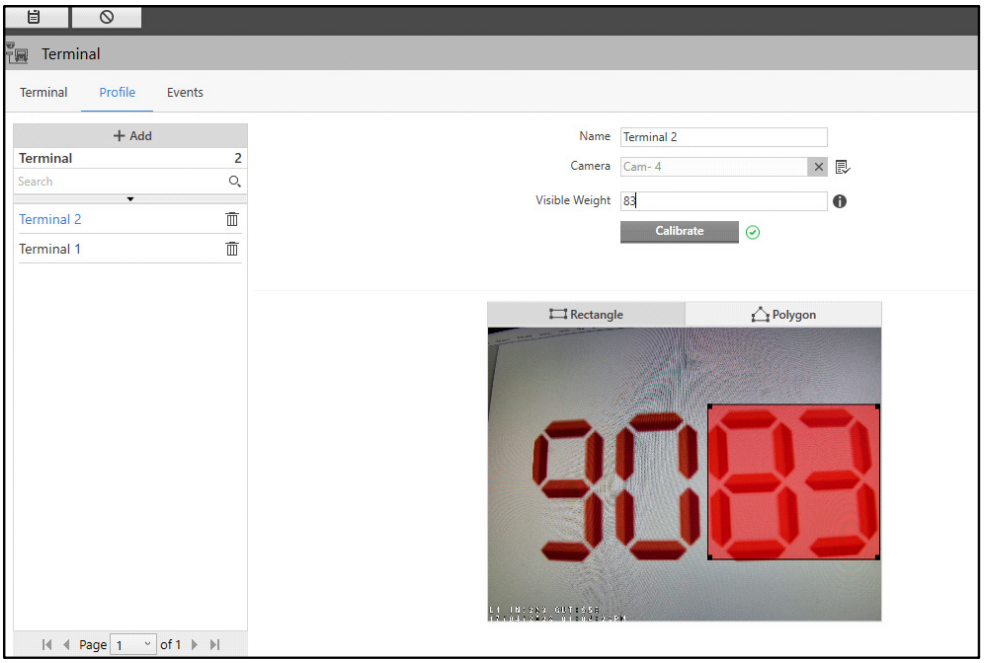


Wait till the calibration of weight is completed successfully.

Weight will not be captured from the weighbridge display until the calibration is successfully done.

The new Terminal will appear on the left hand side.

You can edit the configurations of the Terminal or delete it.



- Select the desired Terminal from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Terminal.

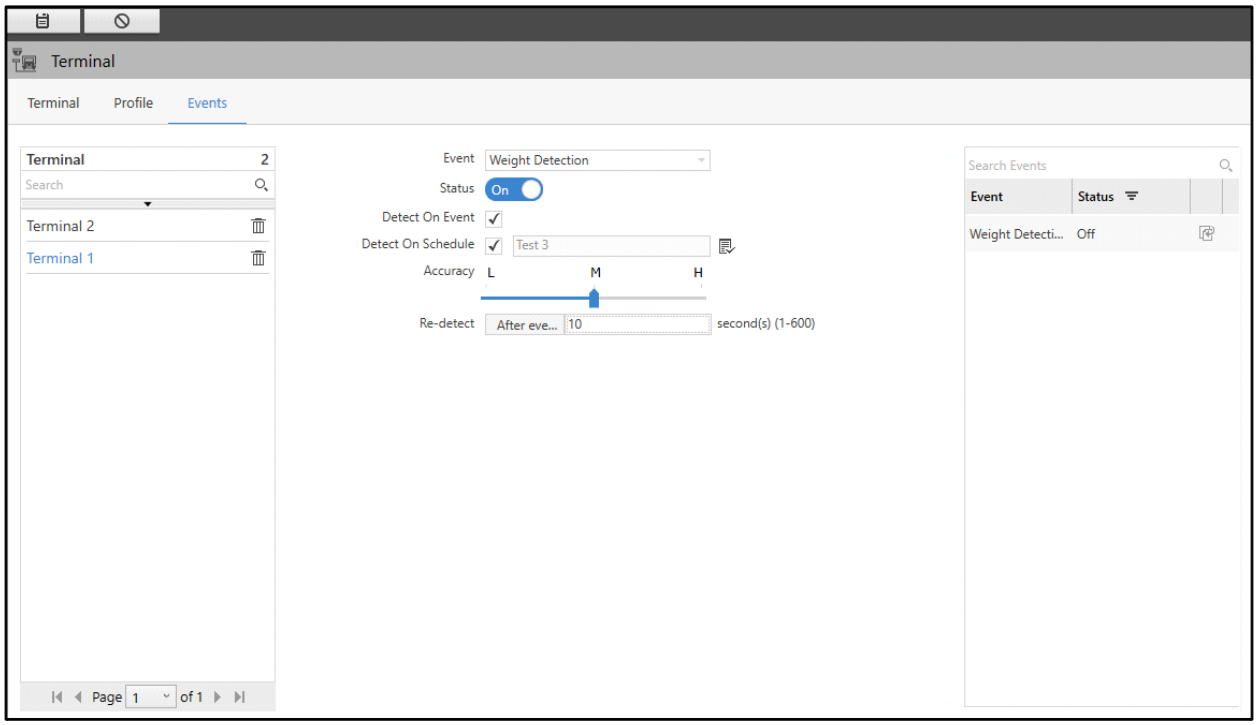
Similarly, you can configure the other Terminals.

Events

This tab enables you to configure the Weight Detection Event for the Terminals. All the configured Events appear under the **Terminal** tab.

To configure the Weight Detection Event,

- Click the **Events** tab.
- Select the desired Profile from the left hand side for which you wish to configure the Event.

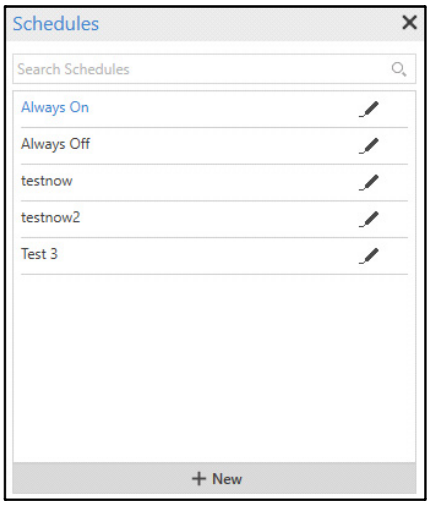


Configure the following parameters:

- **Event:** Select the Weight Detection Event from the drop-down list.
- **Status**: By default the Switch is Off, click to turn it on.

  Once the Status switch is **On**, you can configure the remaining parameters:

- **Detect on Event**: Select the check box to detect Event only on the occurrence of Event.
- **Detect on Schedule**: Select the check box to detect Event as per a specific schedule. Select the desired schedule which you wish to assign to the profile using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



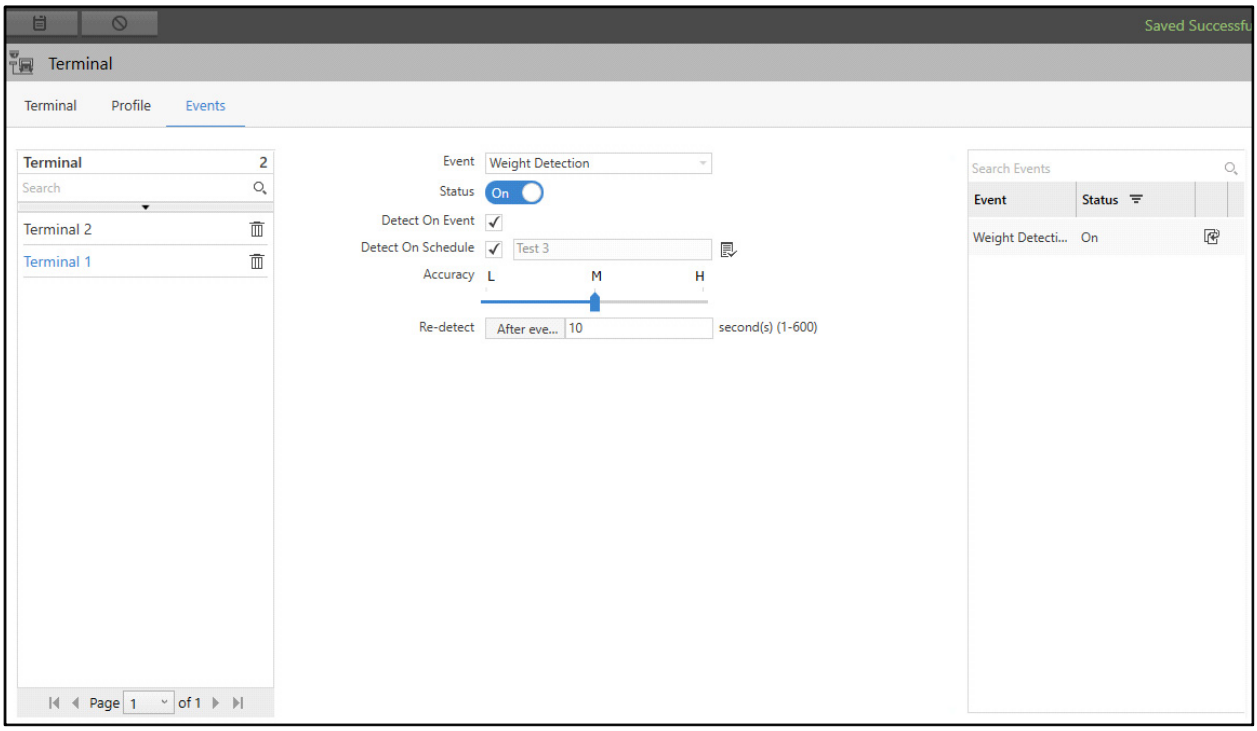
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Accuracy**: Drag the slider to set the desired accuracy for the Weight Detection Event — Low, Medium or High.

- **Re-detect**: Specify the time after which the Weight Detection Event will be detected again after the previous detection. Valid Range: 1- 600 seconds. Default: 5.

- Click **Save** to save the settings or **Cancel** to discard.

Once you have configured the Event, you can edit its configurations or disable it.



- Select the desired Profile from the list on the left hand side, for which the Event has been configured. Edit the configurations on the right hand side.

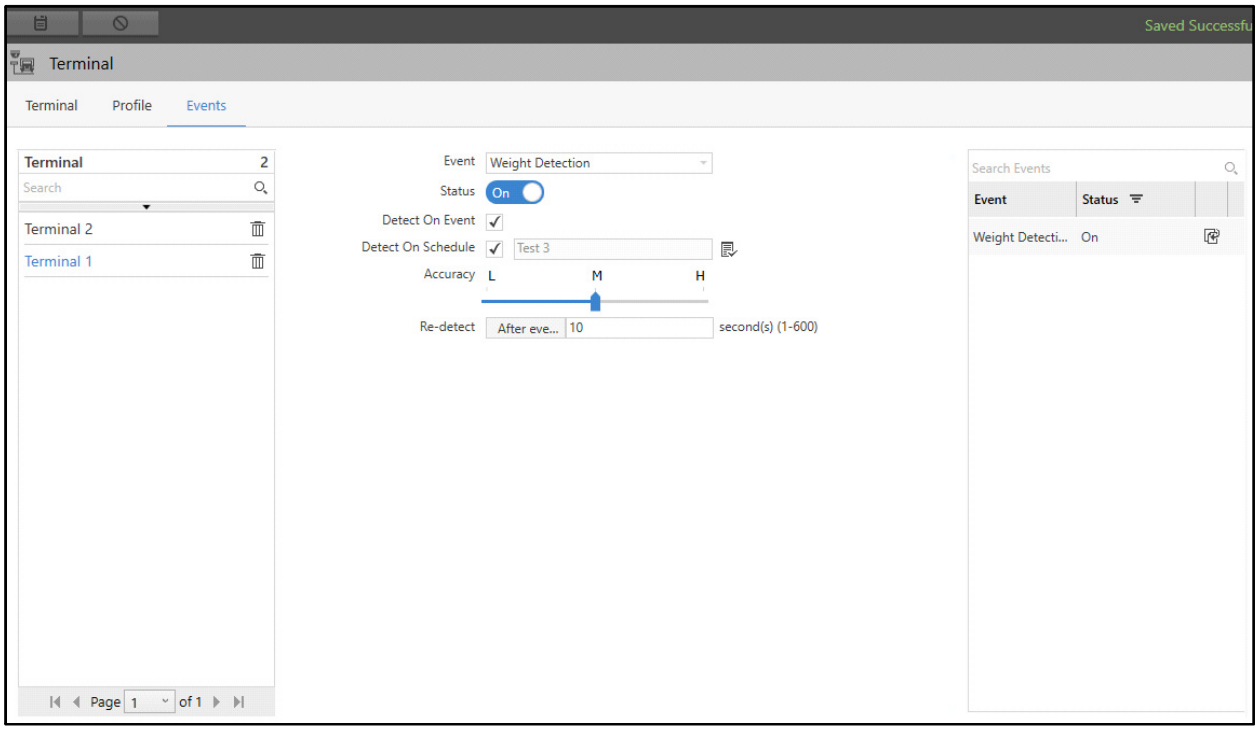
- Click **Save** to save the settings or **Cancel** to discard.

- You cannot delete the configured Event for any Profile, however if you do not wish the Event to be executed, select the desired Profile for the list on the left hand side and then click the Event **Status** switch to turn it **Off**.

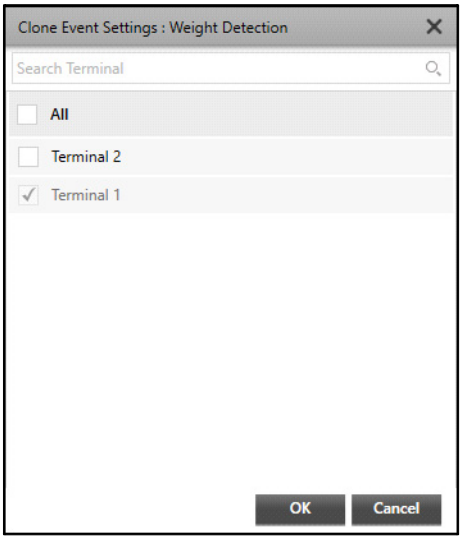
Once the Event is configured, you can copy the Event configurations to other Events. To do so,

*Clone option will be enabled only if system contains more than one source/entity with same Event Source Type. For example, when second profile of Terminal is created, the **Clone Event Settings** option gets enabled.*

- Select the desired Profile from the list on the left hand side, for which the Event has been configured. The Event Name and Status appear on the right hand side.



- Click **Clone Event Settings** . The **Clone Event Settings: Weight Detection** pop-up appears.



- Select the desired Events to which you wish to copy the configurations.

- Click **OK** to confirm or click **Cancel** to discard.

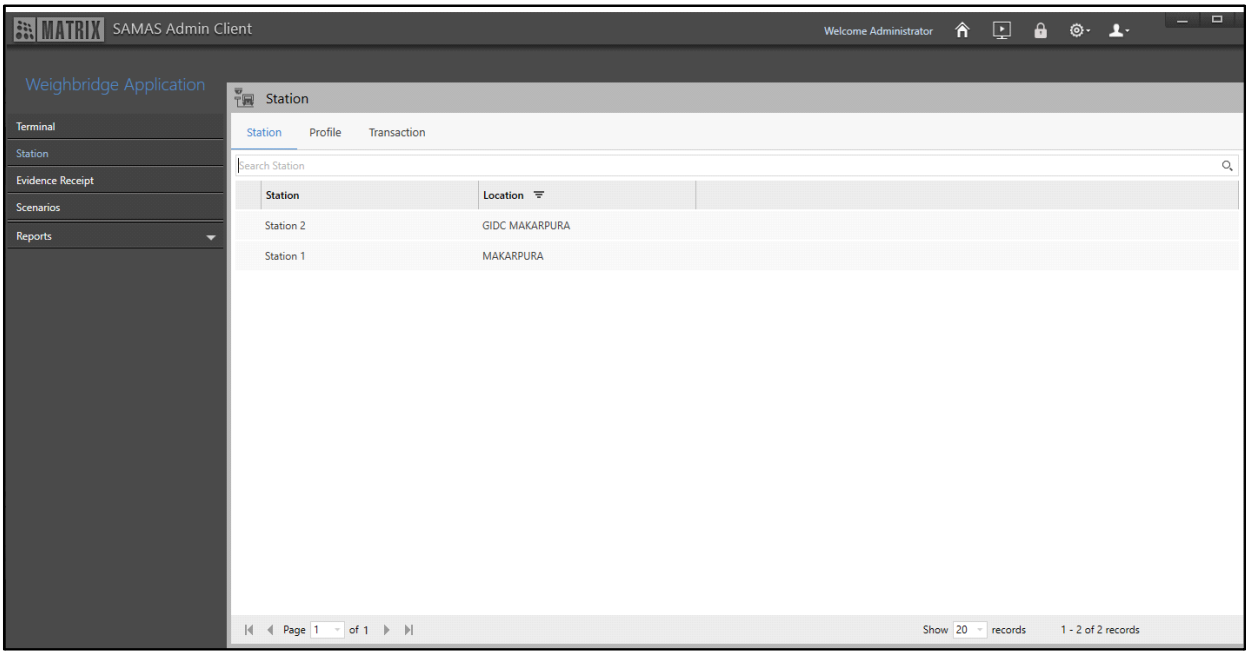
Station

The Weighbridge Application allows you to configure Stations which can be defined as places where a vehicle is to load or unload goods. The Station feature is useful to initiate Entry and Exit transactions.

The Station page displays all the configured Stations. You can view and configure the Stations from this page.

To configure Stations,

- Click **Weighbridge Application > Station**.



The Station page consists of the following tabs:

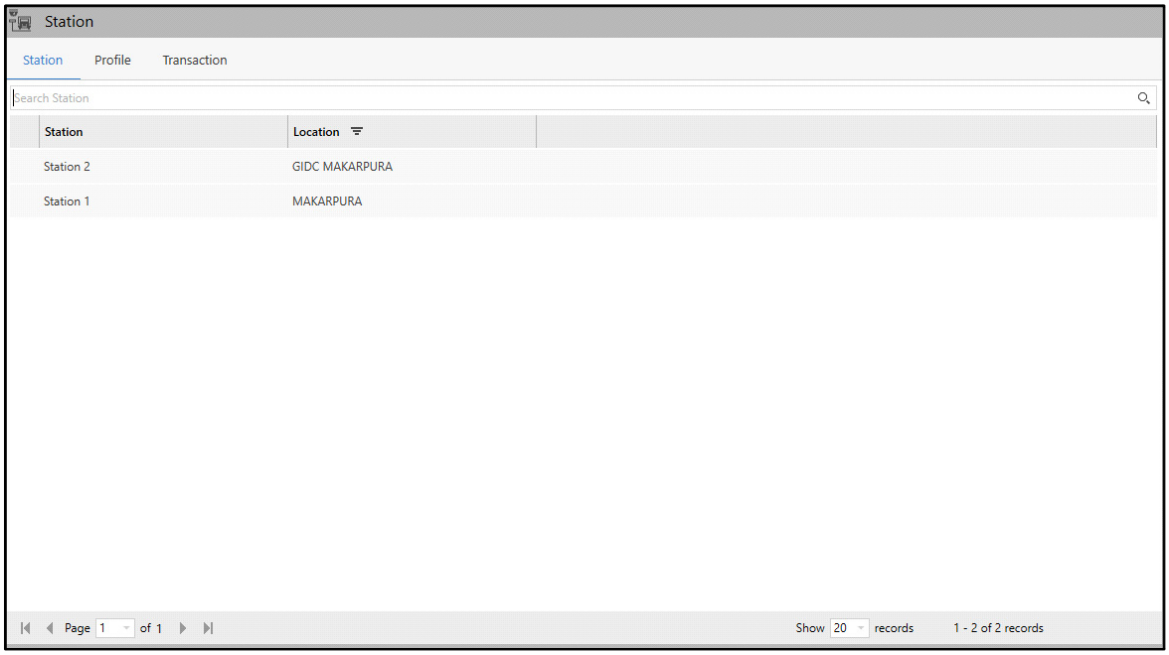
- “Station”
- “Profile”
- “Transaction”

Station

This tab enables you to view Stations. You can configure the Stations from “Profile”.All the Stations and the Locations configured for them appear under this tab. The Terminal details displayed are — Station and Location.

To view Station,

- Click the **Station** tab.



- Click **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

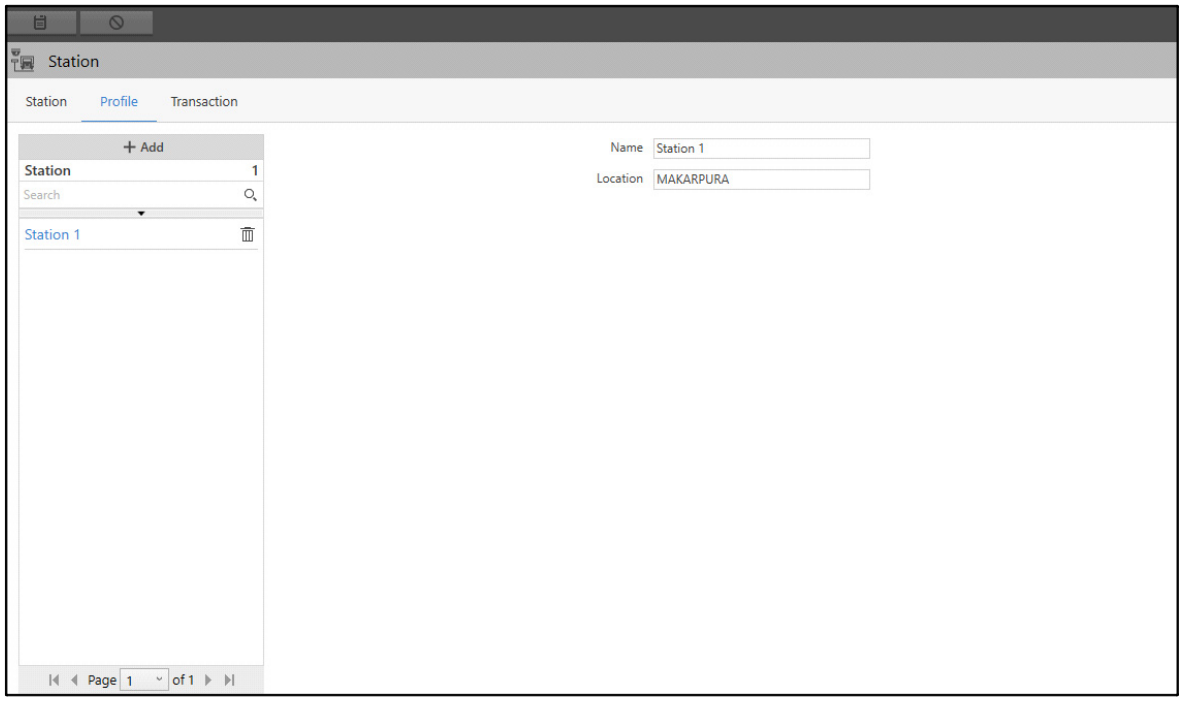
- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

Profile

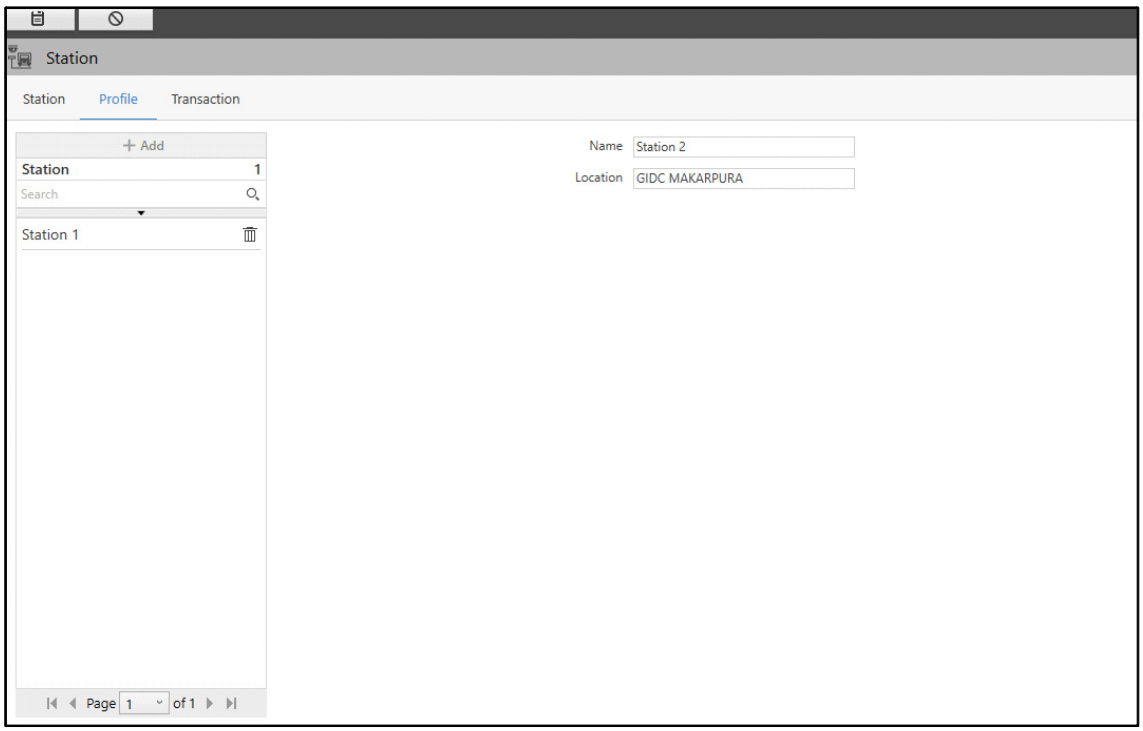
This tab enables you to configure Station. All the Stations configured here appear under the **Station** tab.

To configure Stations,

- Click the **Profile** tab.



- Click **Add**.



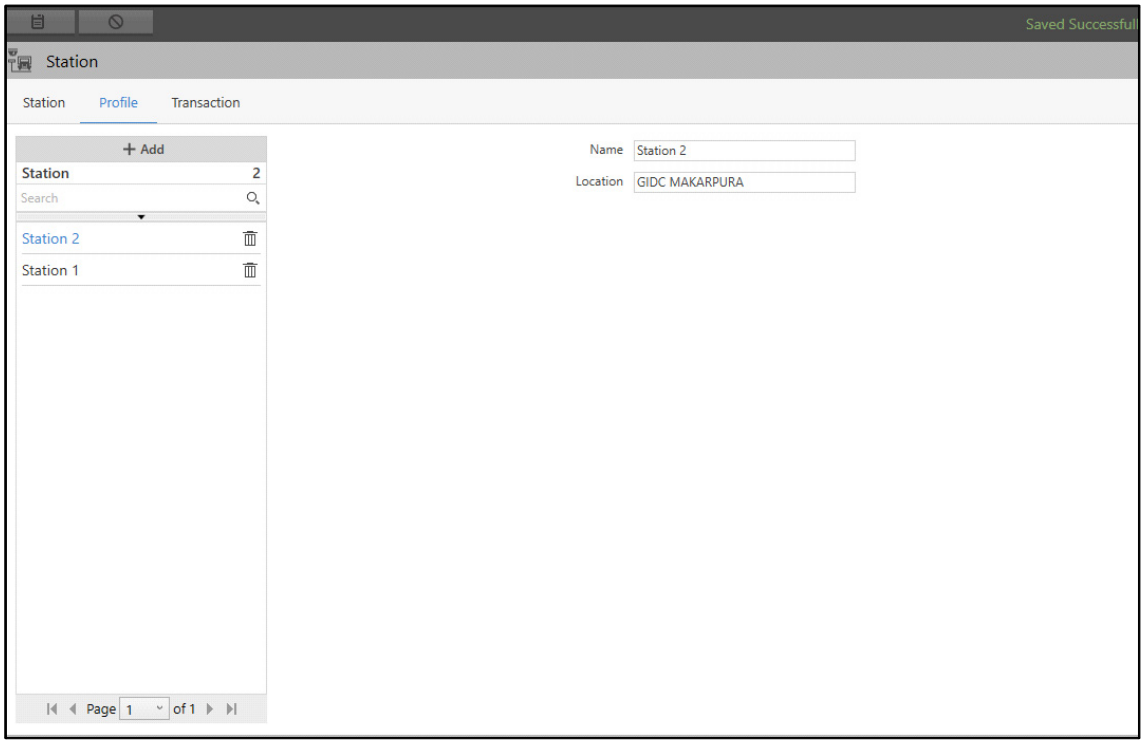
Configure the following parameters:

- **Name**: Specify a suitable name for the Station. In Name, you can enter upto 50 characters.Default: Blank.
- **Location**: Specify the location of the Station. In Location, you can enter upto 150 characters. Default: Blank.

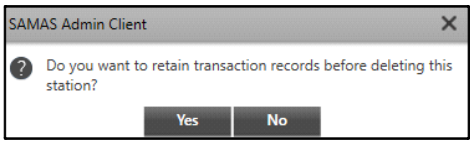
- Click **Save** to save the settings or **Cancel** to discard.

The new Station will appear in the list on the left hand side.

You can edit the configurations of the Station or delete it.



- Select the desired Station from the list and edit the configurations on the right hand side.
- Click **Save** to save the settings or **Cancel** to discard.
- Click **Delete** to delete the desired Station. The following pop-up appears.



- Click **Yes** to retain the Transaction records or click **No** to delete the Station along with its Transaction records.

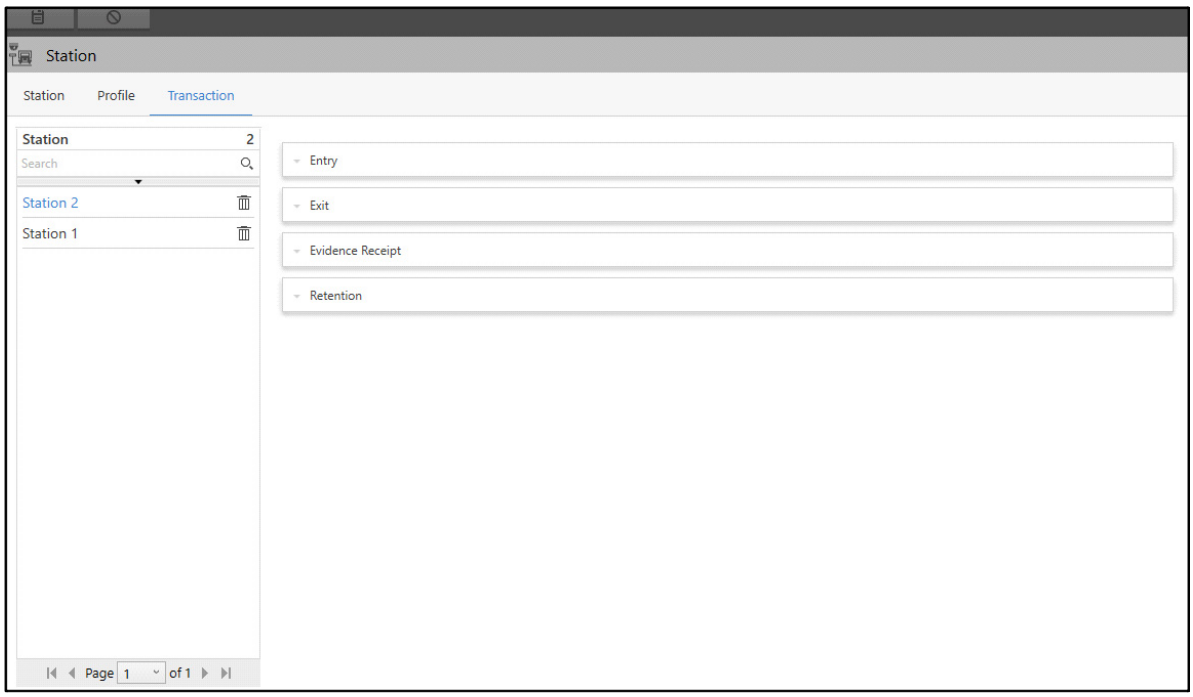
Similarly, you can configure the other Stations.

Transaction

This tab enables you to configure the Transactions for Stations. The loading and unloading of goods in a premise is done in one Transaction, that is, Entry of Vehicle in a Premise and Exit of Vehicle from the Premise. For the Transaction to take place, Entry and Exit triggers/ initiators must to be configured.

To configure Transaction,

- Click the **Transaction** tab.



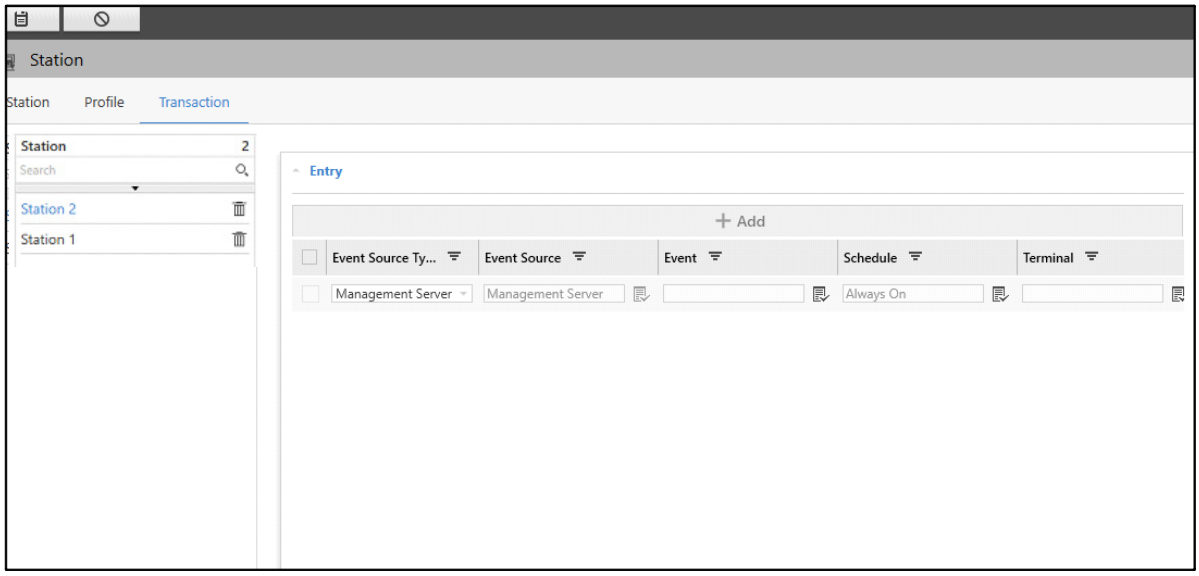
The Transaction tab contains four collapsible panels — “Entry”, “Exit”, “Evidence Receipt” and “Retention”.

Entry

This panel displays the Events configured for Entry Transaction. This panel allows you to configure Events for Entry Transaction.

To configure the Entry Transaction,

- Click the **Entry** collapsible panel.
- Click **Add**.



The number of Entry Transactions must be equal to the Entry Terminals defined for a Station.

For example, consider a Premise having two Entry gates from where Entry of vehicle is allowed. So, configure two Entry Terminals where Weighbridge is installed and define two Entry Transactions for each Entry Terminal.

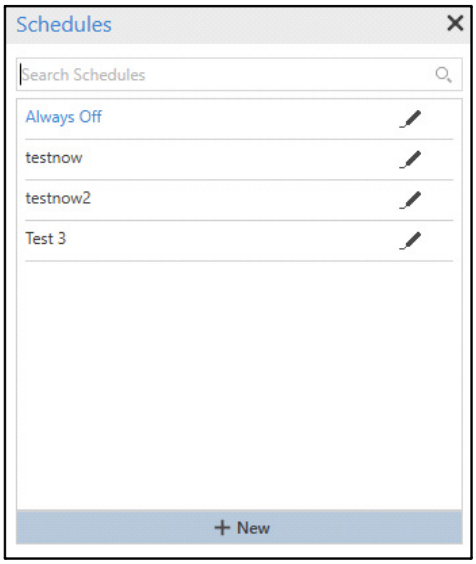
Configure the following parameters:

- **Event Source Type**: Select the type of Event Source for the Entry Transaction from the drop-down list.
- **Event Source**: Select the Event Source where the Entry Transaction has to be initiated using the **Event Source** picklist. The Event Source depends on the selected Event Source Type. For example, if you select Camera as the Event Source Type, a list of all the configured cameras appear in the Event Source picklist. Double-click to select the desired option.
- **Event**: Select the Event which will be used as the Entry Transaction Initiator using the **Event** picklist. Double-click to select the desired option.

Event Source Type, Event Source and Event defined here will be treated as Entry Transaction Initiator.

Entry/Exit transaction Initiator (i.e. Event Source Type + Event Source + Event) must be unique for each transaction of station.

- **Schedule**: Select the desired Schedule which you wish to assign to the Entry Transaction using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Terminal**: Select the desired Terminal where you wish to configure the Entry Transaction using the **Terminal** picklist. Double-click to select the desired option.

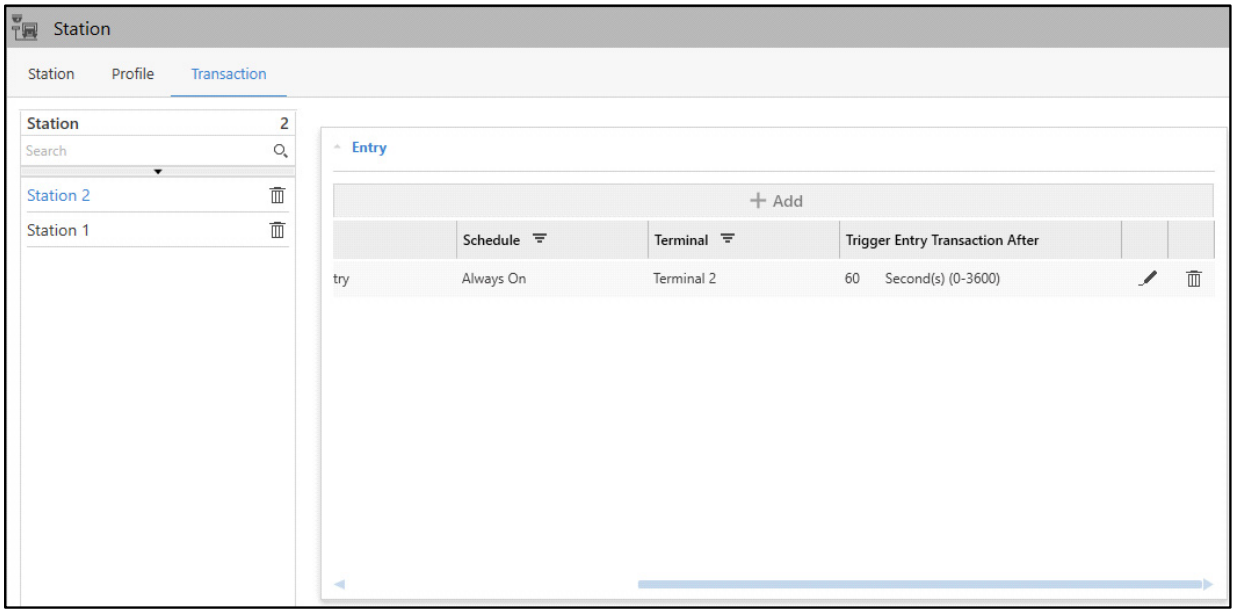
A Terminal can belong to one Station only. You cannot assign the same Terminal to other Station.

- **Trigger Entry Transaction After**: Specify the time in seconds till when the system should wait before triggering the Entry Transaction. For example, the Trigger Entry Transaction After is configured as 60 seconds. Once the Event is triggered, the system will wait for 60 seconds before initiating the Entry Transaction. Valid Range: 0-3600 seconds. Default: 0.

- Click **Save** to save the Entry Transaction or click **Cancel** to discard.

The configured Entry Transaction appears in a list.

You can edit the configurations of the Transaction or Delete Transactions.



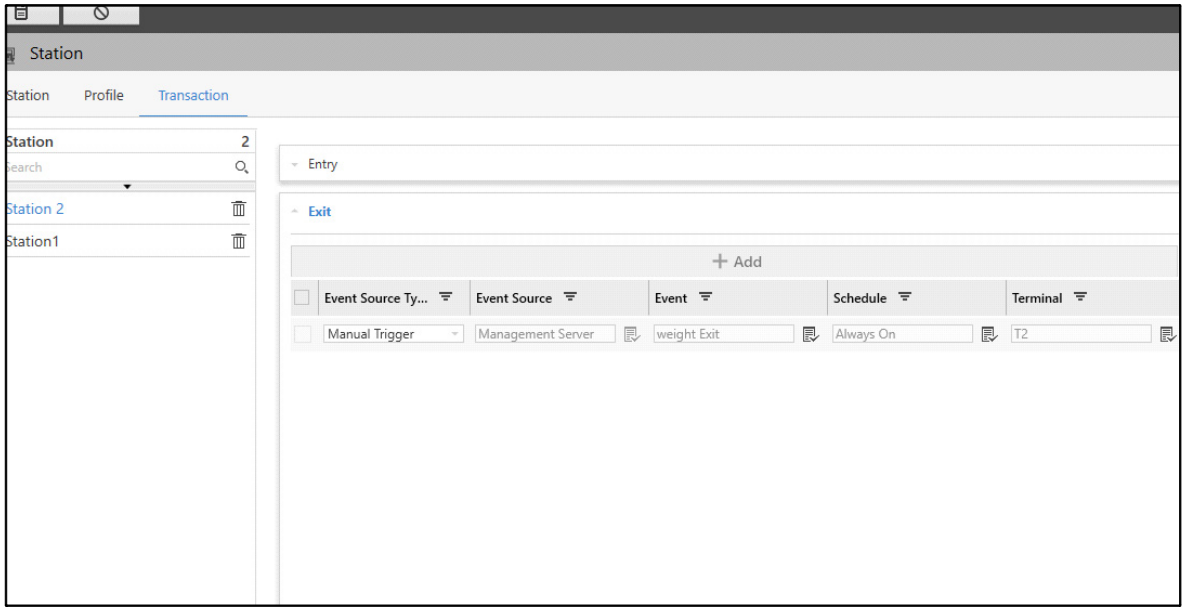
- Click **Edit** to edit the Entry Transaction configurations.
- Click **Delete** to delete the Entry Transaction.

Exit

This panel displays the Events configured for Exit Transaction. This panel allows you to configure Events for Exit Transaction.

To configure the Exit Transaction,

- Click the **Exit** collapsible panel.
- Click **Add**.



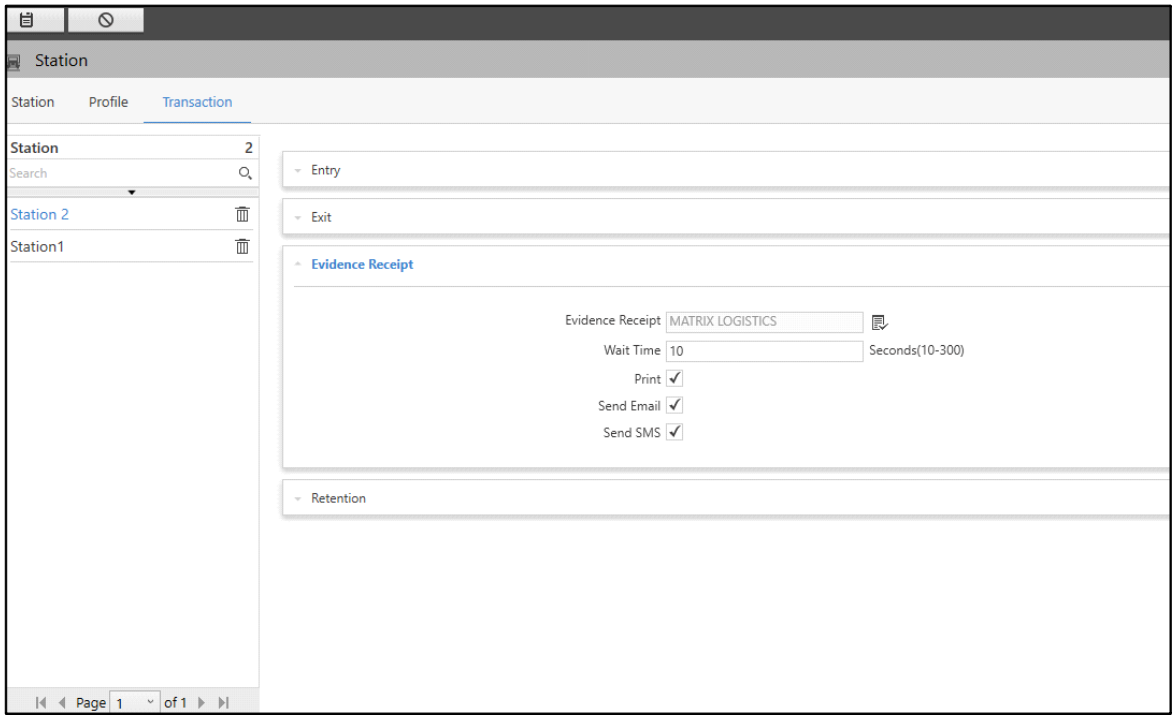
The configurations of Exit Transaction is similar to that of the Entry Transaction. For more details, refer to “Entry”.

Evidence Receipt

This panel displays the Evidence Receipt configured for Transaction. Based on this configuration, the Entry and Exit Receipts are generated. This panel allows you to configure Evidence Receipt for the entire Transaction.

To configure the Evidence Receipt,

- Click the **Evidence Receipt** collapsible panel.



Configure the following parameters:

- **Evidence Receipt**: Select the desired Evidence Receipt which you wish to use at the Station using the **Evidence Receipt** picklist. Double-click to select the desired option. To create the Evidence Receipt, refer to “Evidence Receipt”.
- **Wait Time**: Specify the time in seconds till when the system should wait to fetch the Event details and print it on the Evidence Receipt. In Wait Time, you can enter upto 3 characters. Valid Range: 10-300 seconds. Default: 10.
- **Print**: Select the check box to enable printing of the receipt from the Smart Client.
- **Send Email**: Select the check box to Email the receipt from the Smart Client.
- **Send SMS**: Select the check box to send the receipt over SMS from the Smart Client.

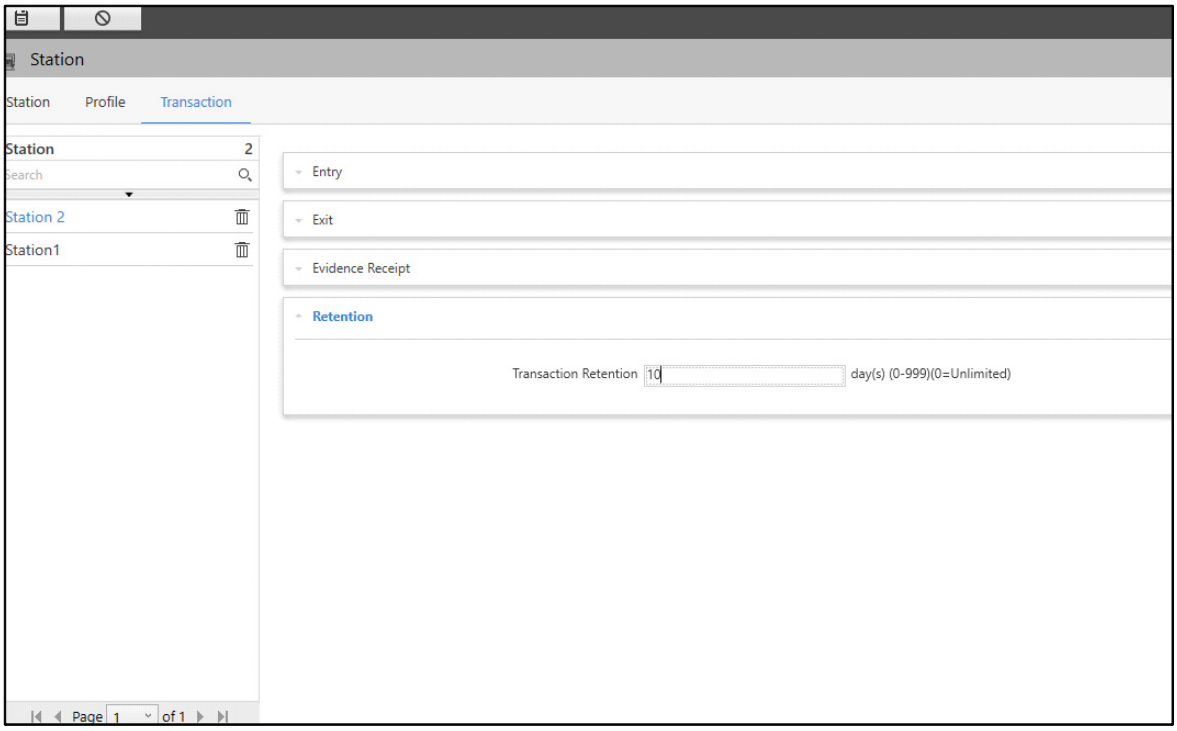
- Click **Save** to save the settings or click **Cancel** to discard.

Retention

This panel displays the Retention settings configured for the Transaction. Based on this configuration, the Transaction can be retained for required amount of time. This panel allows you to configure Retention for the entire Transaction.

To configure the Retention,

- Click the **Retention** collapsible panel.



Configure the following parameters:

- **Transaction Retention**: Specify the number of days till when the system should retain the Transaction records in the database. The records are deleted automatically once the configured time period expires. Valid Range: 0-999 days. Default: 0.

- Click **Save** to save the settings or click **Cancel** to discard.

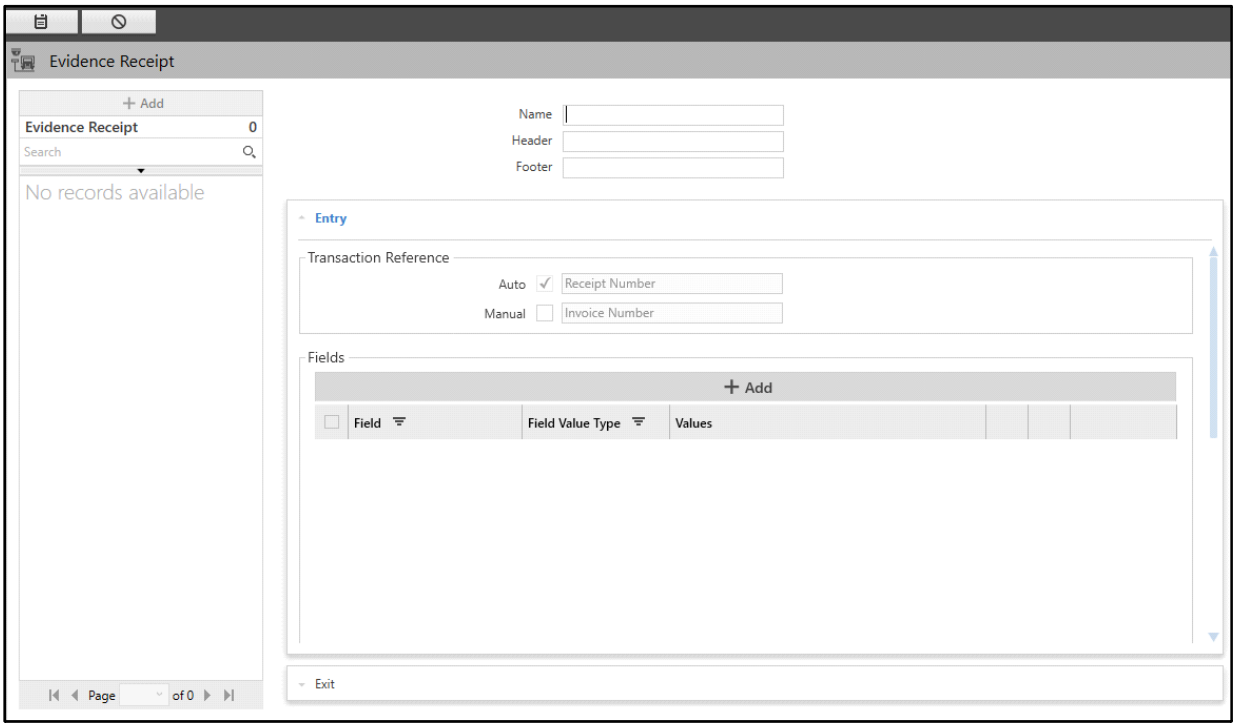
Evidence Receipt

The Weighbridge Application allows you to configure Evidence Receipt which consists of the entire Transaction record. This receipt is a proof of the whole loading and unloading process of goods between two stations. It holds the records of actual weight of goods, weight of loaded/empty vehicle, date and time of the Transaction, necessary snapshots, vehicle and user information etc.

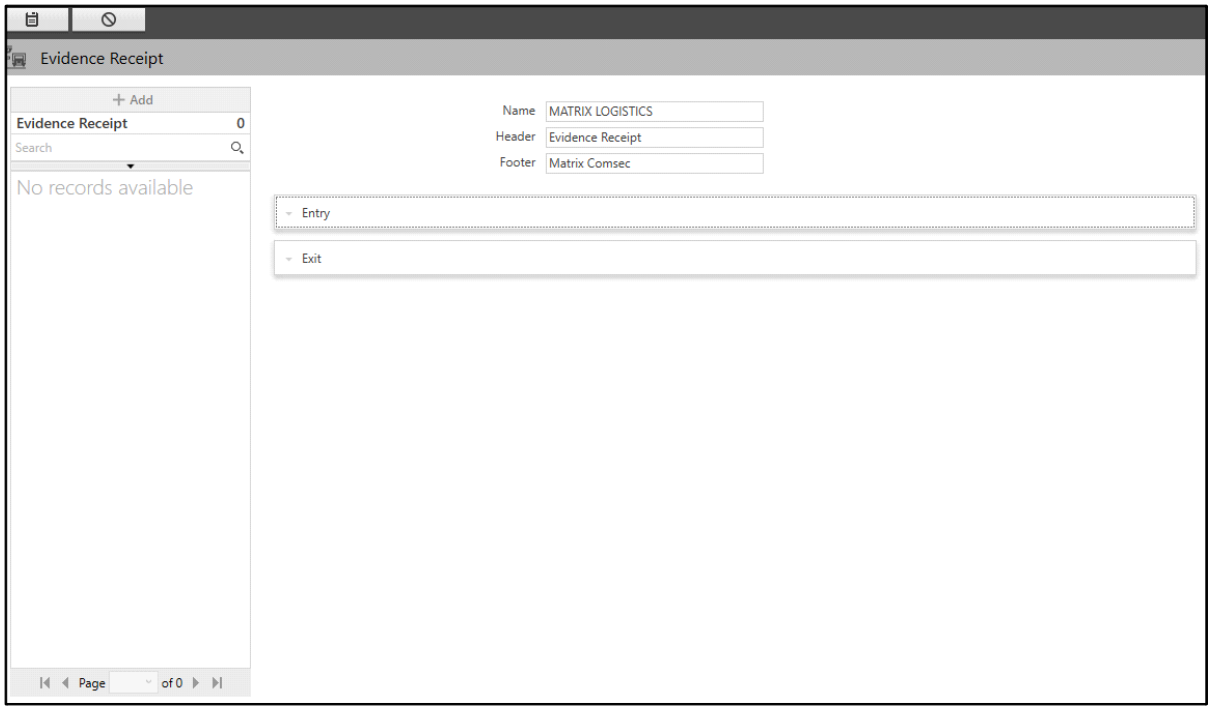
The Evidence Receipt page displays all the configured receipts. You can view and configure the Evidence Receipts from this page.

To configure Evidence Receipts,

- Click **Weighbridge Application > Evidence Receipt**.



- Click **Add**.



Configure the following parameters:

- **Name**: Specify a suitable name for the Evidence Receipt. In Name, you can enter upto 50 characters. Default: Blank.
- **Header**: Specify a suitable header for the Evidence Receipt. This will be printed on the top of the receipt. In Header, you can enter upto 50 characters. Default: Blank.
- **Footer**: Specify a suitable footer for the Evidence Receipt. This will be printed at the bottom of the receipt. In Footer, you can enter upto 50 characters. Default: Blank.

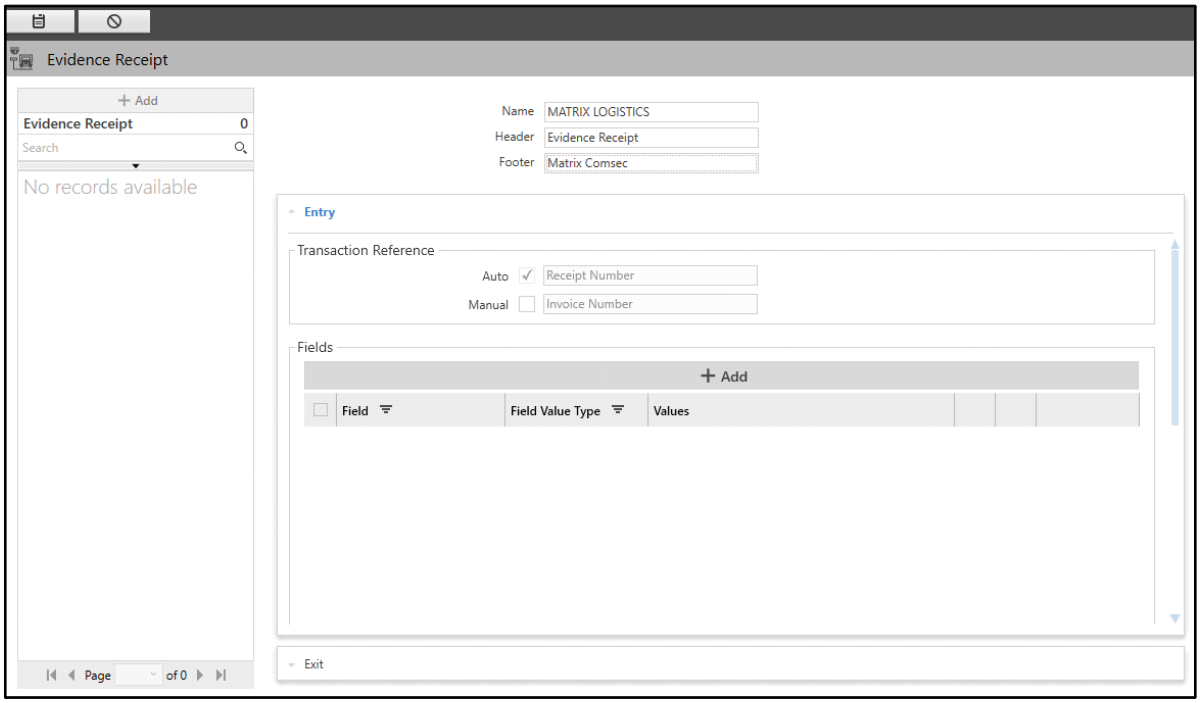
The Evidence Receipt page contains two collapsible panels — “Entry” and “Exit”.

Entry

This panel displays the Transaction Reference, Fields and Snapshots details related to Entry Transaction. This panel allows you to configure Transaction Reference, Fields and Snapshots details for Entry Transaction.

To configure the Entry Receipt fields,

- Click the **Entry** collapsible panel.



The Entry collapsible panel contains these sections — “Transaction Reference”, “Fields” and “Snapshots”.

Transaction Reference

This section displays the Transaction Reference for the Transaction Receipt. Transaction Reference is an identification of the Transaction Receipt.

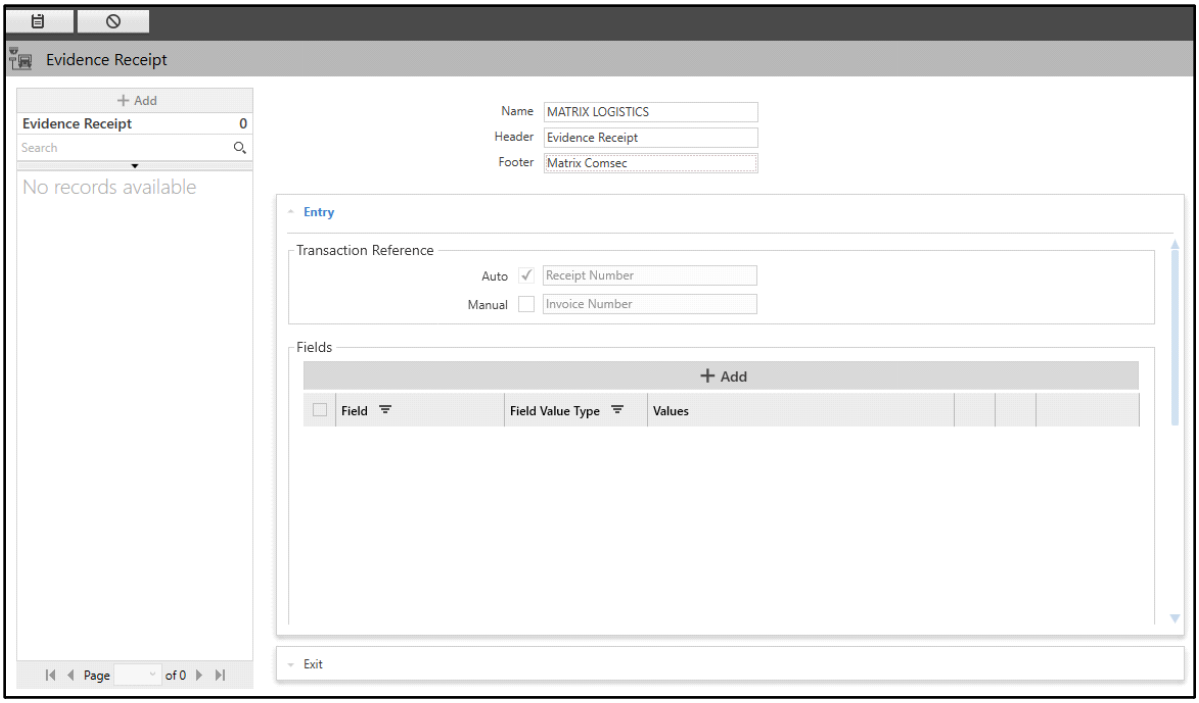
- **Auto**: It is selected and set by default as **Receipt Number.** It is a unique number generated by Weighbridge Application. It will be printed every time on the receipt when the monitoring authority approves or rejects the Entry transaction.

- **Manual**: Select the check box to enable the Manual reference for the Transaction. Specify the required reference. For example, Invoice Number. This will be printed on the receipt along with the Auto Transaction Reference, that is the Receipt Number.

If you select Manual Transaction Reference, Take Auto Action feature in Smart Client will not function.

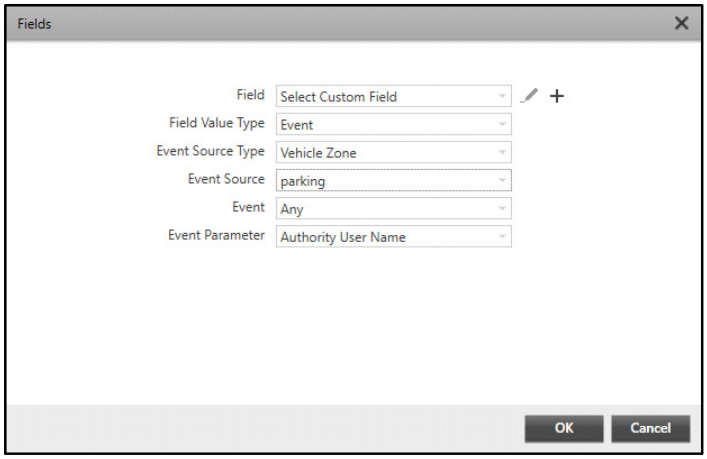
Fields

This section displays the custom fields configured for the Transaction Receipt. You can configure custom fields to display the necessary information on the Transaction Receipt.



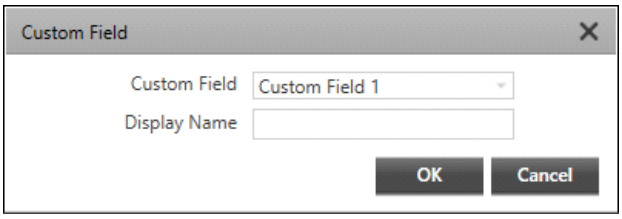
You can add upto 100 Custom Fields in Entry and Exit Transaction Receipt. However in the Evidence Receipt generated in Smart Client, the first 30 fields only will be displayed. Hence configure the fields accordingly.

- Click **Add**. The **Fields** pop-up appears.



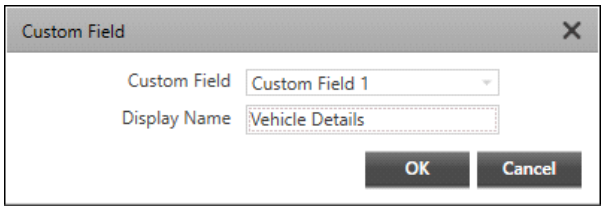
Configure the following parameters:

- **Field**: Select the desired custom field from the drop-down list. This field can be created from the "Custom Fields" or at the time of field selection for the Evidence Receipt. To do so,
  - Click **Add** + to add a new custom field. The **Custom Field** pop-up appears.



Configure the following parameters:

- **Custom Field**: Select the desired Custom Field against which you wish to configure the field.
- **Display Name**: Specify the desired Display Name for the Custom Field. In Display, you can enter upto 50 characters. Default: Blank.



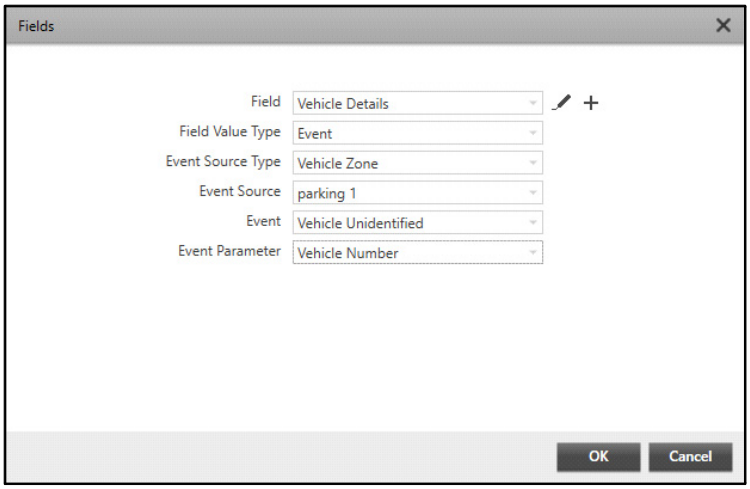
- Click **OK** to confirm or click **Cancel** to discard.

You can also edit the custom field after selection from the drop-down list.

- Click **Edit** to edit the custom field. The **Custom Field** pop-up appears.
- You can change the **Display Name** as desired.
- Click **OK** to confirm or click **Cancel** to discard.

- **Field Value Type**: Select the desired Field Value Type from the drop-down list — Event, Static, Manual, Expression or Weight.

  If you select **Event**, configure the following parameters:

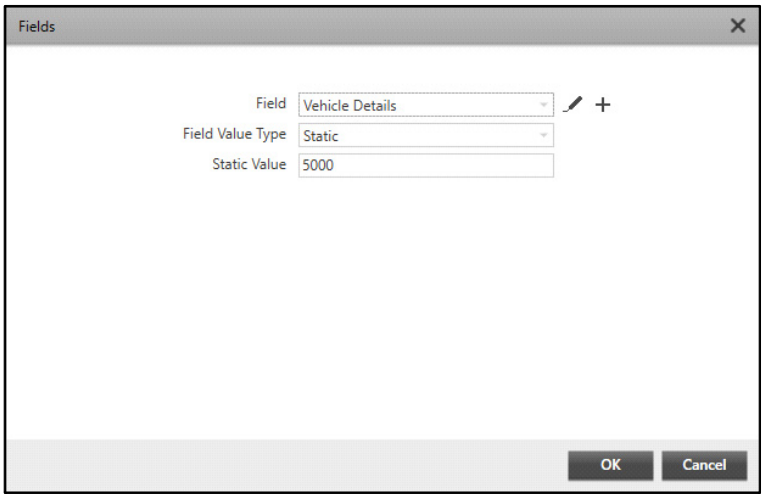


- **Event Source Type**: Select the desired Event Source Type from the drop-down list.

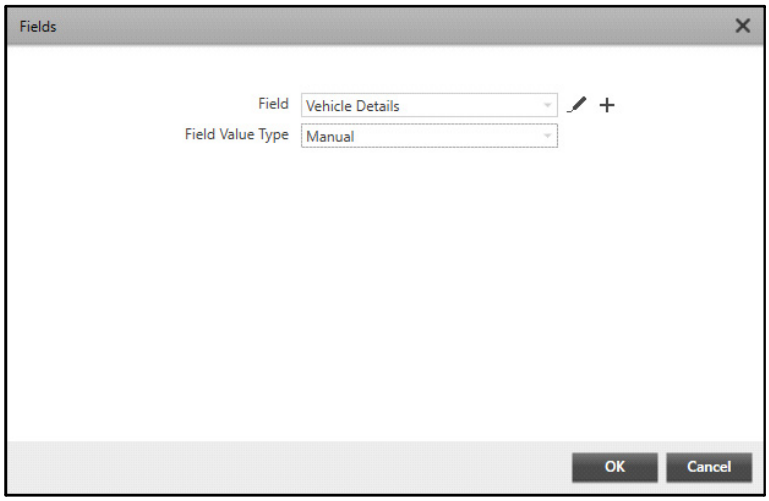
- **Event Source**: Select the desired Event Source from the drop-down list.
- **Event**: Select the desired Event from the drop-down list.
- **Event Parameter**: Select the desired Event Parameter from the drop-down list.

  If you select **Static**, configure the following parameters:

- **Static Value**: Specify the desired Static Value. This value cannot be edited or updated on the receipt.In Static Value, you can enter upto 50 characters. Default: Blank.

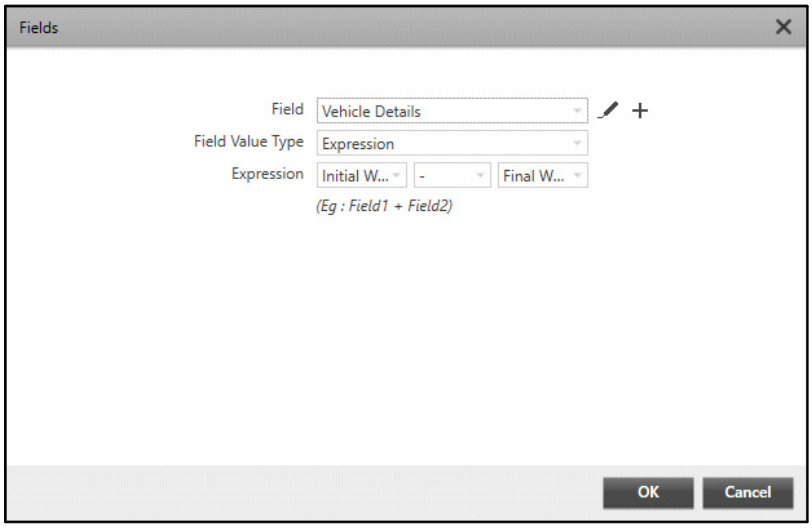


If you select **Manual**, the custom field value has to be entered manually through the Smart Client at the time of receipt generation. In Manual Value, you can enter upto 50 characters. Default: Blank.

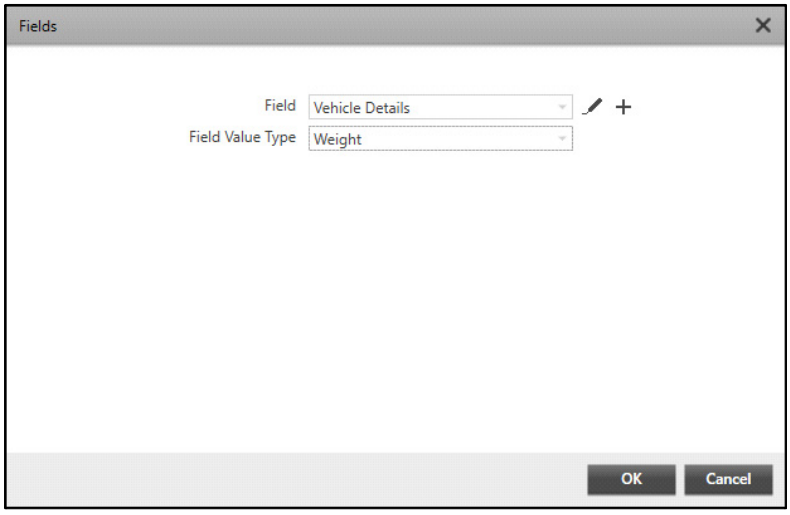


If you select **Expression**, configure the following parameters:

- **Expression**: Select the desired configured field from the drop-down list and select the mathematical expression between the expressions, that will result in the final value. For example, if you select Final Weight and Entry Weight as parameters and Subtraction (-) as the mathematical expression, the subtraction of both will give the Goods Weight.



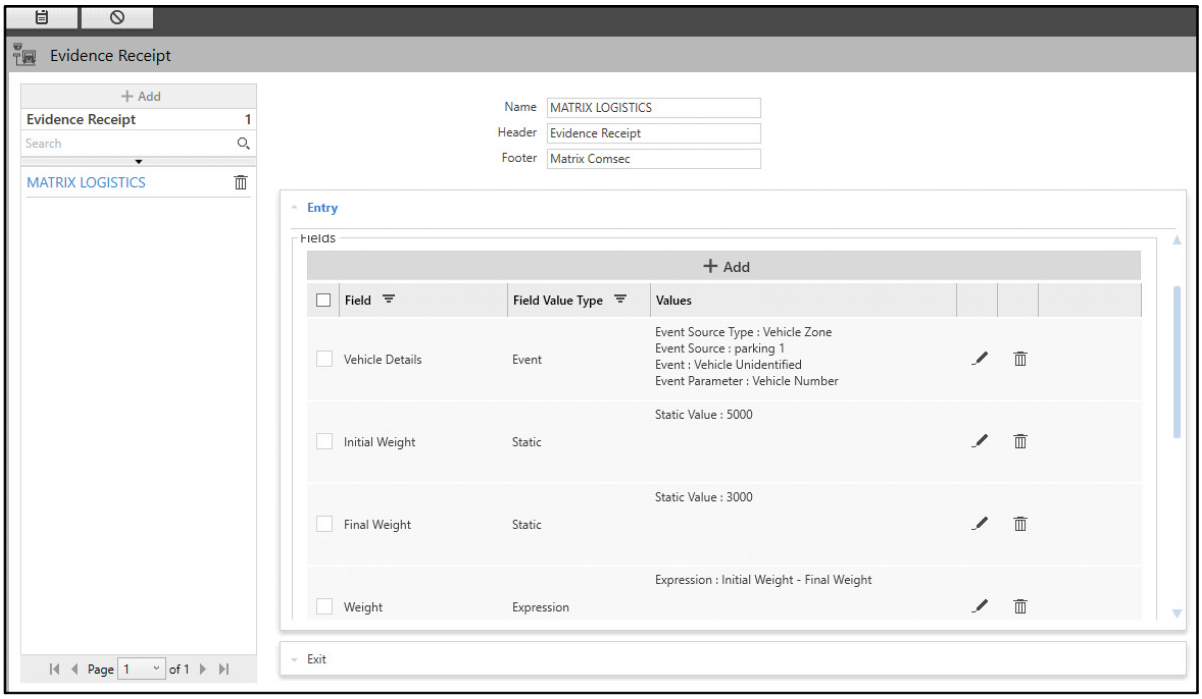
If you select **Weight**, the custom field value will be fetched from the Weight Detected Event.



- Click **OK** to save the Entry Fields configuration or click **Cancel** to discard.

The configured fields appear in a list.

You can edit the entry under Fields or delete it.



- Click **Edit** of the desired entry field. The **Fields** pop-up appears.



  - Edit the desired parameters.

- Click **OK** to confirm or click **Cancel** to discard.
- Click **Delete** to delete the Field.
- lick **Filter** of the respective parameter in the header row.

  Select the check box of the desired options and click outside the filter pop-up. The records appear as per the set filters.

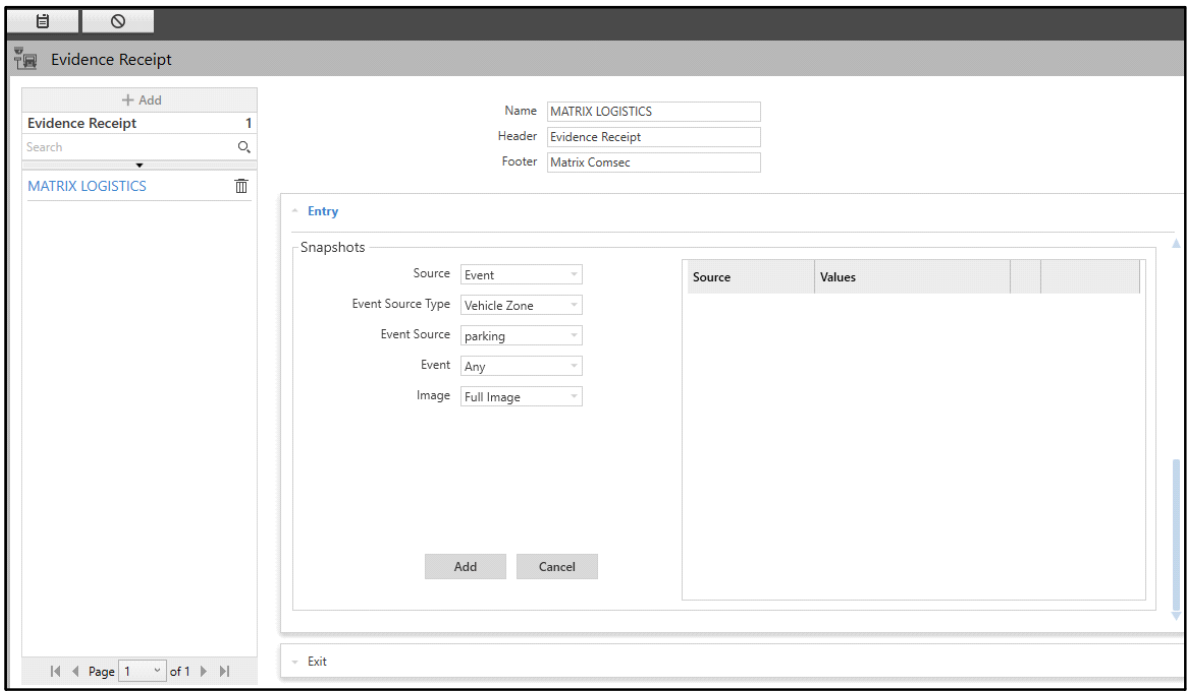
  To clear the filter, click **Filter** and then click **CLEAR FILTER**.

- You can also **Sort** records. To do so, click on the desired option in the header row. An arrow icon appears. Click on it. Records can be sorted in ascending or descending order.

- Click **Save** to save the settings or **Cancel** to discard.

Snapshots

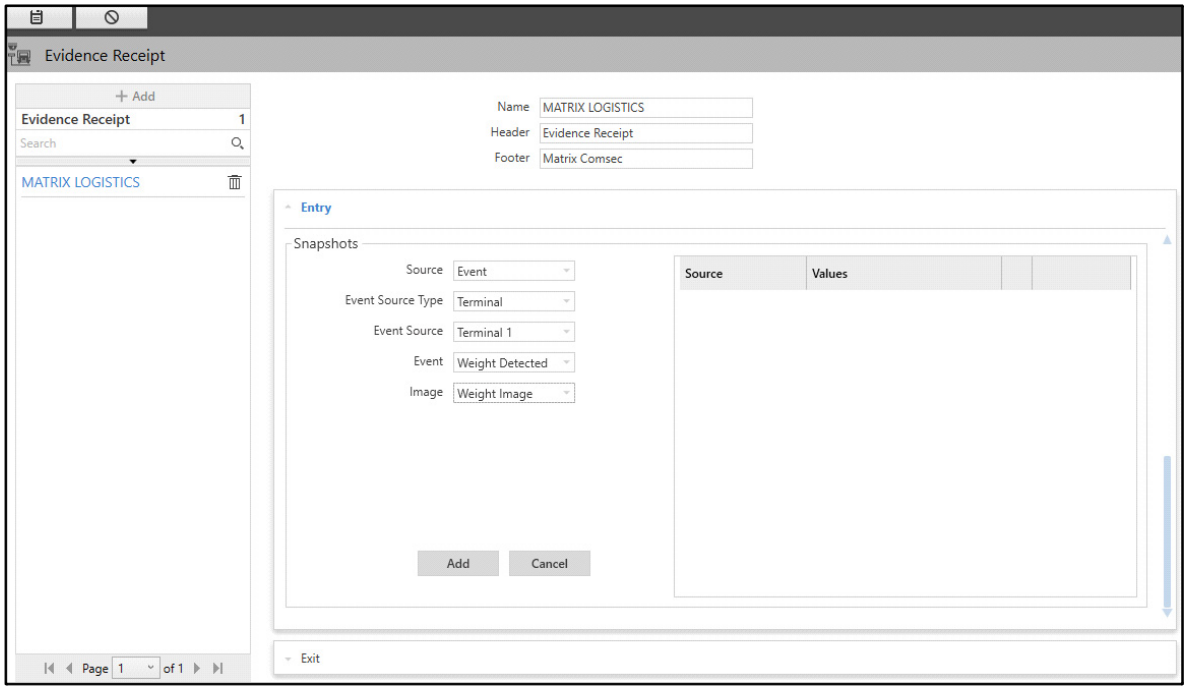
This section displays the Snapshot sources configured for the Transaction Receipt. You can configure Snapshots to display the desired images on the Transaction Receipt.



Configure the following parameters:

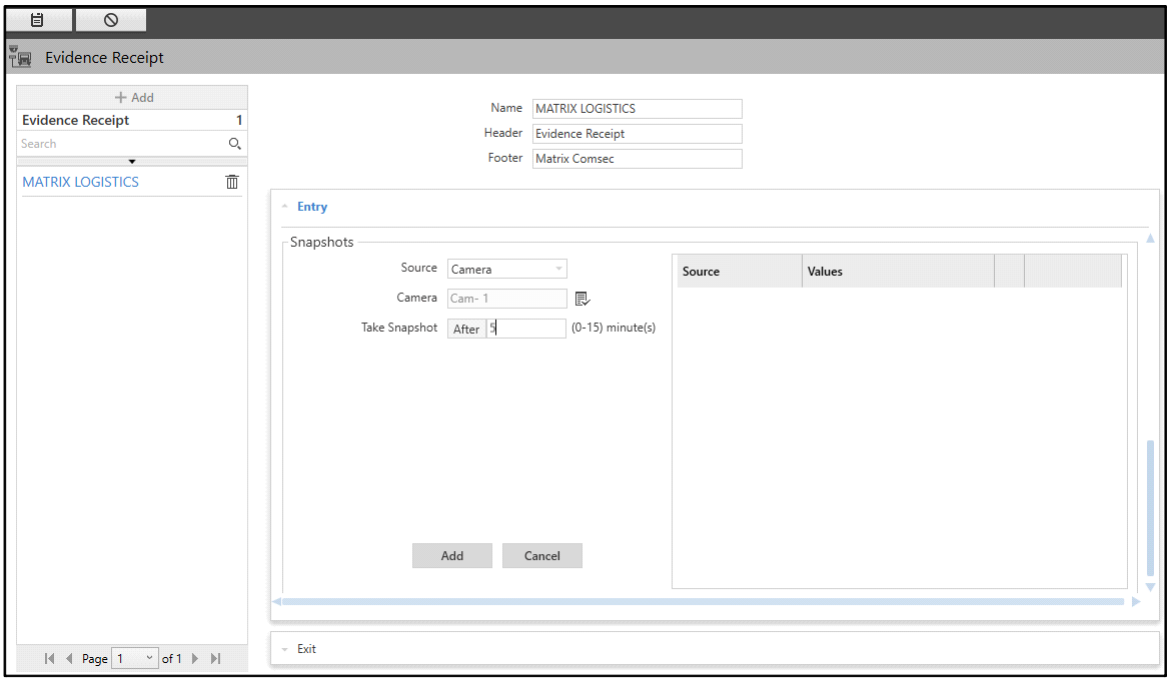
- **Source**: Select the desired Source for the Snapshots from the drop-down list — Event or Camera.

  If you select the source as **Event**, configure the following parameters:

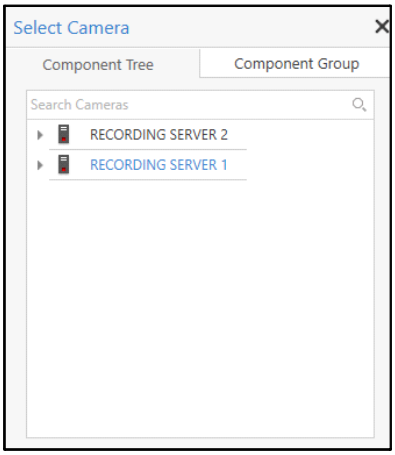


- **Event Source Type**: Select the desired Event Source Type from the drop-down list.
- **Event Source**: Select the desired Event Source from the drop-down list.
- **Event**: Select the desired Event from the drop-down list.
- **Image**: Select the desired type of Image from the drop-down list.

  If you select the source as **Camera**, configure the following parameters:

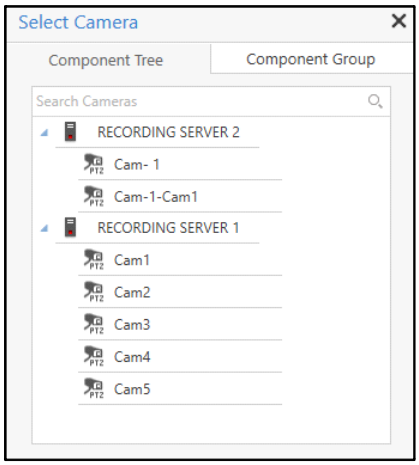


- **Camera**: Select the desired camera which you wish to assign to get the Snapshots using the **Camera** picklist.
    - Click **Camera** picklist. The **Select Camera** pop-up appears.



    - The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. Double click the desired camera. You can also search for the desired cameras using the **Search Cameras** search bar.

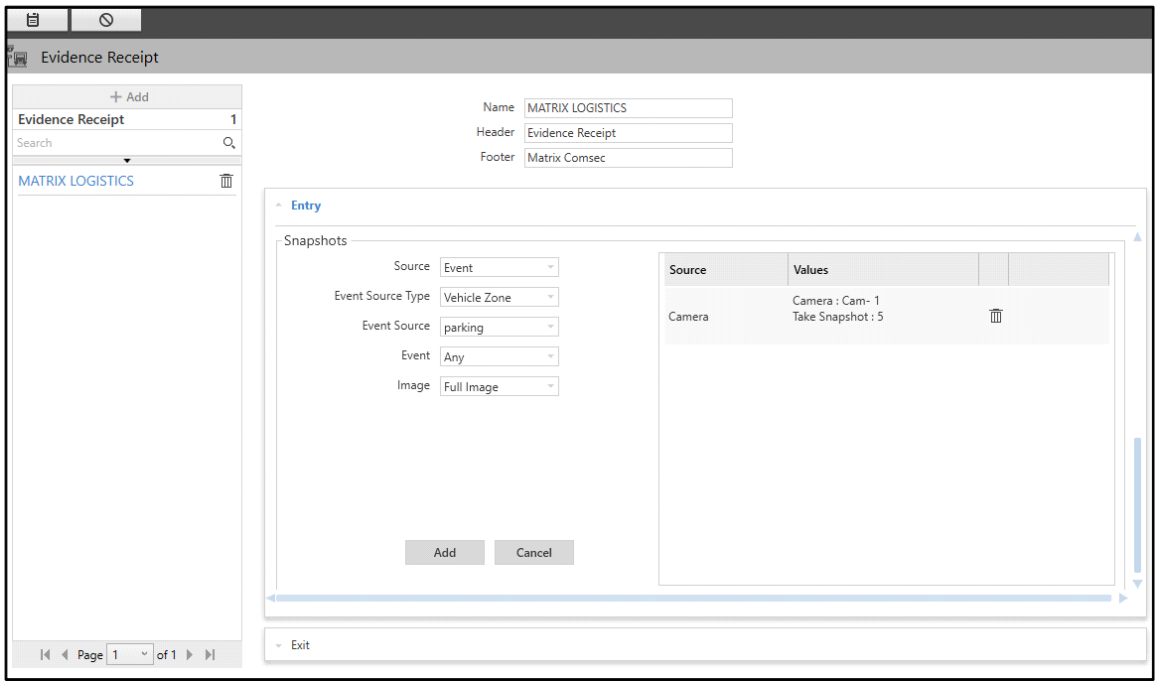
Mobile Camera will not be displayed in the list of cameras as Take Snapshot functionality is not supported by Mobile Cameras.



    - **Take Snapshot**: Specify the time in minutes after which the system should take a snapshot. Valid Range: 0-15 minutes. Default: 0.

- Click **Add** to add the Snapshot Source or click **Cancel** to discard.

The new Snapshot Source will appear in a list on the right hand side. You can only Delete the added Snapshot Source.



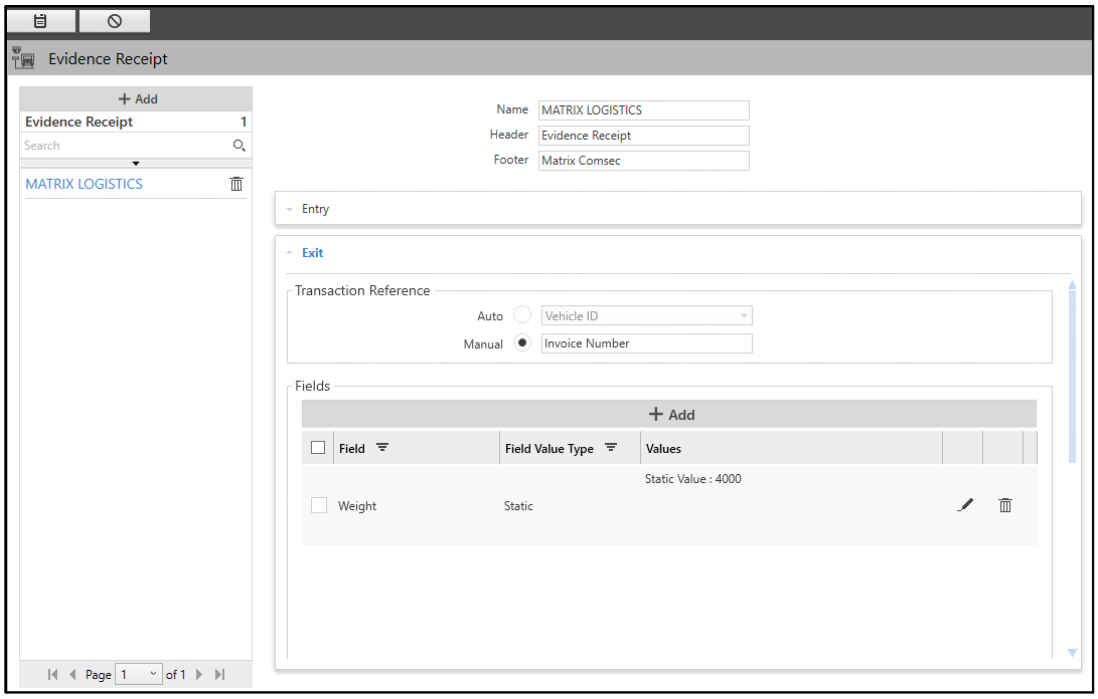
- Click **Delete** to delete the Snapshot Source.
- Click **Save** to save the settings or **Cancel** to discard.

Exit

This panel displays the Fields and Snapshots details related to Exit Transaction. This panel allows you to configure Fields and Snapshots details for Exit Transaction.

To configure the Exit receipt fields,

- Click the **Exit** collapsible panel.



The Exit collapsible panel contains these sections — Transaction Reference, Fields and Snapshots.

For Transaction Reference, refer to "Transaction Reference". The configurations of Fields and Snapshots for Exit collapsible panel are similar to that of the Entry collapsible panel. For more details, refer to "Fields" and "Snapshots".

Transaction Reference

This section displays the Transaction Reference for the Transaction Receipt. Transaction Reference is an identification of the Transaction Receipt. You can select either Auto or Manual options.

- **Auto**: Select the option if you wish to set the Transaction Reference as Auto. Select the desired Reference from the drop-down list. The selected Reference will be printed every time on the receipt when the monitoring authority approves or rejects the Exit Transaction.

In Transaction Reference,

- *User ID is the COSEC User ID (If the Database Type is Cosec) or SAMAS User ID (if the Database Type is Custom). For details, refer to "User Profiles".*
- *Vehicle ID is the Vehicle Number Plate as detected in Vehicle Detection Event. For details, refer to "Events" in "Vehicle Management-Zone"*

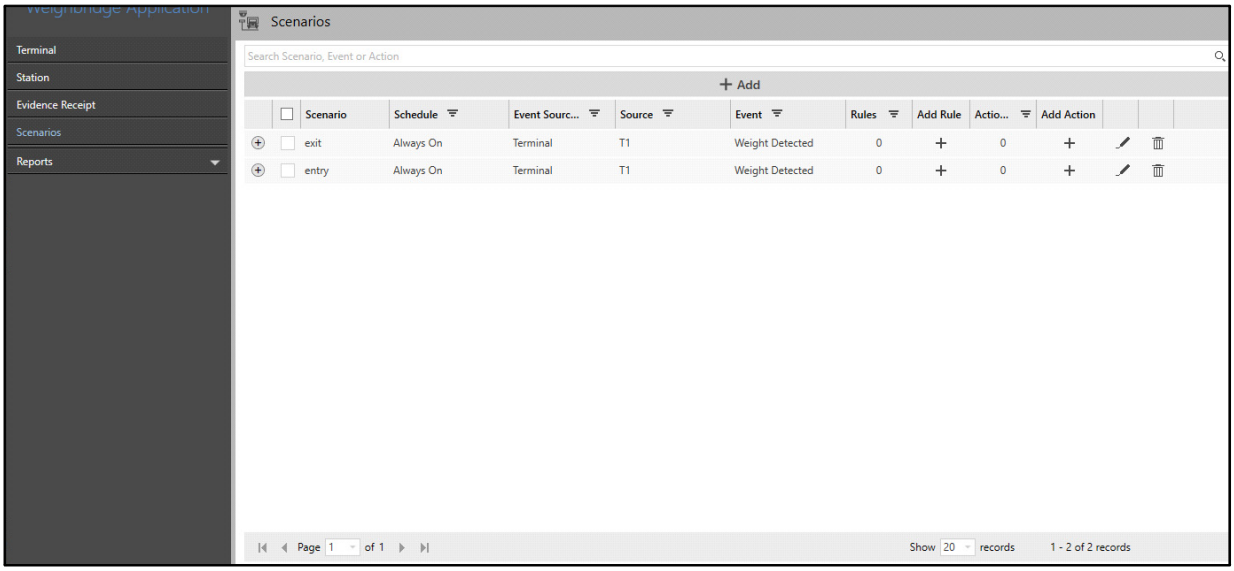
- **Manual**: Select the option to enable the Manual reference for the Transaction. Specify the required reference. For example, Invoice Number. This will be printed on the receipt when it is generated.
- Click **Save** to save the settings or **Cancel** to discard.

Scenarios

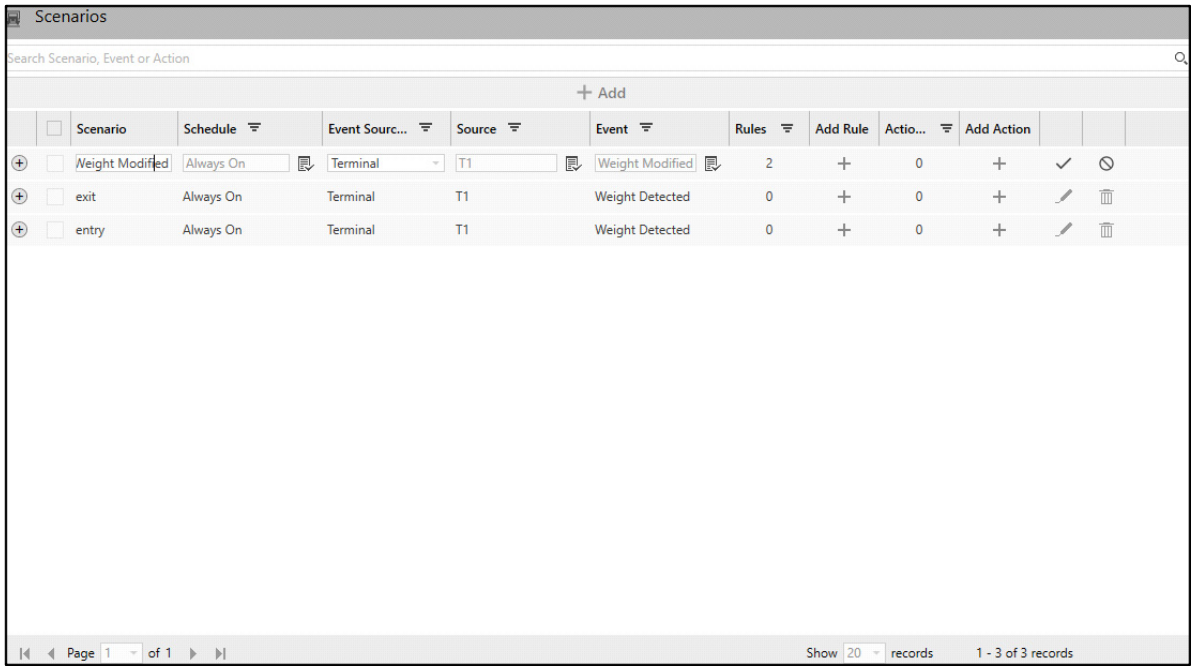
In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send SMS) on Events occurring at certain sources (For example, Entry Transaction Rejected). The Scenarios page displays all the configured Scenarios for Weighbridge Application. You can view and configure the Scenarios for all the configured Terminals and Stations.

To configure Scenarios,

- Click **Weighbridge Application > Scenarios**.



- Click **Add.**



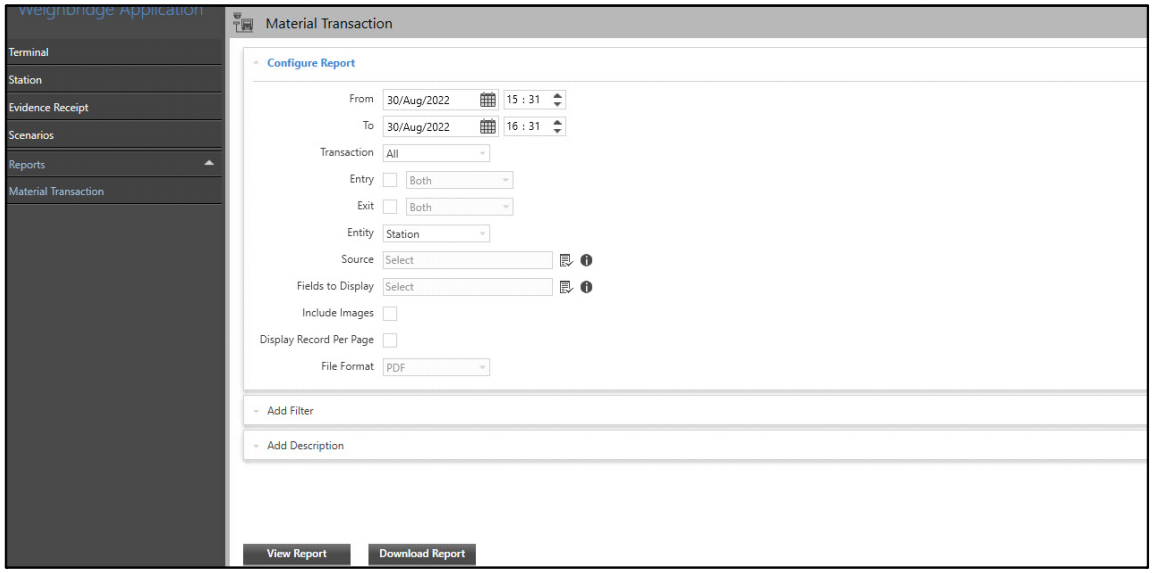
The configurations of Scenarios for Weighbridge Application are similar to the Basic Scenario. For details, refer to “Basic Scenario”.

Reports

The Material Transaction Report provides statistics on the Transactions that occurred during the selected time period. The Material Transaction page enables you to configure parameters for Material Transaction Reports. You can view and configure Material Transaction Reports on Monthly, Daily and Hourly basis.

To configure Material Transaction Report,

- Click **Weighbridge Application > Reports > Material Transaction**.



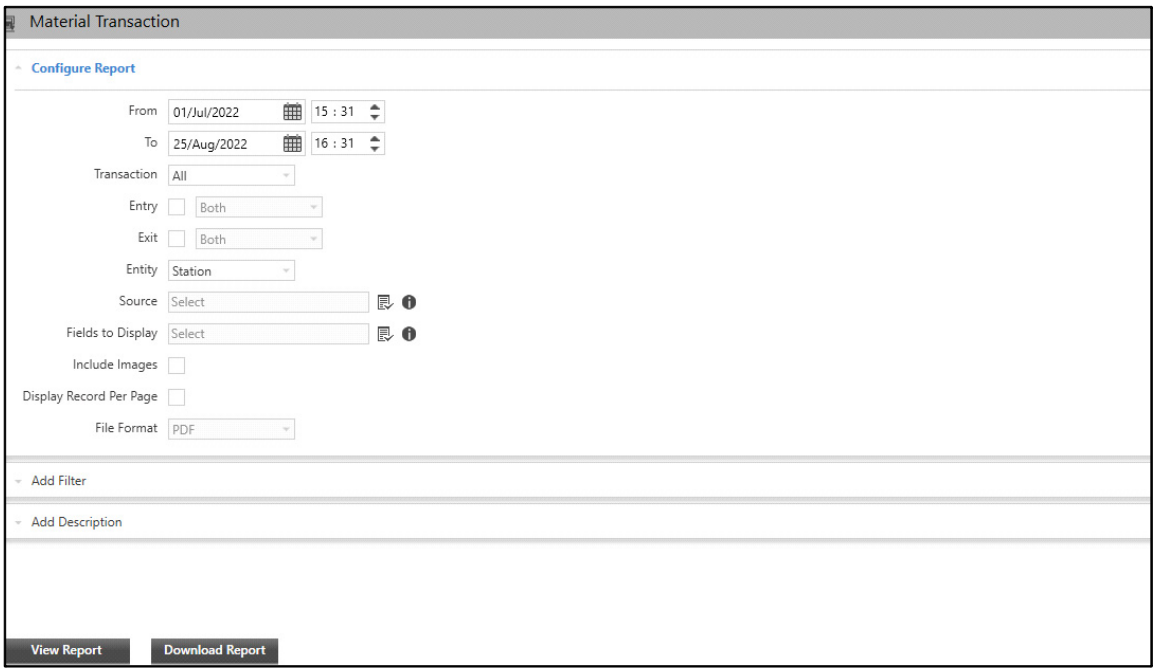
The Material Transaction page contains three collapsible panels — “Configure Report”, “Add Filter” and “Add Description”.

Configure Report

This panel displays the report configurations. You can edit and configure the Material Transaction Report from this collapsible panel.

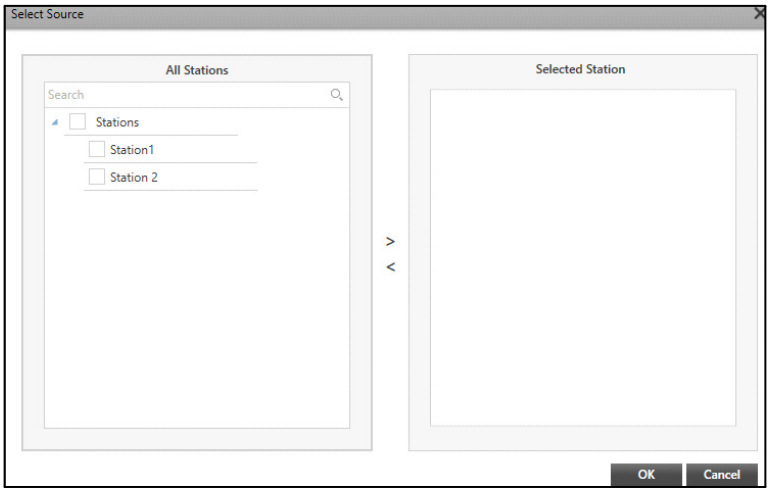
To configure the report parameters,

- Click the **Configure Report** collapsible panel.



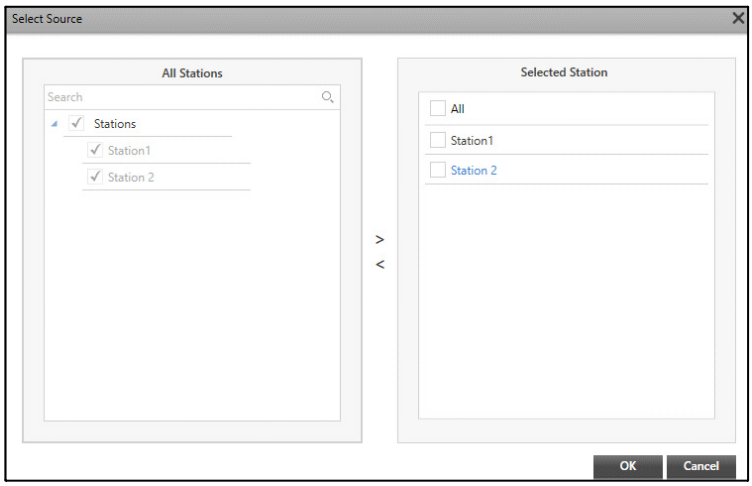
Configure the following parameters:

- **From**: Select the date from the calendar and set the time from when you wish to generate the Transaction records. Valid Range: 00:00-23:59. Default: Blank.
- **To**: Select the date from the calendar and set the time till when you wish to generate the Transaction records. Valid Range: 00:00-23:59. Default: Blank.
- **Transaction**: Select the desired Transactions for which you wish to generate the report from the drop-down list.
- **Entry**: Select the check box to generate the report for Entry Transactions. Select the desired Entry Transactions which you wish to include in the report.
- **Exit**: Select the check box to generate the report for Exit Transactions. Select the desired Exit Transactions which you wish to include in the report.
- **Entity**: Select the desired Entity from the drop-down list — Terminal or Station.
- **Source**: Select the desired Source to be included in the report using the **Source** picklist.
    - Click **Source** picklist. The **Select Source** pop-up appears.

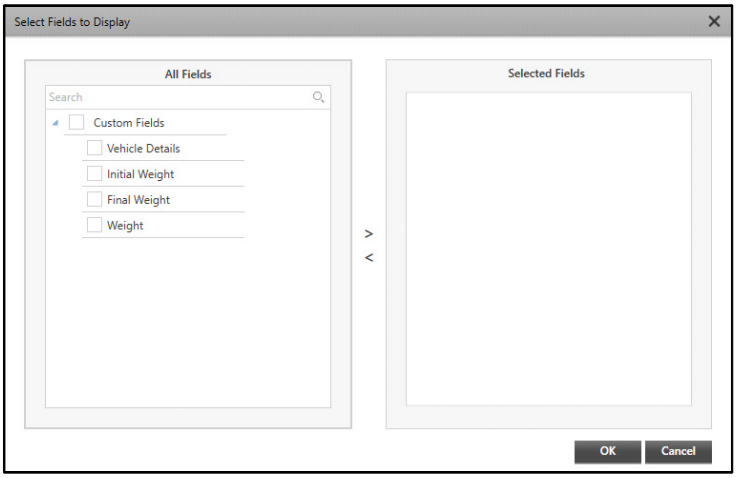


- Select the check boxes of the desired Stations or Terminals you wish to add from the **All Stations** or **All Terminals** list. Click the right arrow button to add these Stations or Terminals in the **Selected Station** or **Selected Terminal** list. You can also search for the desired Stations or Terminals using the search bar.

  To remove fields, select the check boxes of the desired Stations or Terminals you wish to remove from the Selected Station or Selected Terminal list. Click the left arrow button to remove the fields from the Selected Station or Selected Terminals list.

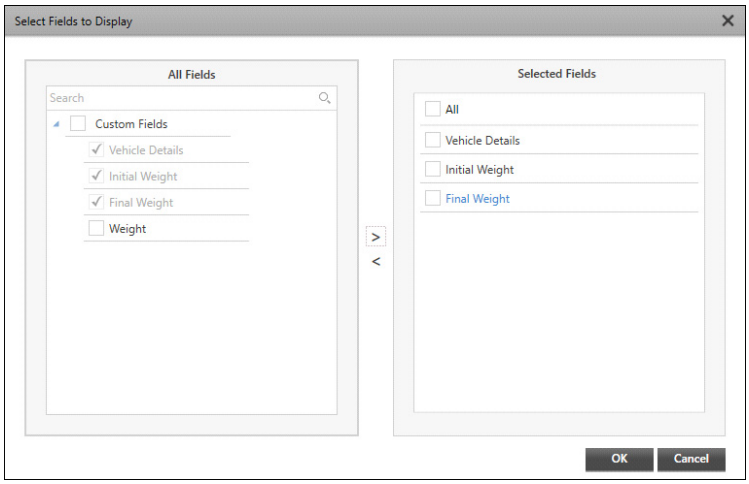


  - Click **OK** to confirm or click **Cancel** to discard.
  - **Fields to Display**: Select the desired fields which you wish to include in the report using the **Fields to Display** picklist.
    - Click **Fields to Display** picklist. The **Select Fields to Display** pop-up appears.



- Select the check boxes for the desired fields you wish to add from the **All Fields** list. Click the right arrow button to add these fields in the **Selected Fields** list. You can also search for the desired fields using the search bar.

  To remove fields, select the check boxes of the desired fields you wish to remove from the Selected Fields list. Click the left arrow button to remove the fields from the Selected Fields list.



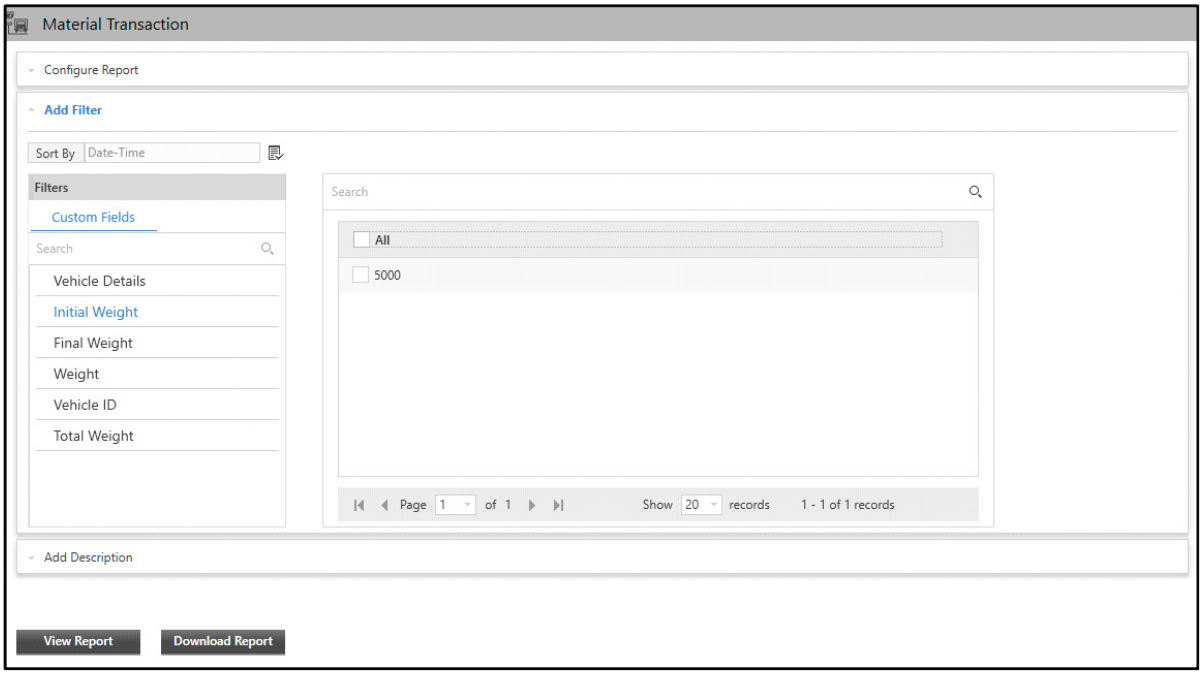
- Click **OK** to confirm or click **Cancel** to discard.
- **Include Images**: Select the type of images that you wish to include in the report using the drop-down list.
- **Display Record per Page**: Select the check box to display each record for the selected fields on a new page.
- **File Format**: Select the desired File Format in which you wish to generate the report from the drop-down list.

Add Filter

This panel allows you to add filters for the Report once the report configurations are done. These filters sort and arrange the report data as per the selected parameters.

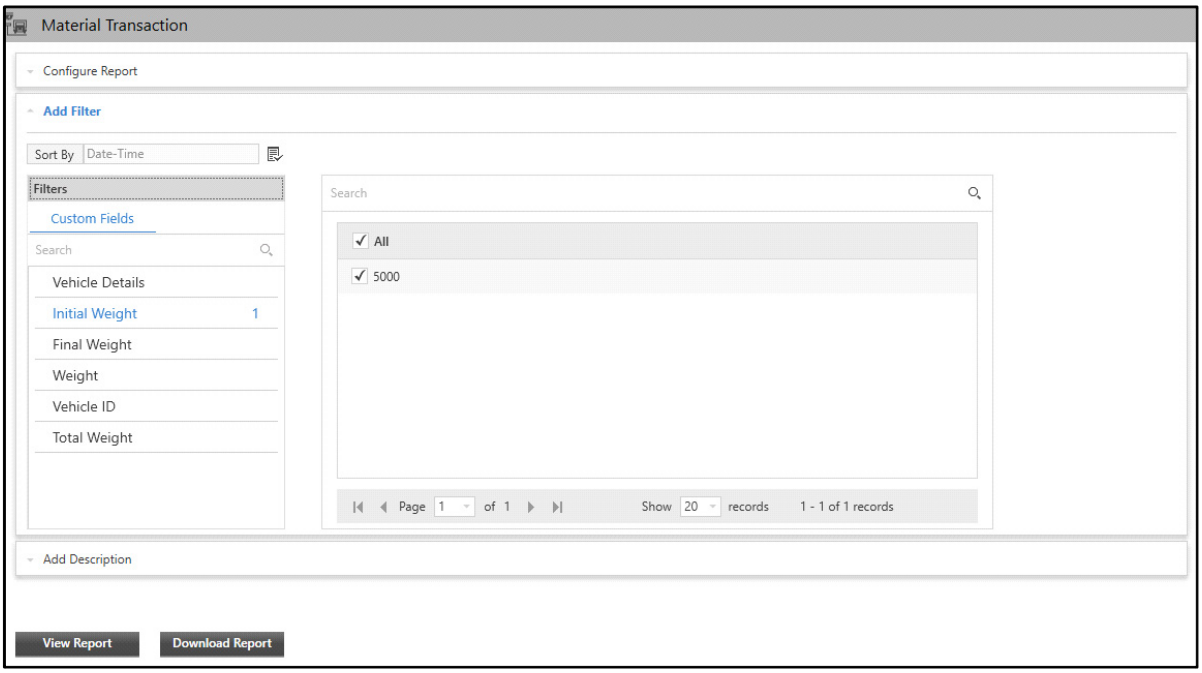
To configure the Filters,

- Click the **Add Filter** collapsible panel.



Configure the following parameters:

- **Sort By**: Select the parameter by which you wish to sort the report data from Event Details in the report using the **Sort By** picklist. Double-click to select the desired option. By default, the sorting is done as per the Date and Time of the Event Occurrence.
- **Filters**: You can get the desired data for the report using Filters. The Filters section displays all the Event Details. Select the tab to view the associated parameters.
  - Click the desired parameter to view the associated entities with the selected Event. For example, if you select Weight Difference as the associated option. In available options for the same are displayed on the right hand side. Select the desired entities to include in the report.



Add Description

This panel allows you to add a description for the Material Transaction Report once the report configurations are done. This description is visible in the generated report

To view and edit the description,

- Click the **Add Description** collapsible panel.



- Enter the desired description for the report you wish to generate. In Description you can enter upto 2000 characters only and it is displayed on the second page of the report. Default: Blank.

Once the report configurations are done and description is added, you can either View or Download the report.

- Click **View Report** to view the report.
- Click **Download Report** to download the report. The report will be saved at the configured storage path.

CHAPTER 16

Scenario Events With Actions

In Admin Client, you can configure Scenarios to trigger a set of actions (For example, Send SMS) on Events occurring at certain sources (For example, Storage Drive Full). You can configure Events and Actions based on Scenarios. You can configure Scenarios from the respective modules or from the CREAM module.

After configuring the Scenario, you can configure various Actions to be triggered on Event occurence. To add Actions, refer to “Configuring Actions for Events”.



The user’s accessibility of various features in the modules depends on the rights — Application, Configuration, Media, Entity, Report — assigned to the User Group of the user. Make sure the User Groups are assigned rights according to the access you wish to provide. For details refer to “User Groups”.

All the Events that can be configured against each Event Source Type have been listed in a table in the next Section. Refer the following links for the module-wise Event table:

- “Servers and Devices Events”
- “Access Control Events”
- “Perimeter Management Events”
- “Parking Management Events”
- “Crowd Management Events”
- “Person Identification Events”
- “Vehicle Management Events”
- “Weighbridge Application Events”
- “Other Events”

Servers and Devices Events

Management Server Events	Recording Server Events	IVA Server Events	License Server Events	Device Events	Camera Events	Sensors and Alarm Events
-CPU Usage Exceeded -CPU Usage Normal -CPU Usage Critical -Memory Usage Exceeded -Memory Usage Normal -Memory Usage Critical -Drive Available -Drive Unavailable -Drive Inaccessible -Drive Error -Storage Normal -Storage Full -Storage Memory Low -Recording Request Sent -Recording Request Failed -Email Request Sent -SMS Request Sent -Set PTZ Position Request Sent -Generate File Request Sent -Generate File Request Failed -Import File Request Sent -Import File Request Failed -File Entry Failed -User Logout -User Login -Access Duration -User Deleted -Entity Deleted -Config Change -Evidence Unlocked -Vehicle Enrolled -Bookmark Unlocked	-Server Connected -Server Disconnected -CPU Usage Exceeded -CPU Usage Normal -CPU Usage Critical -Memory Usage Exceeded -Memory Usage Normal -Memory Usage Critical -Degradation Started -Degradation Stopped -Drive Available -Drive Unavailable -Drive Inaccessible -Drive Error -Storage Normal -Storage Full -Storage Memory Low -File Generation Started -File Generation Completed -File Generation Failed -File import Started -File Import Completed -File Import Failed -File Deleted -File Deletion Failed -Server Stopped -Server Started -Recording Overwriting Started - Recording Overwriting Completed	- Server Disconnected - Server Connected - CPU Usage Exceeded - CPU Usage Normal -CPU Usage Critical - Memory Usage Exceeded - Memory Usage Normal -Memory Usage Critical - Server Stopped - Server Started -Vehicle Detection Failed -Failed To Load GPU Model Library	-Server Connected -Server Disconnected -License Dongle Connected -License Dongle Disconnected -SSL Certificate Expired -SSL Certificate Switched to Default	- Device Connected - Device Disconnected - Storage Normal - No Disk - Storage Full - Storage Memory Low - Storage Fault - Storage Busy - Device Configuration Change - Under Maintenance - Restored	- Camera Connected - Camera Disconnected - Recording Failed - Recording Started - Recording Stopped - Backup Failed - Backup Started - Backup Completed - Archive Failed - Archive Started - Archive Completed - Import Recording Failed - Import Recording Started - Import Recording Completed - Download Failed - Download Started - Download Completed - Motion Started - Motion Stopped - Camera Tampered - Audio Exception - Intrusion Detection - Trip-Wire Detection -Day Highlights Started -Day Highlights Stopped -Day Highlights Failed - Recording Retention Started - Recording Retention Completed - Recording Retention Failed - Backup Retention Started - Backup Retention Completed - Backup Retention Failed - Archive Retention Started - Archive Retention Completed - Archive Retention Failed - Day Highlights Retention Started - Day Highlights Retention Completed - Day Highlights Retention Failed - PTZ Tour Stopped - Schedule PTZ Tour Started -Manual PTZ Tour Started - PTZ Tour Request Failed - PTZ Tour Deleted - PTZ Tour Paused - PTZ Tour Resumed - Recording Unavailable - Clip Capture Started - Clip Capture Completed - Clip Capture Failed - Clip Capture Retention Started	- Sensor Active - Alarm Output Normal - Alarm Output Active

Management Server Events	Recording Server Events	IVA Server Events	License Server Events	Device Events	Camera Events	Sensors and Alarm Events
-Image Migration Failed -Event Log Retention Started -Event Log Retention Completed -Login Failed -Server Started -Server Stopped -SSL Certificate Expired -SSL Certificate Switched to Default -Virtual License Validation Failed -WhatsApp Message Request Sent -Event Shared	-Recording Overwriting Failed -SSL Certificate Expired -SSL Certificate Switched to Default				- Clip Capture Retention Completed - Clip Capture Retention Failed -Image Retention Started -Image Retention Completed -Image Retention Failed - Manual Recording Started - Manual Recording Stopped - People In/Out - Vehicle In/Out -Push Video Started -Push Video Stopped -Pushed Snapshot	

Failover Server Events	Transcoding Server Events	ONVIF Server Events
-Server Connected -Server Disconnected -CPU Usage Exceeded -CPU Usage Normal -CPU Usage Critical -Memory Usage Exceeded -Memory Usage Normal -Memory Usage Critical -Degradation Started -Degradation Stopped -Drive Available -Drive Unavailable -Drive Inaccessible -Drive Error -Storage Normal -Storage Full -Storage Memory Low -Server Stopped -Server Started -Server Active -Server Normal -Recording Overwriting Started - Recording Overwriting Completed -Recording Overwriting Failed -SSL Certificate Expired -SSL Certificate Switched to Default	-Server Connected -Server Disconnected -CPU Usage Exceeded -CPU Usage Normal -CPU Usage Critical -Memory Usage Exceeded -Memory Usage Normal -Memory Usage Critical -Server Stopped -Server Started	-Server Connected -Server Disconnected -CPU Usage Exceeded -CPU Usage Normal -CPU Usage Critical -Memory Usage Exceeded -Memory Usage Normal -Memory Usage Critical -Server Stopped -Server Started

Access Control Events

Event Source Type	Events
Access Control Device	User Allowed User Denied Dead-Man Timer Expired Alarm Panic Alarm Door Abnormal Door force open Tamper Alarm Door Status Changed Duress Detection
Aux Input	AUX Input Active AUX Input Normal
Aux Output	Aux Output Active Aux Output Normal

Perimeter Management Events

Event Source Type	Events
Perimeter-Intrusion Zone	Intrusion In Intrusion Out
Perimeter-Security Line	Trip-Wire In Trip-Wire Out Tailgating
Perimeter-Zone	Camera Tampered Missing Object Motion Started Motion Stopped No Motion Loitering Detection Object Detected

Parking Management Events

Event Source Type	Events
Parking Slot	Unauthorized Parking Improper Parking Prohibited Parking Slot Available Slot Occupied Vehicle Overstay Parking After Closing Hours Vehicle Number Modified
Parking Premises	Vehicle In Vehicle Out Parking Premises Available Parking Premises Full Parking Premises Empty
Parking Driveway	Wrong Way Detection Vehicle Number Modified
Parking Entities (Slot Group, Lane, Area, Level, Facility)	Slot Group Full Lane Full Area Full Level Full Facility Full

Crowd Management Events

Event Source Type	Events
Crowd-Premises	Premises Available Premises Full Premises Empty People In People Out

Person Identification Events

Event Source Type	Events
Person Identification	Face Detection

Vehicle Management Events

Event Source Type	Events
Vehicle-Vehicle Zone Events	Vehicle Detection Vehicle Authorized Vehicle Unauthorized Vehicle Auto-Authorized Vehicle Auto-Unauthorized Vehicle Number Modified Vehicle Identified Vehicle Unidentified Blacklisted Vehicle Identified Whitelisted Vehicle Identified Suspected Vehicle Identified Approved Vehicle Identified Rejected Vehicle Identified Active User Identified Inactive User Identified Blacklisted User Identified

Weighbridge Application Events

Event Source Type	Events
Terminal	Weight Detected Weight Modified
Station	Entry Transaction Initiated Exit Transaction Initiated Entry Transaction Approved Exit Transaction Approved Entry Transaction Rejected Exit Transaction Rejected Transaction Retention Started Transaction Retention Completed

Other Events

The following Events can be configured only from the CREAM module.

Event Source Type	Events
Manual Trigger Event	Events configured in the **General Settings > Manual Trigger** will be listed here.
Emergency Event	Emergency
Scenario	Events configured in **CREAM > Advanced Scenario** will be listed here.

Event Source Type	Events
Custom Events	Events configured in the **General Settings > Custom Events** will be listed here. **Note:** *Custom Events feature is supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.*

Configuring Actions for Events

Configuring Actions for Events enables you to configure when and how the action must occur when the Event occurs. These configurations may generally include setting up a schedule, selecting target users, selecting Message Templates for notification etc. The Actions appear in a different order for different Scenarios. You can also sort the actions to arrange them in alphabetical order. The configurations may vary for each action for as per the Event selected in the Scenarios.

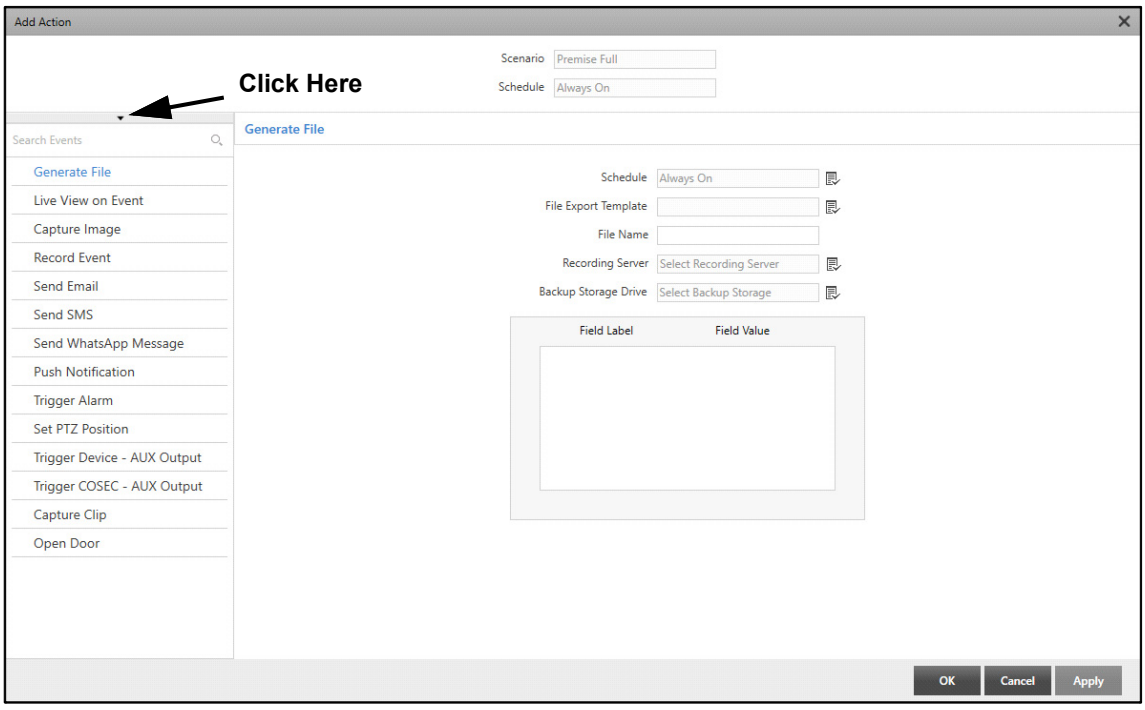
Refer to the following links for the configuration details of different system-defined Actions.

Actions for Basic Scenario

- "Capture Clip"
- "Capture Image"
- "Generate File"
- "Live View on Event"
- "Open Door"
- "Push Notification"
- "Record Event"
- "Send Email"
- "Send SMS"
- "Send WhatsApp Message"
- "Set PTZ Position"
- "Trigger Alarm"
- "Trigger COSEC - AUX Output"
- "Trigger Device - AUX Output"

You can sort the actions alphabetically. To do so,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.



- Click ▼ to sort the actions alphabetically.

Actions for Advanced Scenario

Advanced Scenarios includes all the Actions for Basic Scenarios as well as the following:

- “Import File”
- “Trigger IVA Detection”
- “Wait”
- “Push Notification”

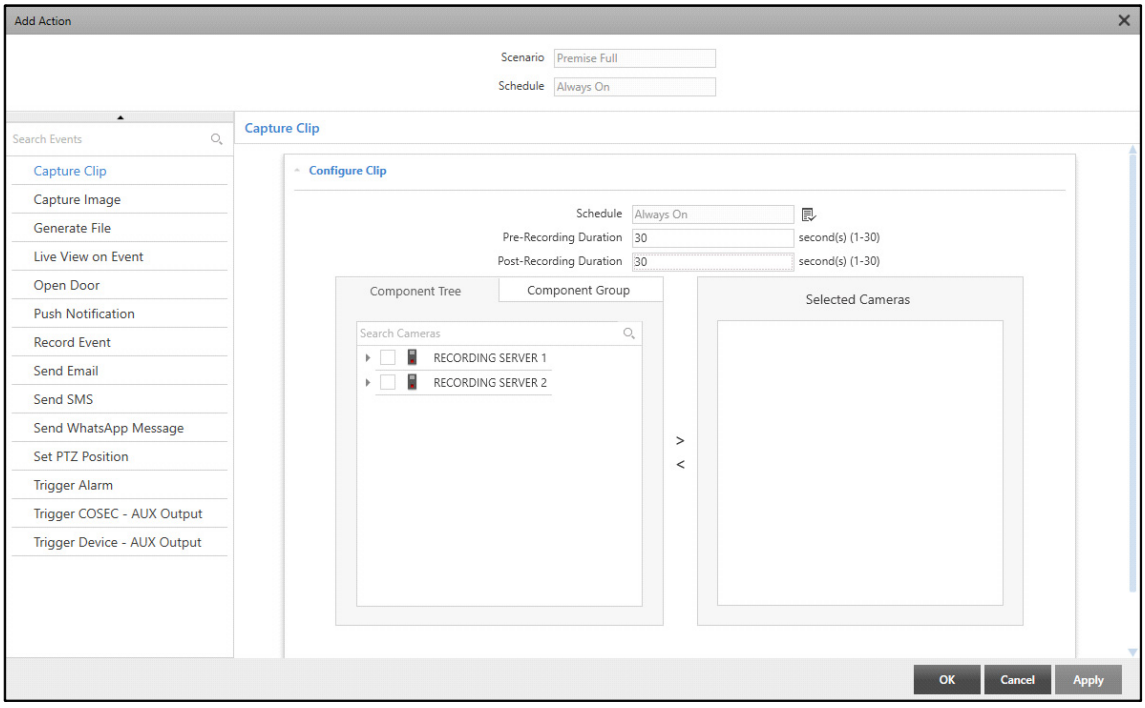
Actions for Basic Scenario

Capture Clip

The Capture Clip action captures a clip from the live view of a camera once the Event occurs.

To configure Capture Clip action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▼ and select **Capture Clip** from the list of Actions.



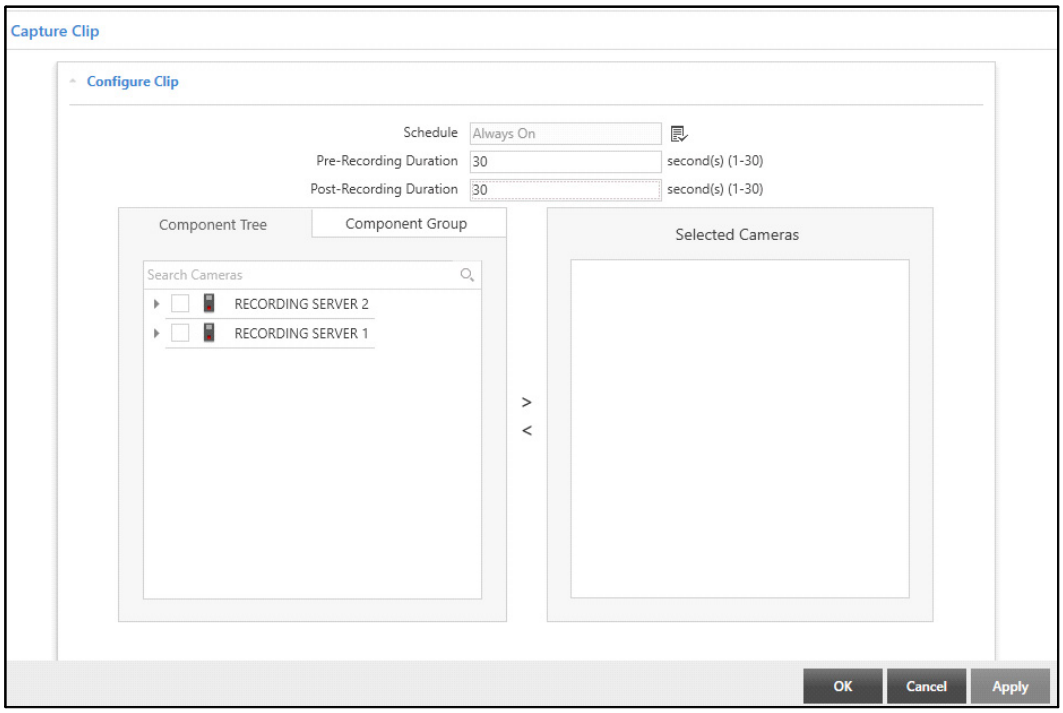
The Capture Clip action contains two collapsible panels — “Configure Clip” and “Email Clip”.

Configure Clip

This panel displays the clip configurations. You can edit and configure the clip recording from this collapsible panel.

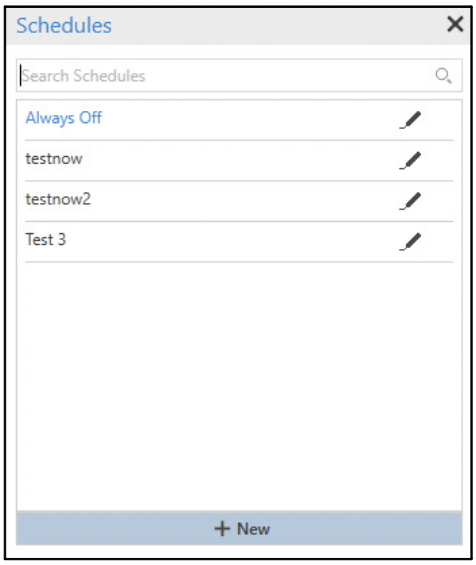
To configure the clip parameters,

- Click the **Configure Clip** collapsible panel.



Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



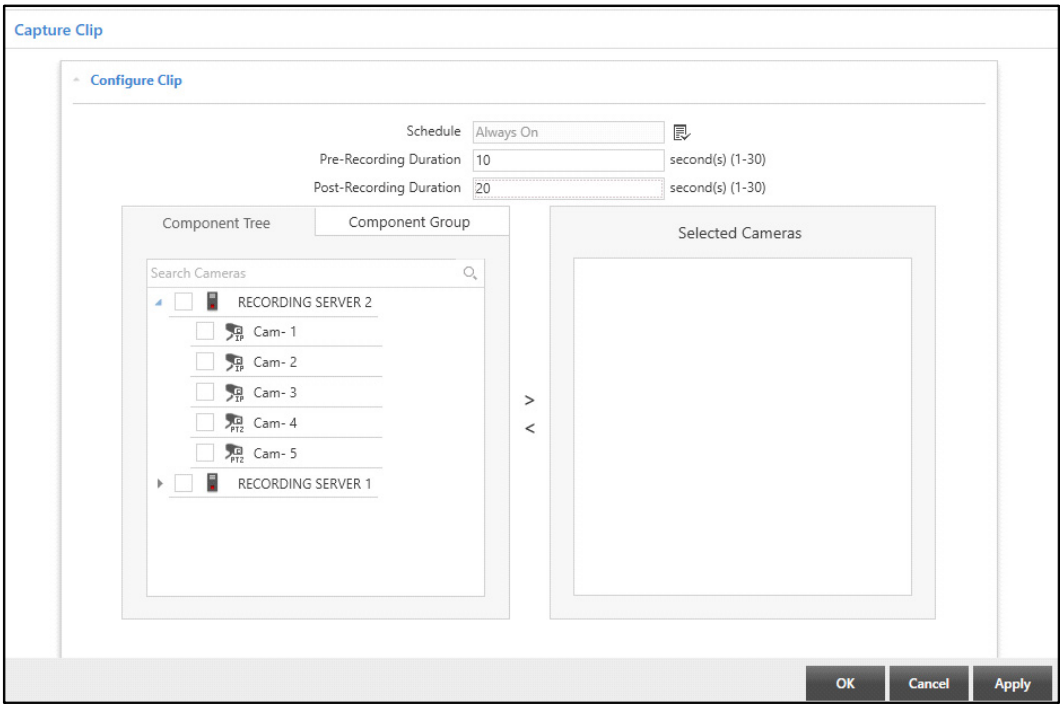
  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Pre-Recording Duration**: Specify the duration in seconds for which the clip needs to be captured before Event occurence. In Pre-Recording Duration, you can enter upto 2 characters. Valid Range: 1-30. Default: 30.

- **Post-Recording Duration**: Specify the duration in seconds for which the clip needs to be captured after Event occurence. In Post-Recording Duration, you can enter upto 2 characters. Valid Range: 1-30. Default: 30.

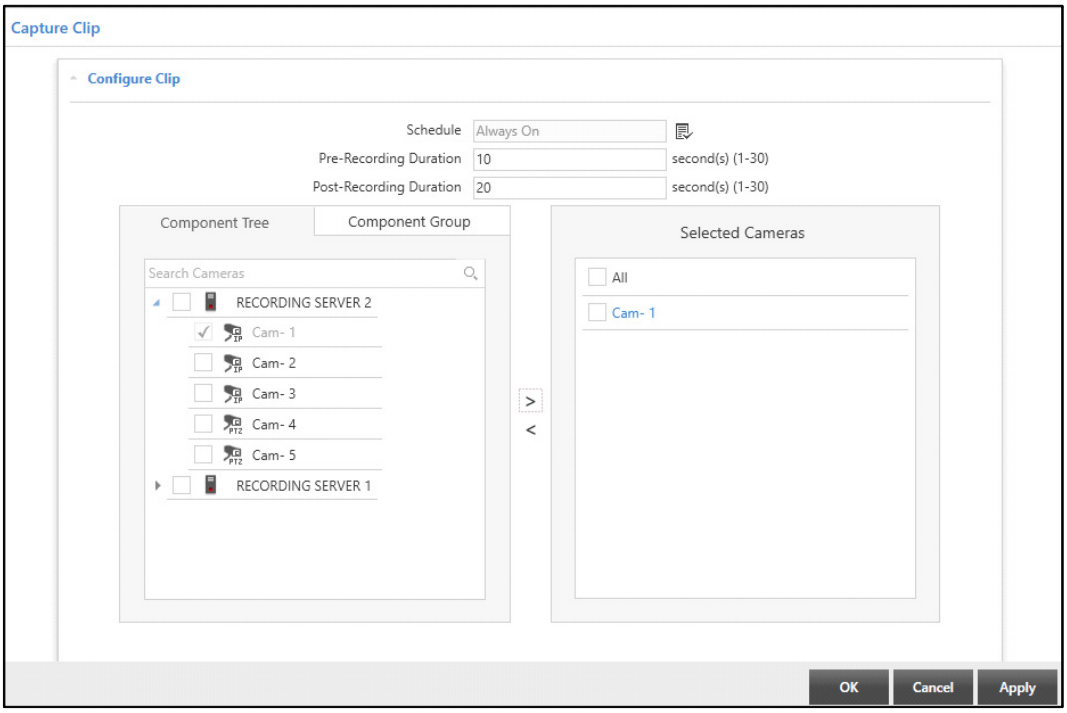
Once these configurations are done, you need to select the cameras to capture the clip on Event occurence.

*Make sure you have configured the storage for the captured clips. You can configure clip storage from **Servers and Devices > Recording Server > Default Settings > Clip Capture**.*



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the desired cameras you wish to add from the Component Tree or Component Group tabs. Click the right arrow button to add the cameras in the **Selected Cameras** list.

  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.

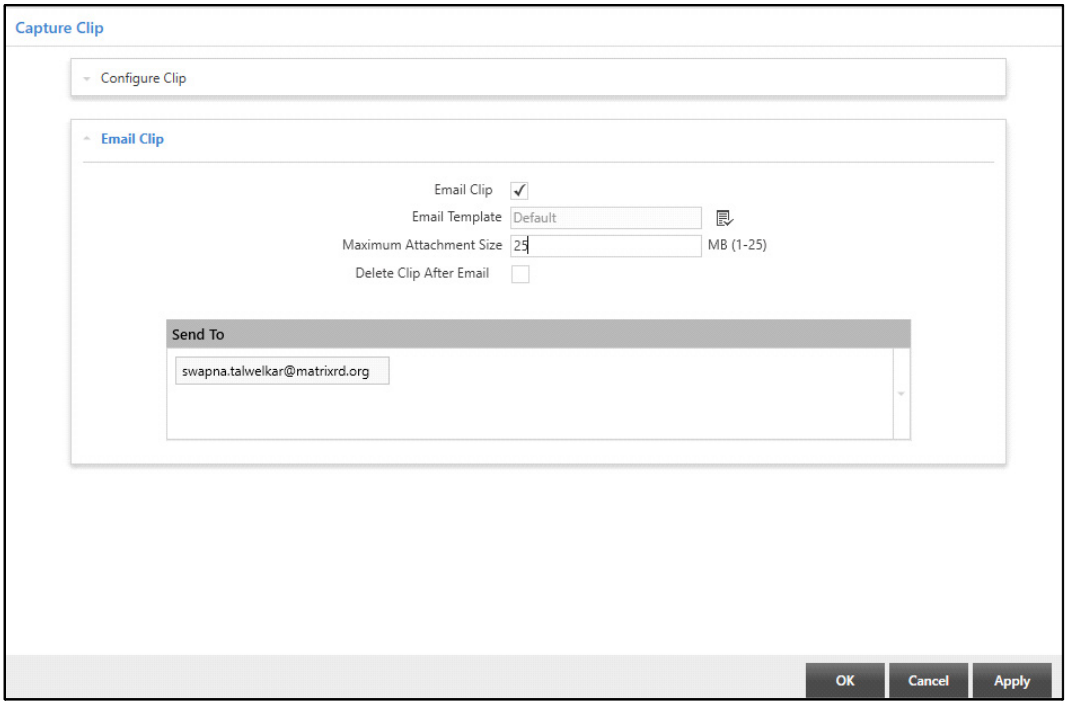


Email Clip

This panel displays the Email configurations for the clip. You can edit and configure the Email settings to send the clip from this collapsible panel.

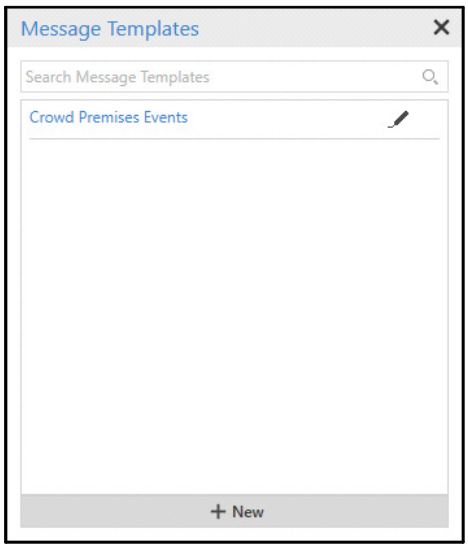
To configure the Email parameters,

- Click the **Email Clip** collapsible panel.



Configure the following parameters:

- **Email Clip**: Select the check box to enable the Email Clip configurations.
- **Email Template**: Select the desired Email Template which you wish to assign to the Action using the **Email Template** picklist.
  - Click **Email Template** picklist. The **Message Templates** pop-up appears.



  - Only those templates appear in the list which are created with the same Event as selected in the Scenario. The Email configurations done in the template will be used to send the Email. Double-click to select the desired template from the list.

    You can edit an existing template by clicking on **Edit** . You can also configure a new template by clicking **New**. For more details, refer to "Message Templates".

- **Maximum Attachment Size**: Specify the maximum size of files that can be attached with the Email. In Maximum Attachment Size, you can enter upto 2 characters. Valid Range: 1-25MB. Default: 25.
- **Delete Clip After Email**: Select the check box if you wish to delete the clip after sending Email.
- **Send To**: Specify the Email Address of the person to whom the Email is to be sent. In Send To, you can enter upto 100 characters (for each recipient). Valid Range: 1-9999 recipients. Default: Blank.

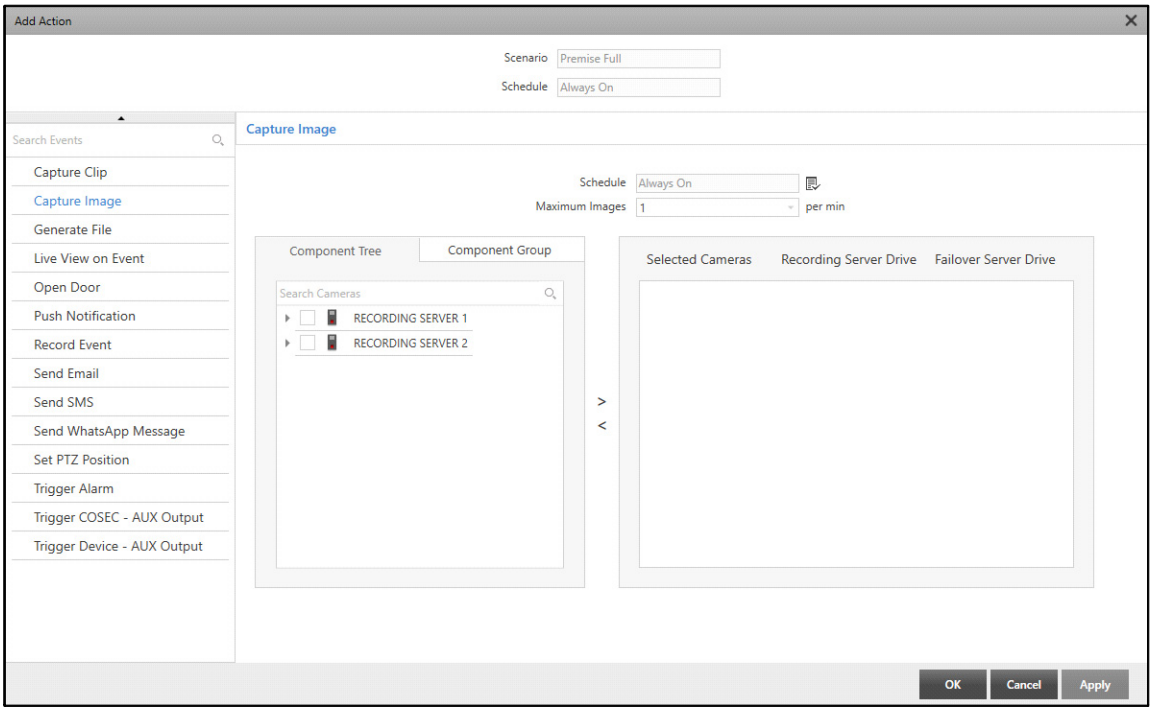
- Click **Apply** and **OK** to save the settings.

Capture Image

The Capture Image action captures an image from the live view of a camera once the Event occurs.

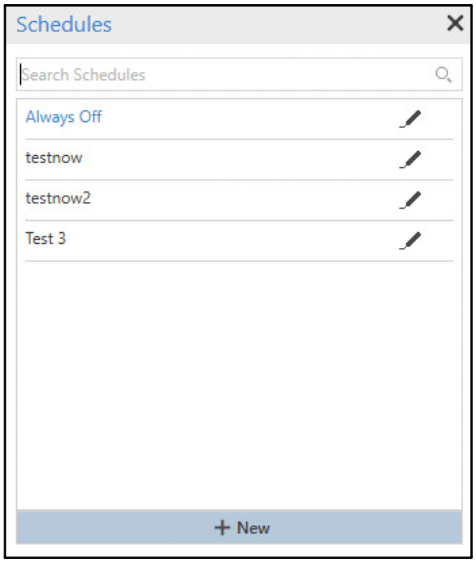
To configure Capture Image action,

- Click **Add Action** to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click and select **Capture Image** from the list of Actions.



Configure the following parameters:

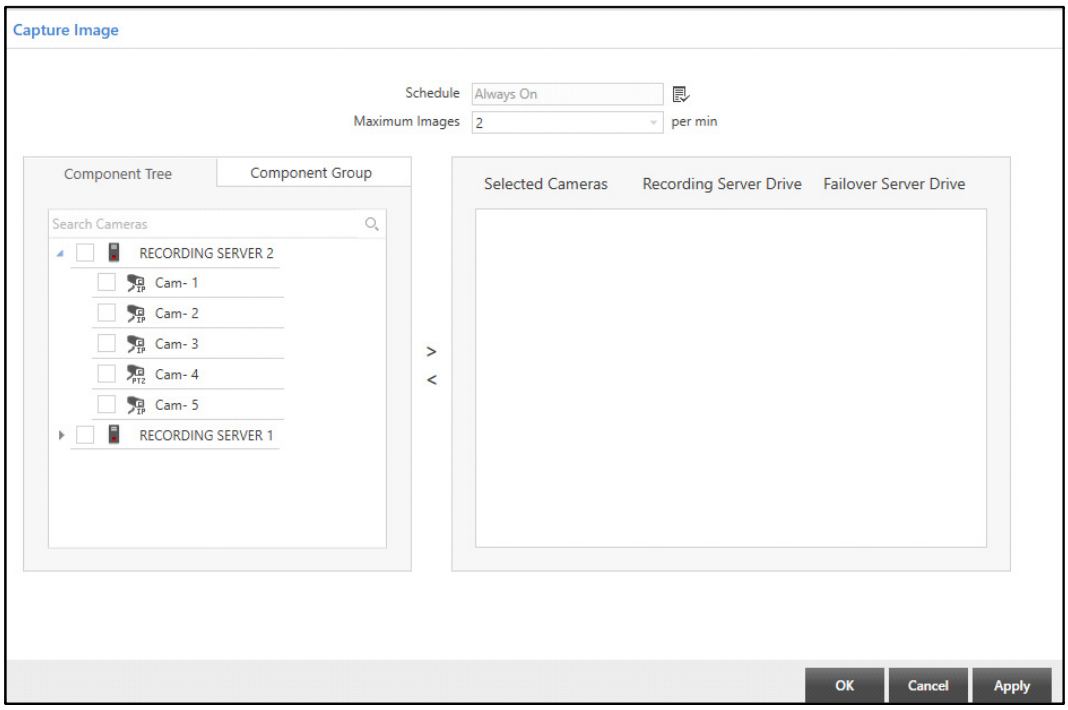
- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Maximum Images**: Select the number of images that should be captured per minute on Event occurrence from the drop-down list.

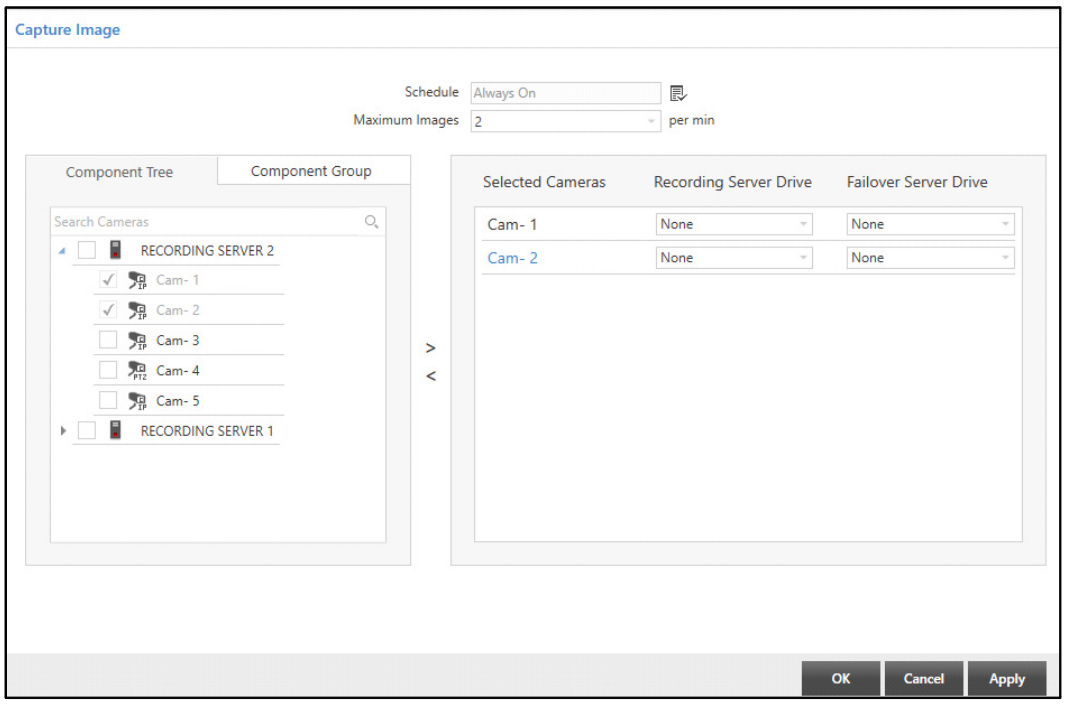
Once these configurations are done, you need to select the cameras to capture the images on Event occurence.



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the desired cameras you wish to add from the Component Tree or Component Group tabs. Click the right arrow button to add the cameras in the **Selected Cameras** list.

Mobile Camera will not be displayed in the list of cameras as Capture Image functionality is not supported by Mobile Cameras.

To remove cameras, select the heck boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.



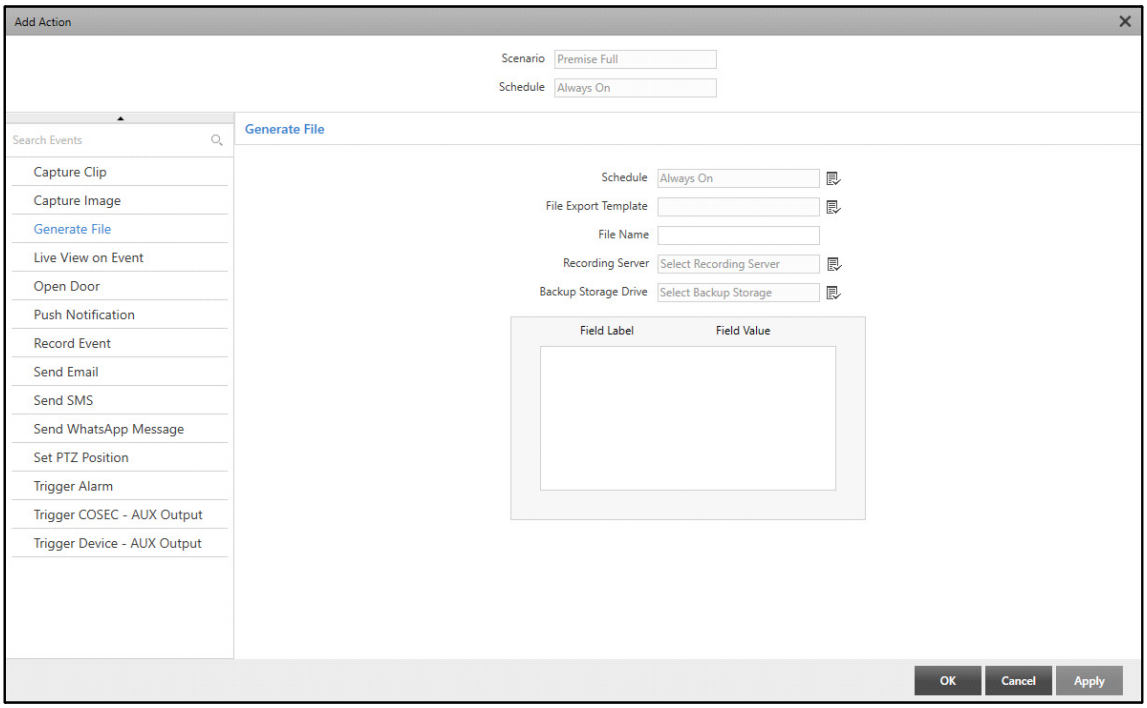
- The added cameras appear in the **Selected Cameras** list. The camera details displayed are — Camera Name, Recording Server Drive and Failover Server Drive.
- For the added camera, select the **Recording Server Drive** where you wish to store the images from the drop-down list.
- For the added camera, select the **Failover Server Drive** where you wish to store the images from the drop-down list.
- Click **Apply** and **OK** to save the settings.

Generate File

The Generate File action generates a file in the configured Storage Drive once the Event occurs.

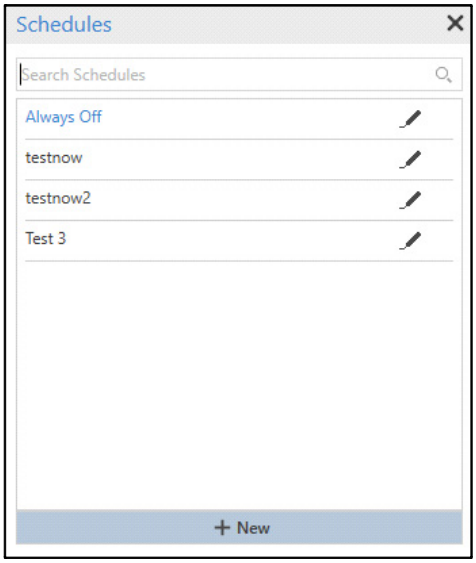
To configure Generate File action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▾ and select **Generate File** from the list of Actions.



Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



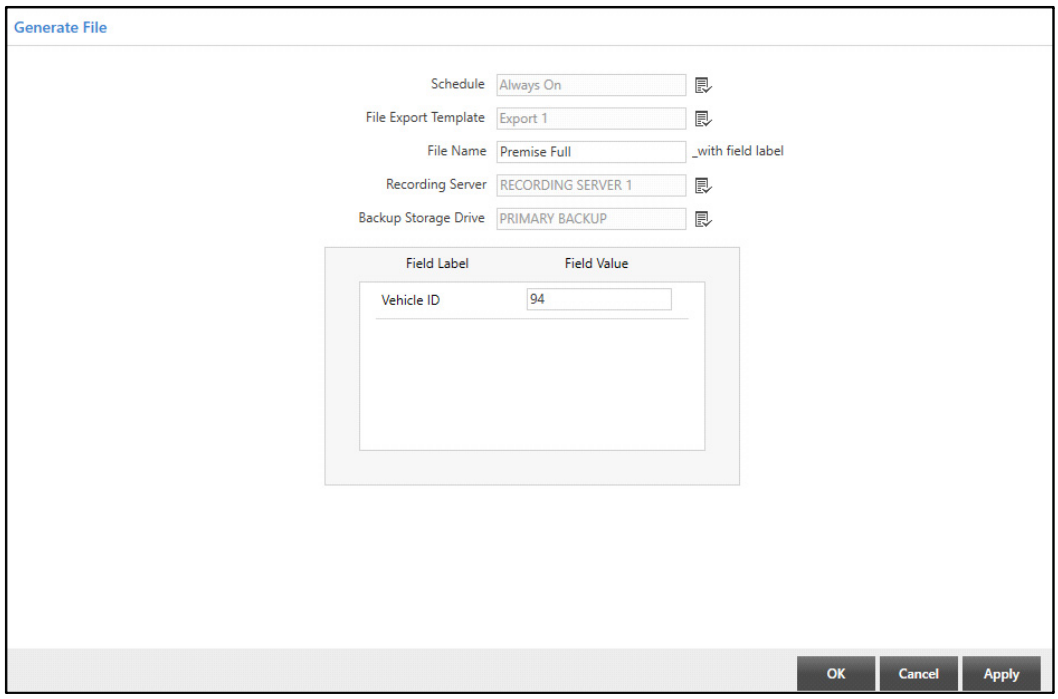
  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **File Export Template**: Select the desired File Export Template which you wish to assign to the Action using the **File Export Template** picklist. Double-click to select the desired option.
- **File Name**: Specify a suitable name for the File to be generated on Event occurence. In File Name, you can enter upto 50 characters. Default: Blank.
- **Recording Server**: Select the desired Recording Server using the **Recording Server** picklist. Double-click to select the desired option.
- **Backup Storage Drive**: Select the desired Backup Storage Drive using the **Backup Storage Drive** picklist. Double-click to select the desired option.

*A folder **Export** will be created in the selected Backup Storage Drive and the exported file will be saved in this drive.*

- The selected File Export Template appears under the Field Label list.
- Click **Apply** and **OK** to save the settings.

The grid displays the parameters containing the field labels and field values configured in the selected export file template.

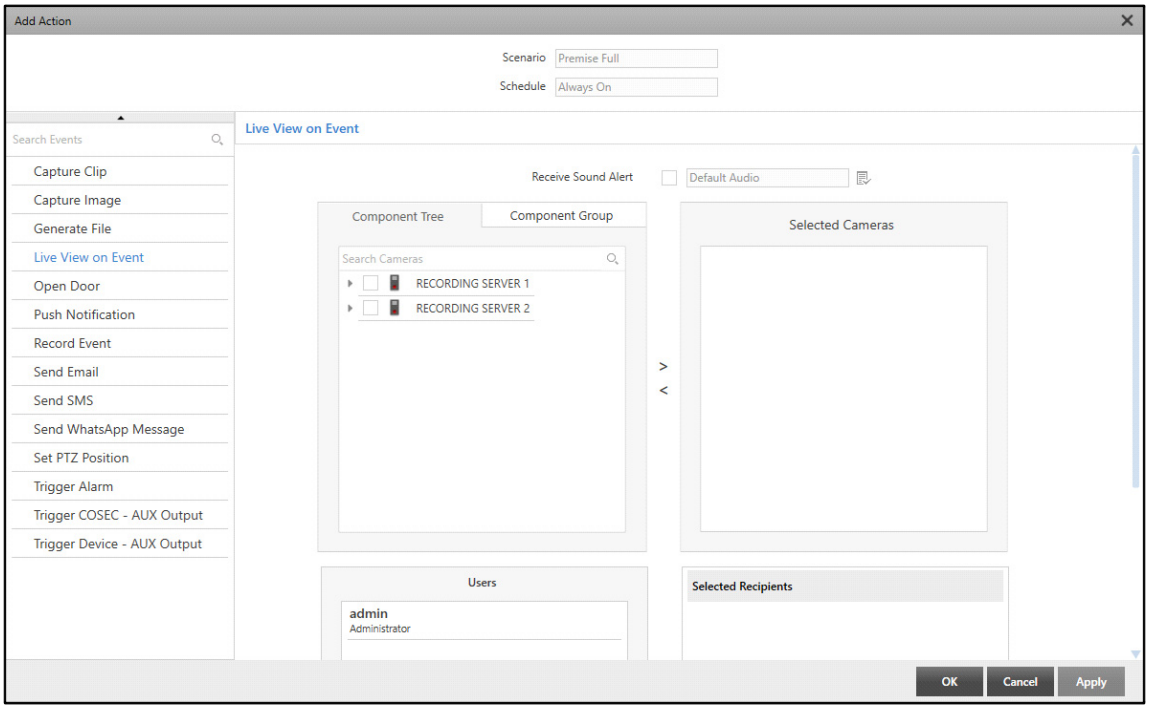


Live View on Event

The Live View on Event action starts the live view of a camera once the Event occurs.

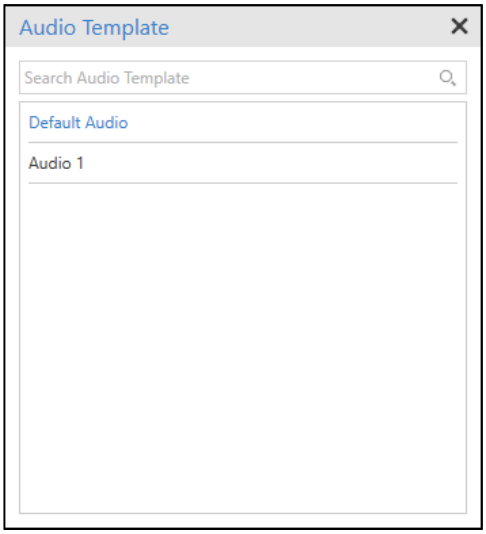
To configure Live View on Event action,

- Click **Add Action** to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click and select **Live View on Event** from the list of Actions.



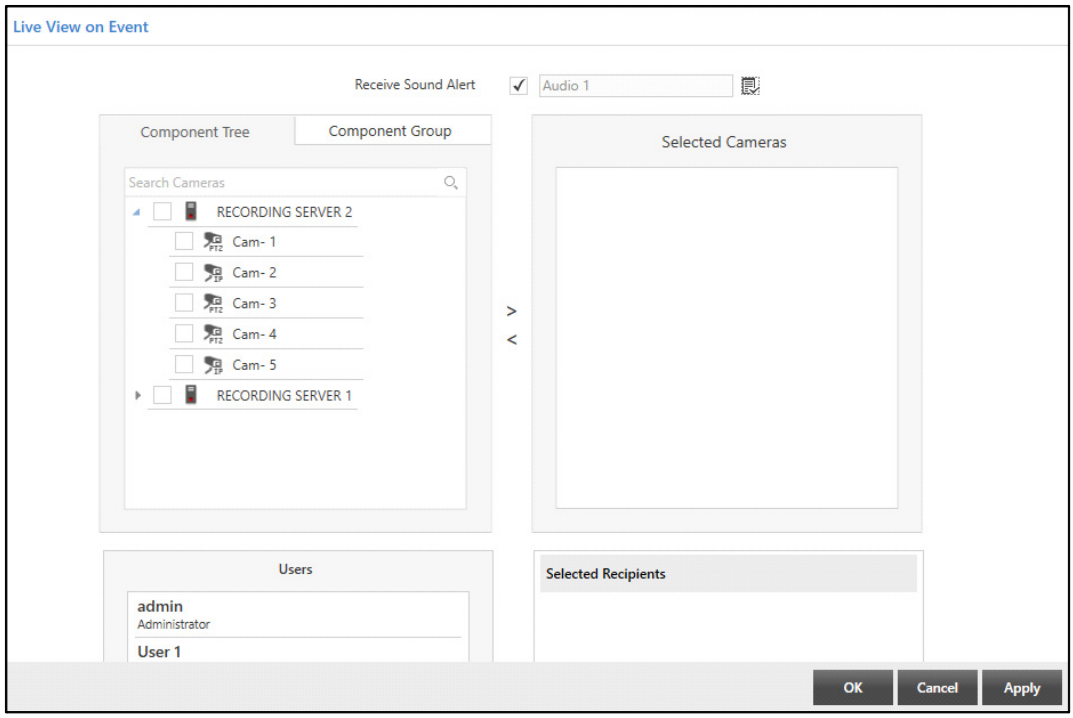
Configure the following parameters:

- **Receive Sound Alert**: Select the check box to receive sound alert when the action is triggered. Select the desired Audio Template you wish to assign to the alert using the **Audio Template** picklist.
    - Click **Select Audio Template** picklist. The **Audio Template** pop-up appears.



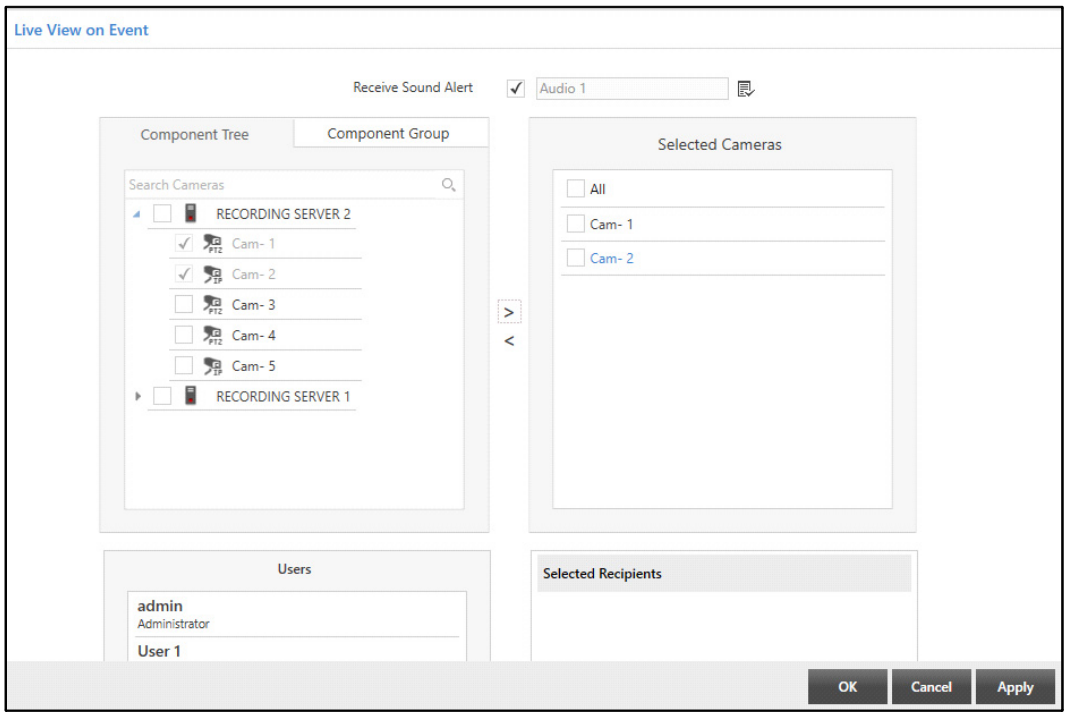
    - Double-click to select the desired Audio Template from the list.

Once these configurations are done, you need to select the cameras to start live view and select users to be notified on Event occurence.

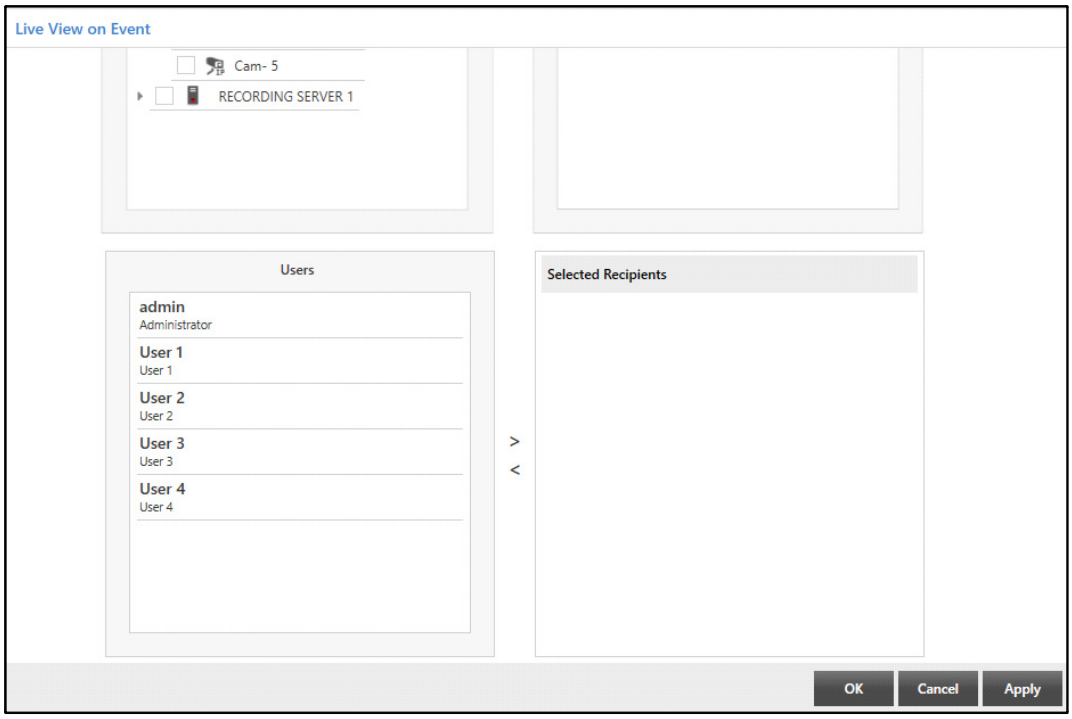


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the desired cameras you wish to add from the Component Tree or Component Group tabs. Click the right arrow button to add the cameras in the **Selected Cameras** list.

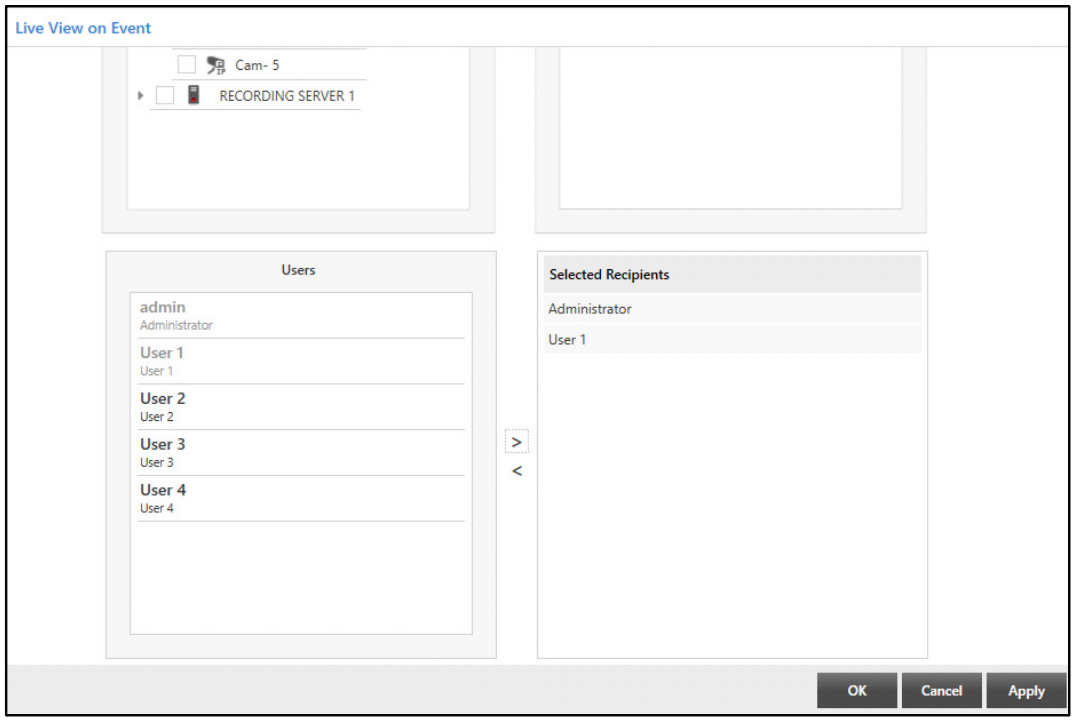
  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.



- The list of configured users appears in the **Users** list. Select the desired users you wish to add from the Users list. Click the right arrow button to add the users in the **Selected Recipients** list.



To remove users, select the desired users you wish to remove from the Selected Recipients list. Click the left arrow button to remove the users from the Selected Recipients list.



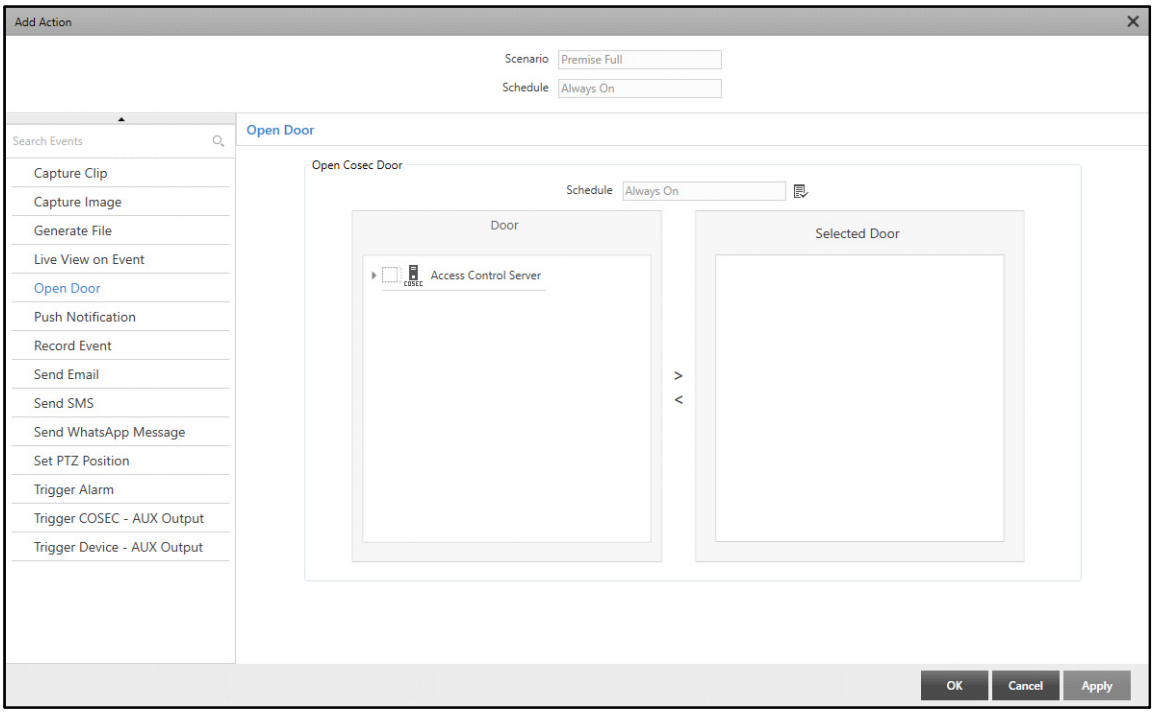
- Click **Apply** and **OK** to save the settings.

Open Door

The Open Door action opens a configured COSEC door once the Event occurs.

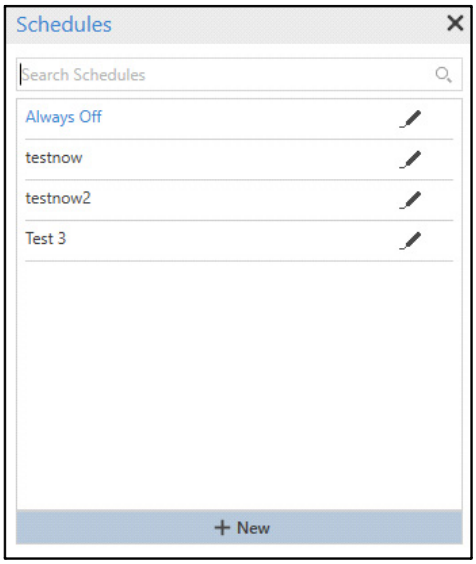
To configure Open Door action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▼ and select **Open Door** from the list of Actions.



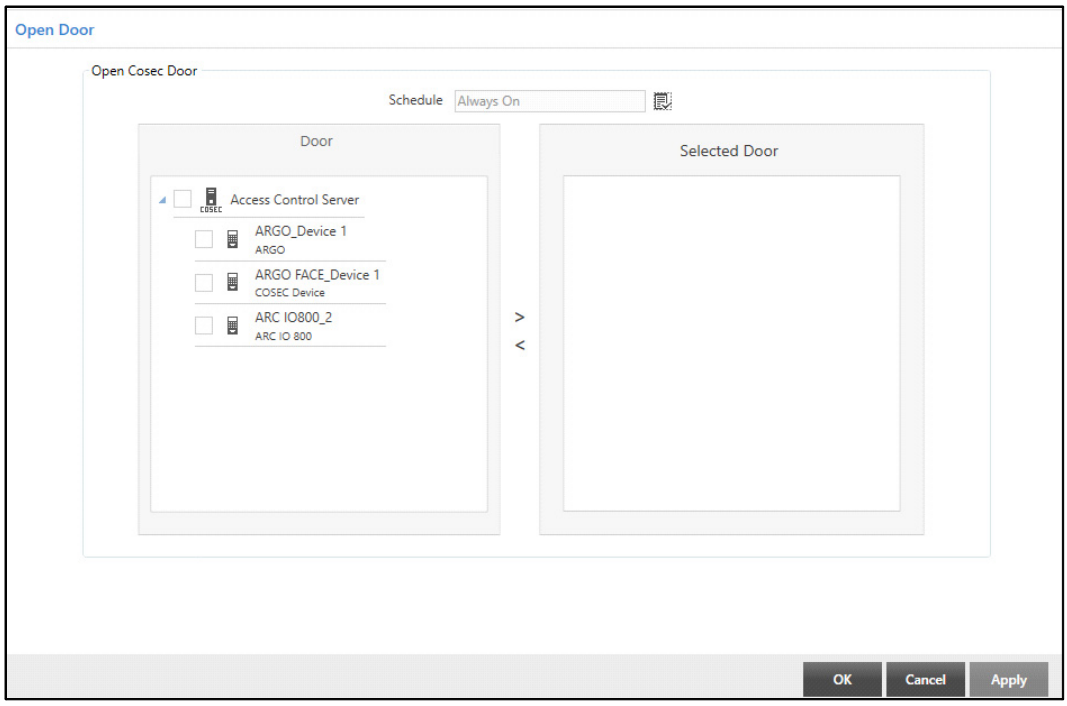
Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



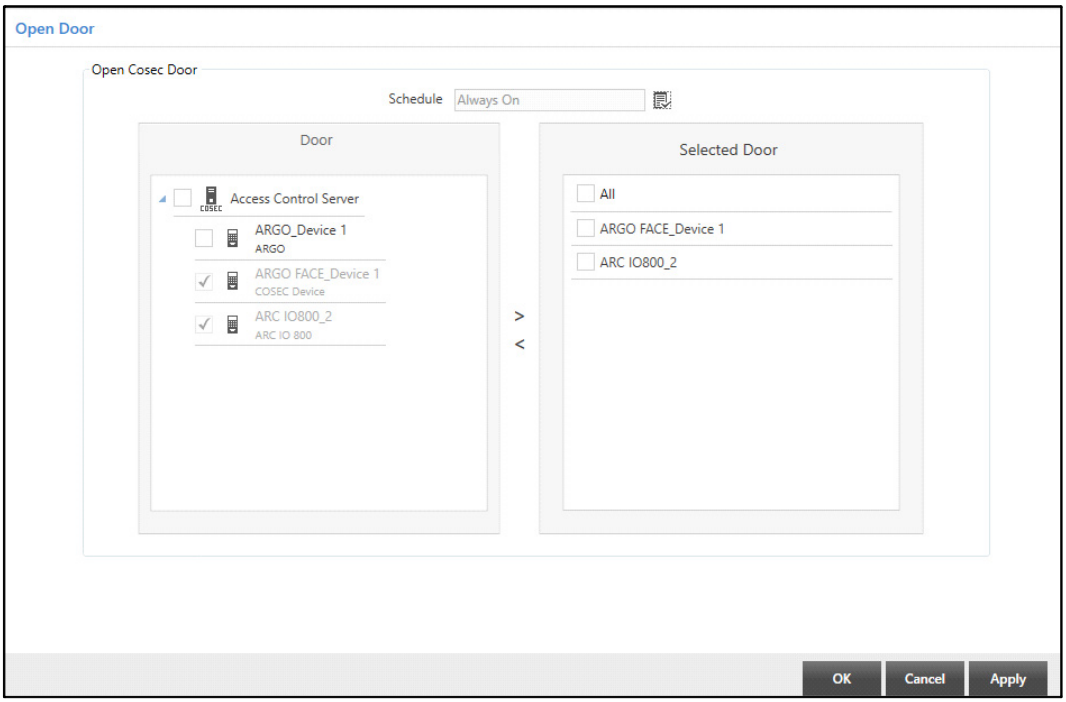
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

Once these configurations are done, you need to select the COSEC doors to be opened on Event occurence.



- The list of COSEC doors added to the Access Control Server appears in the **Door** list. Select the check boxes of the desired doors you wish to add from the Door list. Click the right arrow button to add the devices in the **Selected Door** list.

  To remove doors, select the check boxes of the desired doors you wish to remove from the Selected Door list. Click the left arrow button to remove the doors from the Selected Door list.



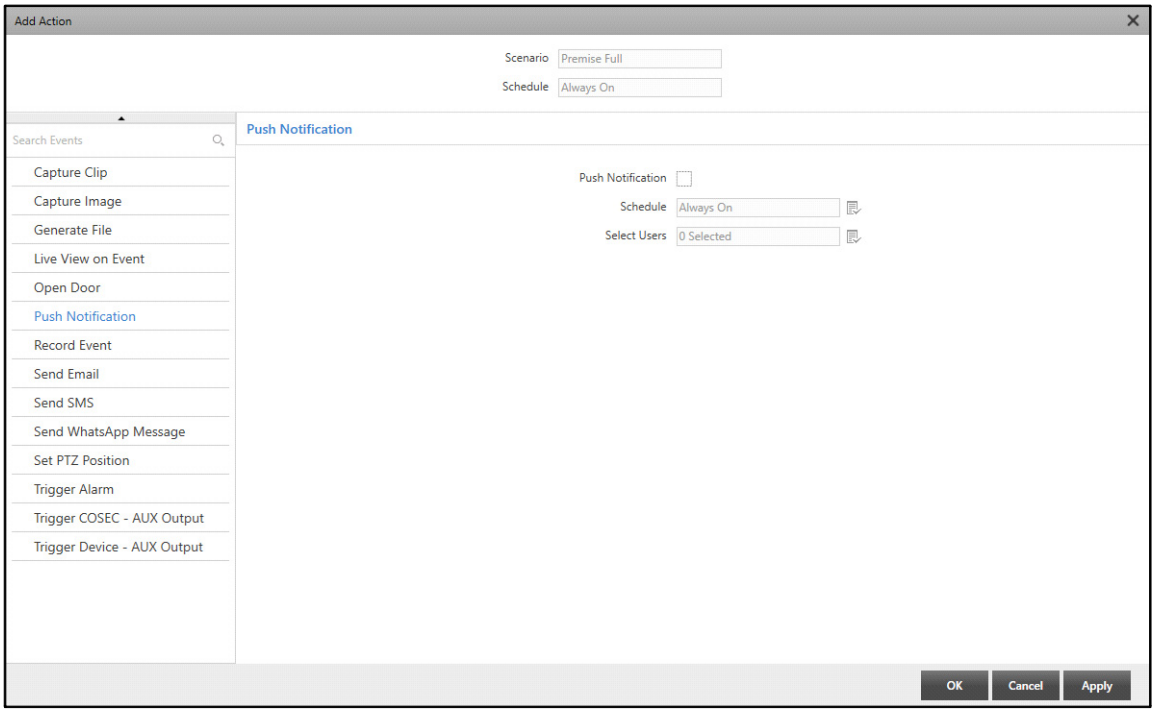
- Click **Apply** and **OK** to save the settings.

Push Notification

The Push Notification action sends Push Notifications to the selected users on SATATYA VISION App for the selected Events. Refer to "Push Notification" before configuring the Push Notification action.

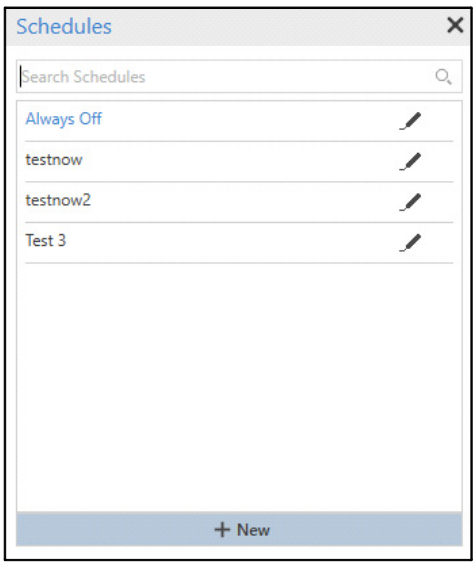
To configure Push Notification action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▾ and select **Push Notification** from the list of Actions.



Configure the following parameters:

- **Push Notification**: Select the check box to enable the configuration.
- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Select Users**: Select the desired users to whom you wish to send the Push Notifications. The users for whom Push Notification is enabled in Mobile Client will only appear in this list.

    - Click **Select Users** picklist. The **Select User** pop-up appears.



    - Select the check boxes for the desired users. Click **OK**.

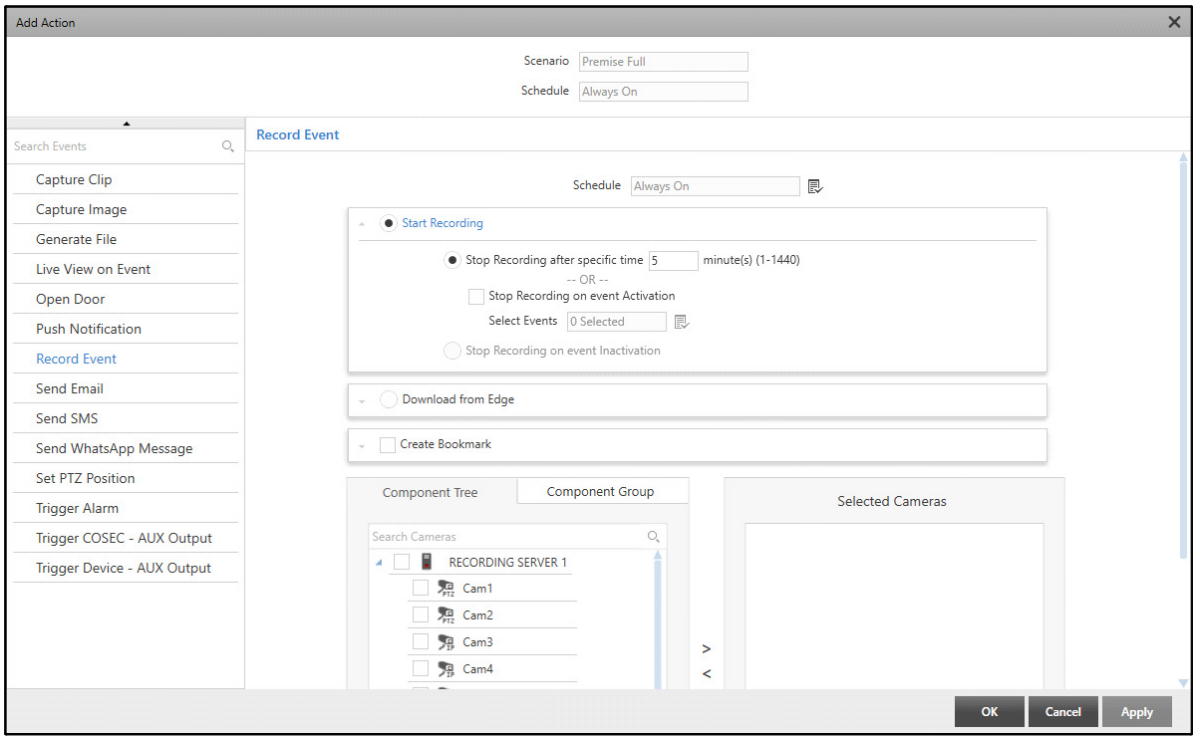
- Click **Apply** and **OK** to save the settings.

Record Event

The Record Event action records the entire Event once it occurs for a defined period of time.

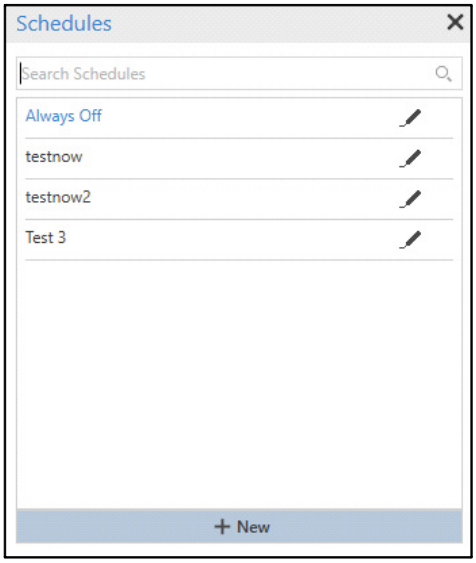
To configure Record Event action,

- Click **Add Action** to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click and select **Record Event** from the list of Actions.



Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

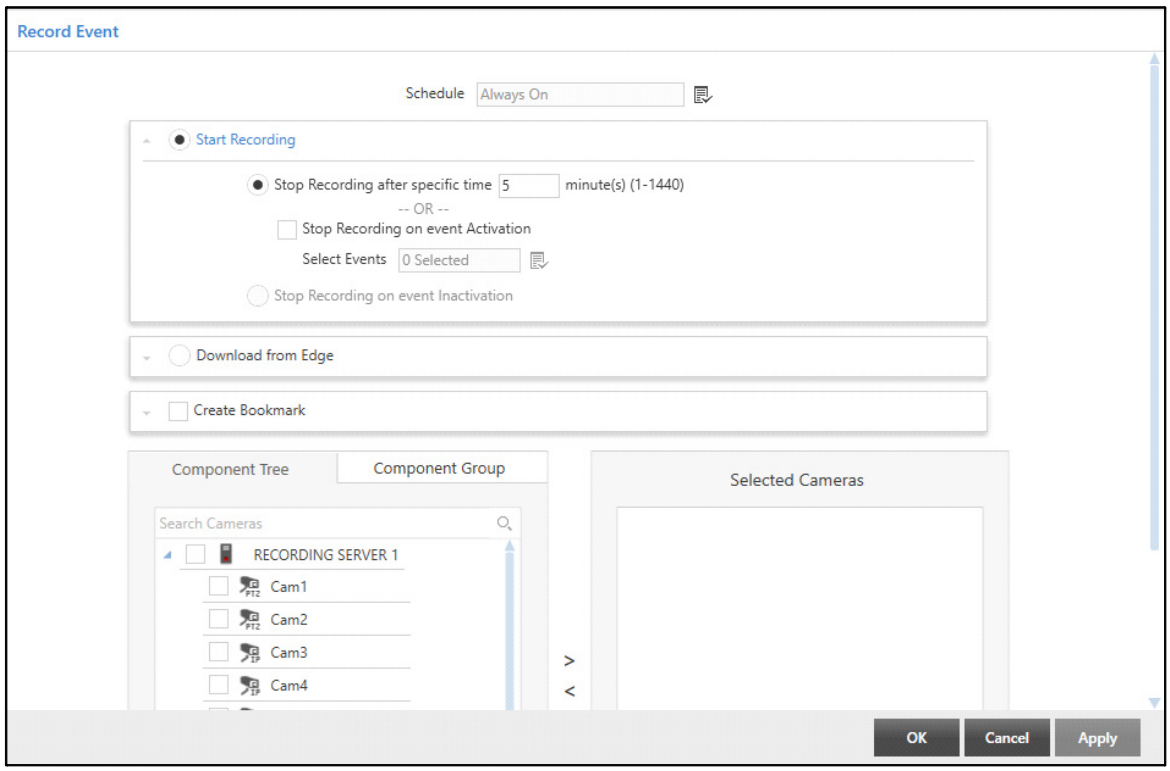
The Record Event action contains three collapsible panels — “Start Recording”, “Download From Edge” and “Create Bookmark”.

Start Recording

This panel displays the recording configurations. You can edit and configure the Event recording from this collapsible panel.

To configure the recording parameters,

- Select the **Start Recording** collapsible panel to enable configuration.
- Click **Start Recording** option.



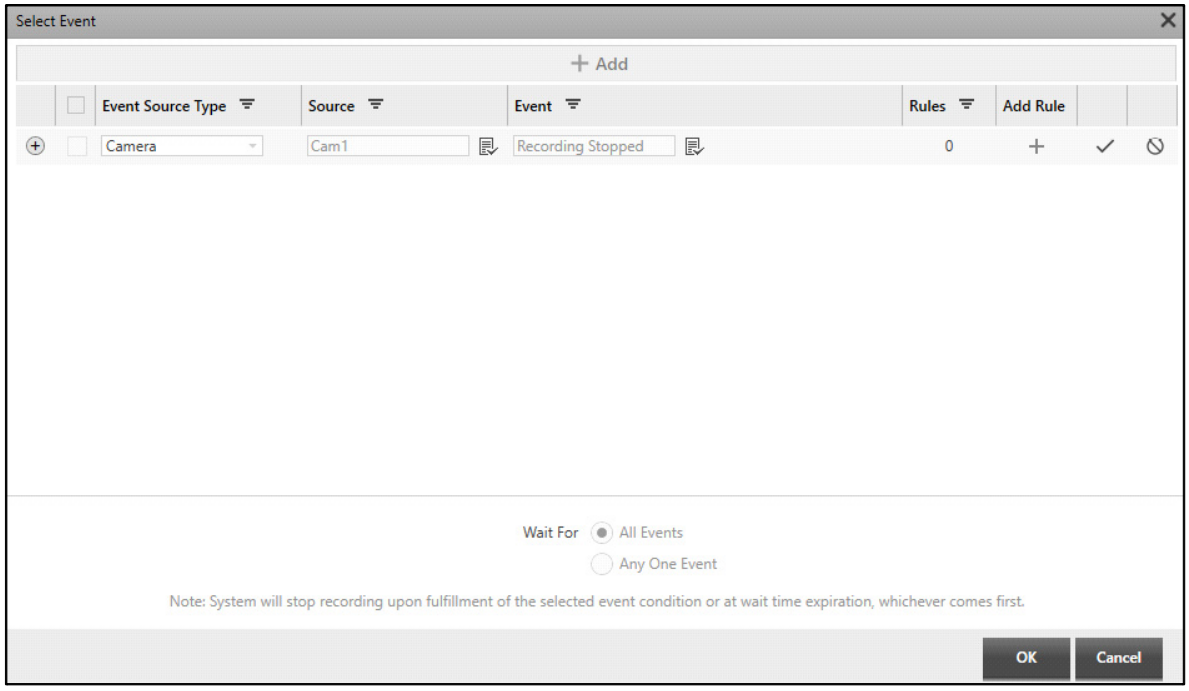
- Then select the desired option — **Stop Recording after specific time**, **Stop Recording on event inactivation.**
  - If you select **Stop Recording after specific time**, specify the time period in minutes after which the action should stop. In Stop Recording after specific time, you can enter upto 4 characters. Valid Range: 1-1440 minutes. Default: 5.
    - You can also select “Stop Recording on event Activation” if you want to stop recording on the occurence of an event.
  - If you select **Stop Recording on event inactivation**, the recording will stop once the event is inactivated.

*If you have configured both **Stop Recording after specific time** and **Stop Recording on event Activation**, the recording will stop after whichever of the two occurs first.*

*For the same camera, if you have configured **Stop Recording after specific time and/or Stop Recording on event Activation** under Record Event along with **Maximum Event Recording Duration** under "Event and Manual Recording" in "Recording Configuration", then priority will be given to the configurations done for **Record Event.***

Stop Recording on event Activation

If you select **Stop Recording on event Activation**, select the desired events on occurence of which the recording should stop using the **Events** picklist. Click **Event** picklist. The **Select Event** pop-up appears.



- Click **Add**.

Configure the following parameters:

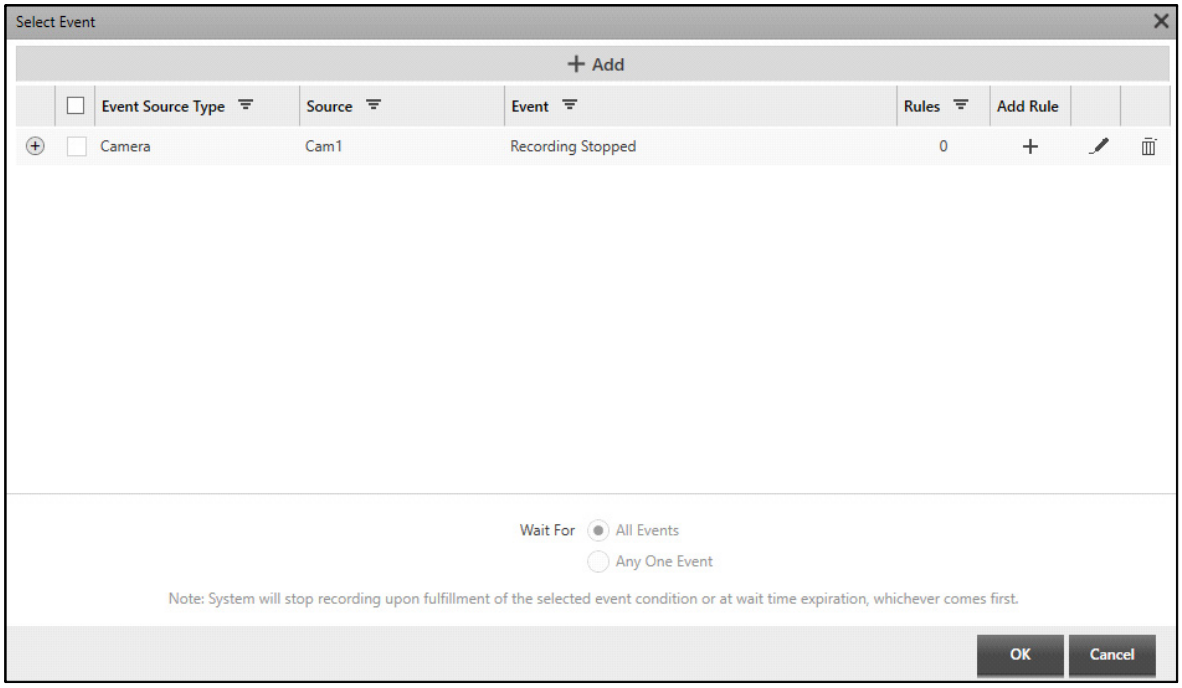
- **Event Source Type**: Select the type of Event Source for which you wish to configure the Action from the drop-down list.
- **Source**: Select the Source for which you wish to configure the Action using the **Source** picklist. The Source depends on the selected Event Source Type. For example, if you select Camera as the Event Source Type, a list of all the configured cameras appear in the Source picklist. Double-click to select the desired option.
- **Event**: Select the desired Event for which you wish to configure an Action using the **Event** picklist.The Event depends on the selected Event Source Type and Source. Double-click to select the desired option.

- **Add Rule**: Click **Add Rule** to add Rules. For details, refer to “Add Rule”.

- Click **Save** to save the Event or click **Cancel** to discard.

The configured Event appears in a list.

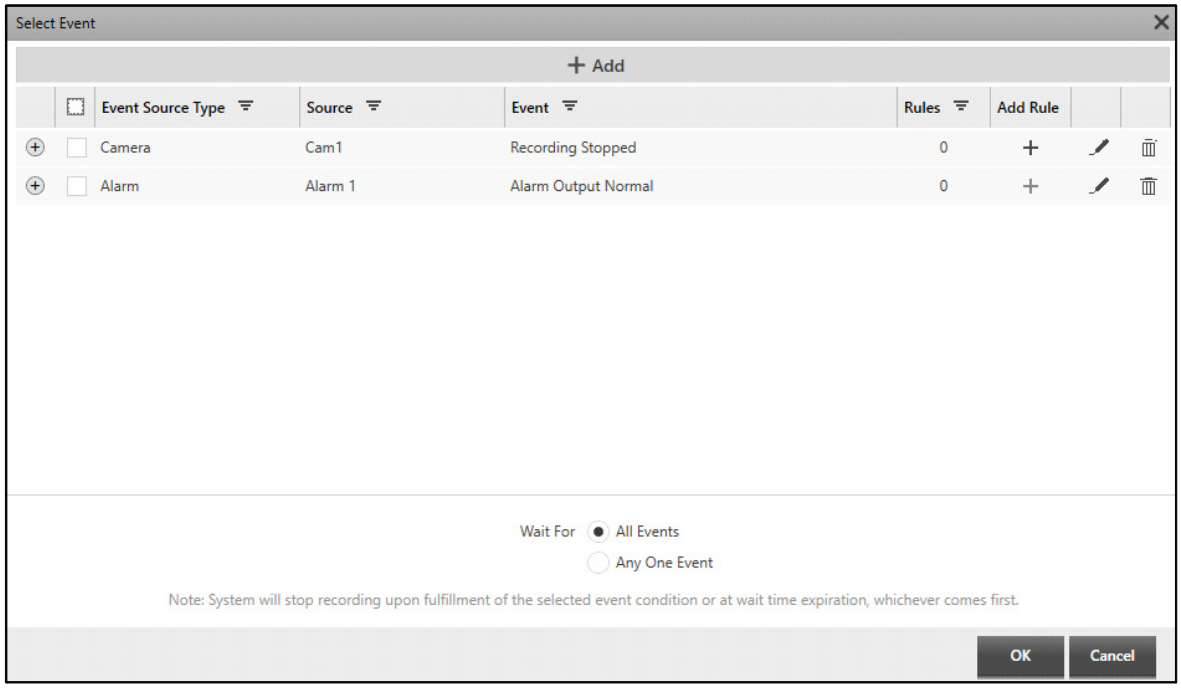
You can edit the Event parameters or delete the Event.



- Click **Edit** to edit the Event configurations.

- Click **Delete** to delete the Event.

Once you have added two or more Events, the **Wait For** parameter is enabled.



- **Wait For**: Select the desired condition from the options — All Events or Any One Event.

  Select **All Events**, if you wish that the system should wait for the specified time to generate all the Events.

  Select **Any One Event**, if you wish that the system should wait for the specified time to generate any one Event.

- Click **OK** to confirm or click **Cancel** to discard the changes.

The number of created Events will appear against **Select Events** under **Stop Recording on event Activation**.

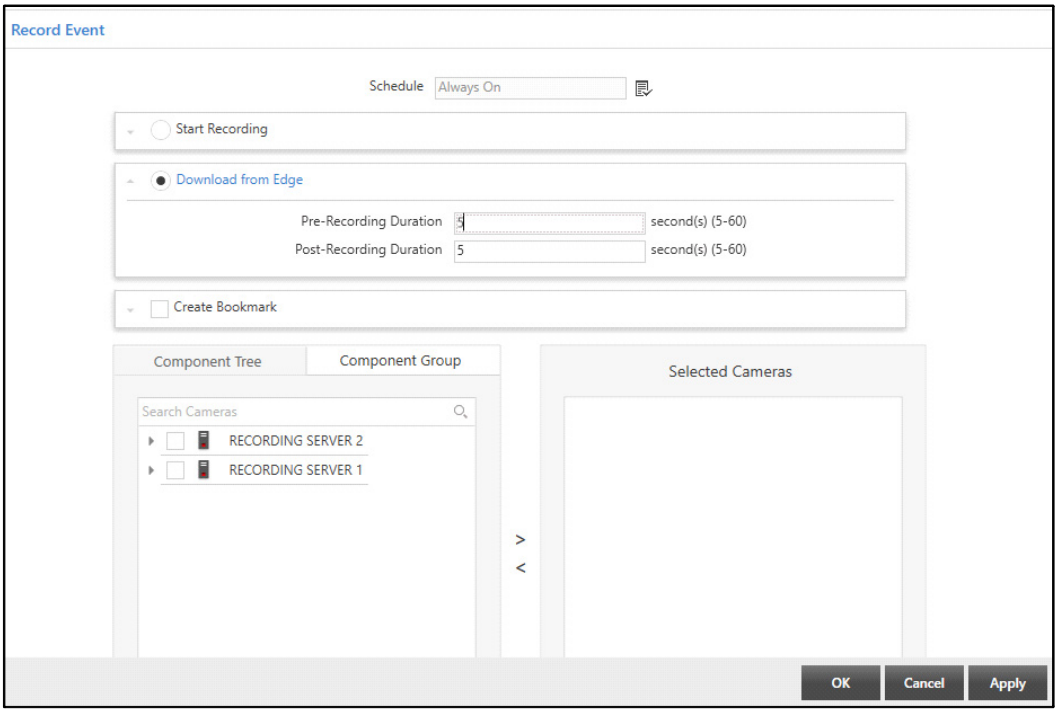
Download From Edge

This panel displays the clip download configurations. You can edit and configure the clip download time from this collapsible panel.

To configure the Download From Edge parameters,

- Select the **Download From Edge** collapsible panel to enable configuration.

- Click **Download From Edge** option.



Configure the following parameters:

- **Pre-Recording Duration**: Specify the Pre-Recording duration that you want the system to download. In Pre-Recording Duration, you can enter upto 2 characters. Valid Range: 5-60 seconds. Default: 5.
- **Post-Recording Duration**: Specify the Post-Recording duration that you want the system to download. In Post-Recording Duration, you can enter upto 2 characters. Valid Range: 5-60 seconds. Default: 5.

  For example, if pre-recording time is 5 seconds and post-recording time is 5 seconds and the event takes place at 12:00:00, then recording from 11:00:55 to 12:00:05 will be downloaded from Edge.

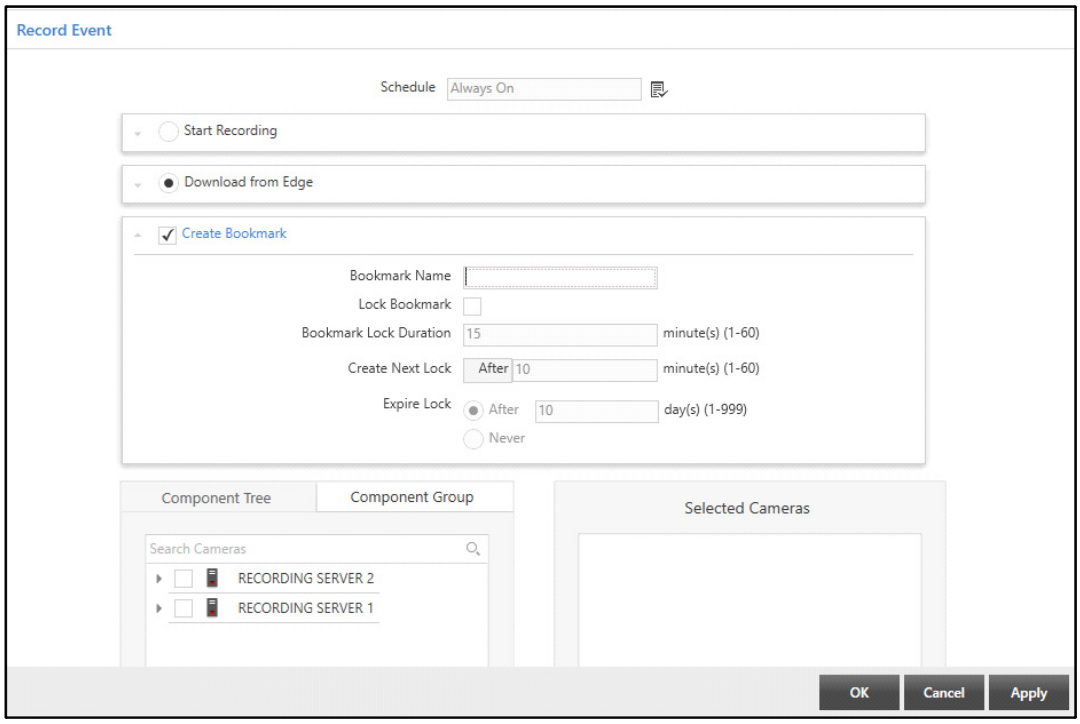
Download from Edge is applicable for Matrix cameras only.

Create Bookmark

This panel displays the bookmark configurations. You can edit and configure bookmark from this collapsible panel.

To configure the Create Bookmark configurations,

- Select the **Create Bookmark** collapsible panel to enable configuration.
- Select the **Create Bookmark** check box.

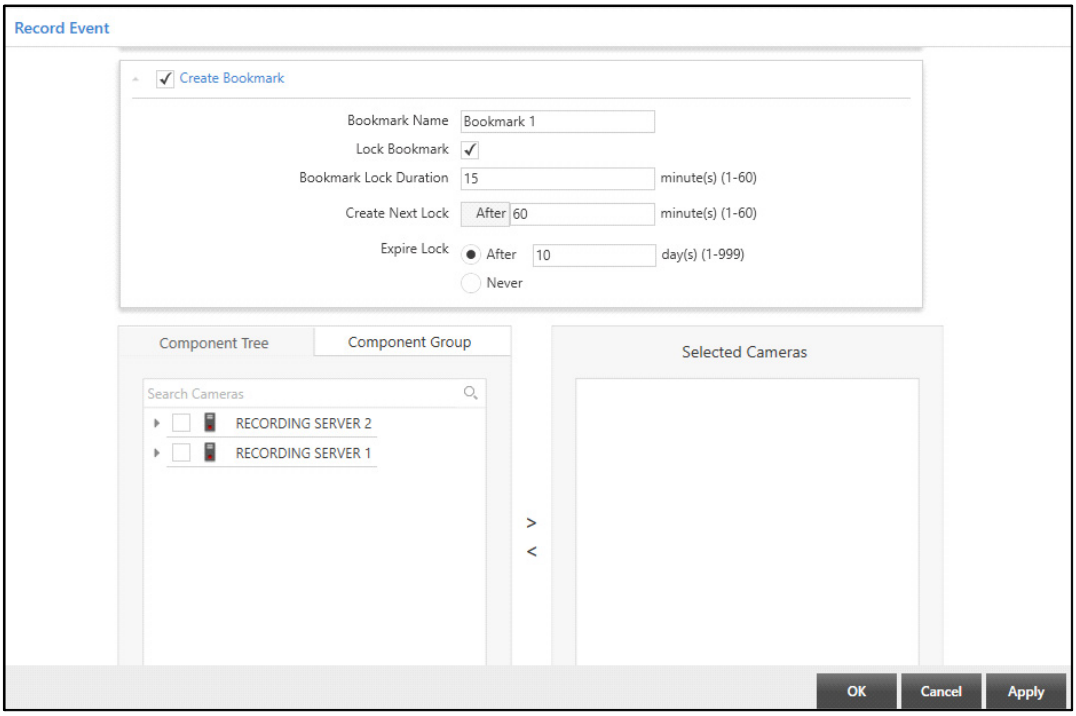


Configure the following parameters:

- **Bookmark Name**: Specify a suitable name for the bookmark. In Bookmark Name, you can enter upto 50 characters. Default: Blank.
- **Lock Bookmark**: Select the check box to lock the bookmark and enable Lock Bookmark configurations.
- **Bookmark Lock Duration**: Specify the time in minutes till which the bookmark should be locked in Event recording. In Bookmark Lock Duration, you can enter upto 2 characters. Valid Range: 1-60 minutes. Default: 15.
- **Create Next Lock After**: Specify the time in minutes after which the next bookmark lock should be created in Event recording. In Create Next Lock After, you can enter upto 2 characters. Valid Range: 1-60 minutes. Default: 10.
- **Expire Lock**: Select when the lock should expire from the options — After or Never. If you select **Never**, the bookmark lock will never expire.

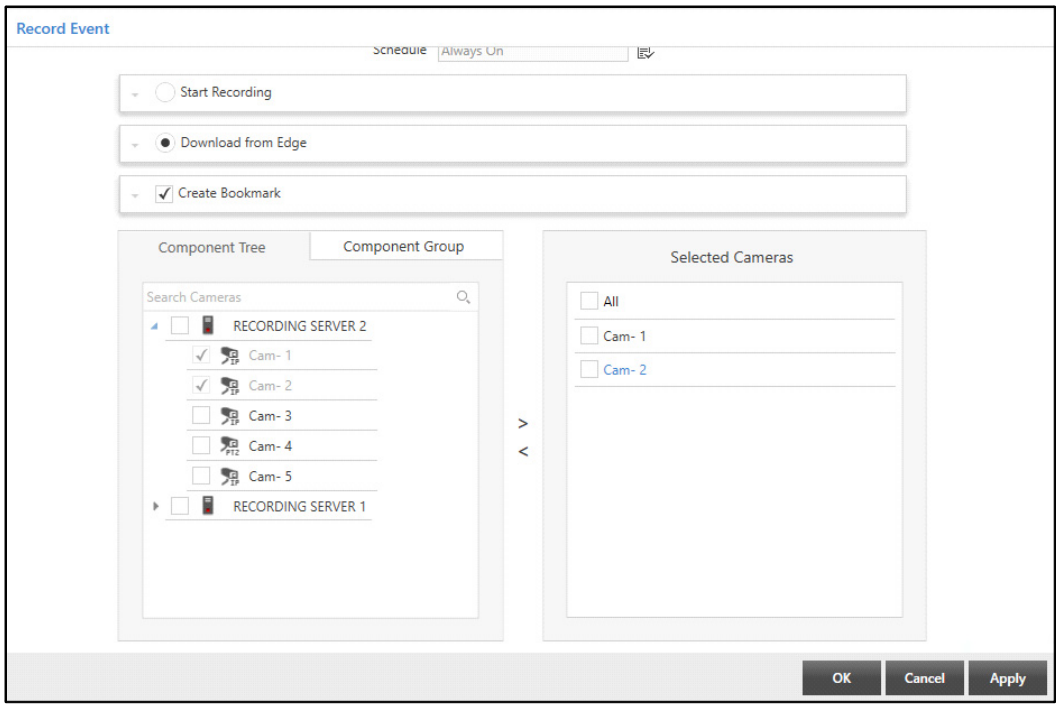
  If you select **After**, specify the time in days after which the bookmark lock should expire. In After, you can enter upto 3 characters. Valid Range: 1-999 days. Default: 10.

Once these configurations are complete, you need to select the camera whose recording is to be saved on Event occurence.



- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the desired cameras you wish to record the Event from the Component Tree or Component Group tabs. Click the right arrow button to add these cameras in the **Selected Cameras** list. You can also search for the desired cameras using the **Search Cameras** search bar.

  To remove cameras, select the check boxes of the desired cameras you wish to remove from the Selected Cameras list. Click the left arrow button to remove the cameras from the Selected Cameras list.



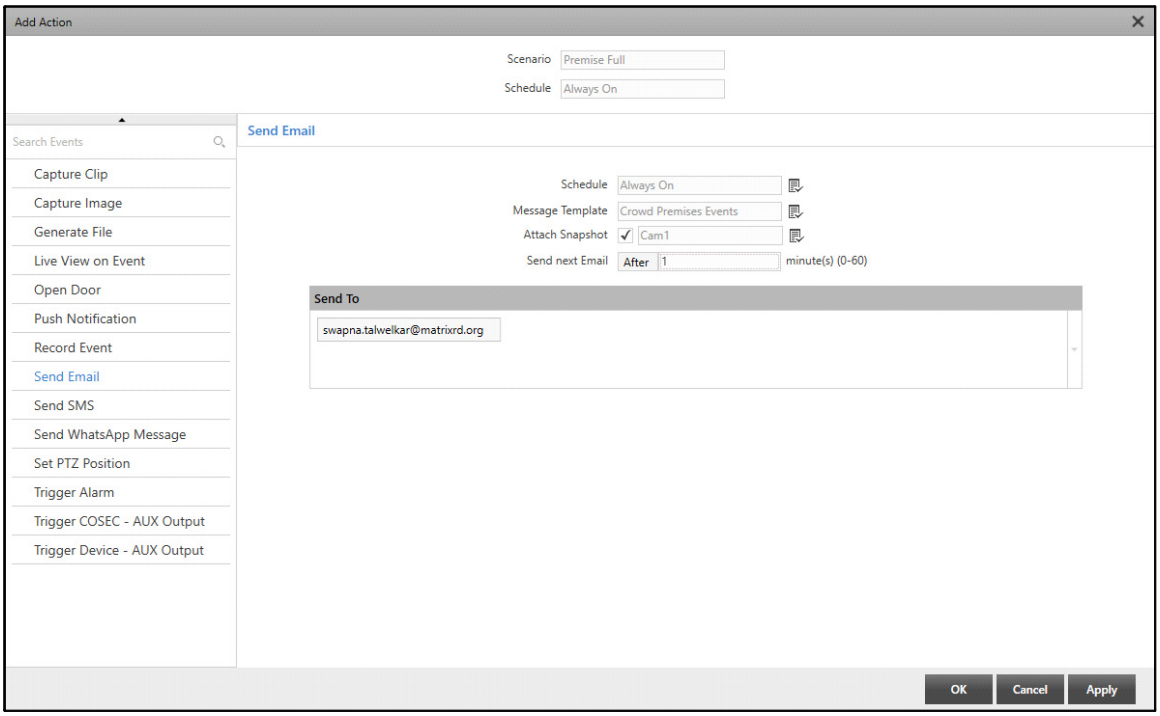
- Click **Apply** and **OK** to save the settings.

Send Email

The Send Email action sends Email to the configured Email ID once the Event occurs.

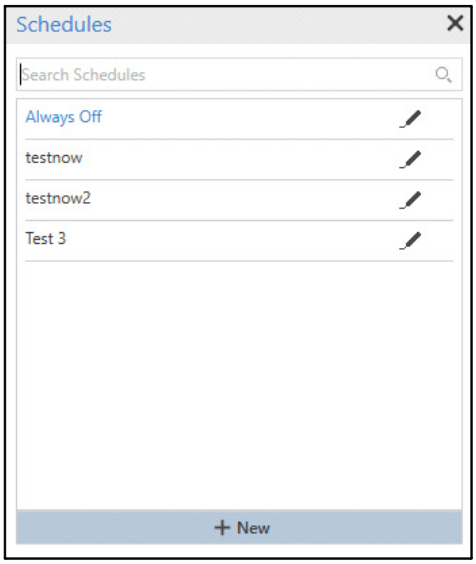
To configure Send Email action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▼ and select **Send Email** from the list of Actions.



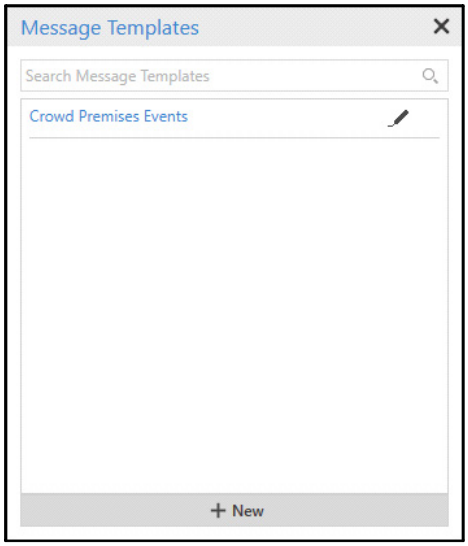
Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

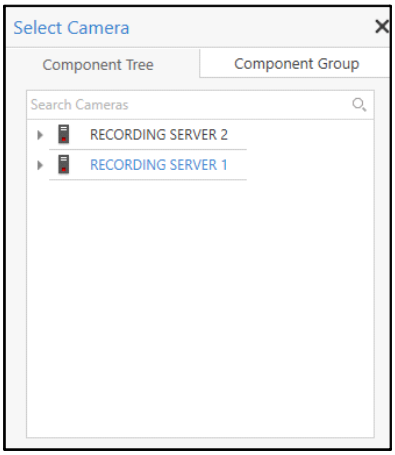
- **Message Template**: Select the desired Message Template which you wish to assign to the Action using the **Message Template** picklist.
  - Click **Message Template** picklist. The **Message Templates** pop-up appears.



- Only those templates appear in the list which are created with the same Event as selected in the Scenario. Double-click to select the desired template from the list.

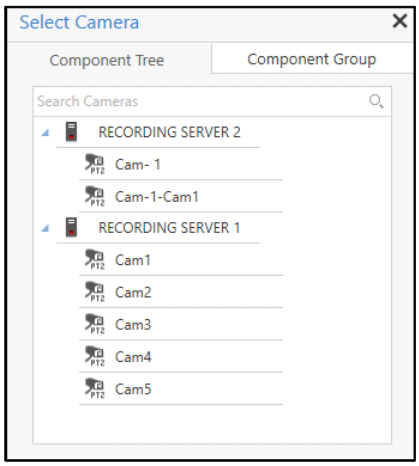
  You can edit an existing template by clicking on **Edit** . You can also configure a new template by clicking **New**. For more details, refer to “Message Templates”.

- **Attach Snapshot**: Select the check box to attach a snapshot along with the Email. Select the desired camera which you wish to assign to the Action using the **Camera** picklist.
    - Click **Camera** picklist. The **Select Camera** pop-up appears.



    - The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to "Component Group". Double click the desired camera to assign it to attach the snapshots. You can also search for the desired cameras using the **Search Cameras** search bar.

Mobile Camera will not be displayed in the list of cameras as Attach Snapshot functionality is not supported by Mobile Cameras.



- **Send next Email**: Specify the time in minutes after which the next Email should be sent after the Event occurence. Configure ***0 minutes*** if you want the Email to be sent every-time when the scenario initiates, fails or resumes. In Send next Email, you can enter upto 2 characters. Valid Range: 0-60 minutes. Default: 1.

- **Send To**: Specify the Email Address of the person to whom the Email is to be sent. You can enter multiple Email Addresses. In Send To, you can enter upto 100 characters (for each recipient). Valid Range: 1-9999 recipients. Default: Blank.

  You can enter the User Name or the Email Address of the user. The matching entries will be visible. Select the desired entry. If you wish to enter an Email Address that is not configured in SAMAS you can

type it manually. To enter multiple Email Addresses, type the Email Address/User Name and the press space bar on the keyboard to enter the next Email Address/User Name.

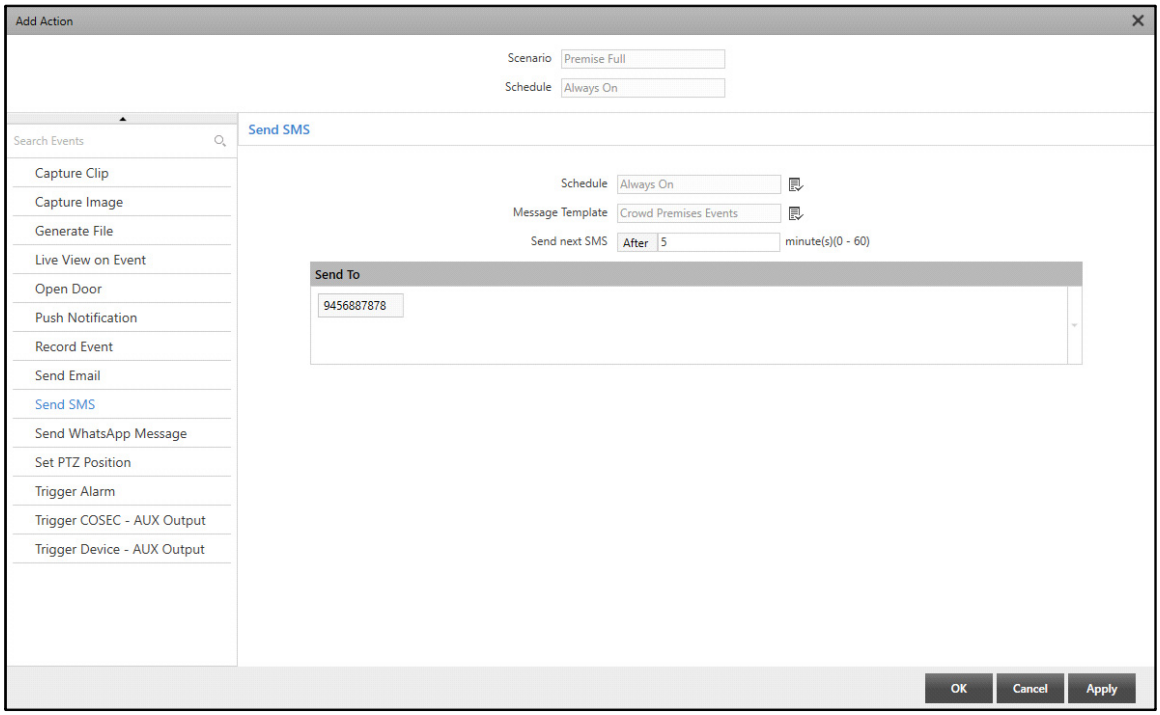
- Click **Apply** and **OK** to save the settings.

Send SMS

The Send SMS action sends an SMS to the configured Mobile number once the Event occurs.

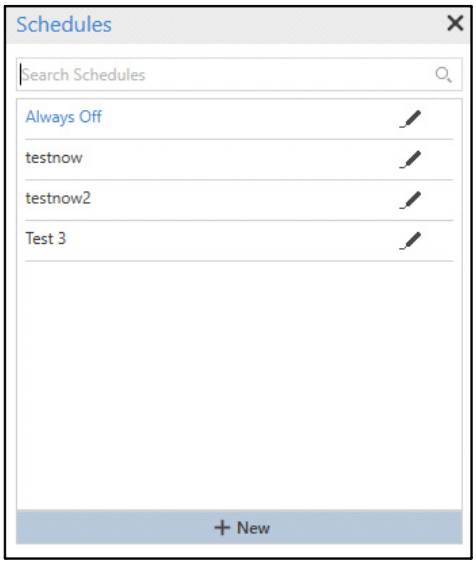
To configure Send SMS action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▼ and select **Send SMS** from the list of Actions.



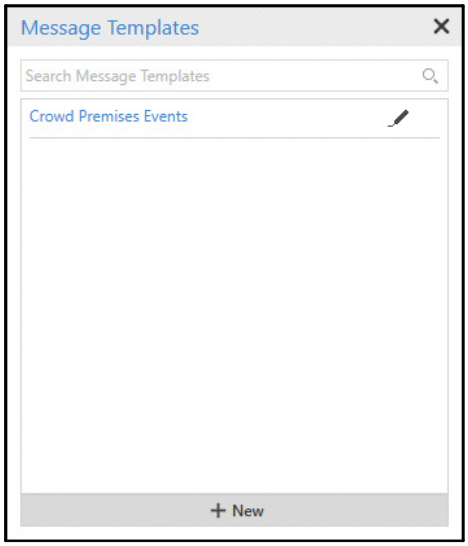
Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Message Template**: Select the desired Message Template which you wish to assign to the Action using the **Message Template** picklist.
  - Click **Message Template** picklist. The **Message Templates** pop-up appears.



- Only those templates appear in the list which are created with the same Event as selected in the Scenario. Double-click to select the desired template from the list.

  You can edit an existing template by clicking on **Edit** . You can also configure a new template by clicking **New**. For more details, refer to “Message Templates”.

- **Send next SMS**: Specify the time in minutes after which the next SMS should be sent after the Event occurence. Configure ***0 minutes*** if you want the SMS to be sent every-time when the scenario initiates, fails or resumes. In Send next SMS, you can enter upto 2 characters. Valid Range: 0-60 minutes. Default: 1.

- **Send To**: Specify the Mobile Number of the person to whom the SMS is to be sent. You can enter multiple Mobile Numbers. In Send To, you can enter upto 15 characters (for each recipient). Valid Range: 1-9999 recipients. Default: Blank.

  You can enter the User Name or the Mobile Number of the user. The matching entries will be visible. Select the desired entry. If you wish to enter a Mobile Number that is not configured in SAMAS you can type it manually. To enter multiple Mobile Numbers, type the Mobile Number/User Name and the press space bar on the keyboard to enter the next Mobile Number/User Name.

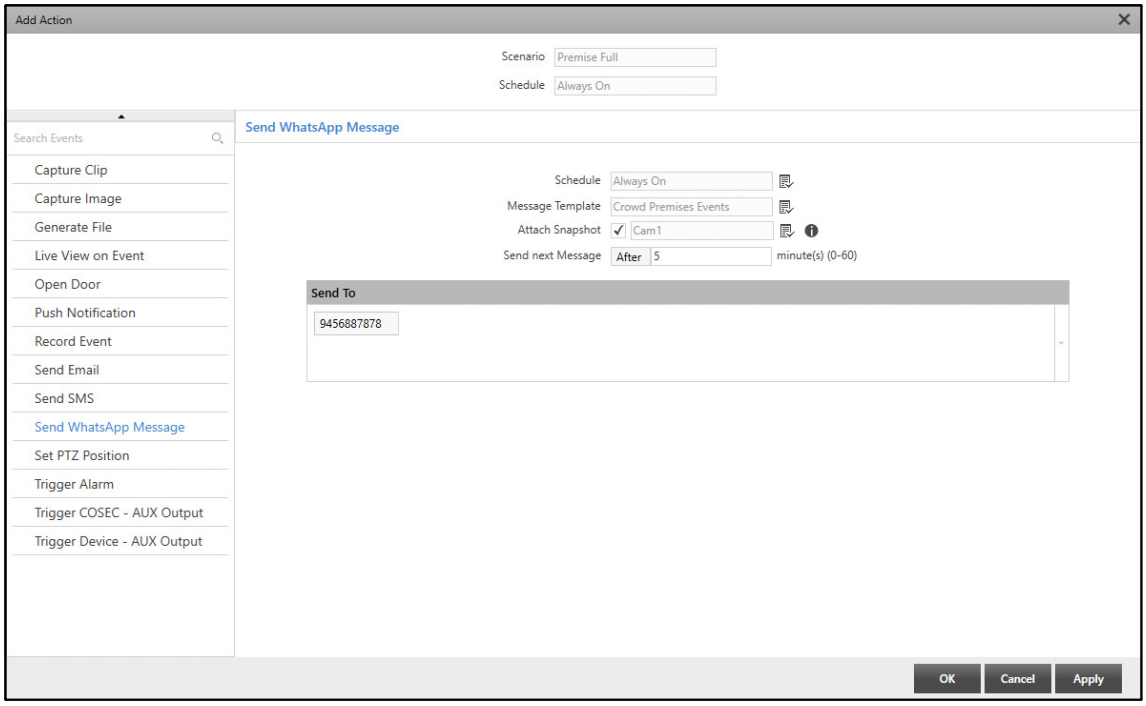
- Click **Apply** and **OK** to save the settings.

Send WhatsApp Message

The Send WhatsApp Message action sends WhatsApp Messages to the selected users on their registered WhatsApp Business Accounts for the selected Events. Refer to "WhatsApp Integration" before configuring the Send WhatsApp Message action.

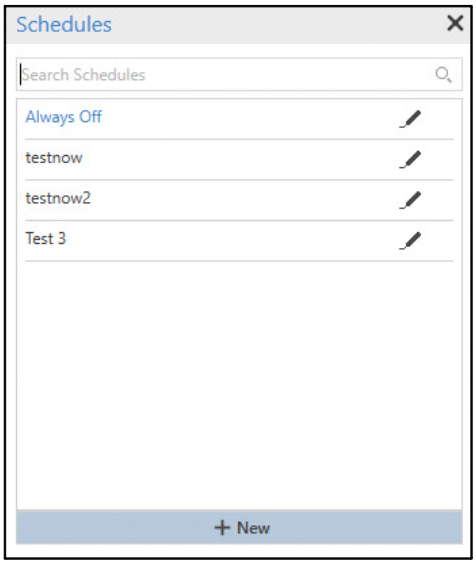
To configure Send WhatsApp Message action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▼ and select **Send WhatsApp Message** from the list of Actions.



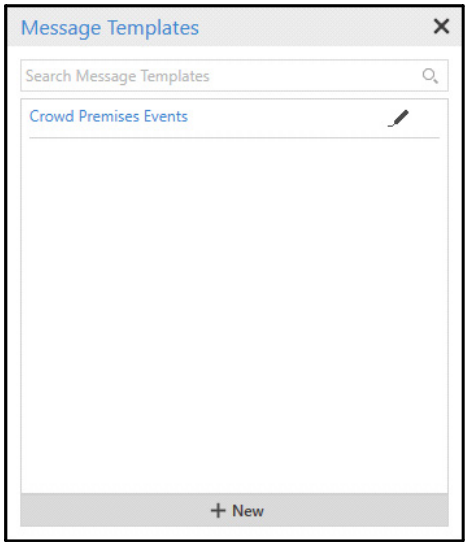
Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



  - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Message Template**: Select the desired Message Template which you wish to assign to the Action using the **Message Template** picklist.
  - Click **Message Template** picklist. The **Message Templates** pop-up appears.



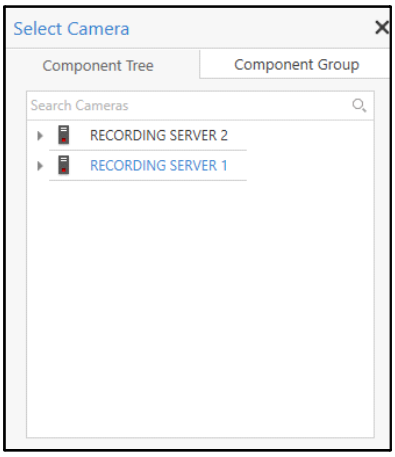
- Only those templates appear in the list which are created with the same Event as selected in the Scenario. Double-click to select the desired template from the list.

  You can edit an existing template by clicking on **Edit** . You can also configure a new template by clicking **New**. For more details, refer to “Message Templates”.

- **Attach Snapshot**: Select the check box to attach a snapshot along with the WhatsApp Message.

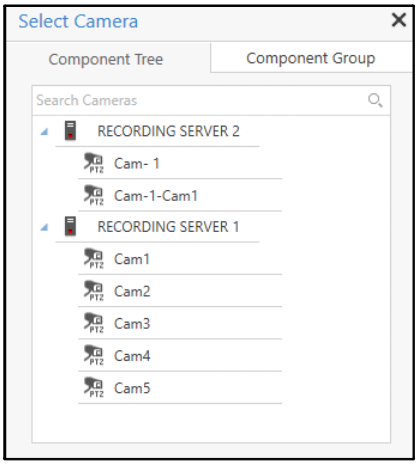
  Select the desired camera which you wish to assign to the Action using the **Camera** picklist.

  - Click **Camera** picklist. The **Select Camera** pop-up appears.



  - The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Double click the desired camera to assign it to attach the snapshots. You can also search for the desired cameras using the **Search Cameras** search bar.

Mobile Camera will not be displayed in the list of cameras as Attach Snapshot functionality is not supported by Mobile Cameras.



- **Send next Message**: Specify the time in minutes after which the next WhatsApp Message should be sent after the Event occurence. Configure ***0 minutes*** if you want the WhatsApp Message to be sent every-time when the scenario initiates, fails or resumes. In Send next Message, you can enter upto 2 characters. Valid Range: 0-60 minutes. Default: 1.

- **Send To**: Specify the Mobile Number of the person to whom the WhatsApp Message is to be sent. You can enter multiple Mobile Numbers. In Send To, you can enter upto 15 characters (for each recipient). Valid Range: 1-9999 recipients. Default: Blank.

  You can enter the User Name or the Mobile Number of the user. The matching entries will be visible. Select the desired entry. If you wish to enter a Mobile Number that is not configured in SAMAS you can type it manually. To enter multiple Mobile Numbers, type the Mobile Number/User Name and the press space bar on the keyboard to enter the next Mobile Number/User Name.

Make sure WhatsApp is activated on the Mobile Number configured here to receive WhatsApp Messages.

In case, few Mobile Numbers are not valid or do not have WhatsApp activated, then no alert will get sent to these users. The error responses will be logged in the Server Log of the Notification Server.

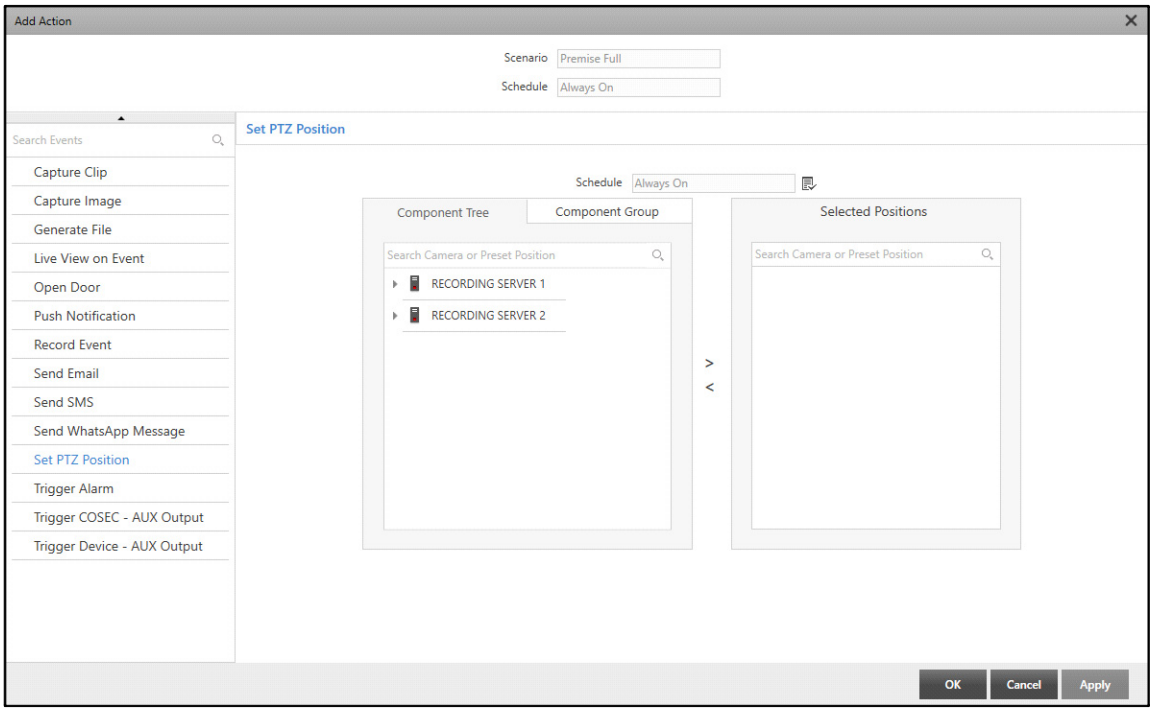
- Click **Apply** and **OK** to save the settings.

Set PTZ Position

The Set PTZ Position action moves the selected camera to the configured preset position once the Event occurs.

To configure Set PTZ Position action,

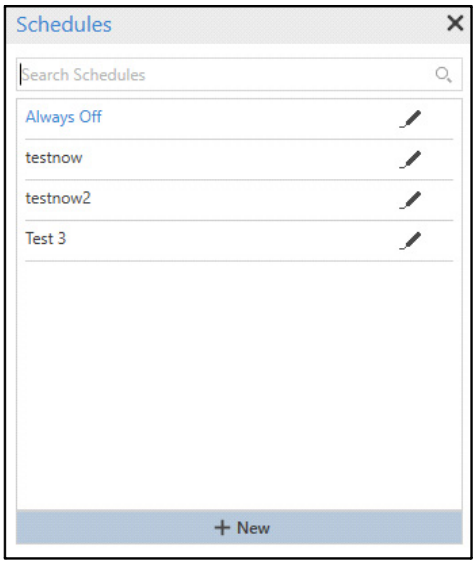
- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▾ and select **Set PTZ Position** from the list of Actions.



Configure the following parameters:

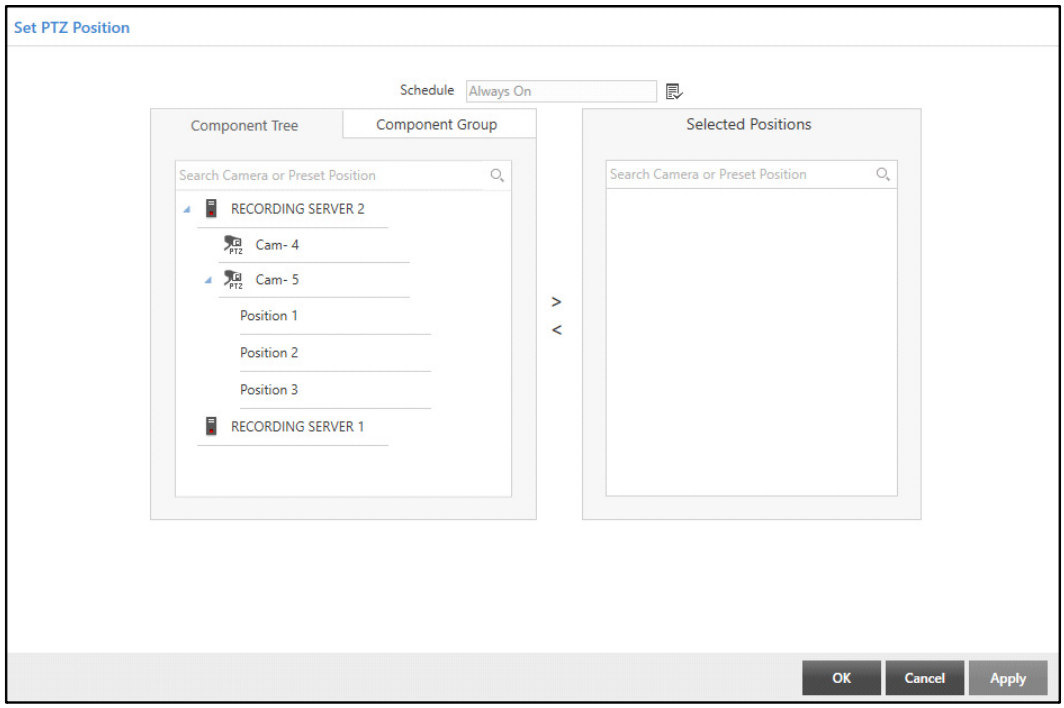
- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.

- Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

Once these configurations are done, you need to select the camera to configure its PTZ position on Event occurence.

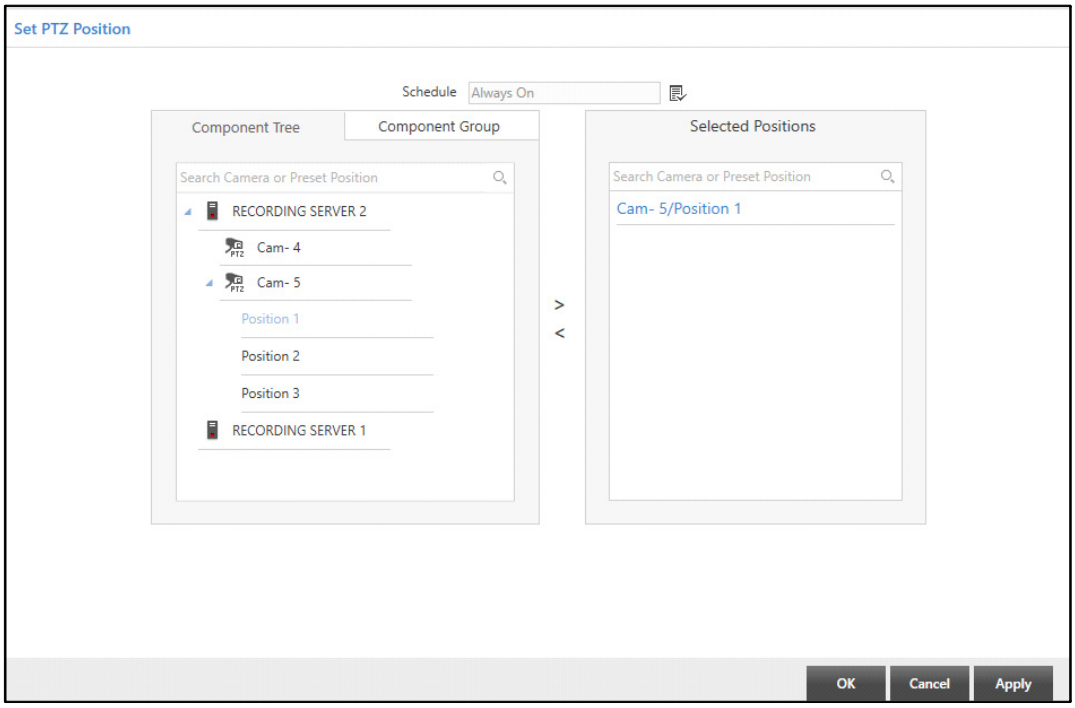


- The list of cameras added to various configured Recording Servers appears under the **Component Tree** tab. The cameras added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the desired cameras for which you wish to set the Preset Position from the

Component Tree or Component Group tabs. Click ▶ to view the Preset Positions of the selected Camera. Select the desired Preset Position and click the right arrow button to add the position in the **Selected Positions** list. You can also search for the desired cameras or Preset Position using the **Search Camera or Preset Position** search bar.

To remove positions, select the desired positions you wish to remove from the Selected Positions list. Click the left arrow button to remove the positions from the Selected Positions list.

You can add only one Preset Position for a PTZ camera. However, you can add multiple PTZ cameras with a single Preset Position for each.



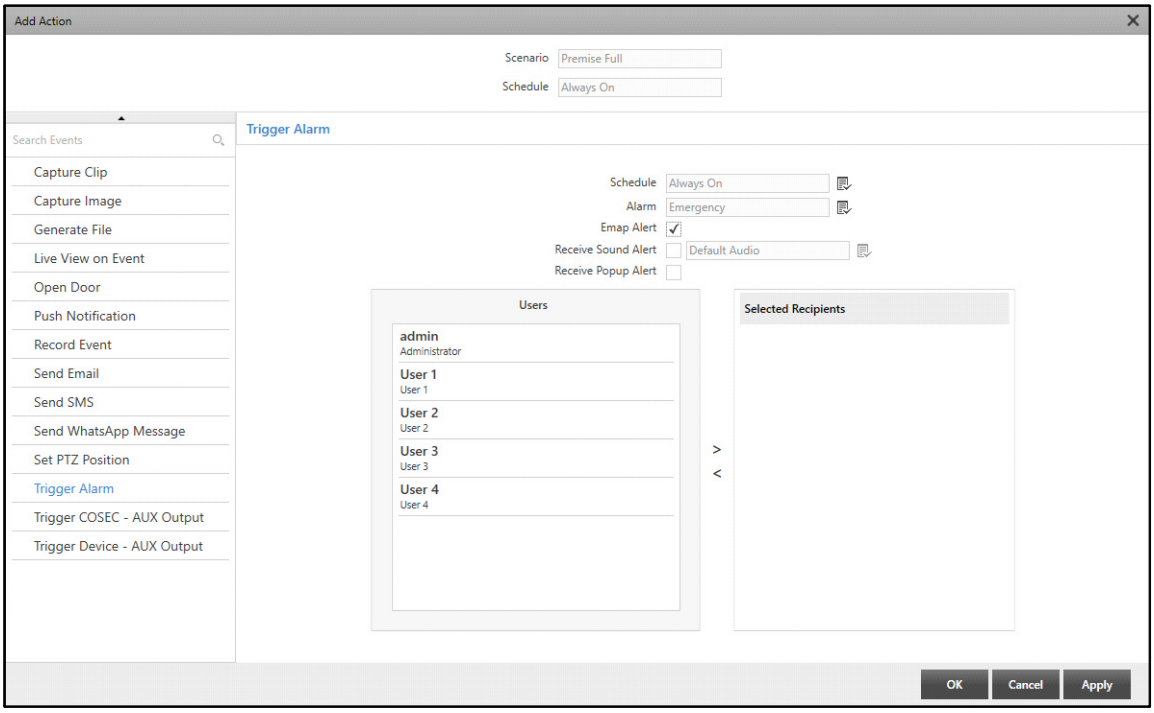
- Click **Apply** and **OK** to save the settings.

Trigger Alarm

The Trigger Alarm action triggers an alarm once the Event occurs.

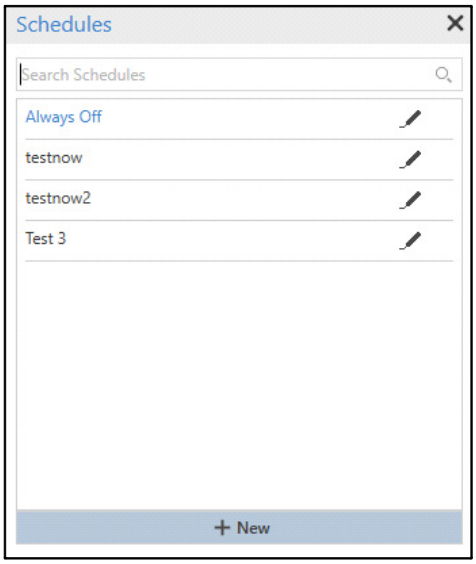
To configure Trigger Alarm action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▼ and select **Trigger Alarm** from the list of Actions.



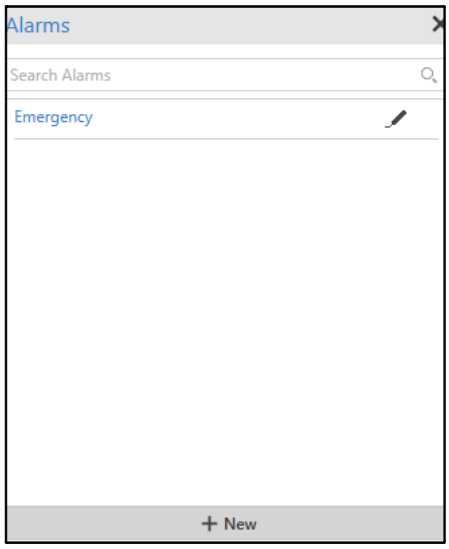
Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



    - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".
- **Alarm**: Select the desired Alarm which you wish to assign to the Action using the **Alarm** picklist.

- Click **Alarm** picklist. The **Alarms** pop-up appears.

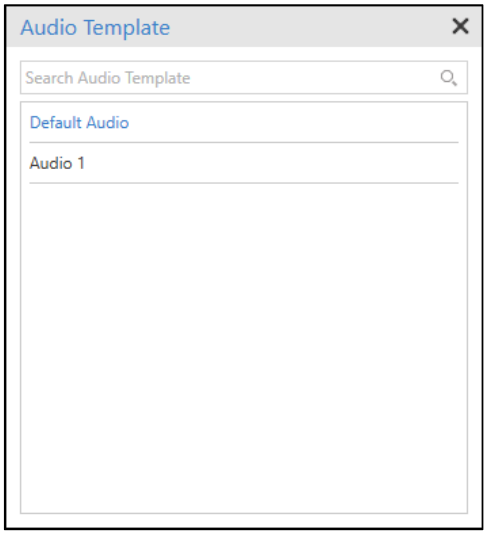


  - Double-click to select the desired alarms from the list. You can edit an existing alarm by clicking on **Edit** . You can also configure a new alarm by clicking **New**. For more details, refer to “Alarms”.

- **Emap Alert**: Select the check box if you wish to receive an EMAP alert for the Action. Whenever Alarm is triggered on Scenario initiation, the EMAP entity linked to the Scenario will start blinking in the Smart Client.

- **Receive Sound Alert**: Select the check box if you wish to receive a sound alert for the Action. Select the desired Audio Template you wish to assign to the alert using the **Audio Template** picklist.

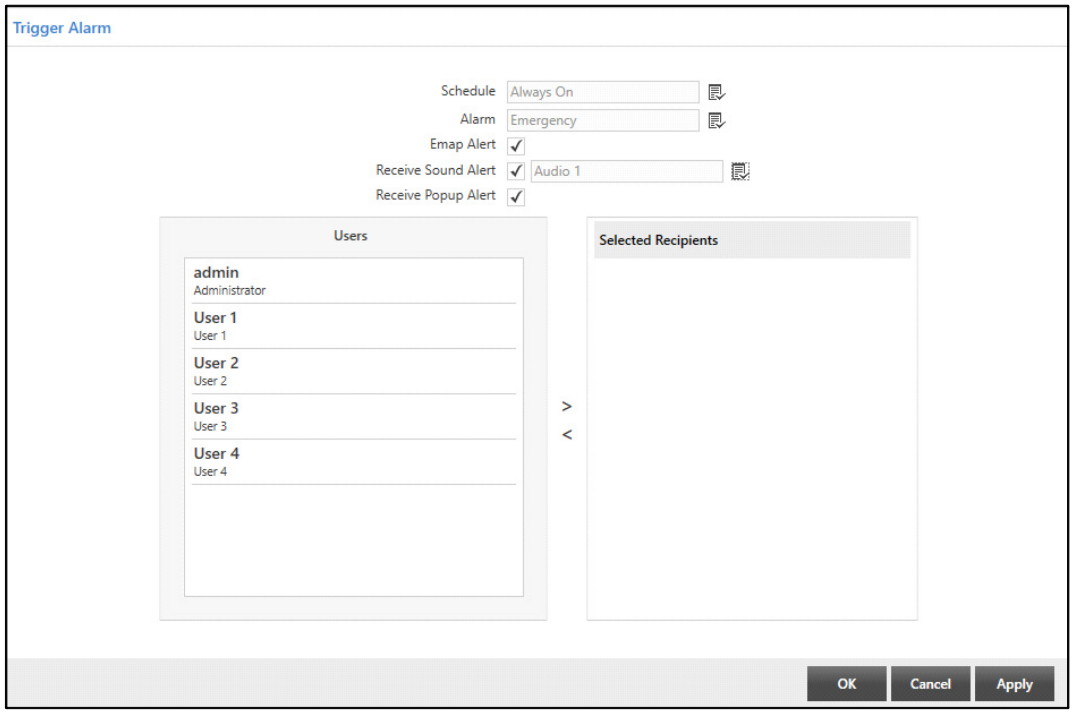
  - Click **Select Audio Template** picklist. The **Audio Template** pop-up appears.



  - Double-click to select the desired Audio Template from the list.

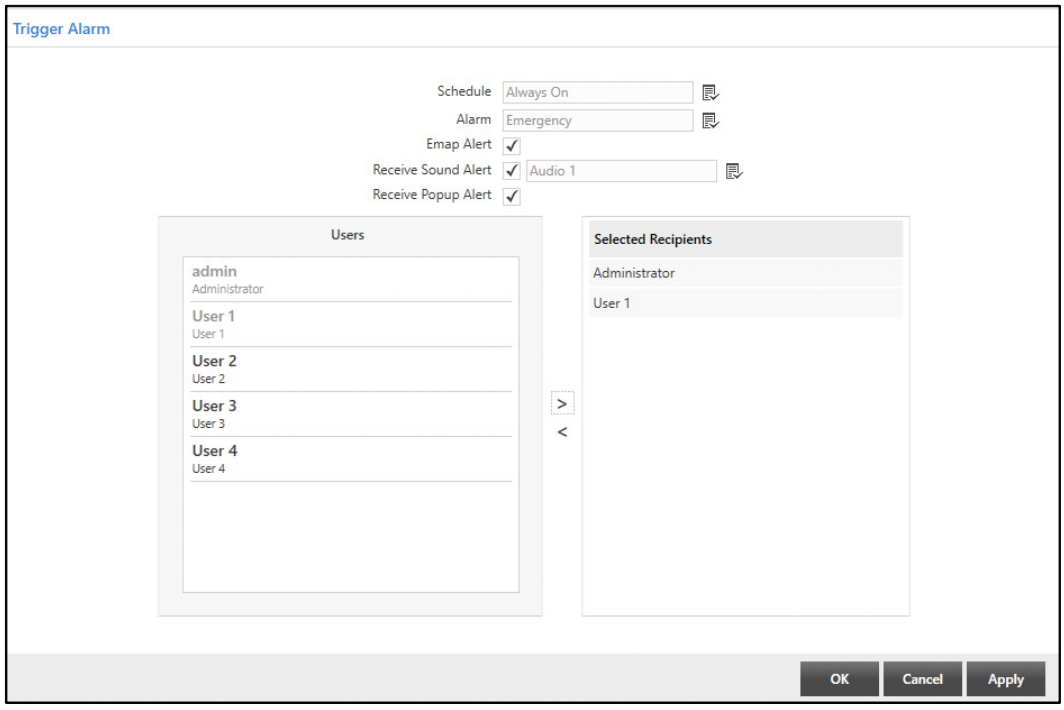
- **Receive Popup Alert**: Select the check box if you wish to receive a pop-up alert for the Action.

Once these configurations have been done, you need to select the users who have to be notified about the Event occurence.



- The list of configured users appears under the **Users** list. Select the desired users you wish to notify about the Action from the Users list. Click the right arrow button to add these users in the **Selected Recipients** list.

  To remove users, select the desired users you wish to remove from the Selected Recipients list. Click the left arrow button to remove the users from the Selected Recipients list.



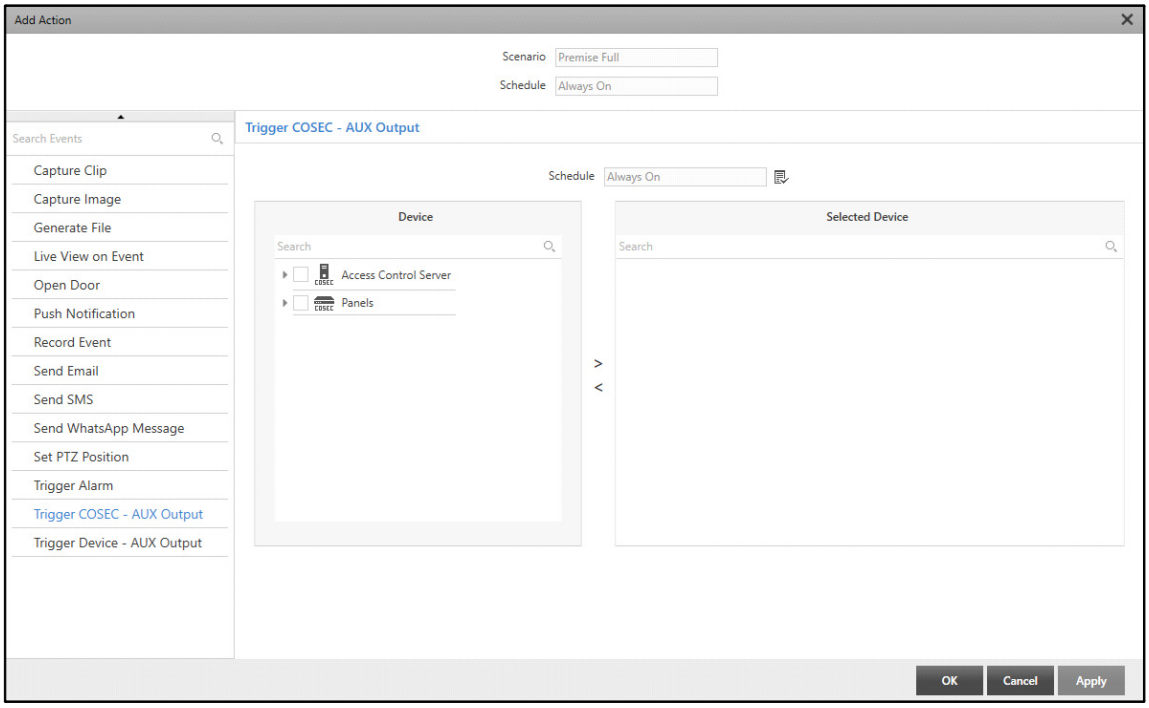
- Click **Apply** and **OK** to save the settings.

Trigger COSEC - AUX Output

The Trigger COSEC- Aux Output action triggers a COSEC device alarm added to the configured devices once the Event occurs.

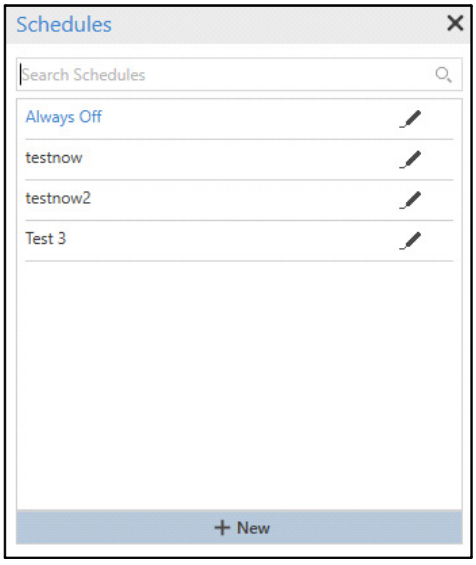
To configure Trigger COSEC- AUX Output action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▼ and select **Trigger COSEC- AUX Output** from the list of Actions.



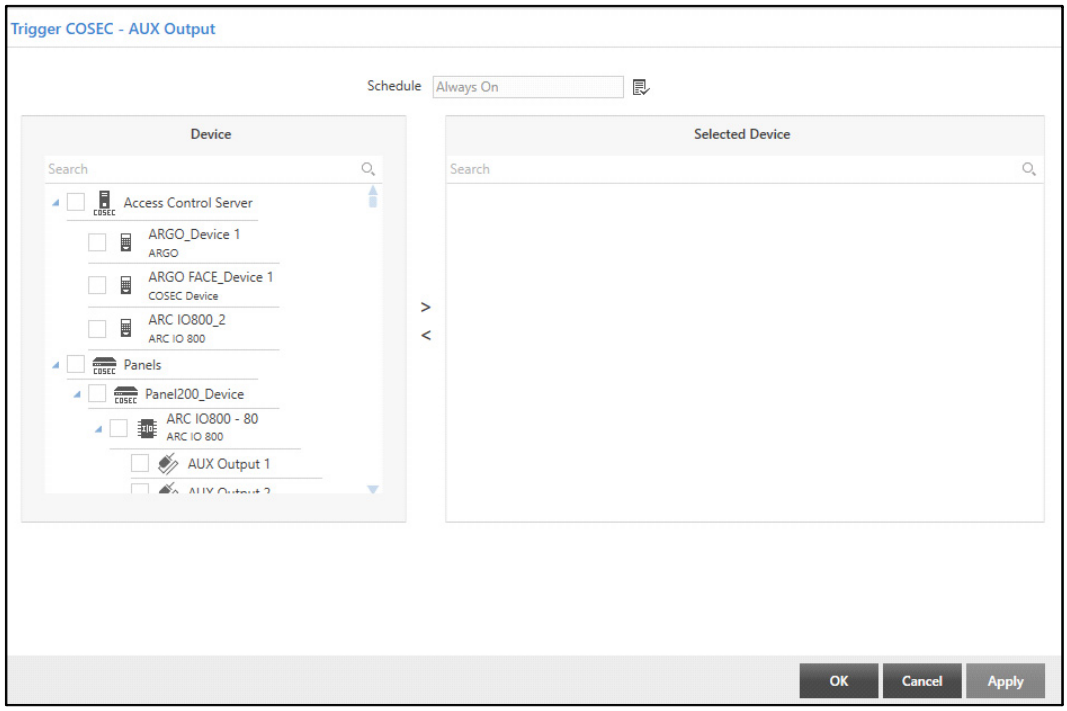
Configure the following parameters:

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



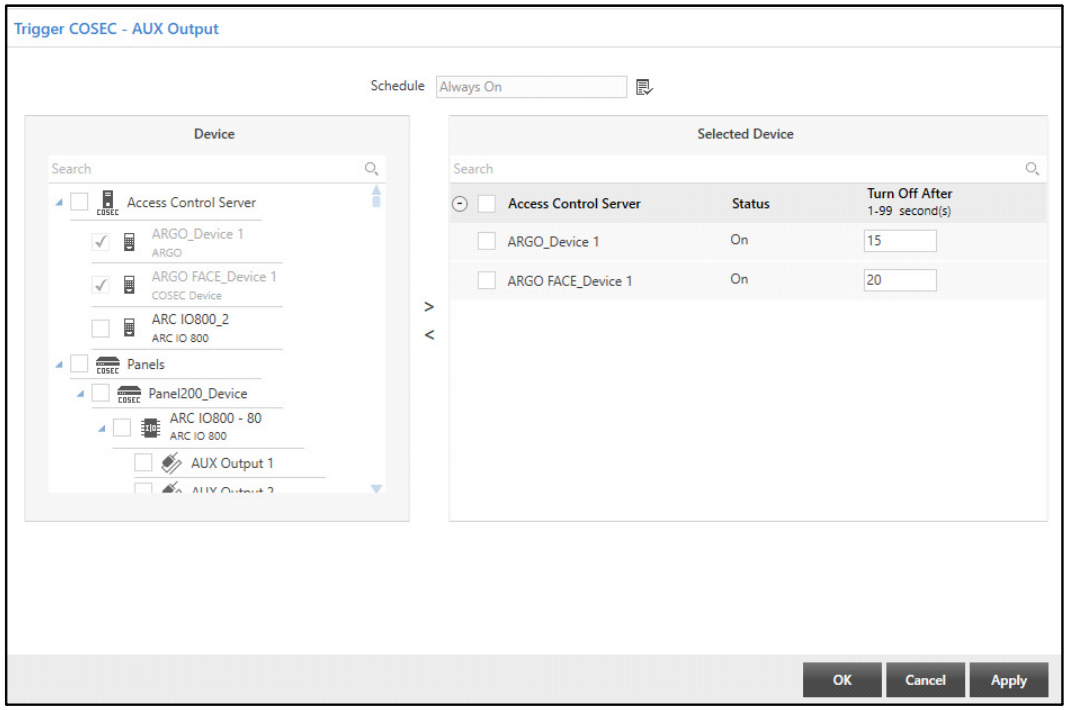
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

Once these configurations are done, you need to select the devices to trigger device alarms Event occurence.



- The list of COSEC devices added to the Access Control Server and COSEC Panel appears in the **Device** list. Select the check boxes of the desired devices you wish to add from the Device list. Click the right arrow button to add the devices in the **Selected Device** list.

To remove devices, select the desired check boxes for the devices you wish to remove from the Selected Device list. Click the left arrow button to remove the devices from the Selected Device list.



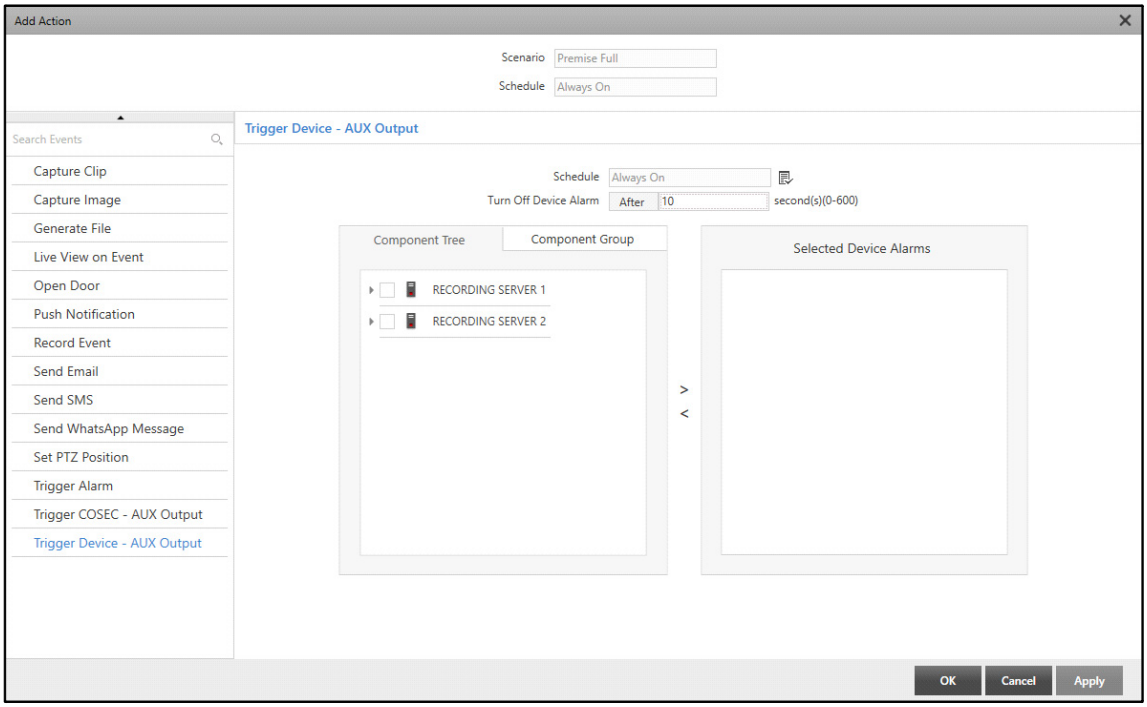
- The added devices appear in the **Selected Device** list. The device details displayed are Device Name, Status and Turn Off After.
- **Turn Off After** is the time in seconds after which the particular device will turn off after Event occurence. In Turn Off After, you can enter upto 2 characters. Valid Range: 1-99 seconds. Default:10. You can configure the same as per your requirement.
- Click **Apply** and **OK** to save the settings.

Trigger Device - AUX Output

The Trigger Device- AUX Output action triggers an alarm added to the configured devices once the Event occurs.

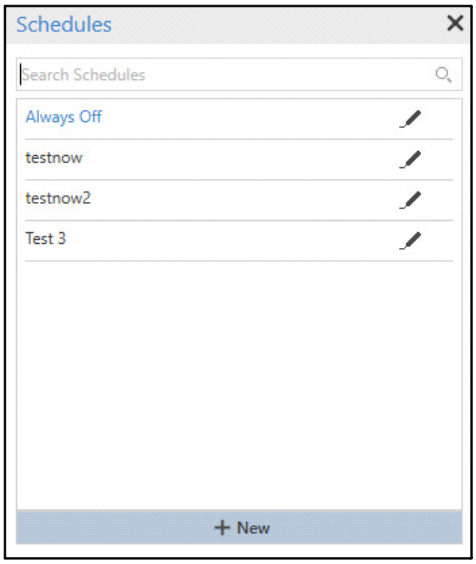
To configure Trigger Device- AUX Output action,

- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.
- Click ▾ and select **Trigger Device- AUX Output** from the list of Actions.



Configure the following parameters:

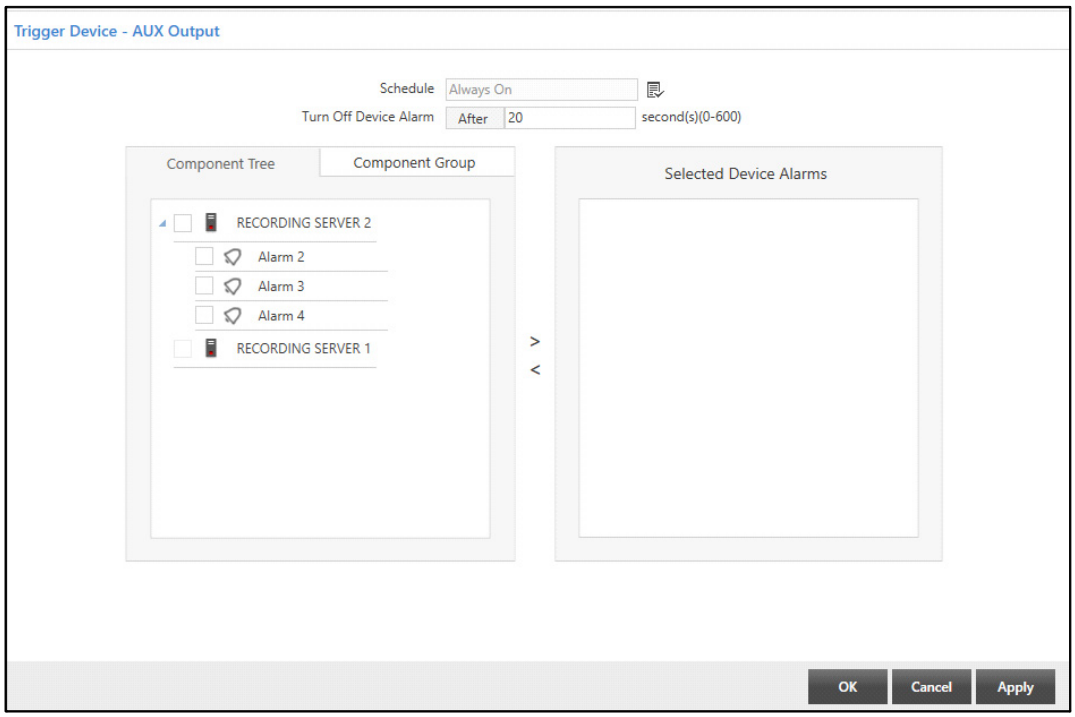
- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

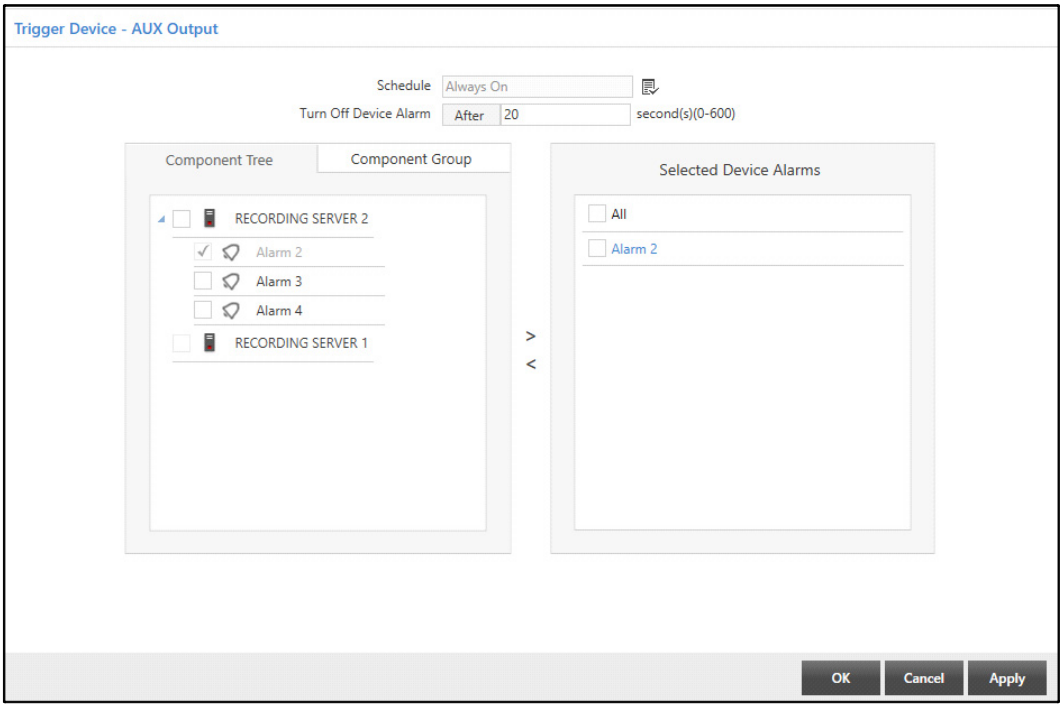
- **Turn Off Device Alarm**: Specify the time in seconds after which the device alarm should turn off after Event occurence. In Turn Off Device Alarm, you can enter upto 3 characters. Valid Range: 0-600 seconds. Default: 10.

Once these configurations are done, you need to select the device alarms to be triggered on Event occurence.



- The list of device alarms added to various configured Recording Servers appears under the **Component Tree** tab. The alarms added to different groups appear under the **Component Group** tab. To know more, refer to “Component Group”. Select the check boxes of the desired alarms you wish to add from the Component Tree or Component Group tabs. Click the right arrow button to add the alarms in the **Selected Device Alarms** list.

  To remove alarms, select the check boxes of the desired alarms you wish to remove from the Selected Device Alarms list. Click the left arrow button to remove the alarms from the Selected Device Alarms list.



- Click **Apply** and **OK** to save the settings.

Actions for Advanced Scenario

All the actions that can be configured for Basic Scenario can be configured for Advanced Scenario as well. However certain actions can be configured from Advanced Scenario only, namely, Import File, Trigger IVA Detection and Wait.

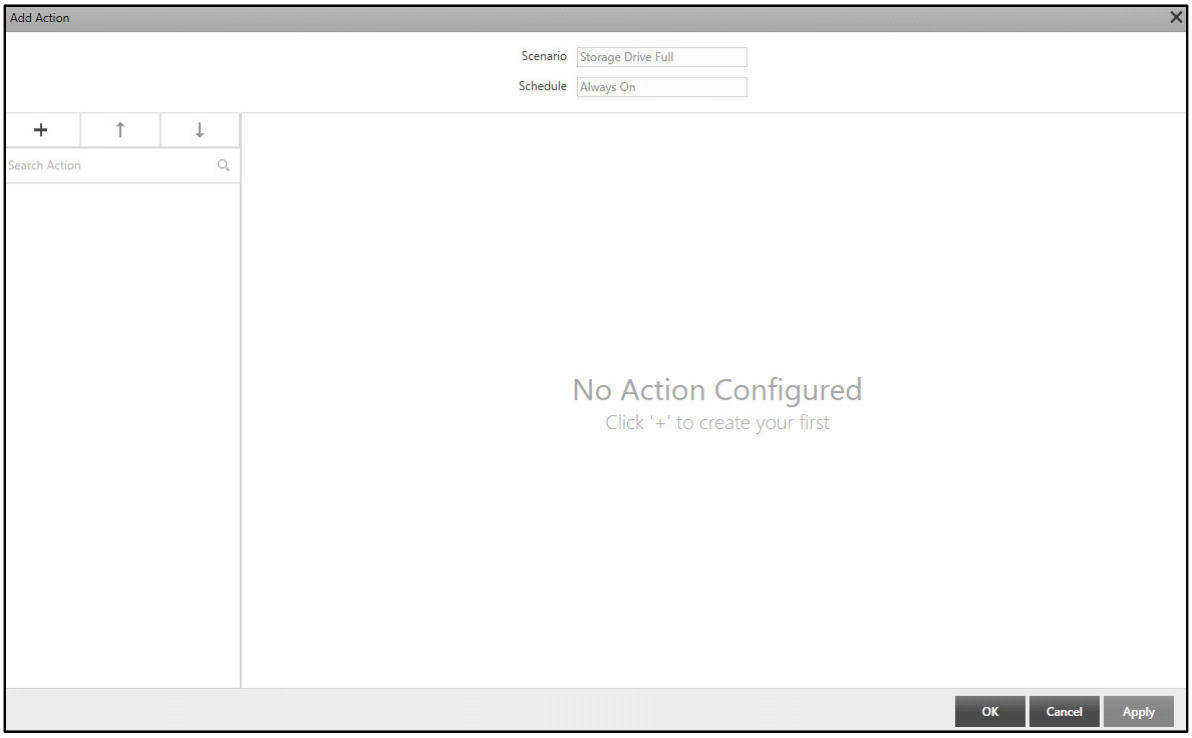
Import File

The Import File action imports a file from the configured Storage Drive once the Event occurs. Make sure you place the desired files which you wish to import in the Backup Storage Drive of the desired Recording Server.

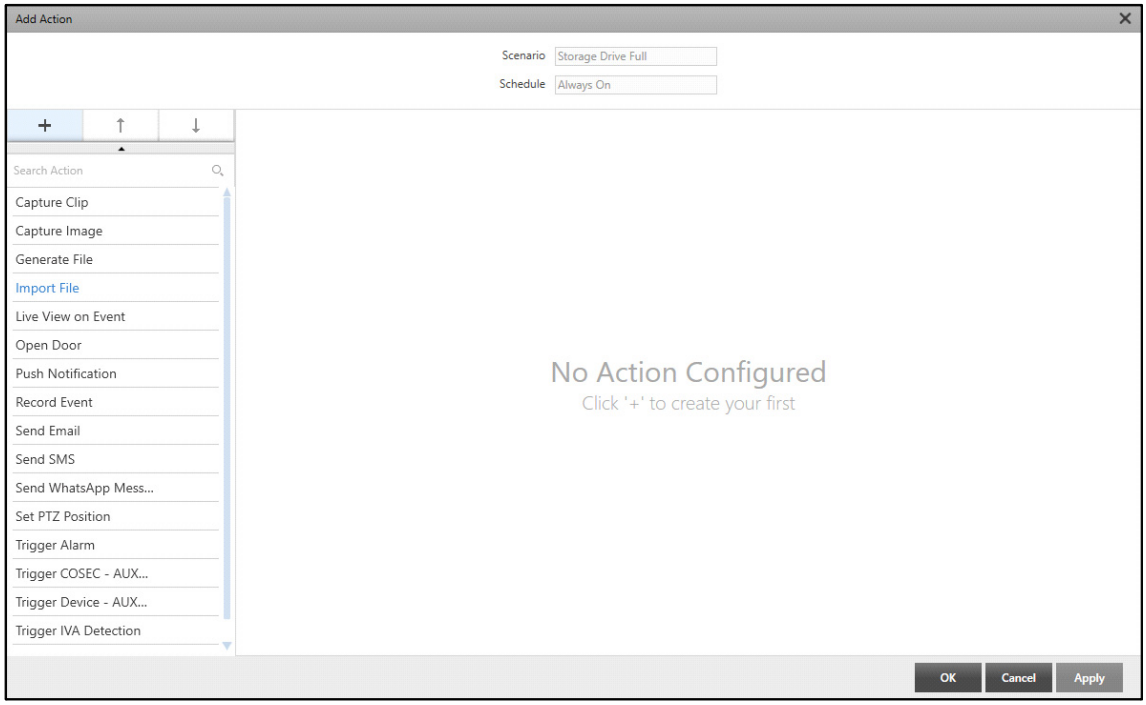
Make sure the Field Length of the fields in the Import file do not exceed 200 characters.

To configure Import File action,

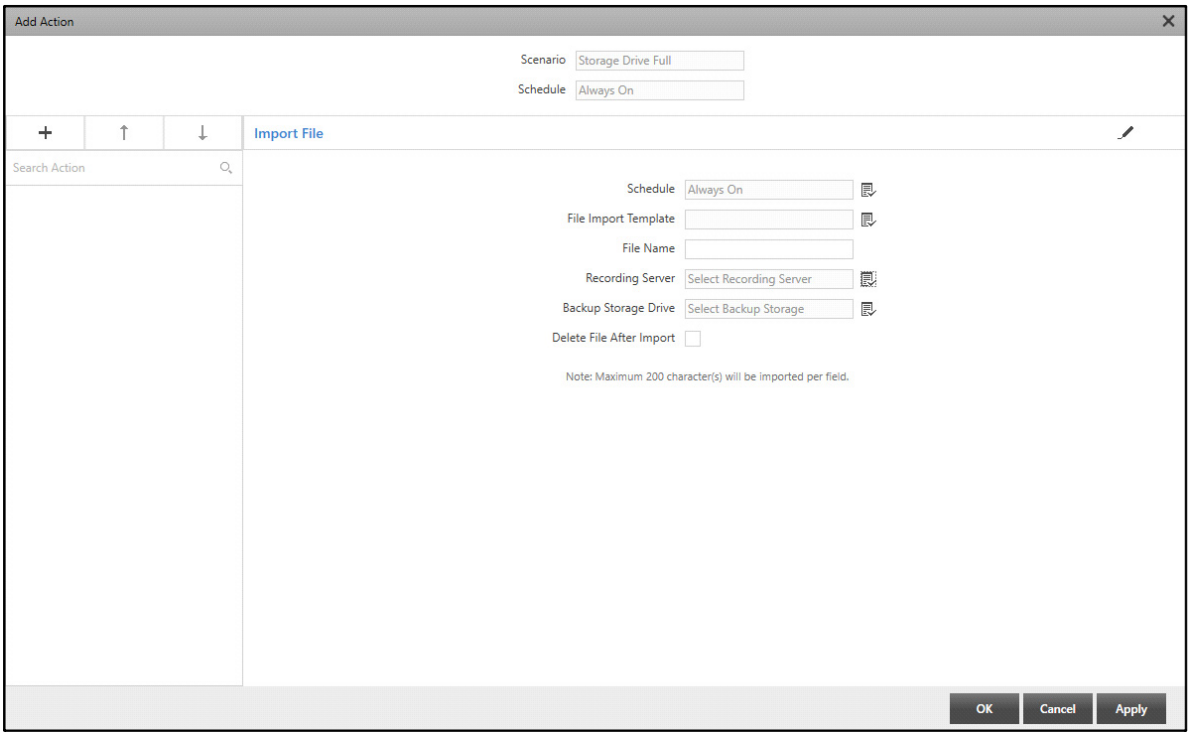
- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.



- Click **Add Action** + **.** A list of all the system-defined actions appear.



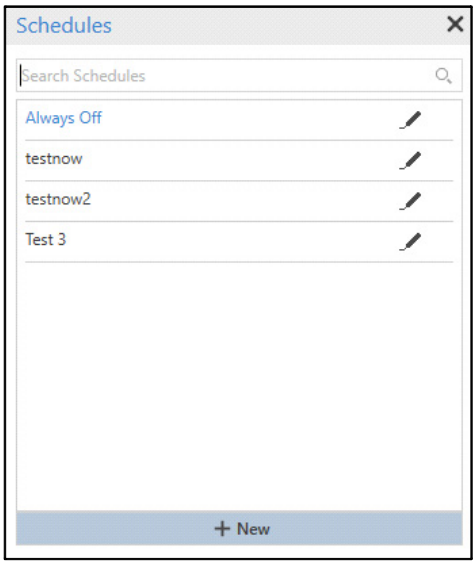
- Select **Import File** from the list of Actions.



- You can edit the name of the Action. To do so click **Edit** , if required.

  Configure the following parameters:

  - **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **File Import Template**: Select the desired File Import Template which you wish to assign to the Action using the **File Import Template** picklist. Double-click to select the desired option.
- **File Name**: Specify a suitable name for the File to be imported on Event occurence. In File Name, you can enter upto 50 characters. Default: Blank.
- **Recording Server**: Select the desired Recording Server using the **Recording Server** picklist. Double-click to select the desired option.
- **Backup Storage Drive**: Select the desired Backup Storage Drive using the **Backup Storage Drive** picklist.Double-click to select the desired option.
- **Delete File After Import**: Select the check box if you wish to delete the file after importing all the data.

- Click **Apply** and **OK** to save the settings.

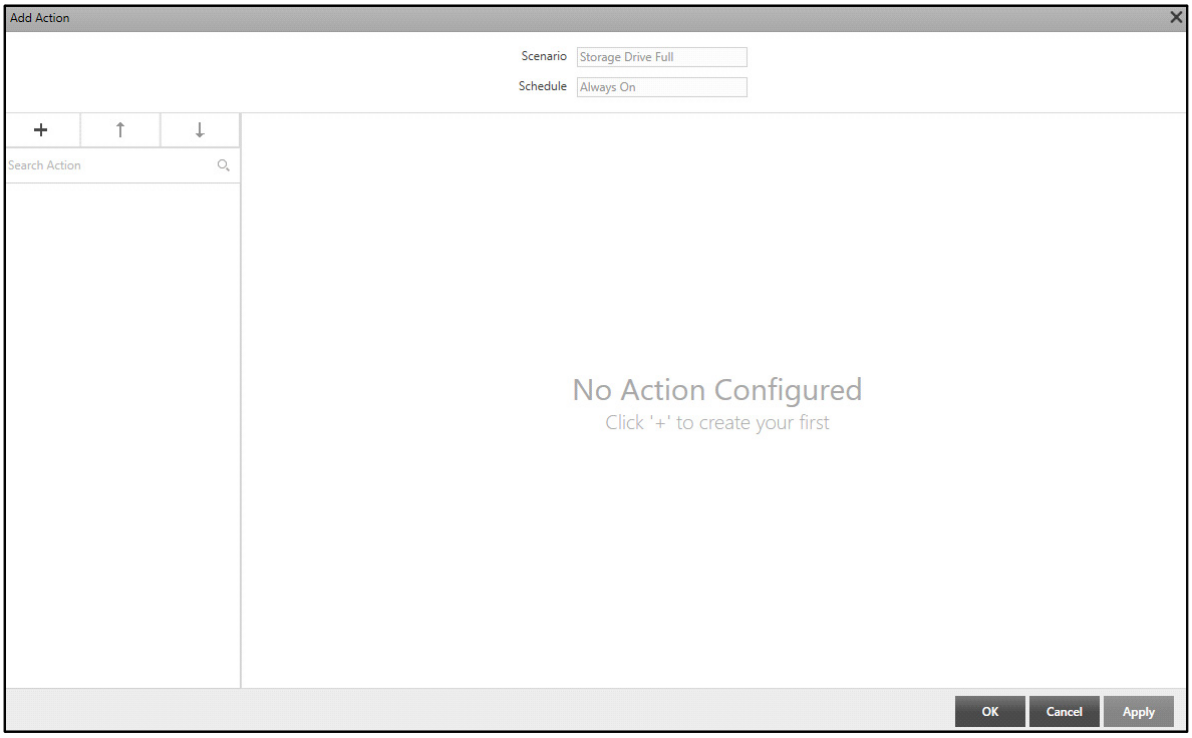
The configured Action appears in the list on the left hand side.

Trigger IVA Detection

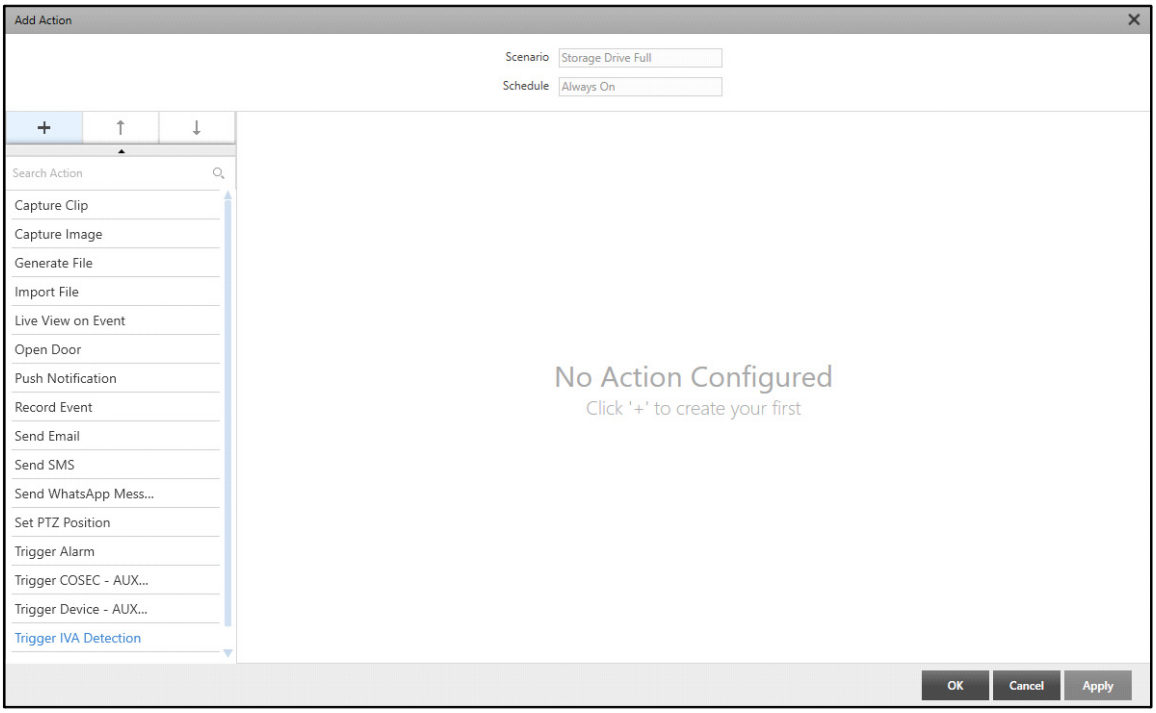
The Trigger IVA Detection action triggers another IVA detection as an action on getting a specific IVA alert once the Event occurs.

To configure Trigger IVA Detection action,

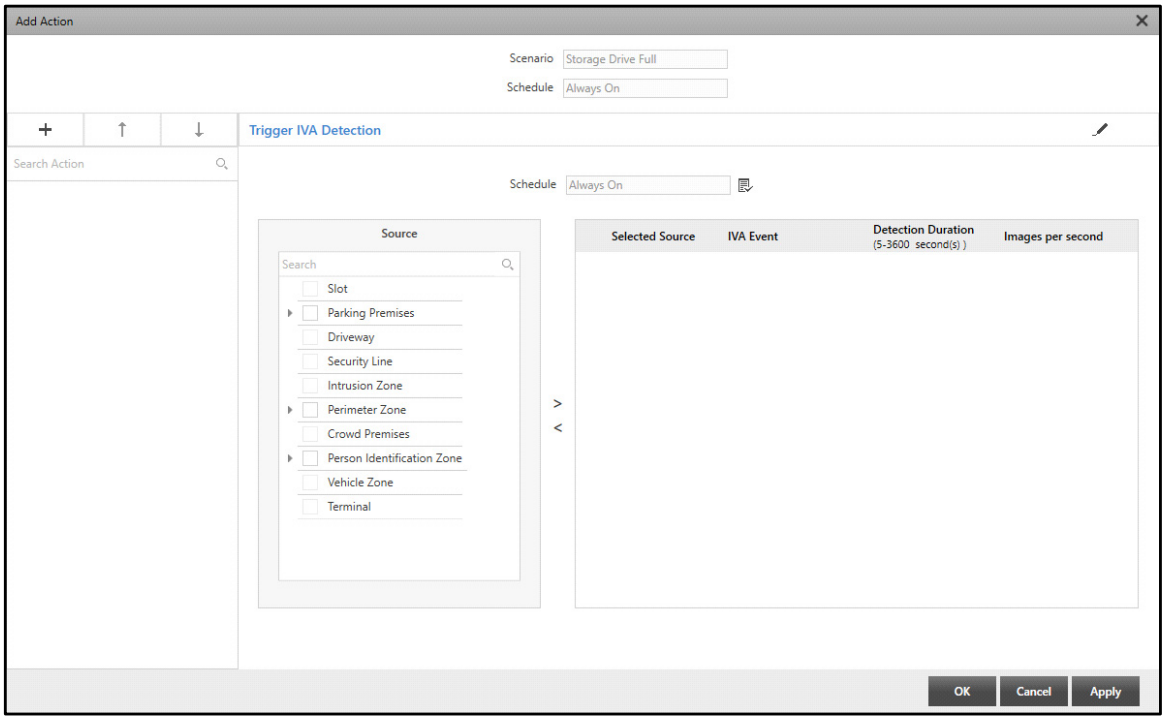
- Click **Add Action** to add Actions to the configured Scenario. The **Add Action** pop-up appears.



- Click **Add Action** + **.** A list of all the system-defined actions appears.



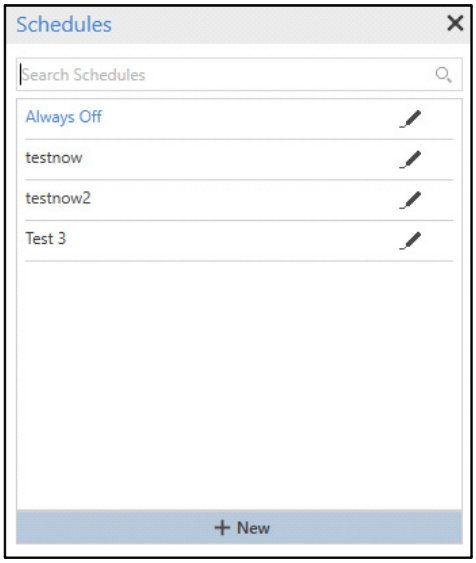
- Select **Trigger IVA Detection** from the list of Actions.



- You can edit the name of the Action using **Edit** , if required.

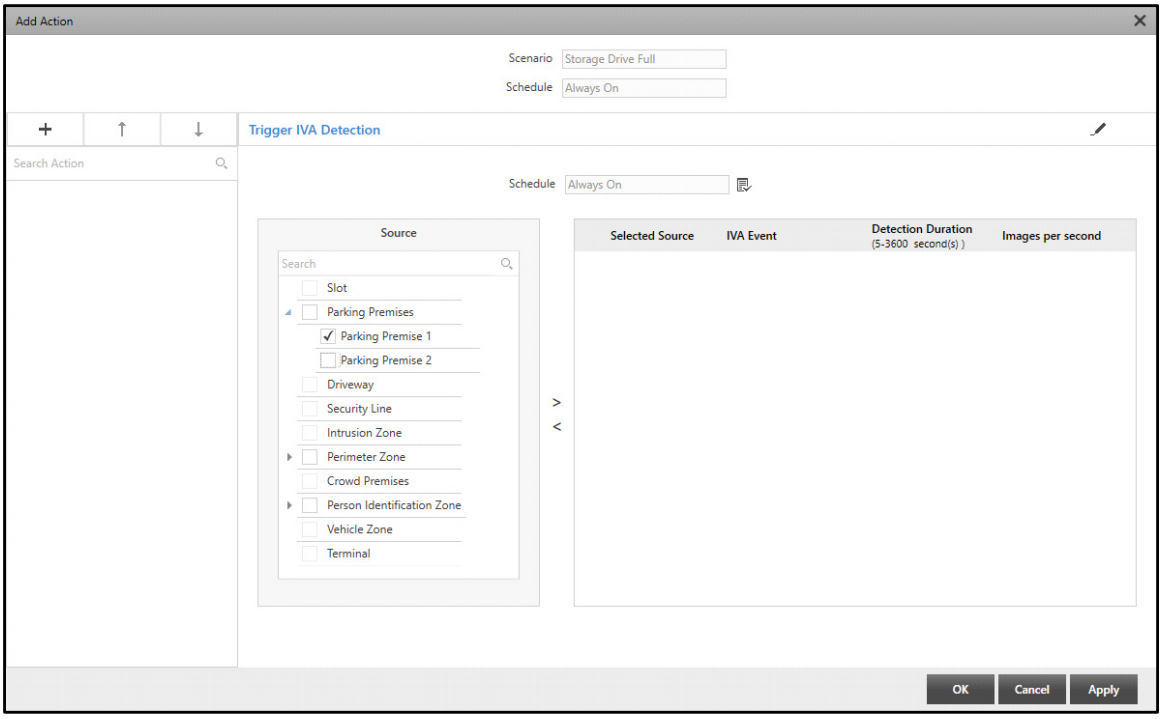
  Configure the following parameters:

  - **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



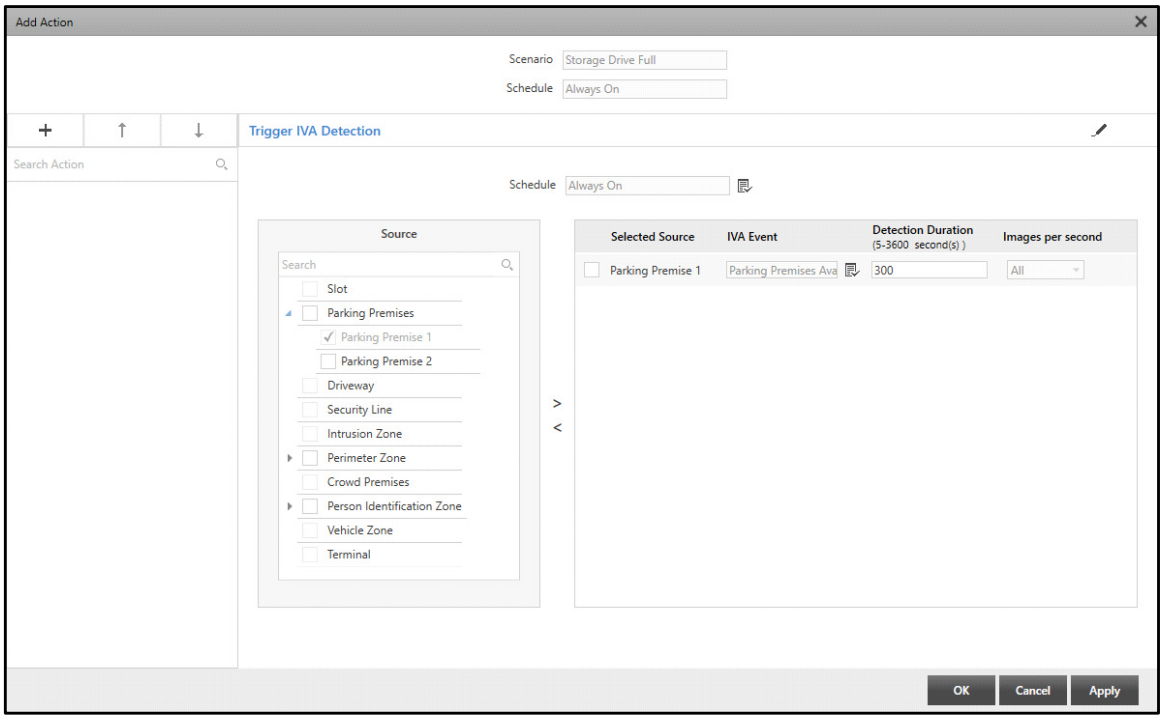
- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

Once these configurations are done, you need to select the **Source** to trigger IVA Detection on Event occurence.



- The list of Source entities for which Events can be detected appears in the **Source** list. Select the check boxes of the desired sources you wish to add from the Source list. Click the right arrow button to add the sources in the **Selected Source** list.

  To remove sources, select the check boxes of the desired sources you wish to remove from the Selected Source list. Click the left arrow button to remove the sources from the Selected Source list.



Once you select a source, configure the following parameters:

- **IVA Event**: Select the IVA Event to be detected using the **IVA Event** picklist. Select the check box for the desired event or select the **IVA Event** check box to select all the events. You can also search for the desired Object Types using the search bar. Click **OK**.
- **Detection Duration**: Specify the duration in seconds for which the Event is to be detected. In Detection Duration, you can enter upto 4 characters. Valid Range: 5-3600 seconds. Default: 300.
- **Images per Second**: Select the number of images from the drop-down list to be sent to ARH Engine by IVA Server when the Trigger IVA Detection action is taking place for the selected source. You can configure this only for Vehicle Zones and Driveways.

- Click **Apply** and **OK** to save the settings.

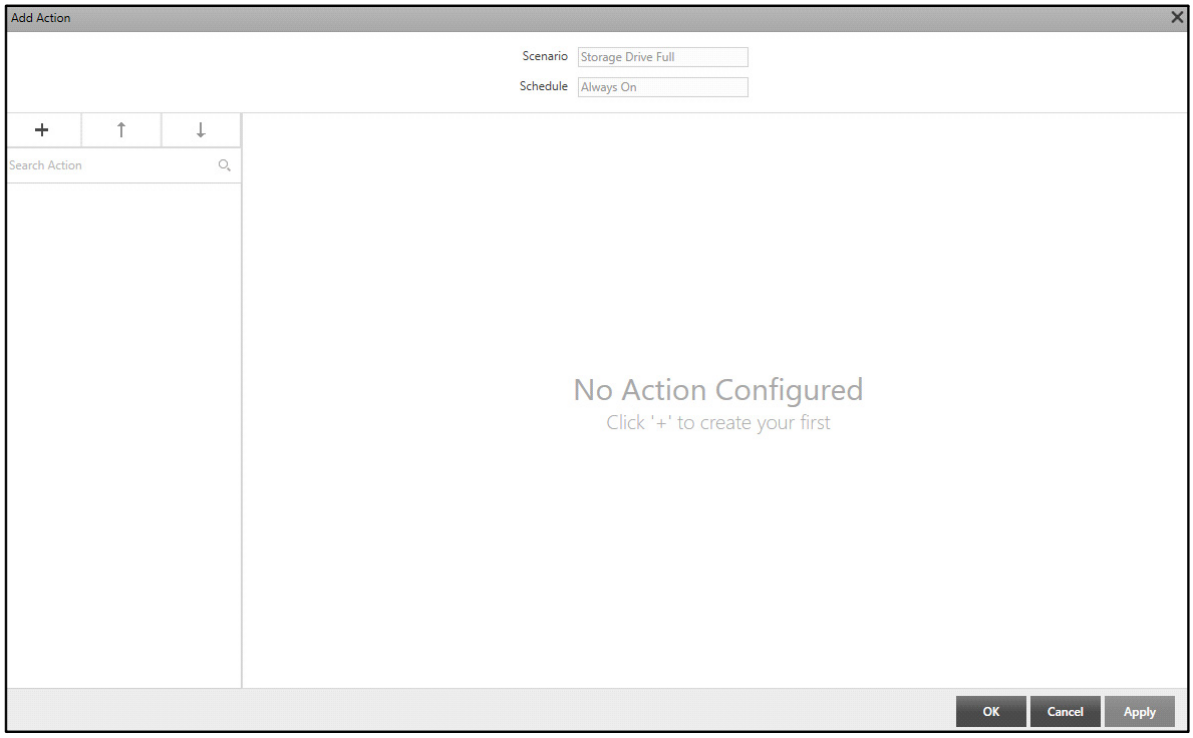
The configured Action appears in the list on the left hand side.

Wait

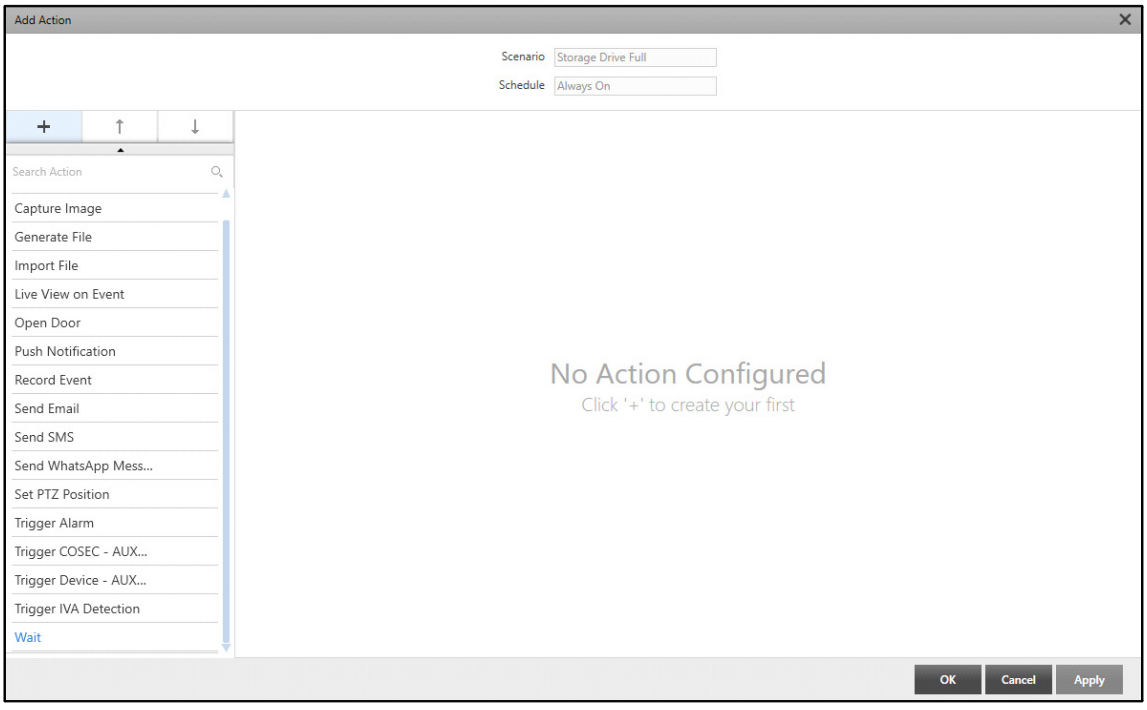
The Wait action enables the system to wait for the Event to occur from the configured Source.

To configure the Wait action,

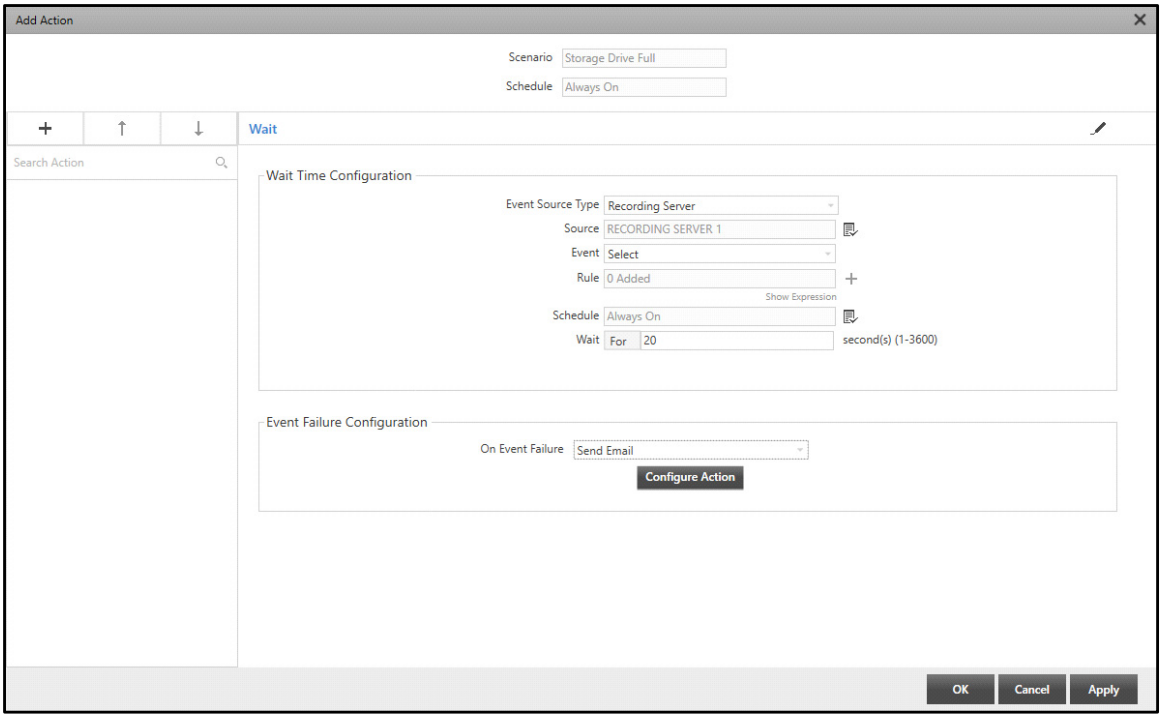
- Click **Add Action** to add Actions to the configured Scenario. The **Add Action** pop-up appears.



- Click **Add Action** + **.** A list of all the system-defined actions appears.



- Select **Wait** from the list of Actions.

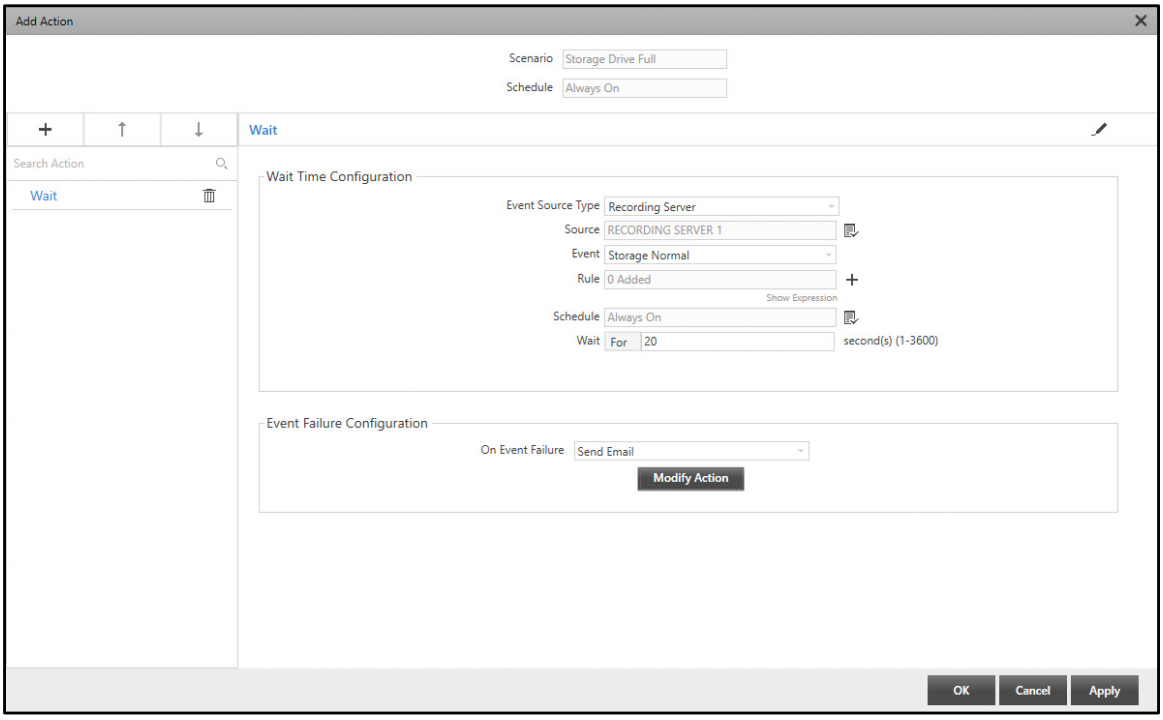


- You can edit the name of the Action using **Edit** , if required.

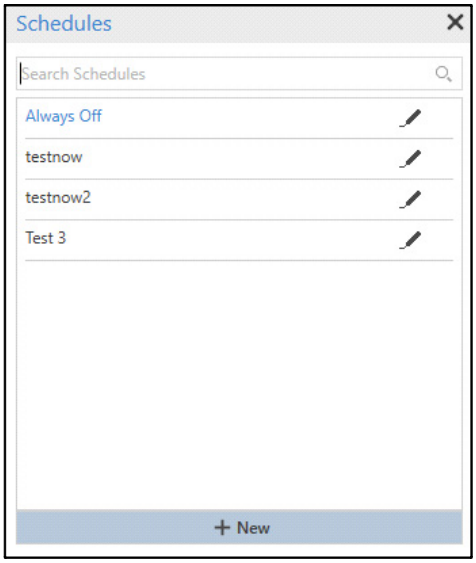
The **Wait** action consists of two sections — "Wait Time Configuration" and "Event Failure Configuration".

Wait Time Configuration

- **Event Source Type**: Select the Event Source Type from the drop-down list.
- **Source**: Select the Source for which you wish to configure the action using the **Source** picklist. The Source depends on the selected Event Source Type. Double-click to select the desired option.



- **Event**: Select the Event for which you wish to configure the action.
- **Rule**: Click **Add** to add a Rule for the action. Double-click to select the desired option. For detailed configuration of Rules, refer to “Add Rule”.
- **Schedule**: Select the desired Schedule which you wish to assign to the Scenario using the **Schedule** picklist.
  - Click **Schedule** picklist. The **Schedules** pop-up appears.



- Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to "Schedules".

- **Wait For**: Specify the time for which the system has to wait for the occurence of the event. In Wait For, you can enter upto 4 characters. Valid Range: 1-3600 recipients. Default: 10.

- Click **Apply** to apply the changes.

Event Failure Configuration

- **On Event Failure**: Select the action to be taken on failure of the Event from the drop-down list.

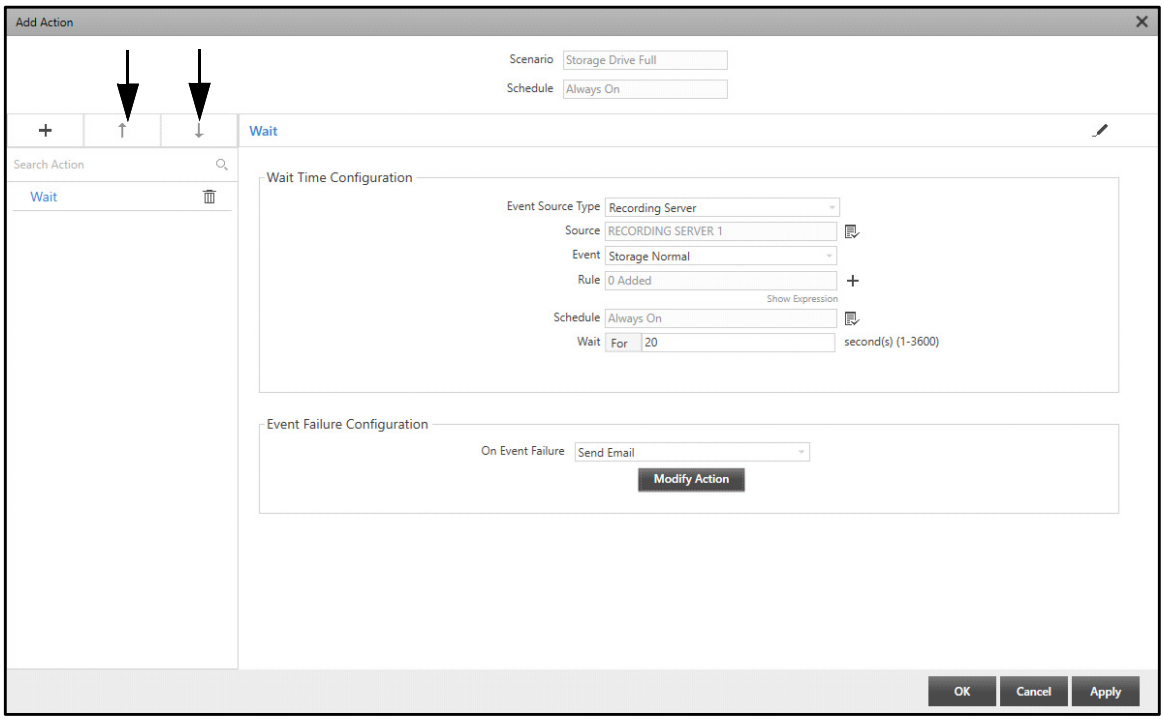
- Click **Configure Action**. A pop-up to configure the selected action appears. These action configurations are similar to that of the Actions of other modules. For detailed configurations, refer to "Configuring Actions for Events".

- Click **OK** to confirm or click **Cancel** to discard.

The configured Action appears in the list on the left hand side.

All the configured Actions appear in a list on the left hand side. You can change the sequence of the Actions to be taken on Event occurence. To do so,

- Select an desired Action. Click **Up** or **Down** arrow to move the selected action up or down in the list.



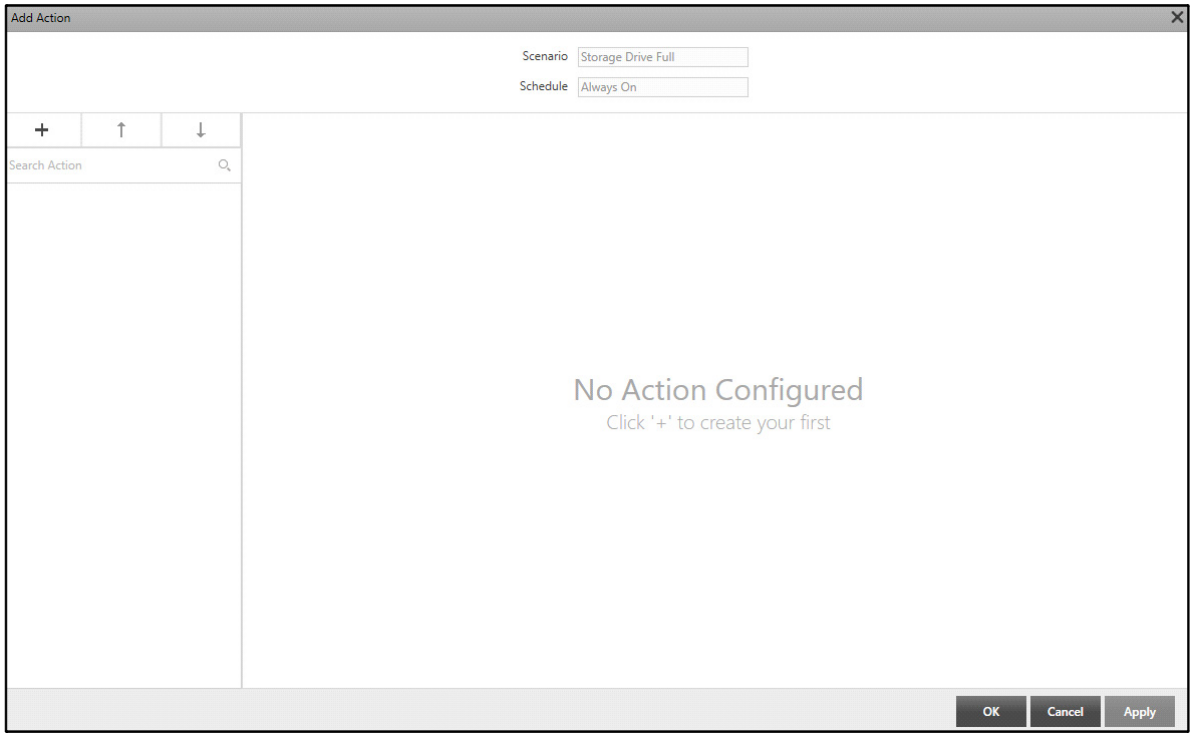
- Click **Apply** and **OK** to save the settings.

Push Notification

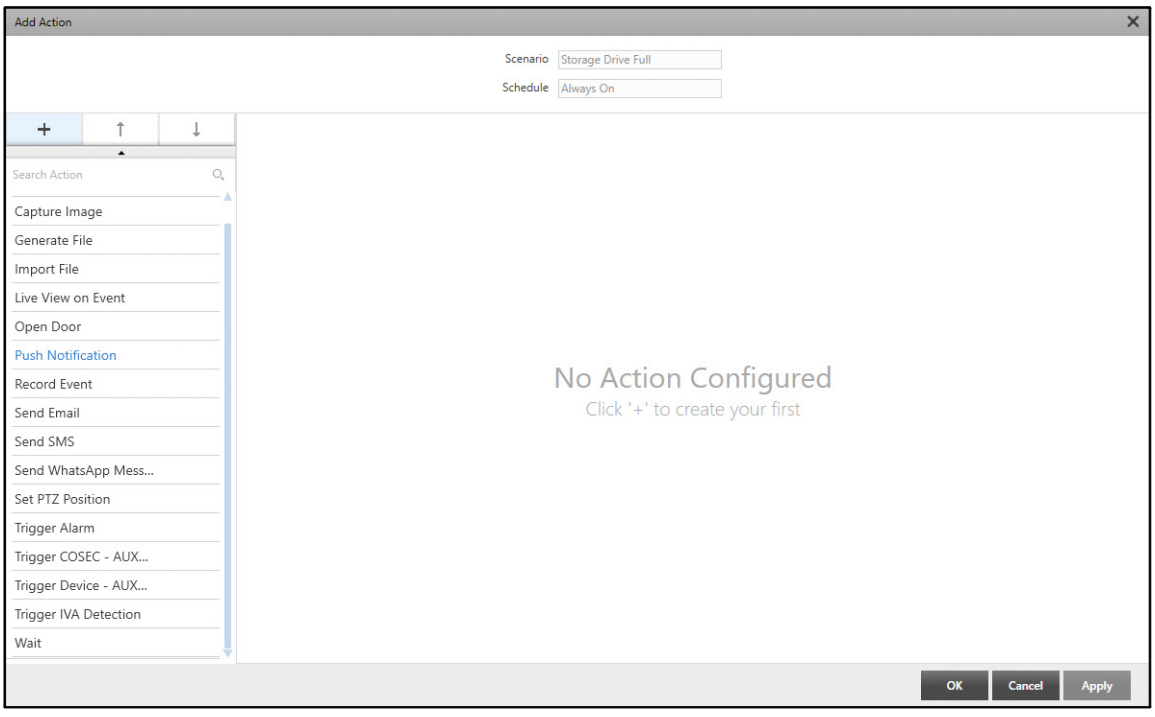
The Push Notification action sends Push Notifications to the selected users on SATATYA VISION App for the selected Events. Refer to “Push Notification” before configuring the Push Notification action.

To configure Push Notification action,

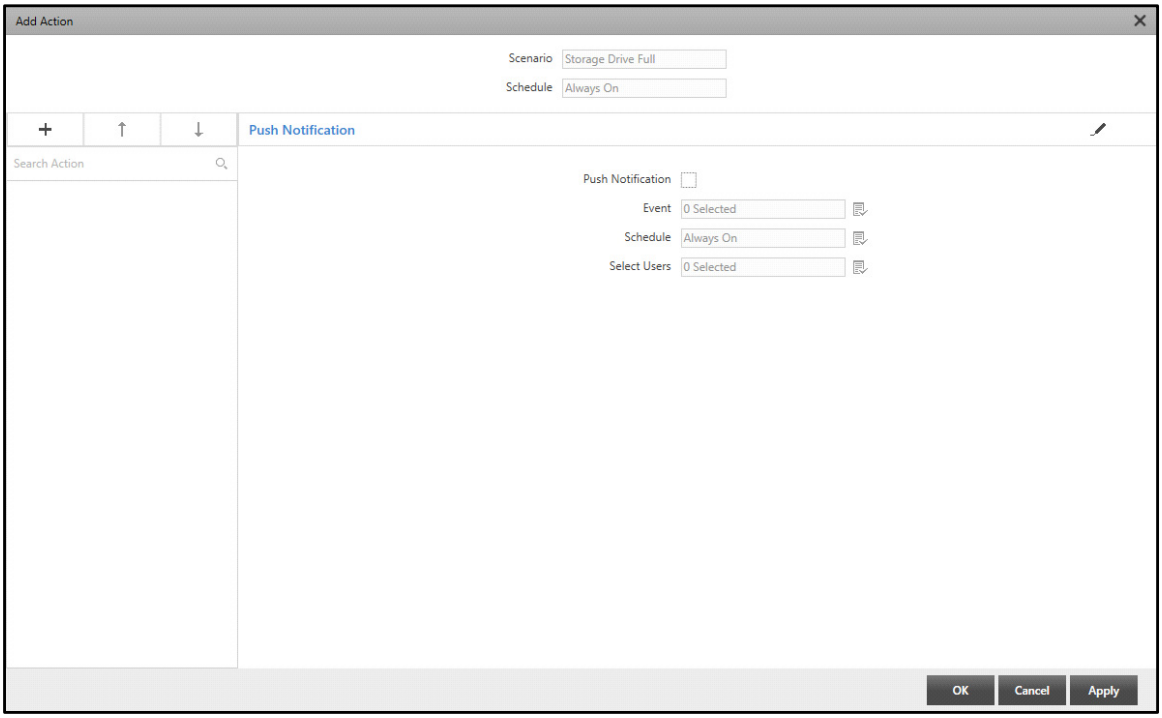
- Click **Add Action** + to add Actions to the configured Scenario. The **Add Action** pop-up appears.



- Click **Add Action** + **.** A list of all the system-defined actions appears.

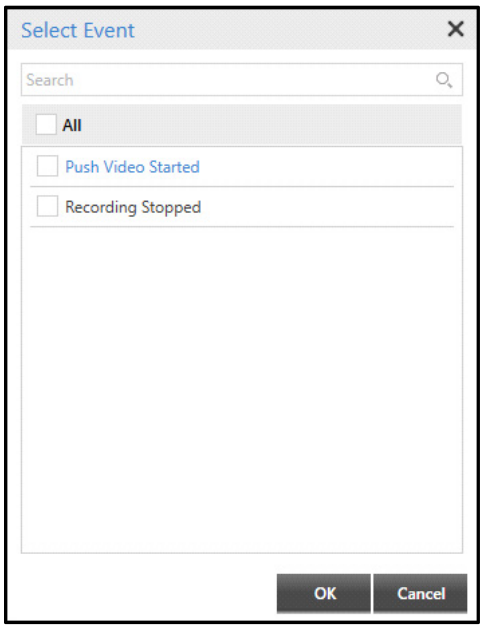


- Select **Push Notification** from the list of Actions.



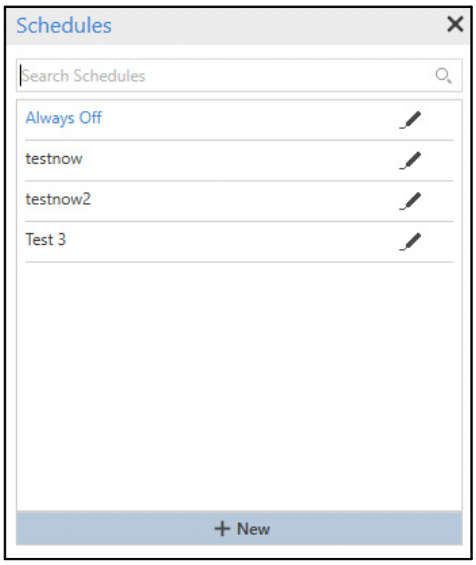
Configure the following parameters:

- **Push Notification**: Select the check box to enable the configuration.
- **Event**: Select the desired events for which you wish to send the Push Notifications.
  - Click **Select Events** picklist. The **Select Events** pop-up appears.



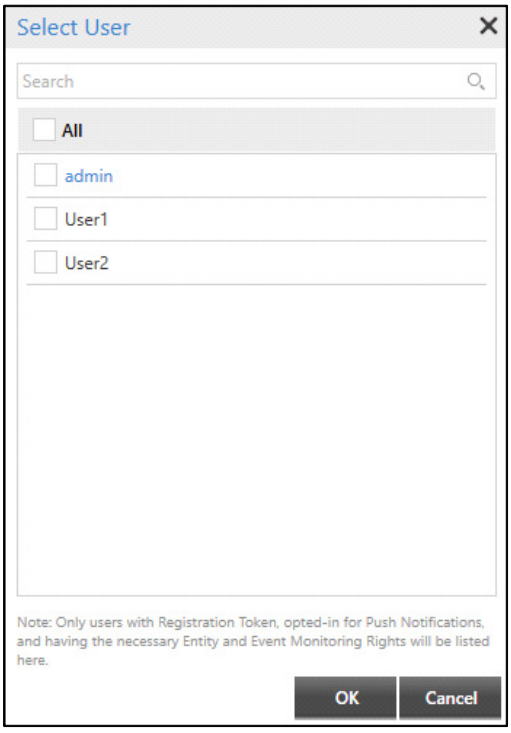
  - All the events configured for the scenario appear in the list. Select the check boxes for the desired events. Click **OK**.

- **Schedule**: Select the desired Schedule which you wish to assign to the Action using the **Schedule** picklist.
    - Click **Schedule** picklist. The **Schedules** pop-up appears.



    - Double-click to select the desired schedule from the list. You can edit an existing schedule by clicking on **Edit** . You can also configure a new schedule by clicking **New**. For more details, refer to “Schedules”.

- **Select Users**: Select the desired users to whom which you wish to send the Push Notifications. The users for whom Push Notification is enabled in Mobile Client will only appear in this list.
    - Click **Select Users** picklist. The **Select User** pop-up appears.



- Select the check boxes for the desired users. Click **OK**.

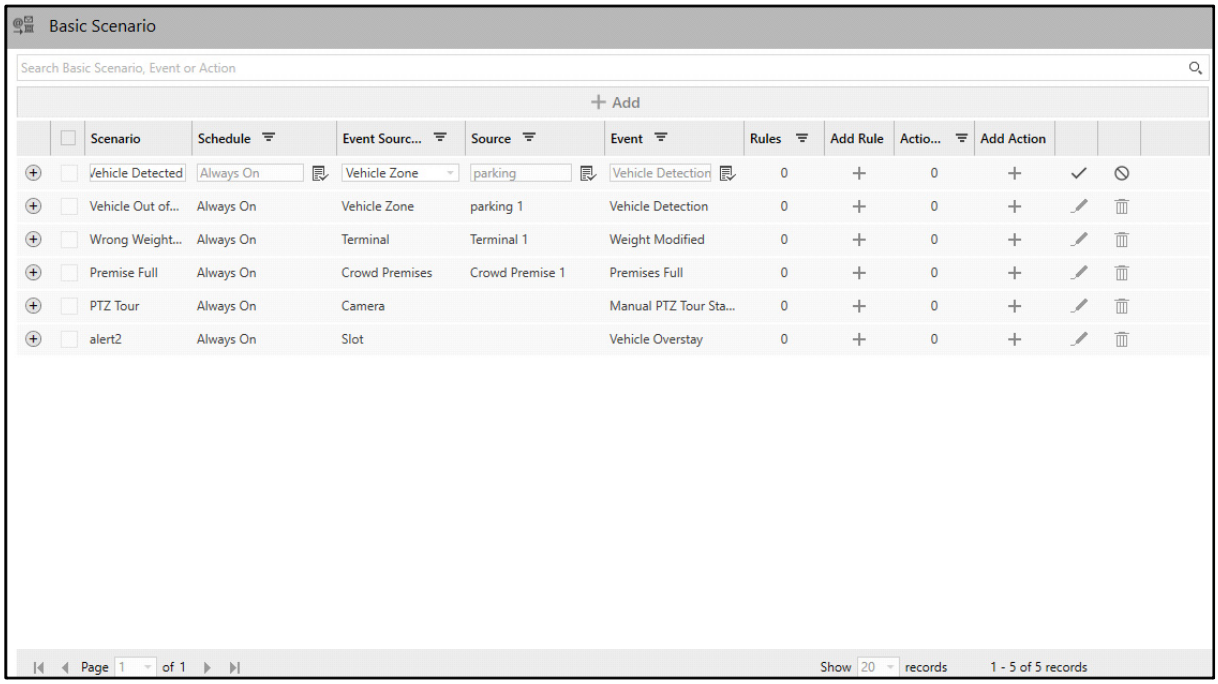
- Click **Apply** and **OK** to save the settings.

Basic Scenario with multiple actions

Consider the following examples for which you can configure different actions on Event occurence in Basic Scenario.

Example 1: Whenever a vehicle is detected at the Entry Gate, an alarm is to be triggered and a file is to be generated.

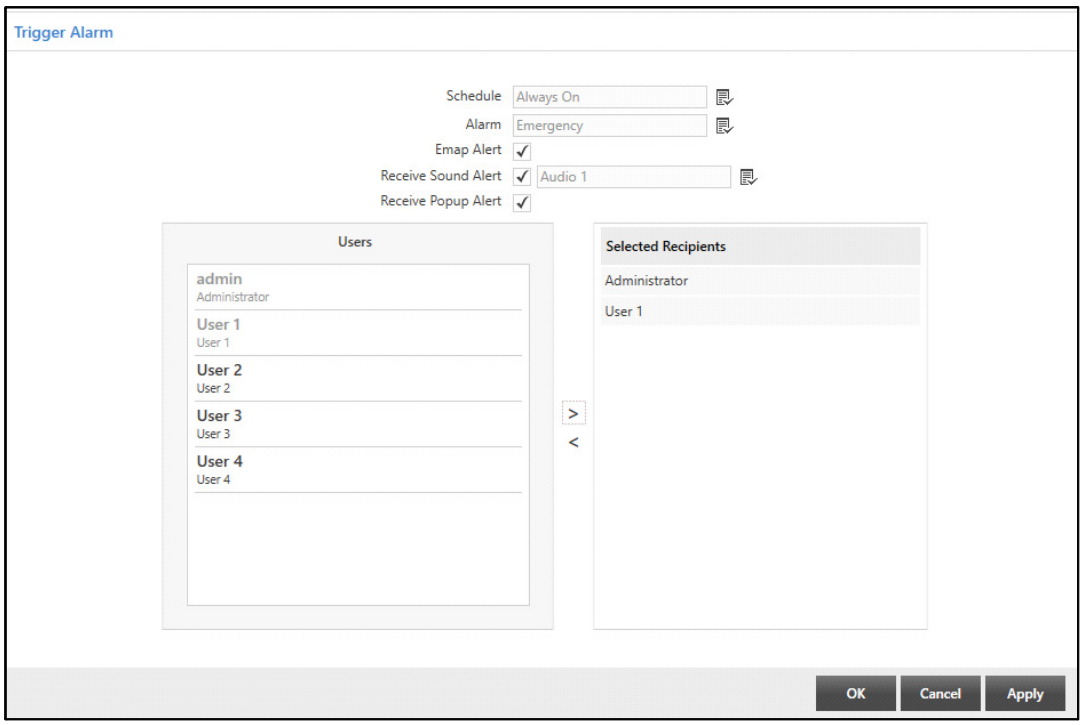
- Configure the Scenario **Vehicle Detected** with the Event Source Type as **Vehicle Zone** and the Event **Vehicle Detection**. For detailed Scenario configurations, refer to “Configure Scenarios”.



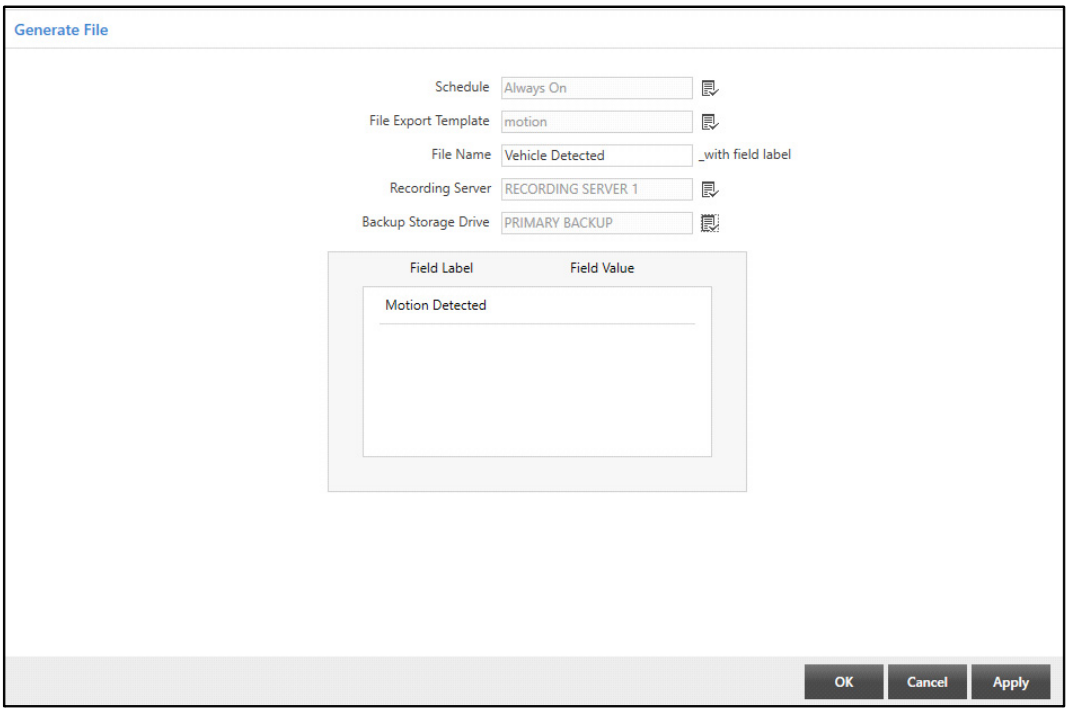
- Click **Save** ✓ to save the Scenario.

You can configure the same Scenario from **Vehicle Management > Scenarios** also**.**

- Click **Add Action** + for configuring **Trigger Alarm** action. For detailed configurations of action, refer to “Trigger Alarm”.



- Click **Apply** and **OK** to save the settings.
- Click **Add Action** + for configuring **Generate File** action. For detailed configurations of action, refer to "Generate File".



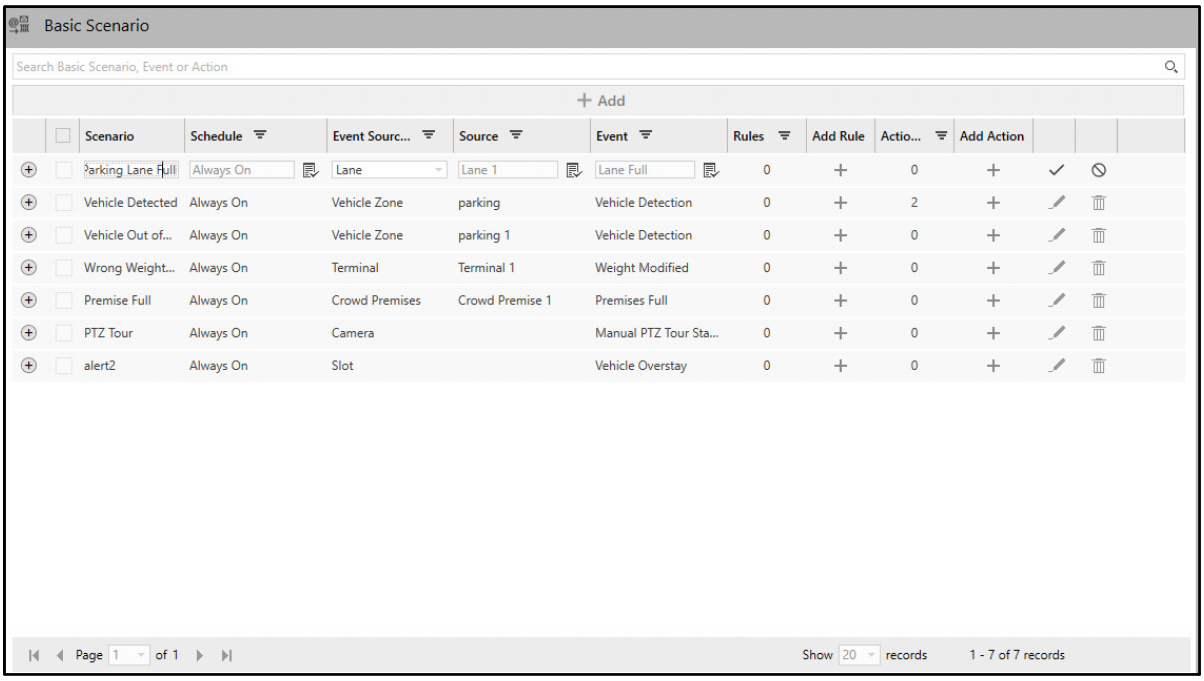
- Click **Apply** and **OK** to save the settings.

Now whenever a car is detected at the Entry Gate, an alarm will be triggered and the configured user will be notified. Also. a file will be generated and saved on the configured Backup Storage Drive. Consider a car entered

the gate and the Scenario is initiated and subsequently actions are taken. While the actions are in progress, if another car enters the gate, the Scenario will be initiated again for this car and the subsequent actions will be taken up.

Example 2: When Parking is full in a Lane, an image is to be captured and a camera should be moved to a configured position.

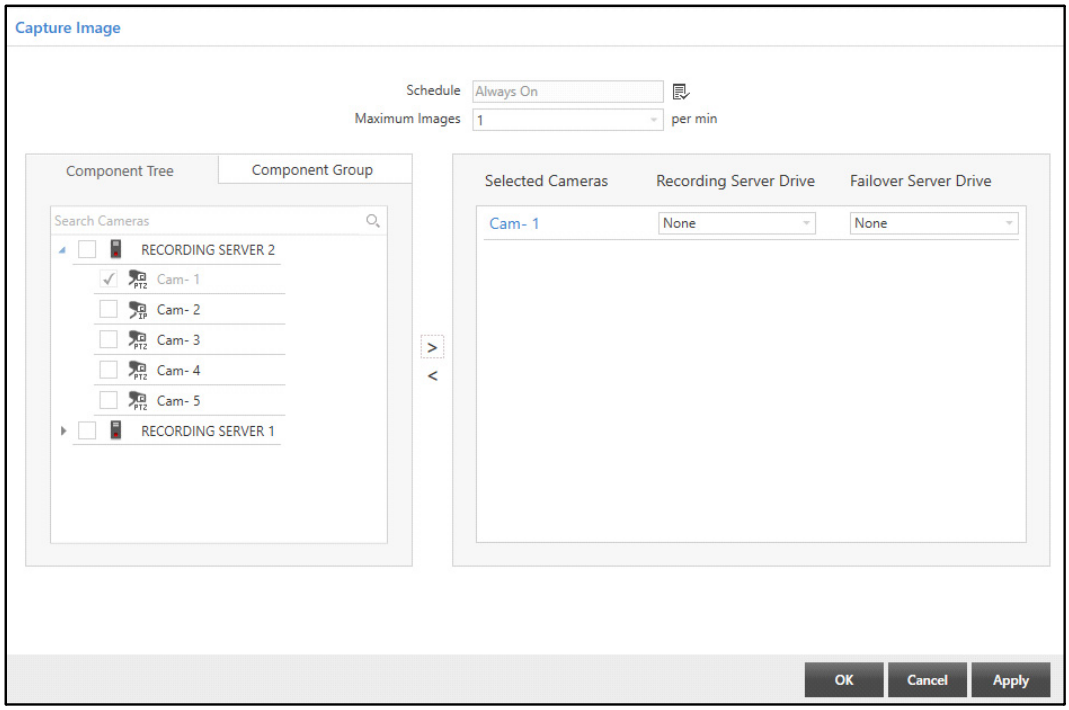
- Configure the Scenario **Parking Lane Full** with the Event Source Type as **Lane** and the Event **Lane Full**. For detailed Scenario configurations, refer to “Configure Scenarios”.



- Click **Save** ✓ to save the Scenario.

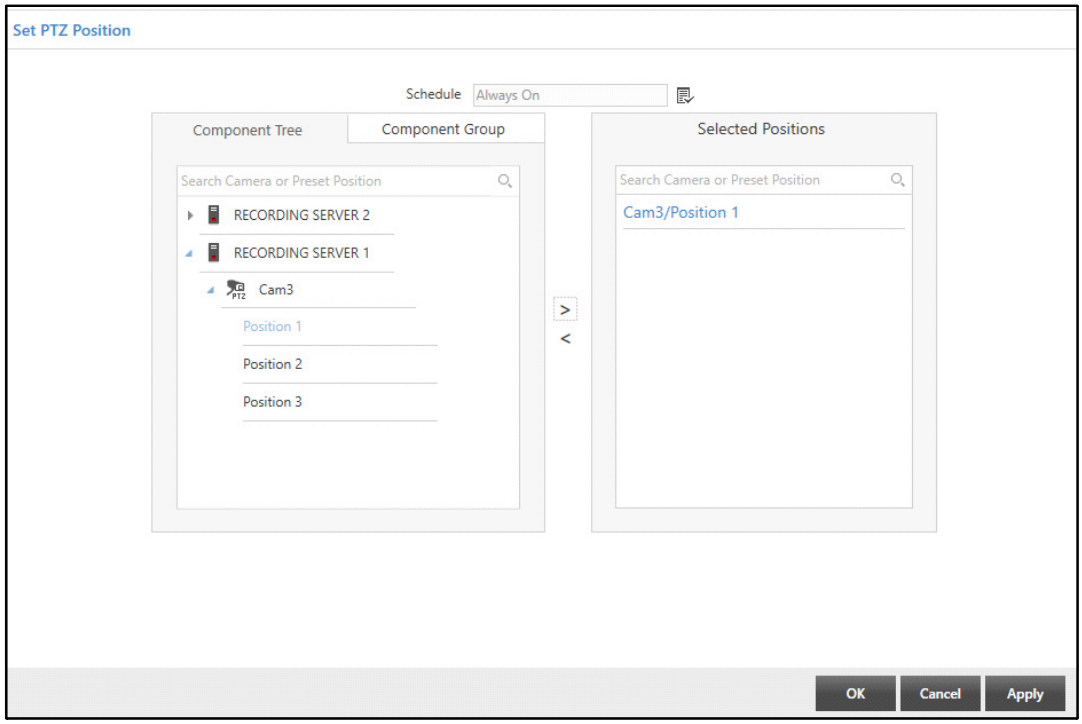
You can configure the same Scenario from **Parking Management > Scenarios** also.

- Click **Add Action** + for configuring **Capture Image** action. For detailed configurations of action, refer to “Capture Image”.



- Click **Apply** and **OK** to save the settings.

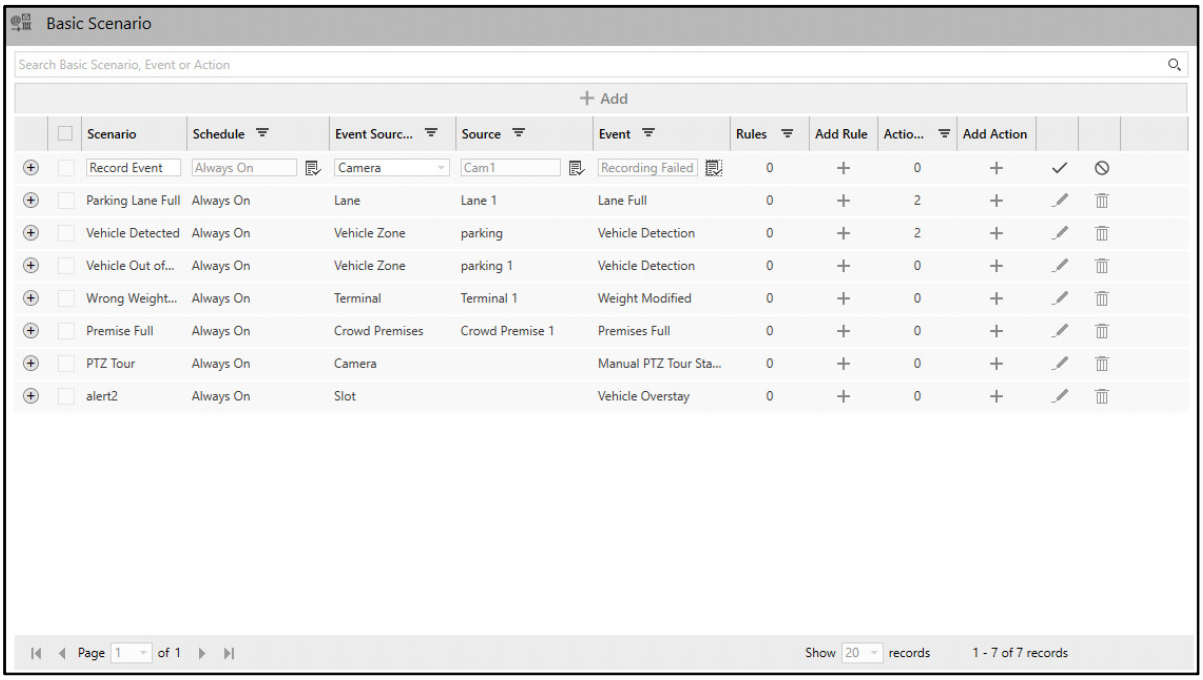
- Click **Add Action** + for configuring **Set PTZ Position** action. For detailed configurations of actions, refer to "Set PTZ Position".



- Click **Apply** and **OK** to save the settings.

Example 3: Consider two cameras (Camera 1 & Camera 2) are mounted at the entry gate of an organization. When Camera 1 is disconnected, recording of Camera 2 should start. And, whenever Camera1 is connected again, the recording of Camera 2 should stop.

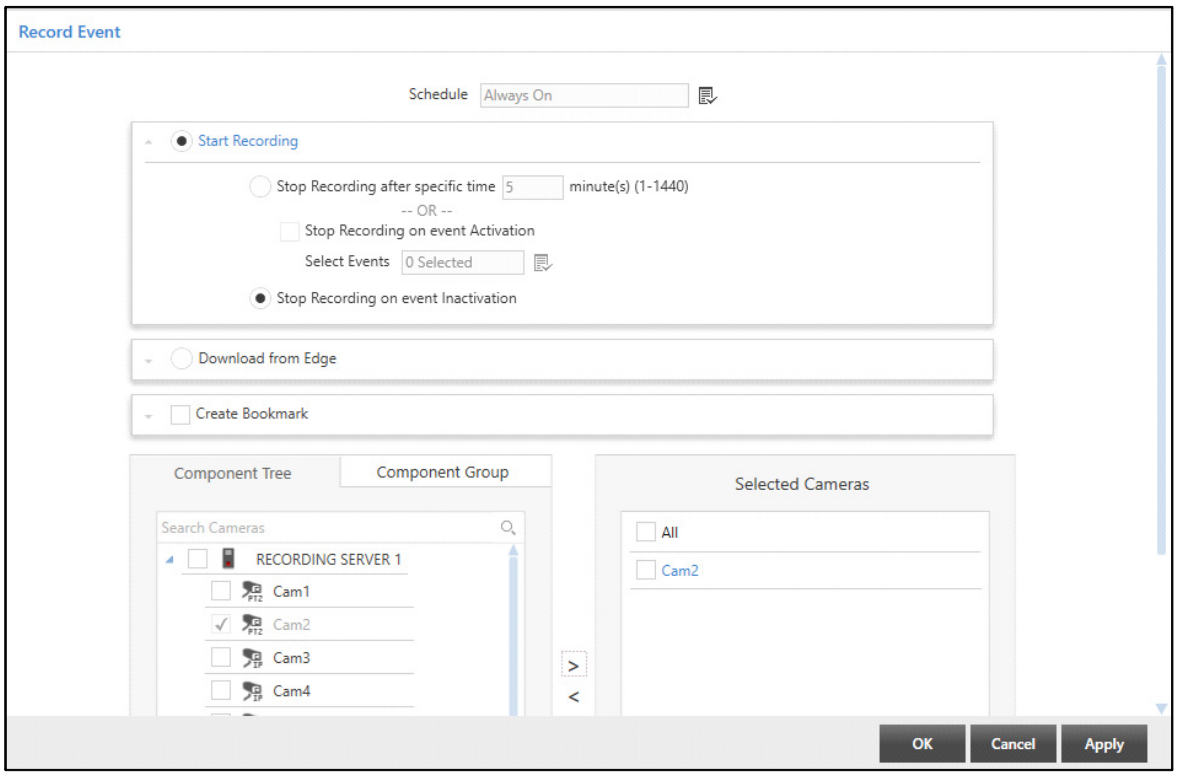
- Configure the Scenario **Record Event** with the Event Source Type as **Camera** and the Event as **Recording Failed**. For detailed Scenario configurations, refer to “Configure Scenarios”.



- Click **Save** ✓ to save the Scenario.

You can configure the same Scenario from **Servers & Devices > Scenarios** also.

- Click **Add Action** + for configuring **Record Event** action. For detailed configuration of actions, refer to “Record Event”.



- Click **Apply** and **OK** to save the settings.

CHAPTER 17 Appendix

Objects and Services supported by BACnet Server

Objects supported by BACnet Server

- Management Server
- Recording Server
- Failover Server
- Device (SAMAS Server)
- Camera
- Network Port
- Notification Class

Services supported by BACnet Server

Who-Is and I-Am Services
The Who-Is service is used by a sending BACnet-user to determine the Device object identifier, the network address, or both, of other BACnet devices that share the same internetwork. The Who-Is service is an unconfirmed service. The Who-Is service may be used to determine the Device object identifier and network addresses of all devices on the network, or to determine the network address of a specific device whose Device object identifier is known, but whose address is not. The I-Am service is also an unconfirmed service. The I-Am service is used to respond to Who-Is service requests. However, the I-Am service request may be issued at any time. It does not need to be preceded by the receipt of a Who-Is service request. In particular, a device may wish to broadcast an I-Am service request when it powers up. The network address is derived either from the MAC address associated with the I-Am service request, if the device issuing the request is on the local network, or from the NPCI if the device is on a remote network.

Who-Has and I-Have Services
The Who-Has service is used by a sending BACnet-user to identify the Device object identifiers and network addresses of other BACnet devices whose local databases contain an object with a given Object_Name or a given Object_Identifier. The I-Have service is used to respond to Who-Has service requests or to advertise the existence of an object with a given Object_Name or Object_Identifier. The I-Have service request may be issued at any time and does not need to be preceded by the receipt of a Who-Has service request. The Who-Has and I-Have services are unconfirmed services.

ReadProperty Service
The ReadProperty service is used by a client BACnet-user to request the value of one property of one BACnet Object. This service allows read access to any property of any object, whether a BACnet-defined object or not.

ReadPropertyMultiple Service
The ReadPropertyMultiple service is used by a client BACnet-user to request the values of one or more specified properties of one or more BACnet Objects. This service allows read access to any property of any object, whether a BACnet-defined object or not. The user may read a single property of a single object, a list of properties of a single object, or any number of properties of any number of objects. A 'Read Access Specification' with the property identifier ALL can be used to learn the implemented properties of an object along with their values.

UnconfirmedEventNotification Service
The UnconfirmedEventNotification service is used by a notification-server to notify a remote device that an event has occurred. Its purpose is to notify recipients that an event has occurred, but confirmation that the notification was received is not required. Applications that require confirmation that the notification was received by the remote device should use the ConfirmedEventNotification service. The fact that this is an unconfirmed service does not mean it is inappropriate for notification of alarms. Events of type Alarm may require a human acknowledgment that is conveyed using the AcknowledgeAlarm service. Thus, using an unconfirmed service to announce the alarm has no effect on the ability to confirm that an operator has been notified. Any device that executes this service shall support programmable process identifiers to allow broadcast and multicast 'Process Identifier' parameters to be assigned on a per installation basis.

Known Points related to addition of 400 Camera

- Data Backup will start from the date when the "Backup" configurations are done for each camera. Hence, no data earlier to the date of configuration will be available in Backup.

- **Take Backup** options available from V5R5 onwards will be 2,4 and 6 hours only. Earlier options, 30 minute and 1 hour are discontinued. If you upgrade from earlier version to V5R5, then by default, the **Take Backup** option will be set as 2 hours. For details, refer to "Backup".

- If multiple Backup Drives are configured for multiple cameras, then the backup process will run in parallel. For example, if 5 cameras are assigned 5 different Backup Drives, then the backup process for all the 5 cameras will start at the same time with one to one mapping, that is, backup of camera 1 will start in Backup Drive 1, backup of camera 2 will start in Backup Drive 2 and so on.

- We recommend Windows Server 2022 Standard or higher edition[8] to host SAMAS when you need to add more than 400 cameras, configured in the System (For Management Server and Recording Server as well).

8. Matrix has tested SAMAS on Windows Server 2022 Standard Edition for 400 cameras. However, if there are any architectural changes/enhancements done by Microsoft in these OS Editions, then due to its impact it may result in non-functionality of certain features/functions.

Supported Licenses

The SATATYA SAMAS provides IVA and Application based license. Each has been classified in the table below.

License Name	Abbreviation
IVA License	
SATATYA SAMAS Enterprise IVA Detection	EIVA Detection
SATATYA SAMAS Automatic Number Plate Recognition	ANPR
Application License	
SATATYA SAMAS Vehicle Tracking and Parking Management	VTPM
SATATYA SAMAS People Movement and Tracking	PMTC
SATATYA SAMAS Cognitive Response Engine with Automated Monitoring	CREAM

The SATATYA SAMAS License is available as SATATYA SAMAS PLT.

If the user wishes to upgrade the existing license or buy a new one, refer the table below. The table lists all the top up vouchers available for each license category.

License Name	License Category/Description	Top up Vouchers Available
SATATYA SAMAS PLT		
SATATYA SAMAS PLT	Enterprise VMS: Software for up to 65,535 Cameras • Direct Connection of Matrix Video Recorders as well as Cameras to the Recording Server • 1 User, 5 Built-in Cameras and Maximum 65,535 Cameras • Unlimited Recording Servers, No License Cost for Additional Recording Servers • Remote and Centralized Viewing and Management by Admin, Smart and Mobile Clients • Automatic License Plate Recognition (ANPR) for 1 Camera • EIVA License for 1 Camera, 1 License for CREAM, Parking Management for 5 VTPM Slots • Multi-Display Supported to Connect to 2/4/8 Monitoring Screens • Real-time Notifications like Video Popup, SMS, Email, Alarms and E-Map • Software Upgradation will be FOC Validated up to one Year from the Date of Activation	-

License Name	License Category/Description	Top up Vouchers Available
MATRIX LICENSE DONGLE 200	Enterprise VMS: USB Dongle to run SAMAS Application • Support All Licenses of SAMAS • Dongle can be inserted on SERVER /COSEC VEGA/ COSEC PANEL LITE • Needs to be activated. For details, refer to License Management Settings in the SATATYA SAMAS Admin Client Manual.	
MATRIX VIRTUAL DONGLE 300	Virtual License Management for all SAMAS Licenses. • Dongle-less Solution for SAMAS Software • Needs to be registered. For details, refer to License Management Settings in the SATATYA SAMAS Admin Client Manual.	
IVA License		
SATATYA SAMAS Enterprise IVA Detection	To Upgrade Number of Cameras in IVA Detection (Includes Perimeter Events and Object Detection Event)	1.SATATYA SAMAS EIVA1 2.SATATYA SAMAS EIVA3 3.SATATYA SAMAS EIVA10
SATATYA SAMAS ANPR	To Upgrade Number of Cameras in ANPR (Includes Vehicle Management Events)	1.SATATYA SAMAS ANPR1 2.SATATYA SAMAS ANPR3 3.SATATYA SAMAS ANPR10
Application License		
SATATYA SAMAS VTPM	To Upgrade Number of Parking Entities in VTPM (Includes Parking Management Events and Vehicle Counting event from camera)	1.SATATYA SAMAS VTPM10 2.SATATYA SAMAS VTPM50 3.SATATYA SAMAS VTPM200
SATATYA PMTC	To Upgrade Number of Cameras in PMTC (Includes Crowd Management Events and People Counting event from camera)	1.SATATYA PMTC1 2.SATATYA PMTC3 3.SATATYA PMTC10
SATATYA SAMAS CREAM	To Upgrade Number of Advanced Scenarios in CREAM	1.SATATYA SAMAS CREAM5 2.SATATYA SAMAS CREAM10 3.SATATYA SAMAS CREAM50
Extra License		

License Name	License Category/Description	Top up Vouchers Available
SATATYA SAMAS Camera	To Upgrade Number of Cameras	1.SATATYA SAMAS CAM5 2.SATATYA SAMAS CAM20 3.SATATYA SAMAS CAM100
SATATYA SAMAS PLT AUP CAM	For Annual Upgradation of Cameras (Annual Upgradation of all the new features)	1. SATATYA SAMAS PLT AUP CAM5 2. SATATYA SAMAS PLT AUP CAM20 3. SATATYA SAMAS PLT AUP CAM100
SATATYA SAMAS User	To Upgrade Number of simultaneous Users	1.SATATYA SAMAS User1 2.SATAYA SAMAS User3 3.SATATYA SAMAS User10

The **maximum upgradeable** limit of SATATYA SAMAS license is as shown below:

Category	SATATYA SAMAS PLT
Maximum number of simultaneous users	65535
Maximum number of cameras	65535
Maximum number of cameras for EIVA Detection	1023
Maximum number of cameras for ANPR	1023
Maximum number of slots for VTPM	65535
Maximum number of cameras for PMTC	1023
Maximum number of scenarios for CREAM	1023

Frequently Asked Questions (FAQs)

1. **Why can't I connect to my Management Server?**

   - Ensure that the license dongle is available.
   - Check that the Management Server is connected to the database to authenticate the user.
   - Ensure that the Server and Client are connected to the Network.
   - Verify that the ports in the Server and Client are configured properly. The IP Address and ports in Server and Client should be same.
   - The default ports are:

Service	Port Number
Admin Client Port	8711
Smart/Media Client Port	8085
Recording Server Port	8090
COSEC Port	8089
License Server Port	8095
IVA Server Port	8100
Transcoding Server Port	8400
ONVIF Server Port	8500

   - Make sure firewall is off for the configured ports.
   - If you are already using the ports specified here then you can change the port from the configuration settings of the Management Server.
   - Ensure that the Management Service is running on the Server, that is the PC where Management Server is installed.

2. **Why can't I connect to my Recording Server?**

   - Check that the Recording Server, that is the PC where Recording Server is installed is connected to the Network.
   - Make sure firewall is off for the configured ports.
   - Ensure that the Recording Service is running.

3. **What are the system requirements for SATATYA SAMAS Application?**

   Different components have different System requirements. Please refer to the **SATATYA SAMAS Installation Guide** for the each component.

4. **Which operating systems support SATATYA SAMAS Solution?**

   Please refer to the **SATATYA SAMAS Installation Guide** for details.

5. **Which ports must be open to connect SATATYA SAMAS with DVR, NVR or HVR behind the firewall?**

   If the ports of devices are not changed, then the default ports required to be free are:

- HTTP: 80
- RTSP: 554
- TCP: 8000

6. **How can I navigate through my Recordings?**

   Recordings can be stored in Local Drive or Network Drive as configured from the Admin Client. Local drive is the PC where the Recording Server is installed. Network drive can be any system in the network of the Recording Server.

   The recordings from the Local or Network Drive can be viewed in the SAMAS Media Player.

   - If the Media Player and the local Recordings are in the same PC, then you can easily scan the drive in Media Player and view the recordings.

   - If the Media Player is on PC-1, local drive recordings on PC-2 and Network Drive recordings on PC-3 then add both PC-2 and PC-3 drives to Map Network Drive tab from My Computer of PC-1. Now you will be able to scan the added drives and view the recordings.

7. **How to configure Network Drive as a Recording Storage Drive?**

   Click Admin Client > Servers & Devices > Select Recording Server > Storage > Add Drive > Network Drive. Specify the Drive settings.

   Specify the name for storage and browse the path to the folder where the recording are to be stored. Specify the username and password of the computer where the network drive is to be configured.

   While Adding Network Drive, Recording Server must be running on the PC with the current user account logged in into the operating system.

   Similarly, the Network Drive can be configured as Backup Drive.

8. **Operating System error is displayed while adding Network Drive. What do I do?**

   Click Control Panel> Administrative Tools> Services on the PC where the Recording Server is installed. Select Matrix SAMAS Recording Service. Right-click and click Properties. Select the Log On tab and click “This Account”. Specify the windows username with prefix “.\” Then Click Apply and restart the Service.

9. **How to configure FTP Drive as a Backup Storage Drive?**

   Click Admin Client > Servers & Devices > Select Recording Server > Storage > Add Backup Drive > FTP Drive. Specify the Drive settings.

   Specify the name for **Storage** (Example: SR) and IP address for the **FTP Server Name,** that is, the IP address of PC where FTP Drive is to be configured. (Example: 192.168.103.46).

   The default **FTP Port** is 21. Specify the **Storage Path** where backup will be stored. (Example: \\192.168.103.46\d\Matrix).
   Specify the **Username** and **Password** of the FTP Drive. Click **Test** to check the connection. Ensure that FTP Service is running on the PC where the FTP Server is configured. After successful connection click **OK**. The FTP Drive will be added to the Backup drives list.

10. **How to configure Recording for a Camera added in SATATYA SAMAS?**

    The Recording for a Camera can be configured in the following ways:

    - Click Admin Client > Servers & Devices > Recording Server > Recording tab. Select the Camera. Configure the Recording Properties. Enable the Event and Manual Recording, if required. You can also configure Pre and Post recording parameters.
    - In the Recording tab, Click Actions > Select Clone Settings. This enables you to copy the recording settings from once camera to all the desired cameras.
    - Also the same parameters can be configured from Recording Server > Select the desired Camera. Select Recording tab and configure the recording.

11. **How to configure Backup for a Camera added in SATATYA SAMAS?**

    The Backup can be configured in the same ways as mentioned in Recording above.

12. **What are the overall functionalities available with SATATYA SAMAS solution?**

    - Live View of Camera Video
    - Simple and Event Based Recording
    - Synchronous Playback, Asynchronous Playback and Instant Playback
    - Intelligent Video Analytics through Investigator
    - IVA Modules with add-on license
    - Basic Scenarios
    - Advanced Scenarios with add-on license
    - Media Player
    - Page and Window Sequencing
    - Event and Action Management
    - System Monitoring
    - Emaps with multi-hierarchy support
    - Dashboard
    - Mail and SMS notification
    - Matrix Access Control

13. **Do I need to have any Network Video Recorder (NVR)/ Digital Video Recorder (DVR)/Hybrid Video Recorder (HVR) apart from the SATATYA SAMAS Solution?**

    No, the SATATYA SAMAS solution is integrated with the Recording Server which provides both Recording and Streaming Capabilities. The IP Cameras can be directly connected to the Recording Server without the need of any NVR.For Analog Cameras you must have DVR or HVR.

14. **How do I add Matrix Devices in SATATYA SAMAS Admin Client?**

    Click the Servers and Devices module of Admin Client. Select the Recording Server to which you wish to add the device. Then select Add Devices button and click the option Add Manually. Specify the parameter details of the Matrix device to be added. You can add online as well as offline devices. The offline devices can come online later on.

    Matrix Devices can also get auto-added on SAMAS by enabling integration of SAMAS with respective device clients. For more details, refer to “Devices”.

15. **What are the types of Camera supported?**

    SATATYA SAMAS supports Analog Cameras through DVR/HVR and IP Cameras.

The brands which are supported are:
Matrix, Acti, Axis, DLink, HIKVISION, Infinova, Samsung, Panasonic, Vivotek, Brickcom, Dahua, Grandstream, Bosch

16. **Does SAMAS support ONVIF Cameras?**

    RS and FOS are using ONVIF Version 23.12 Rev 61 for ONVIF Client activity.

    ONVIF Server is using ONVIF Version 20.16 for ONVIF Server activity.

17. **I have a camera of brand not mentioned in the supported cameras list. How can I connect it?**

    If your camera is UPnP supported then you can connect the camera temporarily through ONVIF. If UPnP is not supported then you have to add the camera manually.

    If your camera is not ONVIF supported then you can add the camera manually as Generic Camera.

    RS and FOS are using ONVIF Version 23.12 Rev 61 for ONVIF Client activity. ONVIF Server is using ONVIF Version 20.16 for ONVIF Server activity.

18. **How many number of cameras can be added to the SATATYA SAMAS System?**

    Virtually unlimited number of cameras can be added from the software provided best hardware configuration is available in terms of processing speed and network bandwidth. SAMAS Client-Server architecture allows you to manage multiple Recording Servers and view all camera live videos in the Smart Client. Ensure that the license is available with the user.

19. **How can I add IP cameras to SATATAYA SAMAS Admin Client?**

    Select the Recording Server to which the camera is to be added. The IP Camera can be added:
    - As a device.
    - If NVR/HVR is connected, the camera will be auto-added.
    - If camera supports UPnP then Add using Auto Discovery Tool.For details, refer to “Add Using Auto Discovery Tool”
    - If camera does not support UPnP then Add Manually. For details, refer to “Add Manually”

20. **Can an IP camera of Generic domain be added to SATATAYA SAMAS?**

    Yes, an IP camera of Generic domain can be added manually. You need to configure the The RTSP and HTTP URL of camera.

21. **Can I add selected Cameras to SATATAYA SAMAS which are connected to the Matrix Device?**

    Yes, you can select the cameras from the device DVR/NVR/HVR to be added to SAMAS. Suppose you have SAMAS license for 50 cameras and you have 5 HVRs of 24 channels each, then you can add selected 10 cameras from each HVRs.

22. **Would SAMAS support NVR, DVR, HVR and Encoders of any other brand other than Matrix?**

    No, as SAMAS supports only Matrix Devices.

23. **How to enable Motion Detection event in IP camera and Analog camera ?**

    For the camera connected as a device:

- Click Servers & Devices. Select the camera. In the Recording tab, select the Enable Event Recording check box.
- Click Events tab. Select the Enable Motion Detection check box.

For the Analog and IP camera connected through device (NVR, DVR, HVR):

- Click Servers & Devices. Select the camera. In the Recording tab, select the Enable Event Recording check box.
- Click Configuration Settings of device > Select the Enable Motion Detection check box.

Ensure that the Motion Detection feature is enabled from the camera web page.

24. How can I view desired cameras in sequence?

You can configure the desired sequence from Admin Client > Window Sequence. Add the desired cameras to the sequence. This sequence can then be viewed from the Smart Client in either Pack or Unpack form.

25. How can I configure two different streams for Live View and Recording in SATATYA SAMAS?

For IP Cameras:

- Click Admin Client > Servers & Devices > Recording Server > Camera. Select the Stream Profile tab. Click Add Profile and configure the profiles to be used for different stream usages.
- Now click Stream Usage tab. Select Live Stream. Click the drop-down and select the desired profile for the live streaming.
- Similarly for Recording, select the stream profile from the drop-down list. And click Apply to save the settings.

For Cameras connected through Device:

- Click Admin Client> Servers & Devices > Recording Server > Device. Select the Profile tab. Click on Configure Device link. Here you can configure Main and Substream settings for the camera.
- Now select the Camera. Click Stream Usage tab. Select Live. Click the drop-down and select the profile for the live streaming.
- Similarly for Recording, select the stream profile from the drop-down list. And click Apply to save the settings.

26. How to configure a group of favorite cameras in SATATYA SAMAS?

Click Admin Client > Logical Grouping. Click Add to configure a group of favorite or desired cameras.

27. How do I configure an Alarm template?

Click Admin Client > General Settings > Templates > Alarms. Click Add to create a new alarm template. Set Priority and Alarm Life for the template and select member cameras to which this alarm is to be assigned. Save the changes. Maximum 4 cameras can be added to an Alarm template.

28. How to use Event and Action Module?

On SATATYA SAMAS, events occurring at certain sources (for example: Storage Memory Low on) can be configured to trigger a set of actions (for example: Send SMS). Events may be either System-defined or Custom Events, which can be created by the Administrator (from *General Settings*).
To configure Events and Actions, click Admin Client > Event & Action

Select an entity as the Event source (for example: an IP camera) and select a corresponding event for which action is to be assigned (for example: Camera Tampered). Click the **Add Action** button and select an action. Perform required configuration for the action (for example: Send SMS, Send Email or Trigger Alarm).

Once saved, the system will trigger the configured action every time the event occurs at the event source (for example: Alarm will be generated if Motion is detected in the camera view).

User can also create custom events to manually trigger specific actions through the SATATYA SAMAS.



Custom Events feature is supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.

29. **When can Event Recording take place for a camera?**

    Event Recording will start when a camera event occurs, (such as Camera Tampered) for which Start Recording has been configured as an action from the Event & Action module. Event Recording can be scheduled and may be enabled and performed even when recording mode is set as Off for a camera.

30. **How can I configure Scheduled Recording?**

    In SAMAS, any Motion Recording and Continuous Recording which run as per pre-defined schedules, fall under the category of Scheduled Recording. To configure Scheduled Recording:

    Click Admin Client > Schedules. Create schedules as required for scheduled recording.

    Click Admin Client > Servers & Devices. Select a camera and select the Recording tab on the camera page. Select the Recording Mode as Scheduled and specify schedules for Motion and Continuous Recording and specify the Recording Storage configuration.

31. **How can I configure an event that can be triggered manually from the Smart Client whenever required?**

    Other than system-defined events, user can also define custom events in the Admin Client which can be manually triggered using the Smart Client.
    To define a new custom event, click Admin Client > General Settings > Custom Events

    To assign an action to a custom event, click Admin Client > Event & Action > Custom Events



Custom Events feature is supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.

32. **Will I receive an alert from SAMAS if any of the configured devices get disconnected from the system?**

    Yes, you can get SMS and Email Alert on device disconnection. Configure these from Admin Client > General Settings > Message Templates > Device Events.

33. **Can I restrict the rights of a user?**

    The rights are assigned according to the user group. You can configure a group with limited rights from System Account of Admin Client. Then assign the configured user group to the desired user.

34. **How Do I integrate SAMAS with COSEC to receive events?**

Click SAMAS > Admin Client > General Settings > Access Control. Enable the Access Control Integration.

- Specify the IP address (for example: 192.168.153.146) and HTTP Port (default=80) of the PC from where COSEC is to be accessed.
- Specify the User Name and Password of the System Account User (SA,SE,SO). Make sure for this user the Enable API Access check box is enabled in Admin > System Accounts of COSEC.

Click COSEC > Admin >System Configuration > Monitor Configuration.

- Select the type of events to be exported from Export Events.
- Specify the IP address of the Management Server and Port Number as the COSEC port.

35. **Does SAMAS support Video Wall?**

Yes, SAMAS supports Video Wall feature.

36. **In a case where one of my PCs where Recording Server was configured gets corrupted, does SAMAS provide a way through which I can move my devices from that Recording Server to a new Recording Server? Cam the Recordings stored in previous Storage Drives also be moved?**

Yes, SAMAS provides an option to move devices from one Recording Server to another. However existing recordings cannot not be moved along with the device.

To move a device, click Admin Client > Servers & Devices

Select a Recording Server and on the server page, select the Move Devices button. Specify the source and destination servers and pick the devices to be moved.

Moving a device from one Recording Server to another will not affect the old recordings of the device.

37. **Which kind of Storage Drives can be configured in SAMAS?**

Two types of Storage Drives can be configured in SAMAS – Local Drives and Network Drives. Local Drive is the PC where Recording Server is installed. Network Drive can be any system in the same network as the Recording Server.

38. **How to use the Alarms that I have configured in Alarm Output Group Module?**

Alarm templates created in the Admin Client can be assigned as actions to System-defined as well as Custom events using the Event & Action module. When the occurrence of the configured event is detected, the Alarm will appear in the Smart Client based on the priority and alarm life defined. If the Alarm template has been associated with any camera, live view from the camera will also be available in the Smart Client as soon as the alarm is generated.

39. **How to configure Emap Alerts?**

- Create an Emap.
- Assign the desired entity to the Emap.
- In Event & Action module, select the same entity and the corresponding event for which Emap Alerts are to be generated. Add Trigger Alarm as action. On the Trigger Alarm Action pop up, enable the Emap Alert check box.

Any alarm triggered on the selected entity will now appear as an Emap Alert in the Smart Client.

- *Custom events cannot be assigned to Emap Alerts.*
- *Ensure that the alarm template associated with the Emap Alert is assigned on all concerned cameras from the Alarm Output Group module.*

40. How can I purchase the SAMAS License?

The SAMAS License is available based on Number of Cameras supported, Number of Simultaneous Active User sessions and Number of Parking Entities. The Detection through IVA and other IVA Module features are available as Add-on license.

To buy the license please contact the Matrix Channel Partners.

41. Is there any license for the Client Software? Are there any additional charges for the Server license?

The Client Software license is included in the package. There is no extra charge for client or server license. But after the expiry of Annual Support Package you have to renew the license for new upgradations.

42. Where can I install the SAMAS setup?

The SATATYA SAMAS can be installed at any location, within a specific site or multiple sites. This allows the flexibility in design of the video surveillance infrastructure from centralized to distributed to anywhere in between. The servers can be easily integrated into an existing network for ease of management within current IT infrastructures.

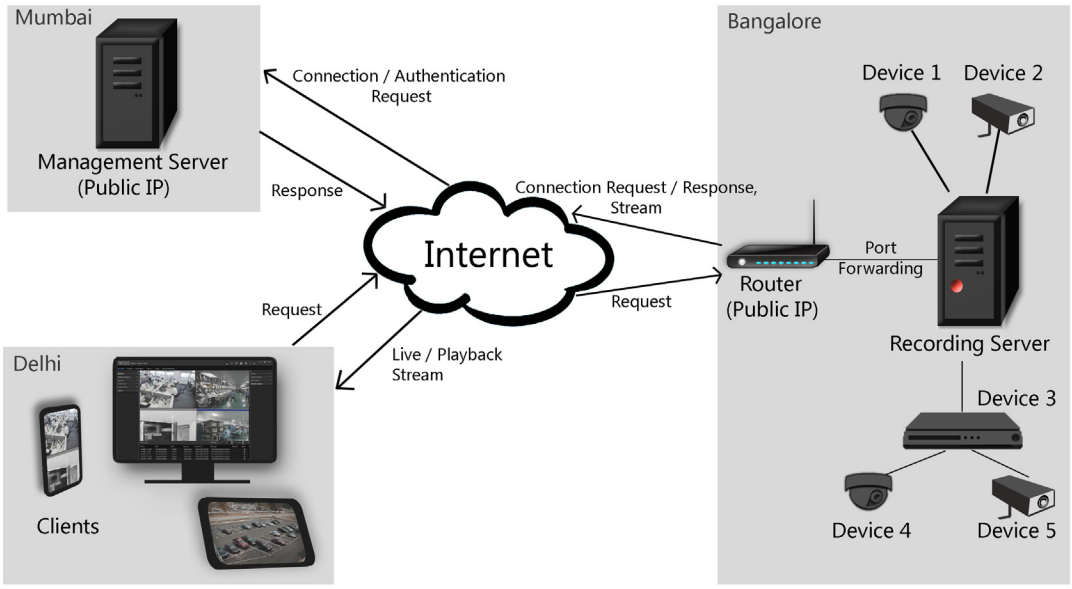
43. I have cameras which do not support Event Detection like Motion Detection, Intrusion Detection etc. Can I still use Intelligent Video Analytics feature?

Yes, SAMAS provides IVA Server which enables detection of events like Motion detection, Intrusion detection, Camera Tampering, No Motion Detection, Trip-wire Security, Tailgating, Unauthorized Parking Prohibited Parking, Improper Parking, Premises Availability, Wrong Way Detection, Vehicle Detection, People Counting and Vehicle Counting.

44. My Management Server is at Mumbai, Recording Servers and cameras are at Bangalore and Smart Client is at Delhi. How can I connect to the servers and view the camera stream?

Provide a Public IP to the Management Server. So that it can be connected though the Internet.

Now for the Recording Server, Port is to be forwarded through Router through which it is connect to the Management Server. Similarly, for the Smart Client at Delhi, Port is to be forwarded through Router which request the Recording Server for the camera stream.



45. **Can I control IP Addresses from accessing my SAMAS?**

    Yes, using IP Filter facility you can allow or deny any particular IP Address range from accessing your SAMAS.

    To use IP Filter, click General Settings > System Settings > IP Filter. Enable IP Filter and enter the range of IP Addresses to be blocked or allowed access.

46. **How can I generate report automatically and send it to the desired recipients?**

    Using Report Scheduler feature you can generate the desired report automatically and send it to desired people or store it at regular intervals as per your requirement. These reports can be sent via Email at specified time interval.

    To do this, click General Settings > Report Scheduler and configure the scheduling parameters for the required report.

47. **Can I configure Schedule based event detection?**

    Yes, you can configure schedule based event detection.

48. **Can I access Live View / Playback from third party clients?**

    Yes, SAMAS supports an ONVIF Server as well as ONVIF Users. The ONVIF Server provides the streams to the third party clients.

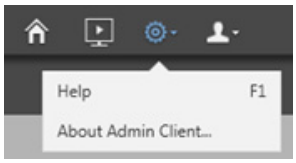
49. **I am facing buffering issues in Live View as well as Playback. How can I resolve this?**

    SAMAS provides a Transcoding Server, which optimise's the network bandwidth thus resolving the buffering issues. To configure the Transcoding Server Settings, refer to Servers & Devices > Transcoding Server Configuration as well as Camera Configuration (Stream Usage).

50. Can I increase/decrease the login time for a User?

Yes, you can do so by configuring the Remaining Access Duration for the user as per your requirement. This will be applicable for the current day only. Refer to General Settings > Users for details.

Keyboard Shortcuts



For enhanced accessibility and faster navigation, various functions on the SATATYA SAMAS Admin Client can be performed using keyboard shortcuts. A list of available shortcut keys have been provided below with the actions they perform. Shortcut keys are also displayed on the mouse tool tip, wherever applicable (see image).

GENERAL

Ctrl + Shift + Esc	**Open Task Manager**
Ctrl + TAB (Cyclic)	**Switch to next TAB (Application Pages/Tabs)**
Ctrl + Shift + TAB (Cyclic)	**Switch to previous TAB (Application Pages/Tabs)**
Enter	**Trigger Call to Action button – Apply, Save**
Esc	**Cancel**
Alt + F4	**Close**
Ctrl + A	**Select All**
Ctrl + X	**Cut**
Ctrl + C	**Copy**
Ctrl + V	**Paste**
Ctrl + F	**Find**
Ctrl + Z	**Undo**
Ctrl + Y	**Redo**
F3	**Search**
F5	**Refresh**
F11	**Full Screen**
Windows + D	**Desktop**
Enter	**Pop up > OK**
Esc	**Pop up > Cancel**
Alt + F4	**Pop up > Close**
Alt + A / Ctrl + S	**Pop up > Apply (Only in combination with OK button)**
Ctrl + `	**Open Smart Client**
Alt + D / Ctrl + N	**Add**
Alt + E / Ctrl + D	**Delete**
Alt + A / Ctrl + S	**Apply**
Alt + C / Esc	**Cancel**
Ctrl + Home	**Open Home Page**

TITLE BAR

F1	**Help**
F7	**Minimize**
F8	**Restore Down/Restore Up Application**
Alt + F4	**Close Application**

SERVERS & DEVICES

Alt + R	**Camera > Stream Profile > Add Profile**
Alt + T	**Camera > PTZ Tour > Add Tour**
Alt + S	**Camera > PTZ Tour > Camera Tour Settings**

EVENT & ACTION

Alt + V	**View All**
Alt + N	**Add Action**

SYSTEM MONITOR

F5	**Refresh**
Alt + X	**Export Event Log Details**

Disposal of Products/Components after End-Of-Life

Main components of Matrix products are given below:

- **Soldered Boards:** At the end-of-life of the product, the soldered boards must be disposed through e-waste recyclers. If there is any legal obligation for disposal, you must check with the local authorities to locate approved e-waste recyclers in your area. It is recommended not to dispose-off soldered boards along with other waste or municipal solid waste.

- **Batteries:** At the end-of-life of the product, batteries must be disposed through battery recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved batteries recyclers in your area. It is recommended not to dispose off batteries along with other waste or municipal solid waste.

- **Metal Components:** At the end-of-life of the product, Metal Components like Aluminum or MS enclosures and copper cables may be retained for some other suitable use or it may be given away as scrap to metal industries.

- **Plastic Components:** At the end-of-life of the product, plastic components must be disposed through plastic recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved plastic recyclers in your area.

After end-of-life of the Matrix products, if you are unable to dispose-off the products or unable to locate e-waste recyclers, you may return the products to Matrix Return Material Authorization (RMA) department.

Make sure these are returned with:
- proper documentation and RMA number
- proper packing
- pre-payment of the freight and logistic costs.

Such products will be disposed-off by Matrix.

"SAVE ENVIRONMENT SAVE EARTH"



MATRIX COMSEC

Head Office
394-GIDC, Makarpura, Vadodara - 390010, India.
Ph:(+91)1800-258-7747
E-mail: Tech.Support@MatrixComSec.com

Website: www.matrixcomsec.com