

# **SATATYA SAMAS API**

*User Manual V6*

# 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 variants of the product. The product may not support all the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise 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. Neither is any liability 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.

*Version 6*

*Release date: November 15, 2024*

# Contents

<b>Introduction.....</b>	<b>5</b>
<b>About the Document .....</b>	<b>5</b>
Communication between SAMAS and the Client .....	6
Client Side Validations .....	7
Server Side Notes .....	7
Common Message Structure (MATRIX Proprietary) .....	8
Communication between Third Party Client and Management Server.....	9
Communication Overview .....	9
HEADER .....	10
Header Type 1 (Third Party Client to Server) .....	10
Header Type 2 (Management Server to Third Party Client) .....	11
PAYLOAD .....	12
PAYLOAD Type 1 .....	12
ACCESS .....	12
Access Request Message Structure .....	12
Access Response Message Structure .....	13
<b>SESSION COMMANDS .....</b>	<b>15</b>
• Set Command Message Structure .....	15
• Reply Command Message Structure.....	16
• Get Configuration.....	17
<b>Logout .....</b>	<b>25</b>
<b>Trigger a custom event.....</b>	<b>26</b>
<b>Bookmark Addition .....</b>	<b>28</b>
<b>Search Bookmark .....</b>	<b>30</b>
<b>Snapshot.....</b>	<b>33</b>
<b>Status Codes .....</b>	<b>37</b>
<b>Glossary.....</b>	<b>40</b>
ASCII Set-I.....	40



# Introduction

Welcome to the *SATATYA SAMAS API Manual*.

This document aims at providing third party developers with a comprehensive overview of the communication structure and protocols to be used for integrating their software applications with SATATYA SAMAS.

It describes the process of channel establishment between communication components of the system, the command structure, commands, their values and replies which must be used during communication. This document defines the XML structure which can be used for transmission of large hierarchical data between system components.

## About the Document

This document explains:

- The process to communicate with SAMAS.
- The details to be stored by the third party application when communicating with SAMAS.
- The response codes that SAMAS shall send to the third party application and their exact meanings.



## Client Side Validations

1. Inter-poll time should be zero in the client side.

2. Response Timer of the client should be greater than the Response Timer of the Server.

E.g.: - 5 Sec. > 3 Sec.

3. Similarly, Keep Alive Wait Timer should be greater than (>) 3 x [Response Timer (Client)]

Ex.: - 16 Sec. > 3 Sec. x [5 Sec.]

4. Client should start Response Timer & open connection for almost every request (such as polling request, configuration request, command request & event) to the Server (SAMAS); and Client should close the specific connection (Except the Connection on which media is expected) either after expiry of response timer or if reply received from the server before expiry of the response timer.

## Server Side Notes

1. Keep-alive timer available in the server (SAMAS) side shall be restarted on every request, configuration request, command request & event request from the client.

2. When server receives 'Login Request', it shall check for IP Filter, Credentials, and Maximum User Sessions etc. If all the above checks are satisfactory, then Server should assign Session ID, start 'Keep Alive Timer' and send login ACK message with 'Login Status' Success.

3. If any of the checks are unsatisfactory, then Server shall not assign Session ID, it shall not start the 'Keep Alive Timer' and will send login ACK message with respective 'Login Status'.

## Common Message Structure (MATRIX Proprietary)

- Communication between Server and Client uses Proprietary Protocol.
- Communication between any two components should follow common message structure defined below.
- Message shall always start with SOM and end with EOM.



**HEADER** is a message identifier. It shall be used to recognize a received message. HEADER should start immediately after the SOM. There should be only one HEADER per Message.

**PAYLOAD** is the actual data. It shall be used to carry essential user data. Some messages should only have HEADER; while some messages should have one or more than one PAYLOAD per Message.

**EOM** stands for 'End of Message transmission'. It does indicate end of the message data sent or received. There should be only one EOM per Message. The data received between SOM and EOM shall be considered as one message by the Client and Server.

### SEPARATORS

#### Separators used in the entire message

SOM	Start of Message transmission	char(4)	start of heading
EOM	End of Message transmission	char(1)	end of transmission

# Communication between Third Party Client and Management Server

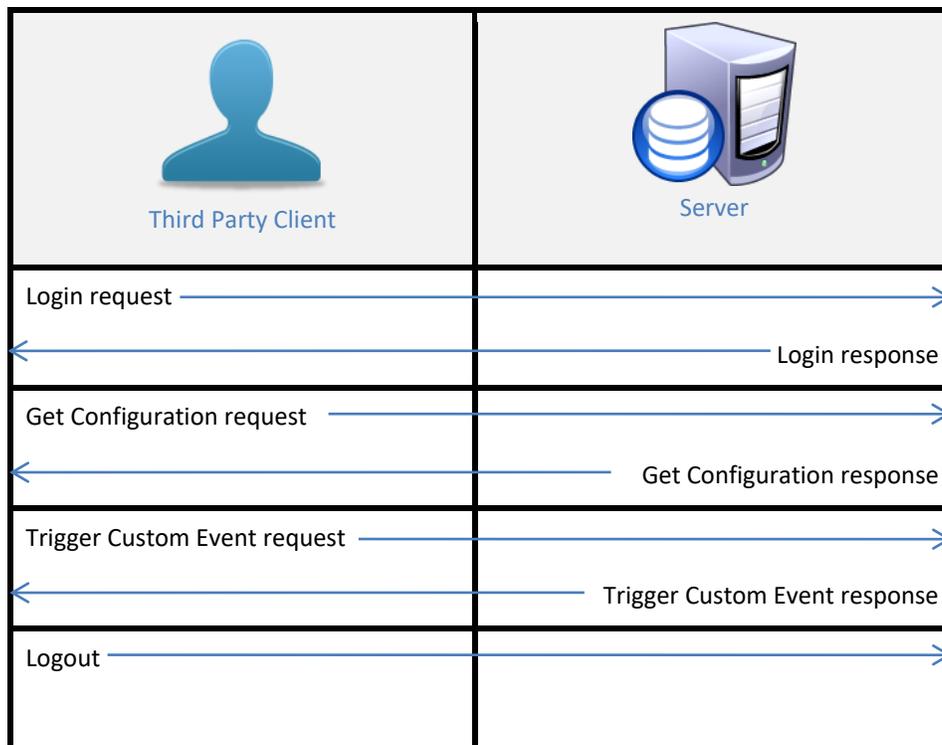
This section describes the communication between the Third Party Application and Management Server.

Here Third Party Application is referred to as Client and Management Server as Server. They might also be used interchangeably.

## Communication Overview

Client shall send a request (or command) to the Server; the Server shall send a corresponding response to the Client depending upon the request received.

The Request and Response Table for the above communication is as below:-



# HEADER

## Header Type 1 (Third Party Client to Server)

'Third Party Client to Management Server' HEADER shall be a message & session identifier.

It shall be used to recognize:

1. Type of message
2. Client Session

<b>Message ID</b>	<b>F</b>	<b>SID</b>	<b>F</b>
	<b>S</b>		<b>S</b>
	<b>P</b>		<b>P</b>

**Note:** - SID should not be available for the Message ID "REQ\_ACCESS".

**Message ID** shall be used by the Management Server to identify the type of message from the Third Party Client.

### Message ID used in Client to Server Header

Message ID	Description
REQ_ACCESS	Access request to Management Server.
REQ_CMD	Request commands in the Management Server from the active session

**SID** is the Client-Management Server Session ID. It shall be used by the Management Server to identify the session of the authenticated Third Party Client.

## Header Type 2 (Management Server to Third Party Client)

'Management Server to Third Party Client' HEADER shall be a message & status identifier.

It shall be used to recognize:–

1. Type of message
2. Status of Message

<b>Message ID</b>	<b>F</b>	<b>Status</b>	<b>F</b>
	<b>S</b>		<b>S</b>
	<b>P</b>		<b>P</b>

**Message ID** shall be used by the Third Party Client to identify the received response from the Management Server.

### **Message ID used in Server to Client Header**

<b>Message ID</b>	<b>Description</b>
RSP_ACCESS	Response of Access Request made to Management Server
RSP_CMD	Response of Request made to Management Server

**Status** shall be used to identify the request sent by the Third Party Client is "SUCCESS" or "FAILED" along with the reason of failure. Status shall be four digit numbers.

# PAYLOAD

## PAYLOAD Type 1

PAYLOAD Type 1 shall be used for following requests and responses:

- Request from Client to Server
  - Access Request (REQ\_ACCESS)
  - Commands in the Management Server (REQ\_CMD)
- Response from Server to Client
  - Access Request acknowledgement (RSP\_ACCESS)
  - Reply of Command Request (RSP\_CMD)

# ACCESS

## Access Request Message Structure

Communication between Third Party Client and Management Server shall start with a 'Access Request'. Third Party Client shall send a login request to the Server, when both are not connected in the system.

Third Party Client should send 'Access Request' to the Management Server regularly at an interval of 10 seconds, until it receives Access Status = "SUCCESS".

Once it is successfully connected to the Server, Client should stop sending the Access request and should send commands to get Initialization configuration (Modules, Hardware entities, Logical groups, Camera Cycles, System Alarms, etc.)

'REQ\_ACCESS' shall be static information for the Management Server to recognize a received message, which indicates the message is for 'Access Request'.

'Access Request' should follow the message structure as defined below:

<b>SOM</b>	REQ_ACCESS&<parameter>=<value>[&<parameter>=<value>....]	<b>EOM</b>
------------	--	------------

Parameter	Valid Values	Mandatory	Description
<b>username</b>	ASCII SET - I	Yes	'username' shall be required for authenticating the user whose login session needs to be created from Client to Server. 'username' value shall be the same value as configured in SAMAS
<b>password</b>	(A-Z), (a-z), (0-9), (~!@#%&^*()- _+[]\ };':",./<>?)	Yes	'password' will be required for authenticating the user whose login session needs to be created from Client to Server.  'password' value will be the same value as configured in the SAMAS

### Access Response Message Structure

Access Response shall be generated by the Management Server to send acknowledgement of 'Access Request'.

'RSP\_ACCESS' shall be static information, which shall be used as message identifier for the acknowledgement received from Management Server for 'Access Request' of Client.

'RSP\_ACCESS' should follow the message structure as defined below:

<b>SOM</b>	RSP_ACCESS&<parameter>=<value>[&<parameter>=<value>....]	<b>EOM</b>
------------	--	------------

Parameter	Value Format	Description
<b>Status</b>	Numeric	'Status' shall be used to identify the request sent by the Third Client is "SUCCESS" or "FAILED" along with the reason for failure. 'Status' shall be four digit numbers.
<b>SID</b>	Numeric	'SID' (Client – Management Server Session ID) shall be used by Client as the Client identification number assigned by the Management Server to Client for the current session.
<b>MS Version</b>	VxxRyy	'MS Version' shall provide the information related to Management service's Version and Revision. 'MS Version' shall be 6 characters long and have the following format: VxxRyy (where xx: version number and yy: revision number)
<b>STime</b>	Numeric	'STime' stands for Session Time. Client should wait for 'STime' to get any response from the connected Server. Client should reload the 'STime' if any response is received from the connected Server. Client should logout the current session after expiry of 'STime'. 'STime' shall be 2 digits number and its default value shall be 16 seconds.
<b>RTime</b>	Numeric	'RTime' stands for Response Time. Client should wait for 'RTime' to get response of the requested message from the Server. Client should close the current connection either after expiry of 'RTime' or if response of the requested message received from the connected Server.

**Note:** - RTime of Server (3 Sec) should be somewhat less than the RTime of the Client (5 Sec.)

If Client doesn't send any request to Management Server for 60 seconds than Management Server shall break that session with Client and for any request after that Client would have to again send a Access Request to Management Server.

# SESSION COMMANDS

- **Set Command Message Structure**

Run-time communication from Client to Management Server should follow the message structure as defined below:

SOM	REQ_CMD<parameter>=<value>[&<parameter>=<value>....]	EOM
-----	--	-----

## REQ\_CMD

'REQ\_CMD' shall be static information for the Management Server to recognize a received message, which indicates the message is to 'Request Command' from an active session.

Parameter	Valid Values	Mandatory	Description
SID	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.
CMDID	Numeric	Yes	'CMDID' shall be used by the Management Server to identify the Command.
... Parameters as per Command ID			

- **Reply Command Message Structure**

Reply from Management Server to Third Party Client should follow the message structure as defined below:-

SOM	RSP_CMD<parameter>=<value>[&<parameter>=<value>....]	EOM
-----	--	-----

**RSP\_CMD**

'RSP\_CMD' shall be static information, which shall be used as message identifier for the acknowledgement received from Management Server for 'REQ\_CMD' of Client.

Parameter	Value format	Description
<b>Status</b>	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
<b>CMDID</b>	Numeric	'CMDID' shall be used by the Client to identify the command for which the response is received.
... Parameters as per CMDID		

- **Get Configuration**

To fetch configuration of devices, cameras or custom events.

**Request:**

SOM	REQ_CMD&SID=<value>&CMDID=1&Entity=<value>	EOM
-----	--	-----

Parameter	Valid Values	Mandatory	Description								
<b>SID</b>	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.								
<b>CMDID</b>	Numeric	Yes	1 – Get configuration								
<b>Entity</b>	Numeric	Yes	<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th style="background-color: #cccccc;">Value</th> <th style="background-color: #cccccc;">Description</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">Devices</td> </tr> <tr> <td style="text-align: center;">2</td> <td style="text-align: center;">Cameras</td> </tr> <tr> <td style="text-align: center;">3</td> <td style="text-align: center;">Custom Events</td> </tr> </tbody> </table>	Value	Description	1	Devices	2	Cameras	3	Custom Events
Value	Description										
1	Devices										
2	Cameras										
3	Custom Events										

**Response:**

SOM	RSP_CMD&Status=<value>&CMDID=1&XMLSIZE=<value>&XML=<XML>	EOM
-----	--	-----

Parameter	Value format	Description
Status	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
CMDID	Numeric	1 – Get configuration
XMLSize	Byte	Size of Xml Data
XML	xml	Xml Data (Depending on Entity Value)

Reply of Get configuration Command with Entity = 1 (Devices)

Tag	Attribute	Valid Value	Description									
Devices	DevId	Numeric	Device ID									
	DevName	String	Device Name									
	RSId	Numeric	Recording Server ID									
	DType	Numeric	Device Type									
			<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #cccccc;">Enum</th> <th style="background-color: #cccccc;">Type</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">0</td> <td style="text-align: center;">DVR</td> </tr> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">NVR</td> </tr> <tr> <td style="text-align: center;">2</td> <td style="text-align: center;">HVR</td> </tr> <tr> <td style="text-align: center;">3</td> <td style="text-align: center;">IP Camera</td> </tr> </tbody> </table>	Enum	Type	0	DVR	1	NVR	2	HVR	3
Enum	Type											
0	DVR											
1	NVR											
2	HVR											
3	IP Camera											
	FosID	Numeric	Failover Server ID									

	DevUnderMaintenance	Numeric	Whether the device is under maintenance or not						
		<table border="1"> <tr> <th>Enum</th> <th>Type</th> </tr> <tr> <td>0</td> <td>Normal</td> </tr> <tr> <td>1</td> <td>Under Maintenance</td> </tr> </table>	Enum	Type	0	Normal	1	Under Maintenance	
Enum	Type								
0	Normal								
1	Under Maintenance								
	Reason	String	If DevUnderMaintenance=1 then only reason will be given						

**Example:**

SOM	<b>RSP_CMD&amp;SID=613844&amp;CMDID=1&amp;XMLSIZE=2106&amp;XML=&lt;ArrayOfDevices&gt;</b>	EOM
<pre> &lt;Devices DevId="18" DevName="192.168.111.177" RSId="1" DType="3" FosID="0" DevUnderMaintenance="0" Reason="" /&gt; &lt;Devices DevId="19" DevName="192.168.111.73" RSId="1" DType="3" FosID="0" DevUnderMaintenance="0" Reason="" /&gt; &lt;Devices DevId="20" DevName="192.168.111.135" RSId="1" DType="3" FosID="0" DevUnderMaintenance="0" Reason="" /&gt; &lt;Devices DevId="21" DevName="192.168.111.78" RSId="1" DType="3" FosID="0" DevUnderMaintenance="0" Reason="" /&gt; &lt;/ArrayOfDevices&gt; </pre>		

Reply of Get configuration Command with Entity = 2 (Cameras)

Tag	Attribute	Valid Value	Description
Camera	SeqNo	Numeric	Camera Sequence Number
	RSId	Numeric	Recording Server ID
CID		Numeric	Camera Number
CName		String	Camera Name
CType		Numeric	Camera Type
DeviceID		Numeric	Device ID
LogGrpID		Numeric	Logical Group ID

IsPTZ		Numeric	Checks if the Camera is a PTZ Camera or not	
			Enum	Type
			0	Non-PTZ Camera
			1	PTZ Camera
SDN		Numeric	Quick View Number	
ILPR		Numeric	Number of camera license for LPR	
IFD		Numeric	Number of camera license for FD	

**Example:**

<b>SOM</b>	<b>EOM</b>
RSP_CMD&SID=613844&CMDID=1&XMLSIZE=15038&XML=<ArrayOfCamera>	
<Camera SeqNo="32" RSId="1" FoSID="0">	
<ILPRDetMode>0</ILPRDetMode>	
<IUnauthorizedDetMode>0</IUnauthorizedDetMode>	
<CID>1</CID>	
<CName>192.168.111.177-Cam1</CName>	
<CType>0</CType>	
<DeviceID>18</DeviceID>	
<LogGrpID>1</LogGrpID>	
<IsMicro>0</IsMicro>	
<IsPTZ>0</IsPTZ>	
<SDN />	
<ILPR>0</ILPR>	
<IFD>0</IFD>	
<IPC>0</IPC>	
<IVC>0</IVC>	

<ITG>0</ITG>  
<IsAnalog>0</IsAnalog>  
<Improper>0</Improper>  
<Unauthorized>0</Unauthorized>  
<Prohibited>0</Prohibited>  
<PremisesPeople>0</PremisesPeople>  
<PremisesVehicle>0</PremisesVehicle>  
<WrongWay>0</WrongWay>  
<Address />  
<LandlineNo />  
<MobNo />  
<DevUnderMaintenance>0</DevUnderMaintenance>  
<Reason />  
</Camera>  
<Camera SeqNo="33" RSId="1" FoSID="0">  
<ILPRDetMode>0</ILPRDetMode>  
<UnauthorizedDetMode>0</UnauthorizedDetMode>  
<CID>1</CID>  
<CName>192.168.111.73-Cam1</CName>  
<CType>0</CType>  
<DeviceID>19</DeviceID>  
<LogGrpID>1</LogGrpID>  
<IsMicro>0</IsMicro>  
<IsPTZ>0</IsPTZ>  
<SDN />  
<ILPR>0</ILPR>

</FD>0</FD>  
</PC>0</PC>  
</VC>0</VC>  
</TG>0</TG>  
</IsAnalog>0</IsAnalog>  
</Improper>0</Improper>  
</Unauthorized>0</Unauthorized>  
</Prohibited>0</Prohibited>  
</PremisesPeople>0</PremisesPeople>  
</PremisesVehicle>0</PremisesVehicle>  
</WrongWay>0</WrongWay>  
<Address />  
<LandlineNo />  
<MobNo />  
</DevUnderMaintenance>0</DevUnderMaintenance>  
<Reason />  
</Camera>  
<Camera SeqNo="34" RSId="1" FoSID="0">  
</LPRDetMode>0</LPRDetMode>  
</UnauthorizedDetMode>0</UnauthorizedDetMode>  
</CID>1</CID>  
<CName>192.168.111.135-Cam1</CName>  
</CType>0</CType>  
</DeviceID>20</DeviceID>  
</LogGrpID>1</LogGrpID>  
</IsMicro>0</IsMicro>

```

<IsPTZ>0</IsPTZ>

<SDN />

<ILPR>0</ILPR>

<IFD>0</IFD>

<IPC>0</IPC>

<IVC>0</IVC>

<ITG>0</ITG>

<IsAnalog>0</IsAnalog>

<Improper>0</Improper>

<Unauthorized>0</Unauthorized>

<Prohibited>0</Prohibited>

<PremisesPeople>0</PremisesPeople>

<PremisesVehicle>0</PremisesVehicle>

<WrongWay>0</WrongWay>

<Address />

<LandlineNo />

<MobNo />

<DevUnderMaintenance>0</DevUnderMaintenance>

<Reason />

```

Reply of Get configuration Command Entity = 3 (Custom Events)

Tag	Attribute	Valid Value	Description
CEvent	EvID	Numeric	Event ID
	EvName	Numeric	Event Name

**Example:**

SOM	RSP_CMD&SID=613844&CMDID=1&XMLSIZE=194&XML=<ArrayOfCEvent> <CEvent EvID="70001" EvName="ss" /> <CEvent EvID="70002" EvName="Sc2" /> <CEvent EvID="70003" EvName="Sc1" /> <CEvent EvID="70004" EvName="sapna" /> </ArrayOfCEvent>	EOM
-----	---	-----

## Logout

To logout from SATATYA SAMAS.

### Request:

SOM	REQ_CMD&SID=<value>&CMDID=2	EOM
-----	-----------------------------	-----

Parameter	Valid Values	Mandatory	Description
SID	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.
CMDID	Numeric	Yes	2- Logout

### Response:

SOM	RSP_CMD&Status=<value>&CMDID=2	EOM
-----	--------------------------------	-----

Parameter	Value format	Description
Status	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
CMDID	Numeric	2- Logout

### Example:

SOM	RSP_CMD&STATUS=0&CMDID=2	EOM
-----	--------------------------	-----

## Trigger a custom event

To trigger a custom event defined on SATATYA SAMAS.

**Note:** Custom Event is supported till Software Release V5R6 as well as from Software Release V6R2 and onwards.

### Request:

SOM	REQ_CMD&SID=<value>&CMDID=3&CEVTID=<value>	EOM
-----	--	-----

Parameter	Valid Values	Mandatory	Description
SID	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.
CMDID	Numeric	Yes	3 – Trigger Custom Event
CEVTID	Numeric	Yes	Custom Event ID

### Response:

SOM	RSP_CMD&Status=<value>&CMDID=3&CEVTID=<value>	EOM
-----	---	-----

Parameter	Value format	Description
Status	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
CMDID	Numeric	3– Trigger Custom Event
CEVTID	Numeric	Custom Event ID

**Example:**

SOM	RSP_CMD&Status=0&CMDID=3&CEVTID=70004	EOM
-----	---------------------------------------	-----

## Bookmark Addition

To add a bookmark to camera playback at a specific time.

### Request:

SOM	REQ_CMD&SID=<value>&CMDID=4&Device ID =<value>&Camera ID =<value>&Camera Name =<value>&Bookmark name =<value>&Bookmark Time=<value>	EOM
-----	---	-----

Parameter	Valid Values	Mandatory	Description
<b>SID</b>	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.
<b>CMDID</b>	Numeric	Yes	4- Add Bookmark
<b>Device ID</b>	Numeric	Yes	Device ID
<b>Camera ID</b>	Numeric	Yes	Camera ID
<b>Camera Name</b>	ASCII Set-I	Yes	Camera Name
<b>Bookmark name</b>	ASCII Set-I	Yes	Bookmark Name
<b>Bookmark Time</b>	Date Time (YYYYMMDD HHMISS)	Yes	Bookmark Time

**Response:**

SOM	RSP_CMD&Status=<value>&CMDID=4	EOM
-----	--------------------------------	-----

Parameter	Value format	Description
Status	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
CMDID	Numeric	4- Add Bookmark

**Example:**

SOM	RSP_CMD&STATUS=0&CMDID=4	EOM
-----	--------------------------	-----

## Search Bookmark

To search for a bookmark within a specified time range.

**Request:**

<b>SOM</b>	REQ_CMD&SID=<value>&CMDID=5&From =<value>&To=<value>&Last Record ID=<value>&device id=<value>&camera id=<value>&bookmark name=<value>	<b>EOM</b>
------------	---	------------

Parameter	Valid Values	Mandatory	Description
<b>SID</b>	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.
<b>CMDID</b>	Numeric	Yes	5-Search Bookmark
<b>From</b>	DateTime (YYYYMMDDHHMISS)	Yes	From Date Time
<b>To</b>	DateTime (YYYYMMDDHHMISS)	Yes	To Date Time
<b>Last Record ID</b>	Long Integer	Yes	For Search – 0 For more Records – Last Record ID
<b>Device ID</b>	Numeric	Yes	Device ID if 0 send all Camera Bookmark
<b>Camera ID</b>	Numeric	Yes	Camera ID (if 0 send all Camera Bookmark)
<b>Bookmark name</b>	ASCII SET - I	No	Bookmark Name if blank – search result shall contain all records between from Date Time and To Date Time

**Response:**

SOM	RSP_CMD&Status=<value>&CMDID=5&XMLSIZE=<value>&XML=<value>	EOM
-----	--	-----

Parameter	Value format	Description
Status	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
CMDID	Numeric	5-Search Bookmark
XMLSize	Byte	Size of Xml Data
XML	xml	Xml Data

**Example:**

SOM	RSP_CMD&STATUS=0&CMDID=5&XMLSIZE=245&XML=<BKMks>	EOM
-----	--	-----

**Bookmark Data XML:**

Tag	Attribute	Valid Value	Description
LastRecordNo		Numeric	Last Record Number
BKMk	CID	Numeric	Camera ID
	DevID	Numeric	Device ID
	CName	String	Camera Name
BKMKName		String	Bookmark Name
BKMKTime		Date Time	Bookmark Time
EvdLckID		Numeric	Evidence Lock ID
Status		Numeric	Status

**Example:**

**Request:**

REQ\_CMD&SID=8331105&CMDID=5&From=20200101000000&To=20201212000000&Last  
Record ID=0&device id=0&camera id=0&bookmark name=kruti

**Response:**

RSP\_CMD&STATUS=0&CMDID=5&XMLSIZE=245&XML=<BKMks>

<LastRecordNo>0</LastRecordNo>

<BKMk CID="1" DevID="18" CName="192.168.111.177-Cam1">

<BKMKName>kruti</BKMKName>

<BKMKTime>20200328190000</BKMKTime>

<EvdLckID>0</EvdLckID>

<Status>0</Status>

</BKMk>

</BKMks>

SOM

EOM

## Snapshot

To get a snapshot or to upload it on an FTP storage drive.

### Request:

S O M	REQ_CMD&SID=<value>&CMDID=6&Device ID=<value>&Camera ID=<value>&Upload=0	EOM
-------------	--	-----

S O M	REQ_CMD&SID=<value>&CMDID=6&Device ID=<value>&Camera ID=<value>&Upload=1 0&FileName=<value>&ServerName=<value>&Port=<value>&StoragePath=<value>&Use rname=<value>&Password=<value>	EOM
-------------	--	-----

Parameter	Valid Values	Mandatory	Description	
<b>SID</b>	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.	
<b>CMDID</b>	Numeric	Yes	4-Search Bookmark	
<b>Device ID</b>	Numeric	Yes	Device ID	
<b>Camera ID</b>	Numeric	Yes	Camera ID	
<b>Upload</b>	Numeric	Yes	Upload Snapshot	
			1	Attach snapshot in response
			0	Upload on ftp Drive
<b>FileName</b>	Alpha-Numeric	Yes (if Upload=0)	Image File Name	

<b>ServerName</b>	Alpha-Numeric	Yes (if Upload =0)	FTP Server Name
<b>Port</b>	Numeric	Yes (if Upload =0)	Port of FTP
<b>StoragePath</b>	ASCII Set-I	Yes (if Upload =0)	Storage Path
<b>Username</b>	ASCII Set-I	Yes (if Upload =0)	Username
<b>Password</b>	ASCII Set-I	Yes (if Upload =0)	Password

**Response:**

<b>SOM</b>	RSP_CMD&Status=<value>&CMDID=6&Image=<value>	<b>EOM</b>
------------	--	------------

<b>SOM</b>	RSP_CMD&STATUS=<value>&CMDID=6	<b>EOM</b>
------------	--------------------------------	------------

<b>Parameter</b>	<b>Value format</b>	<b>Description</b>
<b>Status</b>	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
<b>CMDID</b>	Numeric	6- Snapshot
<b>Image</b>	Hex String	Image file ( if upload = 1)

**Example:**

SOM	RSP_CMD&Status=0&CMDID=6&Image=<Buffered Image>	EOM
-----	---	-----

Parameter	Valid Values	Mandatory	Description				
<b>SID</b>	Numeric	Yes	'SID' shall be used by the Management Server to identify the session of the authenticated Third Party Client.				
<b>CMDID</b>	Numeric	Yes	6-Snapshot				
<b>Device ID</b>	Numeric	Yes	Device ID				
<b>Camera ID</b>	Numeric	Yes	Camera ID				
<b>Upload</b>	Numeric	Yes	Upload Snapshot <table border="1" style="margin-left: 20px;"> <tr> <td style="text-align: center;">1</td> <td>Attach snapshot in response</td> </tr> <tr> <td style="text-align: center;">0</td> <td>Upload on ftp Drive</td> </tr> </table>	1	Attach snapshot in response	0	Upload on ftp Drive
1	Attach snapshot in response						
0	Upload on ftp Drive						
<b>FileName</b>	Alpha-Numeric	Yes (if Upload=0)	Image File Name				
<b>ServerName</b>	Alpha-Numeric	Yes (if Upload =0)	FTP Server Name				
<b>Port</b>	Numeric	Yes (if Upload =0)	Port of FTP				
<b>StoragePath</b>	ASCII Set-I	Yes (if Upload =0)	Storage Path				

<b>Username</b>	ASCII Set-I	Yes (if Upload =0)	Username
<b>Password</b>	ASCII Set-I	Yes (if Upload =0)	Password

**Response:**

<b>SOM</b>	RSP_CMD&Status=<value>&CMDID=6&Image=<value>	<b>EOM</b>
------------	--	------------

<b>Parameter</b>	<b>Value format</b>	<b>Description</b>
<b>Status</b>	Numeric	'Status' shall be used to identify the request sent by the Client is "SUCCESS" or "FAILED" along with the reason of failure. 'Status' shall be four digit numbers.
<b>CMDID</b>	Numeric	6- Snapshot
<b>Image</b>	Hex String	Image file ( if upload = 1)

**Example:**

<b>SOM</b>	RSP_CMD&Status=0000&CMDID=6&Image=<Buffered Image>	<b>EOM</b>
------------	--	------------

## Status Codes

Status Code	Message	Description
0	Success	Indicates success response of request
1	Error in parsing Message ID. Please contact your system administrator	Indicates that an error occurred due to invalid Message ID.
2	Error in parsing Session ID. Please contact your system administrator	Indicates that an error occurred due to invalid Session ID.
3	Syntax error. Please contact your system administrator	Indicates that an error occurred due to invalid Syntax.
14	Invalid Request	Indicates that an error occurred due to invalid Field ID.
17	Invalid Field Value. Please contact your system administrator	Indicates that an error occurred due to invalid Field value.
20	No Records found	Indicates that no records were found for the specified search criteria.
24	Error in performing operation. Please try again	Indicates that error occurred while performing operation
29	Could not connect to the server	Indicates that connection failed with Server
30	The server is disabled	Indicates that server is disabled
31	Error in connection. Please try later	Indicates that error occurred while connecting to server
50	More records available	Indicates that records more than the defined threshold for the response are available.
51	More events available	Indicates that events more than the defined threshold for the response are available.
62	File transfer failed	Indicates that the file transfer has failed because of a mismatch in file length.
68	This feature is not supported by camera	Indicates that the feature is not supported by camera.
116	Your Allowed Access Duration elapsed on Device	Indicates that user's allowed access time has elapsed.
201	Device is not connected	Indicates that the IP device is not connected in the network.
203	Error in receiving stream	Indicates that an error occurred in receiving stream from

		camera.
204	Request timed out. Please try again	Indicates that the command request was timed out.
205	The device connection parameters could not be found	Indicates that the device connection parameters could not be found.
210	An error occurred while triggering alarm	Indicates that an error occurred while triggering an alarm.
211	The Alarm has already been acknowledged	Indicates that the alarm is already acknowledged. This may arise if the alarm status is not updated in a client.
214	Error in parsing command data. Please contact your system administrator	Indicates that an error occurred while parsing the command data.
215	Admin Password has been set to default.	Indicates that Admin password has been set to default.
217	Recording Server is Offline. Please try again later	Indicates that the Recording Server on which request is made is Offline
221	Recording Server has not been authenticated by the Management Server. Please check Recording Server configuration	Indicates that the selected Recording Server has not been authenticated by the Management Server
222	Unable to connect Device	Indicates that a connection request made to the Device has failed.
224	Recording Server has been deleted	Indicates that the selected Recording Server was deleted by the User
225	Request Failed. This operation is not supported by camera.	Indicates that the maximum number of supported profiles has been reached for the selected camera
227	Your current license does not allow any more user sessions. Please upgrade your license.	Indicates that maximum no of user sessions supported by the license are already configured.
229	Invalid Path Or File Name.	Indicates that an error occurred while creating a directory with the given file name at the specified path.
231	License verification failed.	Indicates that verification of license failed.
232	Access Control Integration has been disabled	Indicates that Access Control Integration has been disabled by the user
233	Upgraded software is not supported by your current Upgrade Package Validity	Indicates that Upgraded software is not supported by current Upgrade Package Validity.

234	Your current Upgrade Package Validity does not support upgradation of database	Indicates that Your current Upgrade Package Validity does not support upgradation of database.
235	Total number of currently configured cameras are higher than license permit.	Indicates that Total number of currently configured cameras are higher than available License permit
236	Connection lost with database.	Indicates that connection with database lost.
238	Incorrect Username or Password	Indicates that authentication has failed because of invalid credentials.
239	This user has been disabled on the system	Indicates that the user is disabled.
240	This user has been blocked on the system	Indicates that the user is blocked.
241	Multi-login is not allowed	Indicates that multi-login for the entered username is not allowed.
242	You do not have required permissions for this application	Indicates that current user does not have the required permissions for this application
243	Your Allowed Access Duration elapsed	Indicates that user's allowed access time has elapsed.
244	Generic License Found. License needs to be upgraded	Indicates generic license has been detected.
248	Please set your password.	Indicates User needs to set password as it is a first Time login for user.
249	Your current password has expired.Please change your password.	Indicates user needs to set new password as password has expired.
250	Password must contain minimum <n> characters	Indicates that Password must contain minimum required characters as per defined Password policy.n is number of minimum required characters defined in password policy
254	Your account has been locked due to maximum failed login attempts.Try again after <x> minute(s)	Indicates user's account has been lock for n minutes. N is lock duration defined in password policy
255	Your account has been locked due to maximum failed login attempts.	Indicates user's account has been lock. User needs to contact administrator to reset its password.
260	You do not have permission for this operation	Indicates user doesnot have permission for this operation

261	Your IP Address is blocked	Indicates IP Address of user is block in SAMAS
262	Total number of currently configured cameras for License Plate Recognition are higher than license permit.	Indicates that Total number of currently configured LPR cameras are higher than available License permit
265	Total number of currently configured cameras for Face Detection are higher than license permit.	Indicates that Total number of currently configured Face Detection cameras are higher than available License permit
999	Unknown error occurred	Indicates that an unknown error has occurred while performing action

## Glossary

### ASCII Set-I

ASCII Set-I includes the following characters:

**ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890\_-.()[]:@!#\$%+^**

**White Space**



**TELECOM | SECURITY**

## **MATRIX COMSEC**

### **Head Office:**

394-GIDC, Makarpura, Vadodara - 390010, India,

Ph.:+91 265 2630555

E-mail: [Tech.Support@MatrixComSec.com](mailto:Tech.Support@MatrixComSec.com)

Website: [www.matrixcomsec.com](http://www.matrixcomsec.com)