Raptor Connect – Technical Specification

Contents

Overview

Contacts

Implementation	Customer Service
	customerservice@bogen.com

	1.800.999.2809
Technical	Support
	support@bogen.com
	1.800.999.2809
Leadership	Ken Venuti
	Director, Sales Engineering
	kvenuti@bogen.com
	cell: (407) 504-9187
	office: (201) 995-2005

Raptor to Bogen

Supported Use Cases

- Leveraging the Nyquist Routine API, an emergency in Raptor can trigger a "routine" in the external/public facing Nyquist E7000 server. These routines can be set up to do many different things in their server such as triggering intercom speakers to play a pre-recorded message, trigger alarms/sirens, or even send notifications (email/SMS).

Implementation

Teams

- Raptor Professional Services (PS)
- Raptor Customer Success (CS)
- Bogen/Nyquist Server Administrator (BA)

Raptor Prerequisites

N/A

Partner Prerequisites

1. If using an on-prem installation, the Nyquist server must be accessible from the Internet.
   a. A static IP address or domain name is required.
   b. Configure network to allow external access to the Nyquist server.
2. Provide Authorization Bearer API Key (bearer token) to Raptor.
3. Configure a Nyquist "Routine" and provide Routine ID# (DTMF Code) to Raptor.

Process

[Provide a step-by-step detailed breakdown of how the integration is configured. Make sure to specify what is a Raptor process vs partner process]

Owner (Raptor or Partner)	Team	Task	Comments
Raptor	CS/PS	Create a RaptorConnect implementation and assign it to the integration implementation team.	If client is in active EM implementation, PS will do this. If client is post implementation, CS will do this.
Raptor	PS	Raptor integration implementation team will reach out to Bogen Administrator to schedule a call to discuss getting client set up with integration.	
Partner	BA	The district will work with Bogen Dealer to configure "Routines" to be triggered in Nyquist server upon Raptor initiation.	
Raptor	PS	Get Nyquist server details from client: • Server Address • Authentication Bearer Token • Routine ID's to be mapped to Raptor Emergencies	
Raptor	PS	Configure webhook to trigger Nyquist routine on initiation.	[**https://%3cip_address%3e/routine/api/%3cdtmf_code%3e/%3cpassword%3e/%3cdelay_flag%3e/%3cparam1%3e/%3cparam2%3e2]https://<ip_address>/routine/api/<dtmf_code>/<password>/<delay_flag>/<param1>/<param2>**

Configuration

Credential

An Authorization Bearer API key (Bearer Token) is used in the header of the request to authenticate. This will be provided by the client.

Destination

Server address (ex. https://97.68.97.117) will be provided by the client. The format of the web request is as follows.

https://%3cip_address%3e/routine/api/%3cdtmf_code%3e/%3cpassword%3e/%3cdelay_flag%3e/%3cparam1%3e/%3cparam2%3e2]https://<ip_address>/routine/api/<dtmf_code>/<password>/<delay_flag>/<param1>/<param2>

Rule

Any Emergency Initiated

The following rule will send any Emergency initiated in Raptor Alert to Bogen:

```
{
    "==": [
        {
            "var": "Data.IncidentStatus"
        },
        "Initiated"
    ]
}
```

Lockdown Emergency Initiated

The client may prefer to send only "Lockdown" emergencies. The following rule should be used:

```
{
    "and": [
        {
            "==": [
                {
                    "var": "Data.IncidentType"
                },
                "Lockdown"
            ]
        },
        {
            "==": [
                {
                    "var": "Data.IncidentStatus"
                },
                "Initiated"
            ]
        }
    ]
}
```

Lockdown Emergency Initiated at a specific Building

The client may prefer to send only "Lockdown" emergencies for a specific building. The following rule should be used with the client's building unique identifier:

```json
{
    "and": [
        {
            "==": [
                {
                    "var": "Data.IncidentType"
                },
                "Lockdown"
            ]
        },
        {
            "==": [
                {
                    "var": "Data.IncidentStatus"
                },
                "Initiated"
            ]
        },
        {
            "==": [
                {
                    "var": "Building.Uid"
                },
                "2ff79b2a-df3d-488b-a8e8-7585421742c5"
            ]
        }
    ]
}
```

Payload

Configuration and Credential information below.

Configuration:

```
{
    "ttl": -1,
    "uid": "00000000-0000-0000-0000-000000000000",
    "isDeleted": false,
    "createdBy": "00000000-0000-0000-0000-000000000000",
    "createdDateTime": "2022-07-20T14:39:33.3810691+00:00",
    "modifiedBy": "00000000-0000-0000-0000-000000000000",
    "modifiedDateTime": "2023-03-08T16:19:34.9190777+00:00",
    "id": "cffd6358-72a3-4ec5-bce2-178ae72c7367",
    "name": "Bogen Emergency Lockdown",
    "clientId": "906ce56c-3d38-471b-adab-c2ab10907b10",
    "rule": "{\"==\": [{\"var\": \"Data.IncidentType\"}, \"Police\"]}",
    "url": "https://97.68.97.117/routine/api/7777/0/0/%BUILDING_NAME%/0",
    "template": "",
    "webhookCredentialId": "47279460-ba11-4248-b4d8-253fe4e45eec",
    "customHeaders": [],
    "httpVerb": "GET",
    "configType": "Emergency",
    "contentType": "application/json",
    "isEnabled": true,
    "ignoreSslErrors": true,
    "_rid": "ldReAOER7yTzFAAAAAAAAA==",
    "_self": "dbs/ldReAA==/colls/ldReAOER7yQ=/docs/ldReAOER7yTzFAAAAAAAAA==/",
    "_etag": "\"0d00595a-0000-0500-0000-64bfd9d60000\"",
    "_attachments": "attachments/",
    "_ts": 1690294742
}
```

Credential:

```
{
    "id": "47279460-ba11-4248-b4d8-253fe4e45eec",
    "clientId": "906ce56c-3d38-471b-adab-c2ab10907b10",
    "createdBy": "00000000-0000-0000-0000-000000000000",
    "createdDateTime": "2022-07-27T10:31:56.3173029Z",
    "isDeleted": false,
    "modifiedBy": "00000000-0000-0000-0000-000000000000",
    "modifiedDateTime": "2022-07-27T10:31:56.3173039Z",
    "name": "Bogen Api Key",
    "ttl": -1,
    "type": "ApiKey",
    "uID": "3c17df8e-4371-4065-acbc-9774a9d0ebb4",
    "__jObject": null,
    "apiKey": "Bearer 0a9905335523aaf78cbbbd3591b9c814",
    "apiKeyHeaderName": "Authorization",
    "_rid": "ldReAJ0AKNjhCAAAAAAAAA==",
    "_self": "dbs/ldReAA==/colls/ldReAJ0AKNg=/docs/ldReAJ0AKNjhCAAAAAAAAA==/",
    "_etag": "\"4a00b3f0-0000-0500-0000-64be820c0000\"",
    "_attachments": "attachments/",
    "_ts": 1690206732
}
```

Integration Testing

1. Initiate an Emergency in Raptor Alert
2. Login to the Nyquist Console
3. Confirm routine was triggered

Document Revision History

Date	Comment	Modified By
7/31/2023	Initial Version	Cole Popielarczyk