

# Using HTTP API - 'sendExternalAlarm'

# Introduction

'Security Management System Server' software allows integration with external systems and can receive alarms sent from the external systems.

This document describes HTTP API – 'sendExternalAlarm' which is used by external systems to send external alarm to the 'Security Management System Server' software.

Before the external system sends alarm to the 'Security Management System Server' software, the 'Security Management System Server' software needs to be configured to receive the alarm.

This document has following sections -

(a) 'Security Management System Server' software configuration – for receiving the external alarms

(b) API description -'sendExternalAlarm'

(c) Testing the API using 'Postman' application. Postman application is free 3<sup>rd</sup> party tool, which can be used for quick testing of various HTTP APIs. It allows users to format and send HTTP requests and receive the HTTP responses.

It is advised to follow this document, to configure the 'Security Management System Server' software and to test the API using Postman. This confirms that configuration is correctly done and the API is functioning properly. Then the 'API description' can be reviewed in details and same can be implemented in the external system software. The API tests using Postman application can be used as reference, during API integration.

The 'Security Management System Server' software configuration involves adding one or more 'External alarm modules' in the 'Security Management System Server' software.

(a) Each 'External alarm module' added to 'Security Management System Server' software indicates one 'alarm source' associated with the external system.

(b) Each 'External alarm module' can be linked with one video source (e.g. video camera channel) already configured in the 'Security Management System Server' software. This is used to associated video evidence with alarms received for that 'External alarm module'

(c) For each 'External alarm module', 32 types of 'external alarms' can be generated. 'Security Management System Server' software defines following 32 types of external alarms –

- i. External Alarm 1
- ii. External Alarm 2
- iii. External Alarm 3
- iv. External Alarm 4
- v. External Alarm 5



vi. External Alarm 6 vii. External Alarm 7 External Alarm 8 viii. ix. External Alarm 9 x. External Alarm 10 xi. External Alarm 11 xii. External Alarm 12 xiii. External Alarm 13 External Alarm 14 xiv. xv. External Alarm 15 External Alarm 16 xvi. External Alarm 17 xvii. xviii. External Alarm 18 xix. External Alarm 19 xx. External Alarm 20 External Alarm 21 xxi. xxii. External Alarm 22 xxiii. External Alarm 23 xxiv. External Alarm 24 XXV. External Alarm 25 xxvi. External Alarm 26 xxvii. External Alarm 27 xxviii. External Alarm 28 xxix. External Alarm 29 External Alarm 30 XXX. xxxi. External Alarm 31 xxxii. External Alarm 32

The integration design hence involves the first step - to finalize the 'number of alarm sources' available with it and add one 'External alarm module' for each 'alarm source'

The second step in integration design is listing the 'types of external alarms' which can be generated by the 'alarm sources' and associating each type of external alarm with one of the 32 types listed above.

For example, we will consider a fire alarm system with 10 detectors. Each detector is capable of generating 2 types of alarms – 'Smoke detected' and 'Fire detected'.

(a) In this case, 10 'External alarm modules' will be configured in the 'Security Management System' server software. Each 'External alarm module' will be associated with a detector from external system (this association is flexible and can be finalized by the integration team) –

Detector 1 = EA001Detector 2 = EA002Detector 3 = EA003Detector 4 = EA004



Detector 6 = EA005Detector 7 = EA006Detector 8 = EA007Detector 9 = EA008Detector 10 = EA009Detector 11 = EA010

- (b) The types of alarms may be associated as (this association is flexible and can be finalized by the integration team) –
  'Smoke detected' = 'External Alarm 11'
  'Fire detected' = 'External Alarm 23'
- (c) When 'Smoke detected' alarm is generated in the external system from 'Detector 4'; it will use the 'sendExternalAlarm' API, and will set 'External alarm module name = EA004' and 'External alarm type = External Alarm 11'



## **Security Management System Server configuration**

This section explains steps to add one 'External alarm module' to the 'Security Management System' server software.

Same steps can be repeated to add multiple 'External alarm modules' to the 'Security Management System' server software.

- 1. Execute the 'Security Management System Server' software.
- 2. Navigate to 'External alarms -> External alarm modules' page from the left side navigation panel

192.168.0.75	2	Ext	External alarms → External alarms modules							
Site_18DBF2153E36	<u>/</u>									
Data management	^		📶 📶 👗							
Secondary storage			Sr No.	Module ID	Module Name	Associated Video Channel				
Remote backup										
Tasks										
Linked servers										
Server settings										
Connect to CMS										
Video panorama										
Additional features										
Under vehicle surveillance										
External alarms										
External alarms modules										
External alarm										
External alarm rules										
Data indicators										
Face recognition										
ATM/POS CMS										
User interface settings										
	~									

3. Click on 'Add external alarms module...' button to popup a dialog box as shown in below image

🔕 Add New External Alarms Module						
Module Name:	EA001					
Module ID:	EA_ 001					
Video Channel:	<select> ~</select>					
	Ø					

4. Enter 'Module Name' – any unique string (among all configured external alarm modules in the server software) which will identify the alarms module.

Security Management System - Using HTTP API - 'sendExternalAlarm' www.infinova.com



Enter 'Module ID' – any unique non-unicode string; or accept the default.

Video channel – select video channel from available options. This is used to associate the external alarm source to any configured video channel. The list contains video channels which are already configured in the 'Security Management System Server' software.

🐼 Add New External Alarms Module							
Module Name:	EA001						
Module ID: EA_ 001							
Video Channel:	Cam836 ~						

- 5. After configuring the parameters, click on 'Ok' button to finish adding the module in the 'Security Management System Server' software.
- 6. Image below shows 'EA001' module with 'EA\_001" module ID is added to the system with 'Cam836' is associated with the module.

192.168.0.75	<u>/</u>	External a	larms → External a	larms modules						
Site_18DBF2153E36	<u>/</u>	-0-1								
Data management	^									
Secondary storage		Sr No	. Module ID	Module Name	Associated Video Channel					
Remote backup		1	EA_001	EA001	Cam836					
Tasks										
Linked servers										
Server settings										
Connect to CMS										
Video panorama										
Additional features										
Under vehicle surveillance										
External alarms										
External alarms modules										
EA001										
External alarm										
External alarm rules										
Data indicators										
Face recognition										
ATM/POS CMS										

- 7. Click on any added 'External alarms modules' from the list and use 'Edit' button to edit parameters. Remove button can be used to remove selected alarms module from the system.
- 8. Separate link is provided in the tab control for each added 'External alarms sources' module as shown in below image. Click on the link to see the details for the alarm source.

Security Management System - Using HTTP API - 'sendExternalAlarm' www.infinova.com



192.168.0.75	External alarms → E	External alarms modules → EA001	
Site_18DBF2153E36	Module ID:	FA 001	
Data management ^			
Secondary storage	Module Name:	EA001	
Remote backup			
Tasks			
Linked servers			Primary video channel
Server settings			Video Channel
Connect to CMS			Primary: Cam836 V
Video panorama			
Additional features			
Under vehicle surveillance			
External alarms			
External alarms modules			
▶ EA001			
External alarm			
External alarm rules			
Data indicators			
Face recognition			
ATM/POS CMS			

9. Video channel can be edited using this dialog. Use 'Edit' button available on the dialog to enable 'Video channel' user interface. Select video channel from the available options and click on 'Save' button to save the changes. 'Cancel' button can be used to discard the unsaved changes for 'Video channel' settings



# Security Management System Server – IP address and port number

The external systems need to send the HTTP requests to the IP address and HTTP port number associated with the 'Security Management System' server software.

To locate the IP address and the HTTP port number associated with the 'Security Management System' server software, please follow the steps listed below -

1. In the 'Security Management System Server' software, navigate to 'Communication -> Network' page from the left side navigation panel



- 2. Note the IP address listed under 'Output IP address (Client connections) -> Current'. Also please ensure that the status displayed next to this IP address is 'OK'
- 3. Note the 'HTTP port (TCP)' value



## **Security Management System Server – New user**

The HTTP APIs can be called by authorized users. The authorization requires the username and password. Hence a new user needs to be added to the 'Security Management System' server software, when using the HTTP APIs.

- 1. In the 'Security Management System Server' software, navigate to 'Users and Privileges -> Users' page from the left side navigation page.
- 2. Please add a new user with 'Operator' privilege.



# HTTP API - sendExternalAlarm

### **Request details -**

Server IP	IP address associated with the 'Security Management System'
address	server software
address.	
a transp	
Server HTTP	HTTP port associated with the 'Security Management System'
port number:	server software
HTTP request	/sendExternalAlarm
	Note the request LIPL is case sensitive
UKI.	Note – the request OKI is case sensitive
Request type:	HTTP POST
Authorization	HTTP Digest Authentication
r uunonzunon.	
Dequest	The request should include the 'Content I enoth' header as defined
Request	The request should include the Content-Length header, as defined
headers:	in standard HTTP specifications
POST data:	In XML format –
	<nd ata=""></nd>
	<nrequest1ype>smsExternalAlarmNotificationReal1ime</nrequest1ype>
	stType>
	<pre></pre> <pre></pre> <pre></pre>
	<datastandard></datastandard>
	<smsmodulename>FA001</smsmodulename>
	<datacustom></datacustom>
	The 2 strings highlighted in yellow background will be different in
	and request
	() (F + 1 + 1 + 1) + (F + 1 + 1) + (F + 1) +
	(a) External Alarm 11 string indicates the alarm type. It can be any
	string associated with the 32 exernal alarm types available in the
	'Security Management System Server' software
	(b) 'EA001' string is for the 'External alarm module name' It
	should match the name of the target 'External eleter module'
	should match the name of the target External alatin module
	defined in the 'Security Management System' server software.



### **Response details -**

HTTP response	(a) '200 OK' indicates the request was processed by the 'Security
status code:	Management System server software.
	Please note that this is HTTP request processing status code and
	NOT return code associated with the processing from within
	'Security Management System' server software.
	(b) Any other status code = standard HTTP response status
Response data:	In XML format –
	<nresponse></nresponse>
	<nrequesttype>smsExternalAlarmNotificationRealTime</nrequesttype>
	stType>
	<responsestandard></responsestandard>
	<rcode><mark>1</mark></rcode>
	<rdescription><mark>Success</mark></rdescription>
	The 2 strings highlighted in yellow background may be different in each response -
	<rcode> value = indicates the return code related to the processing from 'Security Management System' server software.</rcode>
	<rdescription> value = human readabale string which eplains the return code</rdescription>
Return codes:	(a) ' <rcode> value =&gt; 1' indicates success</rcode>
	(b) $\leq RCode > value = 0'$ indicates unspecified error
	(c) ' <rcode> value &lt; 0' value indicates specific error</rcode>



## **API test using Postman application**

Postman application is free 3<sup>rd</sup> party tool, which can be used for quick testing of various HTTP APIs. It allows users to format and send HTTP requests and receive the HTTP responses.

- Please download and install the 'Postman' application. Note – this documentation uses 'Postman for Windows - version 7.3.5'. However latest available version for any suitable OS / browser can be used for the tests.
- 2. Execute the Postman application
- 3. Create a new request

0	Postman									
File Edit View Help										
🕂 New 🔻 Import Runner 📭 🔻	👪 My Workspace 🔻 🗼 Invite	<i>G</i>								
. GET GET GET GET GET	GET GET POST + ••••	No Environn								
POST • http://192.168.0.75:9900/sendExter	POST  http://192.168.0.75:9900/sendExternalAlarm									
Params Authorization Headers Body	Pre-request Script Tests									
Query Params										
KEY	VALUE	DESCRIPTION								
Кеу	Value	Description								
Response										

Select 'request type' as 'Post'

Type the URL. In this example we are using URL – http://192.168.0.75:9900/sendExternalAlarm

Where –

- (a) '192.168.0.75' is the IP address associated with the 'Security Management System' server software
- (b) '9900' is the port number associated with the 'Security Management System' server software
- 4. Access the 'Authorization' tab



Untitled Request									
POST • http://192.168.0.75:9900/sendExternalAlarm									
Params Authorization  Headers	Body  Pre-reques	st Script Tests							
TYPE Digest Auth									
The authorization header will be automatically generated when you send the request. Learn more about authorization	Username Password	op ••							
By default, Postman will extract values from the received response, add it to the request, and retry it. Do you want to disable this?	▶ ADVANCED	Show Password							
Yes, disable retrying the request									
Preview Request									

#### Select TYPE 'Digest Auth'

Type the 'Username' and 'Password'. This is the login information for 'Operator' privilege user configured in the 'Security Management System' server software.

5. Access the 'Body' tab

Unti	tled Request									
PO	POST									
Para	ams Autho	rization 🖲	Headers	Body ●	Pre-requ	est Script	Tests		Cooki	es Code
è	none 🔵 for	m-data (	x-www-form	n-urlencoded	🖲 raw	binary	GraphQL BET/	Text 🔻		
2	<pre>kNData&gt;</pre>	e>smsExte	rnalAlarmNot:	ificationRea	lTime <td>equestType&gt;</td> <th></th> <td></td> <td></td> <td></td>	equestType>				
4	<datastandar< td=""><td>.d&gt;</td><td>111(/WType/</td><td></td><td></td><td></td><th></th><td></td><td></td><td></td></datastandar<>	.d>	111(/WType/							
5	<smsmodulena< td=""><td>me&gt;EA001&lt;</td><td>/SMSModuleNa</td><td>me&gt;</td><td></td><td></td><th></th><td></td><td></td><td></td></smsmodulena<>	me>EA001<	/SMSModuleNa	me>						
6	<td>ird&gt;</td> <td></td> <td></td> <td></td> <td></td> <th></th> <td></td> <td></td> <td></td>	ird>								
7	<datacustom <="" td=""><td>&gt;</td><td></td><td></td><td></td><td></td><th></th><td></td><td></td><td></td></datacustom>	>								
8										
-										

Select the option 'raw' Type the XML string –

<NData> <NRequestType>smsExternalAlarmNotificationRealTime</NRequestType> <NType><mark>External Alarm 11</mark></NType> <DataStandard> <SMSModuleName><mark>EA001</mark></SMSModuleName>

Security Management System - Using HTTP API - 'sendExternalAlarm' www.infinova.com



</DataStandard> <DataCustom/> </NData>

The 2 strings highlighted in yellow background should match i. 'External Alarm 11' string indicates the alarm type. It can be any string associated with the 32 exernal alarm types available in the 'Security Management System Server' software ii. 'EA001' string is for the 'External alarm module name'. It should match the name of the target 'External alarm module' defined in the 'Security Management System' server software.

- 6. Click on the 'Send' button. The Postman application will send the request to 'Security Management System' server software, and will receive the response and will display it.
- 7. Please access the 'Params' tab to view the response details

Untitled Request										
POST v http://192.168.0.75:9900/sendExternalAlarm										
Params Authorization •	Headers (10) Boo	dy   Pre-request Script Tests								
Query Params										
KEY		VALUE	D	DESCRIPTION						
Key		Value	[	Description						
Body Cookies Headers (2) T	est Results		Status: 200 Okay	Time: 276ms						
Pretty Raw Preview	XML 🔹 🚍									
1 (NResponse) 2 (NRequestType>sms 3 (ResponseStandard 4 (RCode>15 (RDescription 6 (/ResponseStandard 7 (/NResponse)	ExternalAlarmNotifi  >  de>  >Success d>	.cationRealTime								

Please access the 'Body' sub-tab, which will show the response XML data.