



**ADVANCED**  
NETWORK DEVICES

## Raptor Outbound CAP Integration

Version 1.1

1/27/2026

© 2025 ADVANCED NETWORK DEVICES

3820 NORTH VENTURA DR.

ARLINGTON HEIGHTS, IL 60004

U.S.A

ALL RIGHTS RESERVED

## Proprietary Notice and Liability Disclaimer

The information disclosed in this document, including all designs and related materials, is the valuable property of Digital Advanced Network Devices and/or its licensors. Advanced Network Devices and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

The Advanced Network Devices product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by Advanced Network Devices.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of Advanced Network Devices is prohibited.

## Static Electric Warning



## TROUBLESHOOTING AND ADDITIONAL RESOURCES

User Support: <https://www.anet.com/user-support/>  
Technical Resources: <https://www.anetd.com/user-support/technical-resources/>  
AND Legal Disclaimer: <https://www.anetd.com/legal/>


## OVERVIEW

ClockWise 1.17.22 and higher can initiate emergencies in Raptor. You must contact Raptor for essential information before attempting this integration.

## GENERATING THE CREDENTIAL IN WEB CLOCKWISE

To enable ClockWise to send an outbound Rest request to Raptor, you will need to first generate a credential in ClockWise:

1. Log in to the ClockWise Web Interface ([https://\[CW Machine IP\]:44390](https://[CW Machine IP]:44390)) as an admin. Next, go to the **Admin > Outbound Rest Requests** page (/HttpAction):








The screenshot shows the ClockWise Campus Administration interface. On the left is a dark blue sidebar with navigation options: Home, Support, Plugins, Admin (highlighted with a red box), and Logout. At the bottom of the sidebar, it shows 'Connection: [green dot]', 'ADVANCED NETWORK DEVICES', and 'Version: 1.17.15.8650'. The main content area is titled 'Administration' and contains a grid of 18 icons for various functions. The 'Outbound REST Requests' icon, located in the third row, second column, is highlighted with a red box. Other icons include ClockWise License, SSL Certificate, Permission Editor, Communication Settings, Log Viewer, Endpoint List, Group Editor, Firmware Updates, Site Map, Email, Email Endpoints, Feed Controller, Configurations, LED Graphic Editor, Inbound REST API, Import Settings, and Vigilar GSD.

2. Go to the **Authorization Manager** section and click the **Add New Credential** button:

## Outbound REST Requests

API Endpoints Authorization Manager

### Saved Credentials

Authorization Name	Authorization Type	Actions
Raptor Creds	ClientCredentials	    

First Prev **1** Next Last

1 - 1 of 1 items

**Add New Credential**

3. Give the credential a name of your choosing. The **Authorization Type** must be set to **ClientCredentials**. All other fields including **Client ID**, **Client Secret**, **Authorization URL**, and **Audience** are provided by Raptor:

## Outbound REST Requests

API Endpoints Authorization Manager

Credential Name \*

Raptor Credentials

Authorization Type \*

ClientCredentials

Client ID \*

Client Secret \*

Authorization URL \*

Audience \*

**Save Credential**

**Test Credentials**

Cancel

4. Click **Save Credential** to create the new credential.

## CREATING AN API ENDPOINT IN CLOCKWISE

Next, you will need to create an API Endpoint in ClockWise.






1. Click on the **API Endpoints** tab then click the **Add New Endpoint** Button:

### Outbound REST Requests

**API Endpoints**

Authorization Manager

#### Saved API Endpoints

Endpoint Name	Credential	Authorization Type	Actions
Raptor Evacuate	Raptor Creds	ClientCredentials	    

First Prev **1** Next Last

1 - 1 of 1 items

**Add New Endpoint**

2. Give the endpoint a name, select the credential you just created, select **POST** as the **Http method** and leave the **Body Type** as **application/json**. The **Base URL** and **Body Text** should be provided by Raptor:

**API Endpoints**

Authorization Manager

Endpoint Name \*

Raptor Initiate Lockdown

Credential \*

Raptor Credentials

Http Method \*

POST

Base URL \*

Add Header

Body Type \*

application/json

- Click Save Endpoint once all fields are entered to create the new API endpoint:

Add Header

**Body Type \***

**Body Text**

```
{
  "lat": "",
  "long": "",
  "additionalData": "Test Data",
  "isDrill": false
}
```

Save Endpoint

Test Request

Cancel

- Repeat these steps if you would like to create additional endpoints to initiate different emergencies in Raptor.

## CREATING A NOTIFICATION IN CLOCKWISE

You will need access to the ClockWise desktop application in order to create or edit notifications in ClockWise. If you already have a notification configured in ClockWise you can skip to step 3 since you would only need to add the new API endpoint as a recipient of the pre-existing notification. You can double-click a notification in the **Notifications** tab to edit it.

- Go to the **Notifications** tab and click the **Add a Notification** button:

The screenshot shows the ClockWise Campus desktop application interface. The 'Notifications' tab is selected and highlighted with a red box. Within this tab, the 'Add a Notification' button is also highlighted with a red box. Below the button is a table listing existing notifications.

Label	Endpoint(s)	Type	When	Day	Time	Audio File	Volume	Scrolling Text
Active Shoo...		Triggered	Manual	-	-	notify15.wav	4	TAKE SHELTER
Actualizació...		Triggered	Manual	-	-	beep10.wav	6	Pixmap
Advertencia ...		Triggered	Manual	-	-	beep17.wav	5	Pixmap
Alerta de Fal...		Triggered	Trap Type=Internet A...	-	-		3	La conexión al internet ...
Alerta de To...		Triggered	Manual	-	-	beep2.wav	5	Pixmap
Alerta de Us...		Triggered	Trap Type=ClockWis...	-	-		3	¡El Usuario de Clockwis...
Alerta HTTP...		Triggered	Trap Type=Custom H...	-	-		3	Se ha recibido la solicit...
Amplify Flas...	Hardware Team ...	Triggered	Trap Type=ClockWis...	-	-		3	
AND Logo	Web_Interface_...	Triggered	Manual	-	-		3	

2. Configure the notification as desired. This includes the **Label**, **When**, and **Actions** sections:

**Label**

Name: Lockdown Category: Emergencies Priority: 50

**When**

Trigger: Manual Source: N/A Channel or sub-type: N/A State: N/A Extra Action: None

**Actions**

**Audio**

WAV file: .../evacuate.wav Volume: 3.0 # of Repeats: 1 Sound file length: 00:00:07

**Scrolling Text**

Type: User Text Message: Lockdown Fore Color: Def. Back Color: Def. Font: Def. Brightness: 100

Repeat: 1 times Pause between repeats: 0 seconds Mode: Auto Lines: 1 Speed: 6

**Output devices**

Endpoint	Location	IP Address	Flashers	Inputs	Outputs	Display
<input checked="" type="checkbox"/> All AND Devices	AutoGroup	-	-	-	-	-
<input type="checkbox"/> PC Speakers	-	10.10.6.97	-	-	-	-
<input type="checkbox"/> Vigilant Listeners	AutoGroup	-	-	-	-	-
<input type="checkbox"/> Darren's Rule	AutoGroup	-	-	-	-	-

3. Once the notification is configured as desired, you will need to include the API endpoint in the Output devices list located at the bottom of the Notification Editor window:

**Output devices**

Endpoint	Location	IP Address	Flashers	Inputs	Outputs	Display
<input checked="" type="checkbox"/> All AND Devices	AutoGroup	-	-	-	-	-
<input checked="" type="checkbox"/> Raptor Initiate Lockdown	-	https://api-stag.raptortech...	-	-	-	-
<input type="checkbox"/> Voyager	Tony's Desk	10.10.0.48	yes	0.0	0.0	yes
<input type="checkbox"/> All Endpoints	AutoGroup	-	-	-	-	-
<input type="checkbox"/> DDC: Wall: Lobby IPCSH...	Lobby	10.10.1.0	yes	0.0	0.0	yes
<input type="checkbox"/> DDC: Wall: Becky IPSWD...	BoilerRoom	10.10.0.130	yes	0.0	0.0	yes
<input type="checkbox"/> Demo Room entrance	on kitchen entrance wall	10.10.0.193	yes	0.0	0.0	yes
<input type="checkbox"/> DDC: Wall: SalesMktg IPC...	Sales-Marketing Room	10.10.0.63	yes	0.0	0.0	yes
<input type="checkbox"/> Upstairs Lab Hallway LHD	DemoRoom	10.10.0.240	yes	-	-	yes
<input type="checkbox"/> DDC: Wall: McKinley IPCS...	McKinleyRoom	10.10.0.116	yes	-	-	yes
<input type="checkbox"/> DDC: Wall: Lincoln IPCSH...	LincolnRoom	10.10.0.106	yes	-	-	yes
<input type="checkbox"/> DDC: Catwalk DS - AIO	-	10.10.0.218	yes	-	-	yes

Test Now Stop **OK** Cancel

4. Click OK to save the notification.
5. Repeat these steps if you would like to create notifications to trigger other emergencies in Raptor. Note: you will need to create multiple API endpoints if you would like to be able to initiate different emergencies in Raptor.

## TESTING

It is recommended that testing is performed to confirm everything is functional. To check if everything is working, run the notification(s) that were created in ClockWise. The notifications can be initiated from the **Notifications** tab. Find the notification you would like to test, **right-click** on it, and select the **Run Now** option in the pop-up menu. You should see an active incident on the Incidents page in Raptor:

