Newline Secure User Guides

Please use the following guides below and ensure that you follow all of the steps for proper deployment and activation of Newline Secure.

It is recommended to follow the steps of the Portal Sign-Up Guide, then either the Singlewire or Centegix Integration Guide, and finally the Mass-Deployment Guide.

Portal Sign-Up Guide

Singlewire Integration Guide

Centegix Integration Guide

Mass-Deployment Guide

If you prefer to learn about Newline Secure through an interactive training, check out our training course here!

If you have questions or need assistance with Newline Secure, please contact Newline Technical Support:

- Submit a ticket here!
- Give us a call at +1 (833)-469-9520

If you have questions or need assistance with the Singlewire Portal, please contact Singlewire Support by submitting a ticket using the link below:

- https://support.singlewire.com/s/contactsupport

If you have questions or need assistance with the Centegix Portal, please contact Centegix Support by sending an email:

- support@centegix.com

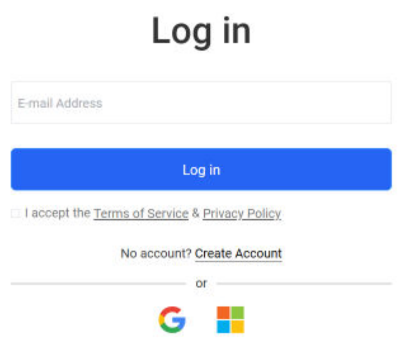
Portal Sign-Up Guide

Signing Up & Registering for Newline Secure

This guide will walk you through how to create and sign-up for your Newline Secure account.

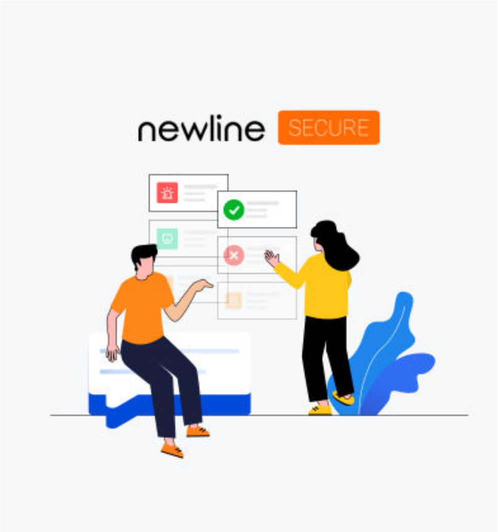
Step 1: Navigate to the Newline Secure Portal

- Please visit the Newline Secure Portal



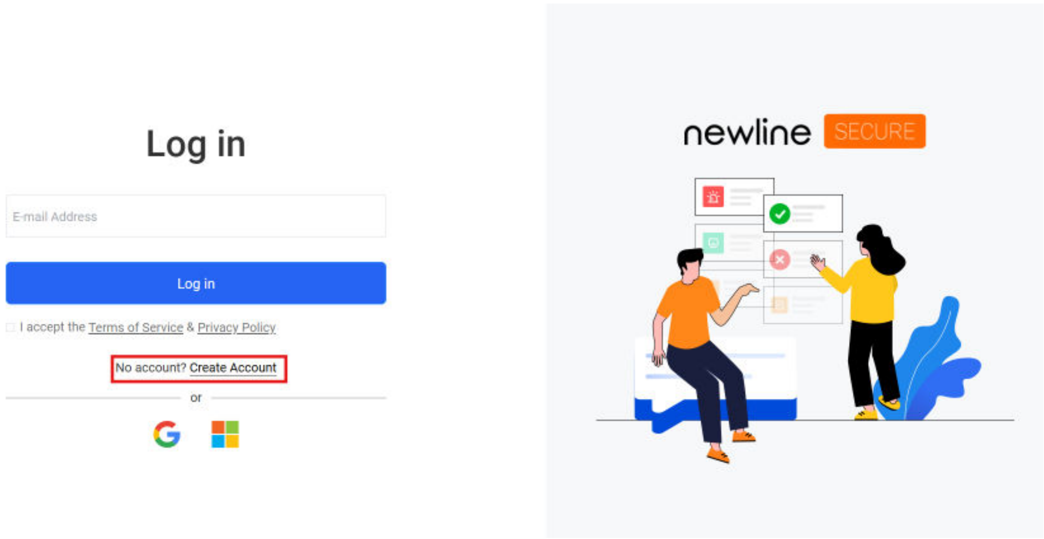
□ I accept the Terms of Service & Privacy Policy

No account? Create Account



Step 2: Creating Your Account

- Select the ‘Create Account’ option in order to begin registration



Log in

E-mail Address

Log in

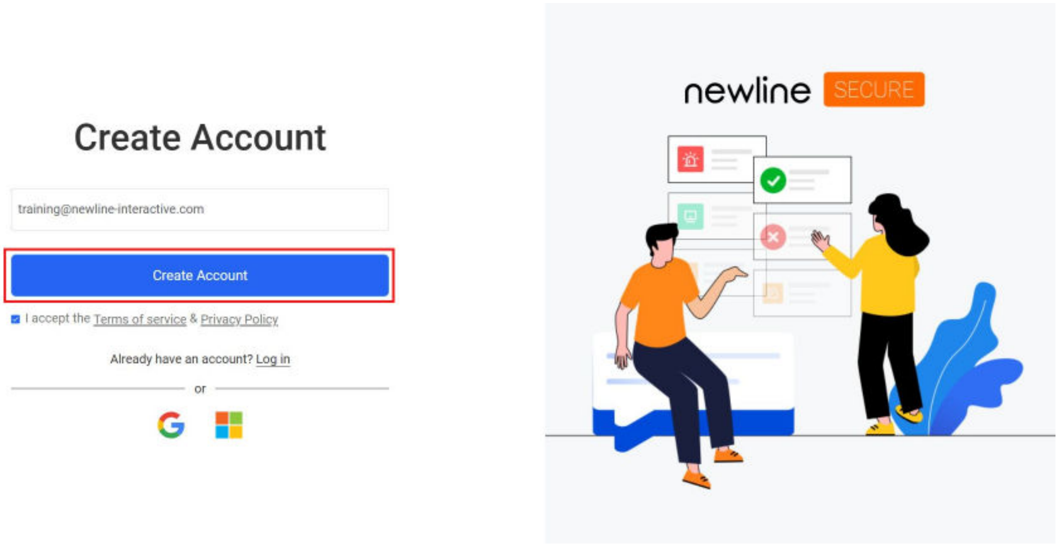
□ I accept the Terms of Service & Privacy Policy

No account? Create Account

or

newline SECURE

- Enter your email in the provided field and select 'Create Account'
    - **Note: An organization domain is required to create an account.**



Create Account

training@newline-interactive.com

Create Account

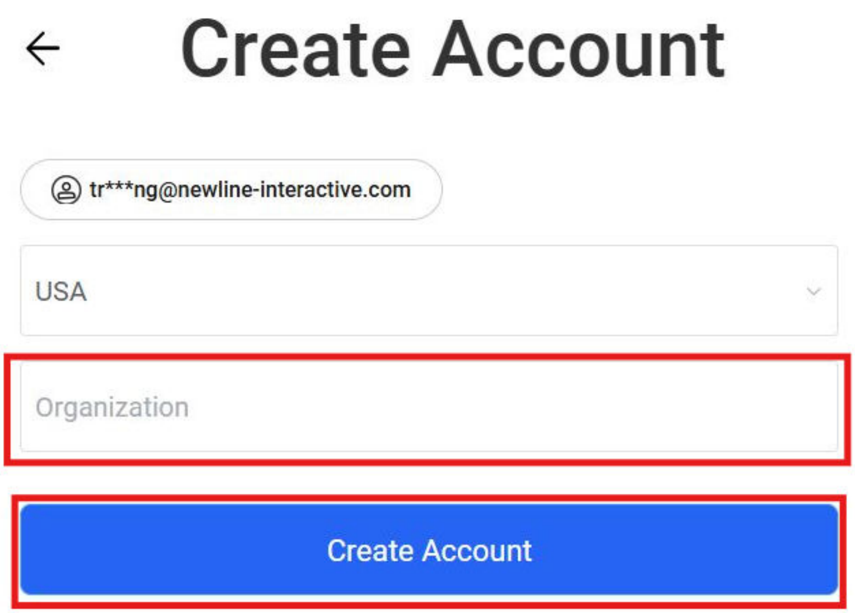
☑ I accept the Terms of service & Privacy Policy

Already have an account? Log in

or

newline SECURE

- Enter your organization name in the provided field and select 'Create Account'

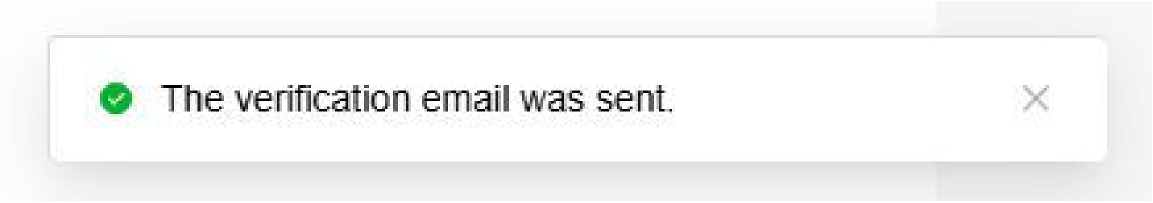


Create Account

tr***ng@newline-interactive.com

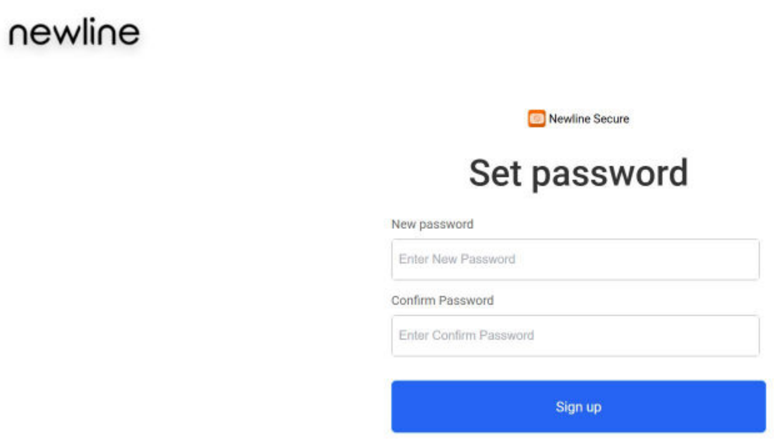
USA

- You will be redirected to a login page and will receive a pop-up message to you verify your email.



The verification email was sent.

- Please login to your associated email account and click the link to verify your email address.
- After email verification, you will be asked to set your password.



newline

Newline Secure

Set password

New password

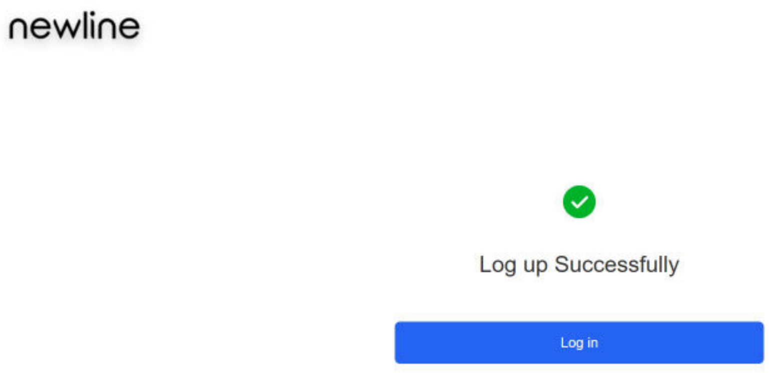
Enter New Password

Confirm Password

Enter Confirm Password

Sign up

- After setting your password, your account has now been created!



newline

Log up Successfully

Log in

Congratulations, you have successfully created and registered your Newline Secure account!

Please continue on to either the
 Singlewire or Centegix integration guides in order to proceed with the setup of Newline Secure.

If you have questions or need assistance with the Newline Secure portal, please contact Newline Technical Support:

- Submit a ticket here!
- Give us a call at +1 (833)-469-9520

Singlewire Integration Guide

Integrating Newline Secure with Singlewire InformaCast

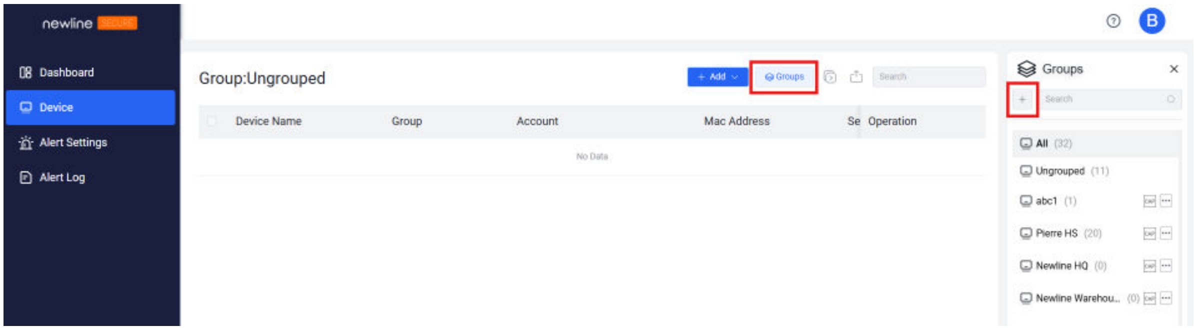
This guide will walk you through integrating Newline Secure with Singlewire InformaCast using InformaCast API connectors and scenarios.

Before proceeding with this guide, please ensure that you have followed the Portal Sign-Up Guide **in order to create your account!**

Note: Only Newline Q Pro Series Panels are currently supported. For best performance and stability, please ensure that your Q Pro is on firmware v1.0.75 or higher.

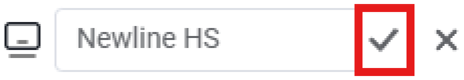
Step 1: Create a Device Group

- On the 'Device' tab, look for the 'Groups' sidebar and click the '+' icon



  - If you do not see the 'Groups' sidebar, then you can click the 'Groups' button to open it.

- Type in a name for your group in the text box that appears, and click the '✓' icon



Newline HS

Step 2: Register Your Devices

Note: Only Newline Q Pro Series Panels are currently supported. For best performance and stability, please ensure that your Q Pro is on firmware v1.0.75 or higher.

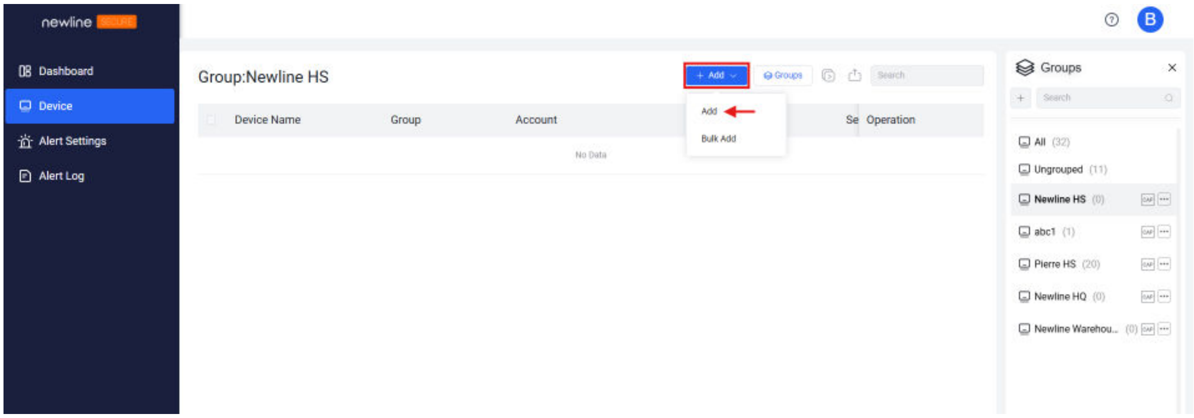
There are three methods for registering your devices to a Newline Secure Device Group:

- Single Device Registration via the Web Console
- Bulk Device Registration via the Web Console
- Registration via the Newline Secure Android Application on the Display

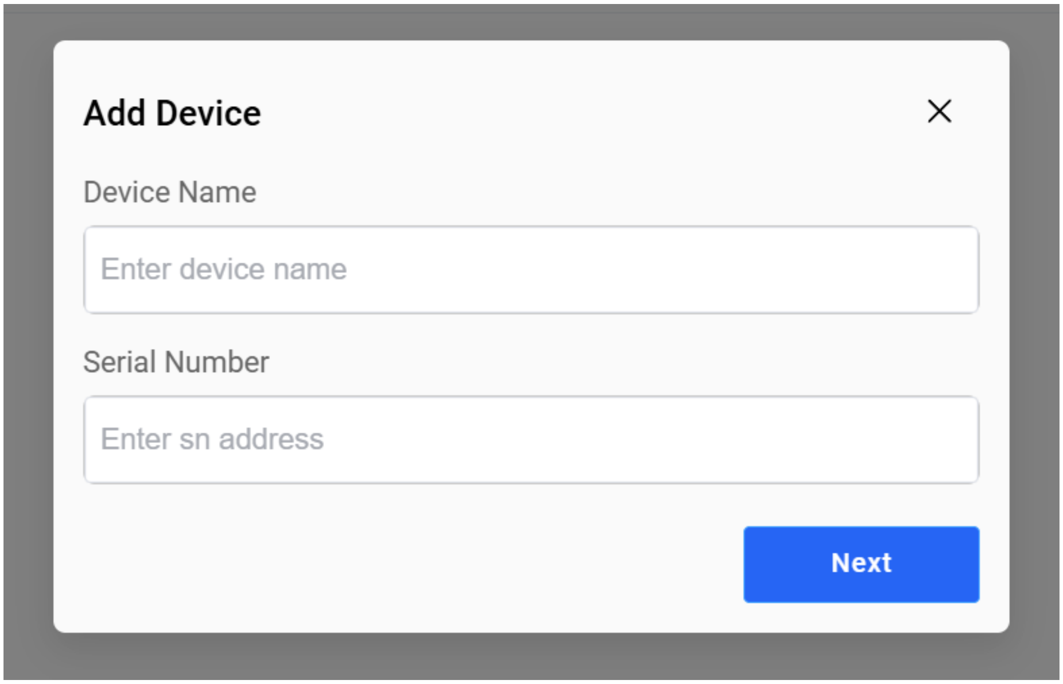
2.1 Register Your Device on the Newline Secure Web Console

2.1.1 Single Device Registration (Method 1)

- On the 'Device' tab, navigate to and click the blue 'Add' button, then select 'Add'

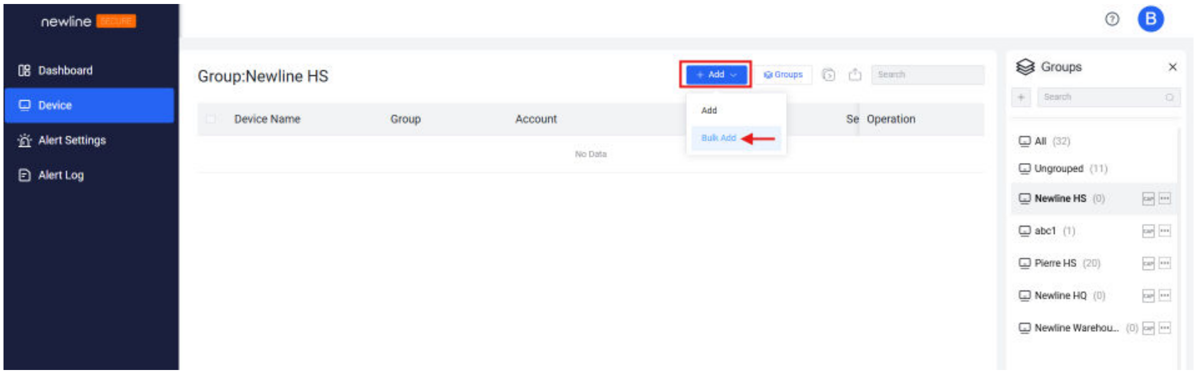


- Input the device's serial number and set a name for the device, then click 'Next'

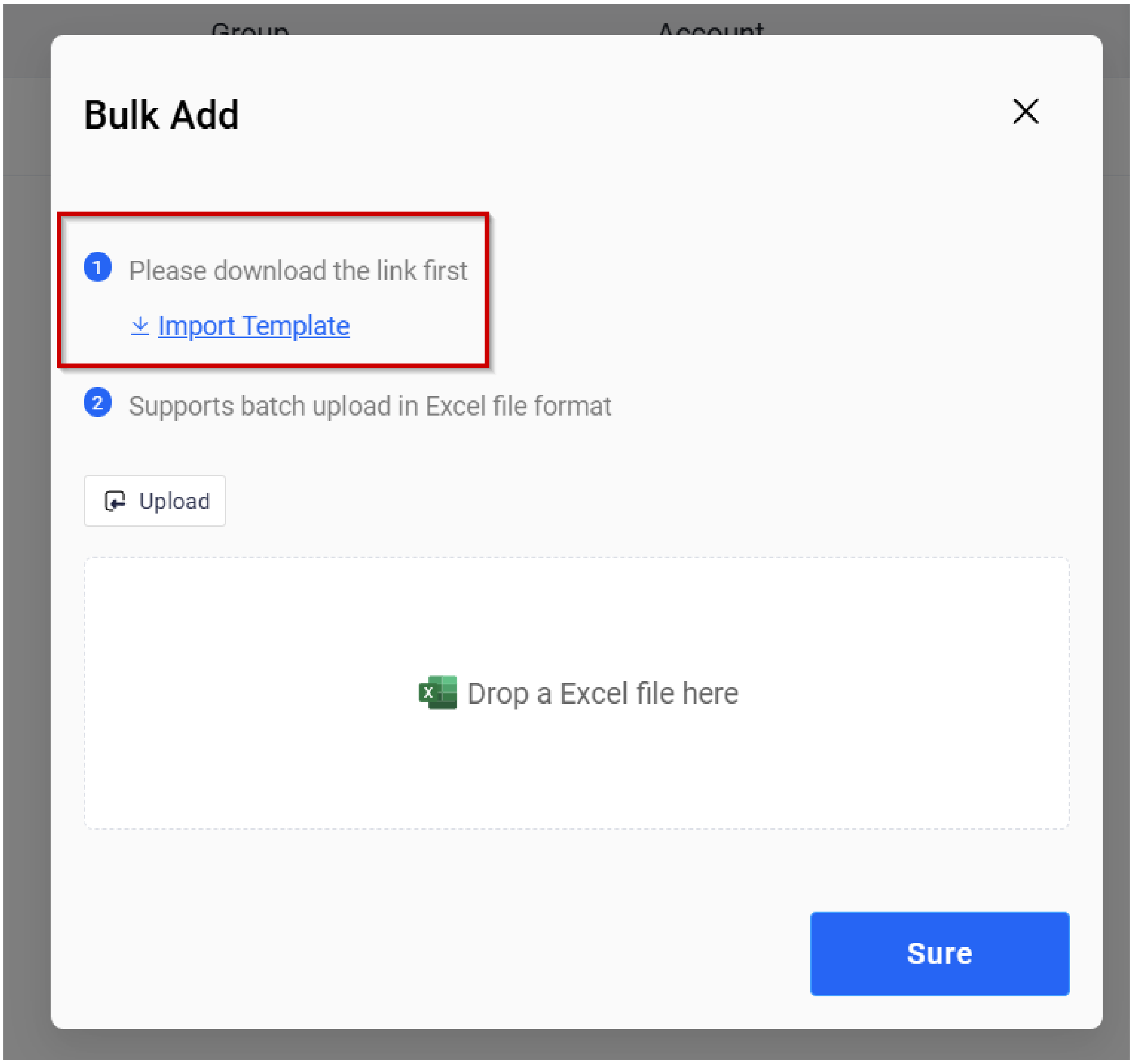


2.1.2 Bulk Device Registration (Method 2)

- On the ‘Device’ tab, navigate to and click the blue ‘Add’ button, then select ‘Bulk Add’



- Download the import template using the provided link



Bulk Add

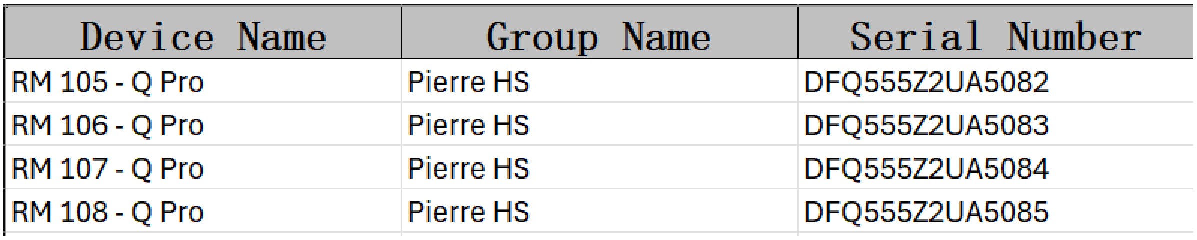
1 Please download the link first

Import Template

2 Supports batch upload in Excel file format

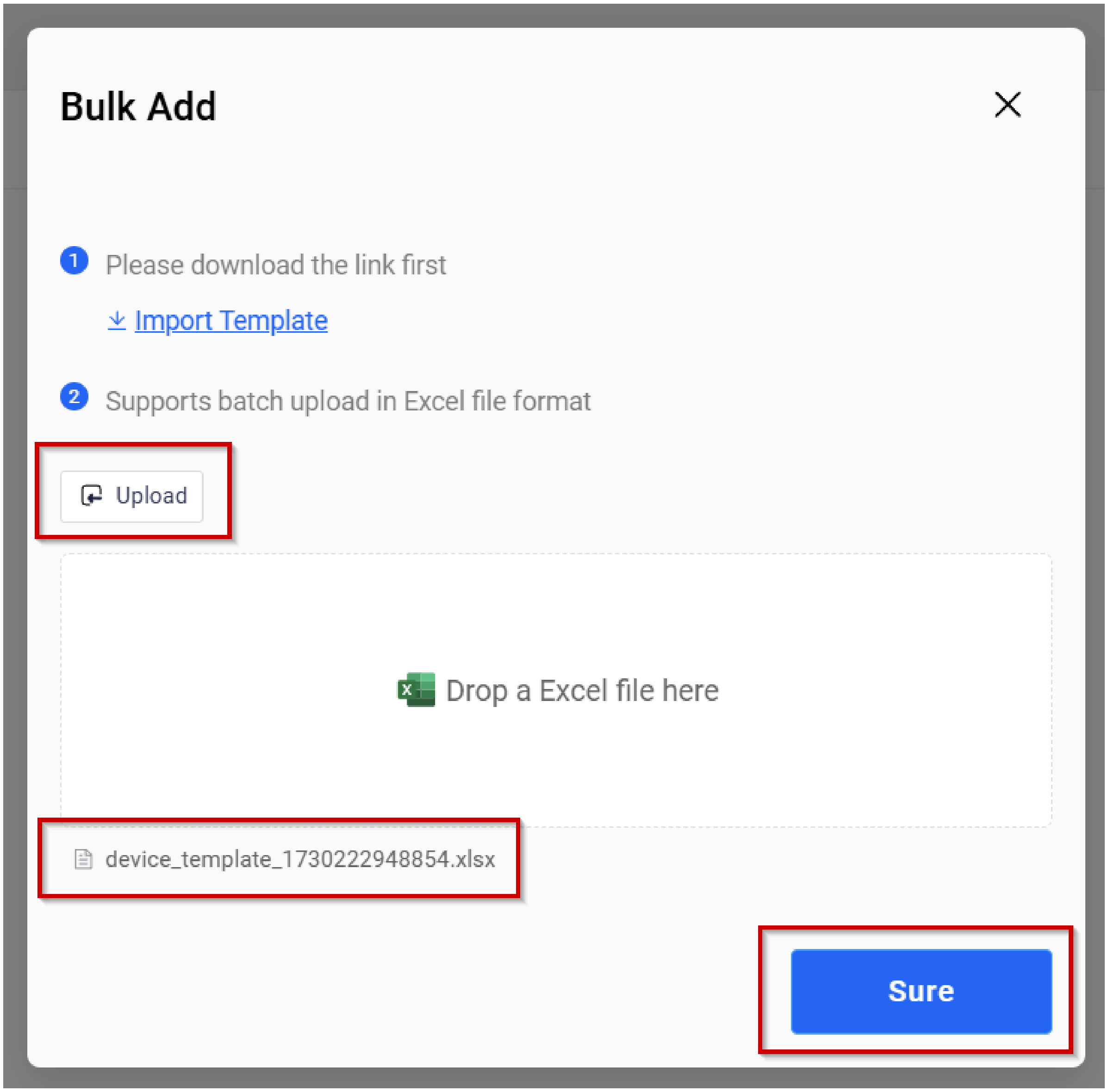
Drop a Excel file here

- Enter your devices into the Excel table and save the import template to your computer (.xlsx format)



Device Name	Group Name	Serial Number
RM 105 - Q Pro	Pierre HS	DFQ555Z2UA5082
RM 106 - Q Pro	Pierre HS	DFQ555Z2UA5083
RM 107 - Q Pro	Pierre HS	DFQ555Z2UA5084
RM 108 - Q Pro	Pierre HS	DFQ555Z2UA5085

- Select ‘Upload’ or drag and drop the Excel file into the designated area, then click the confirmation button to complete bulk-registration



Bulk Add

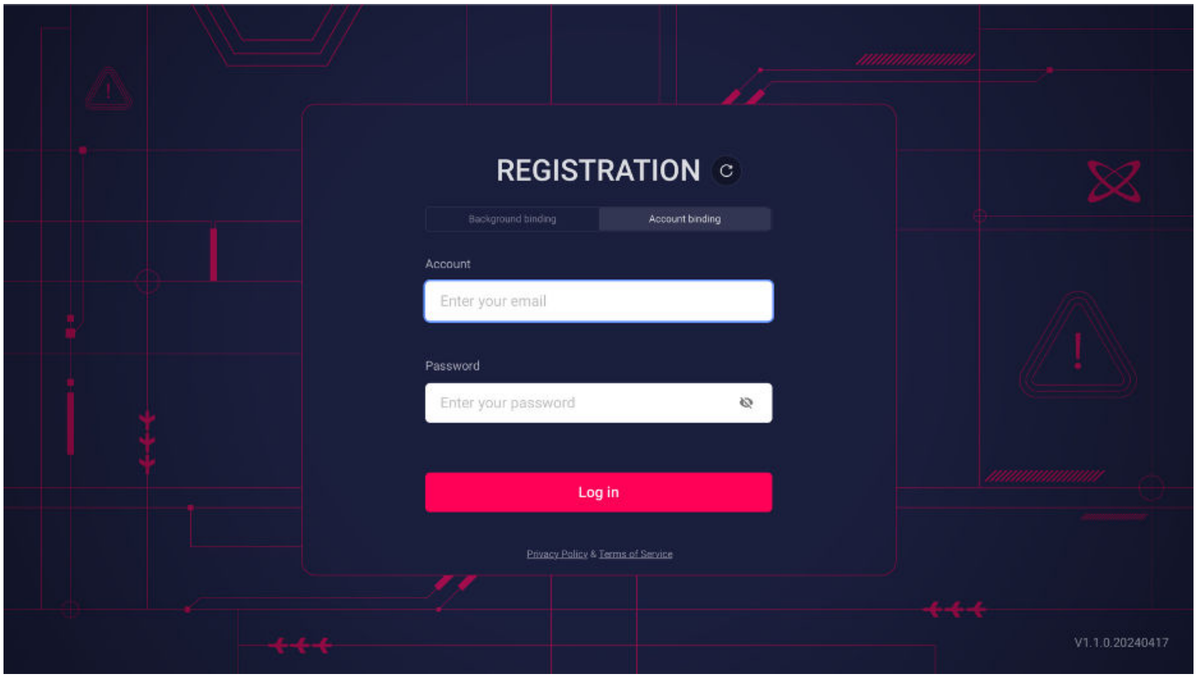
1 Please download the link first

Import Template

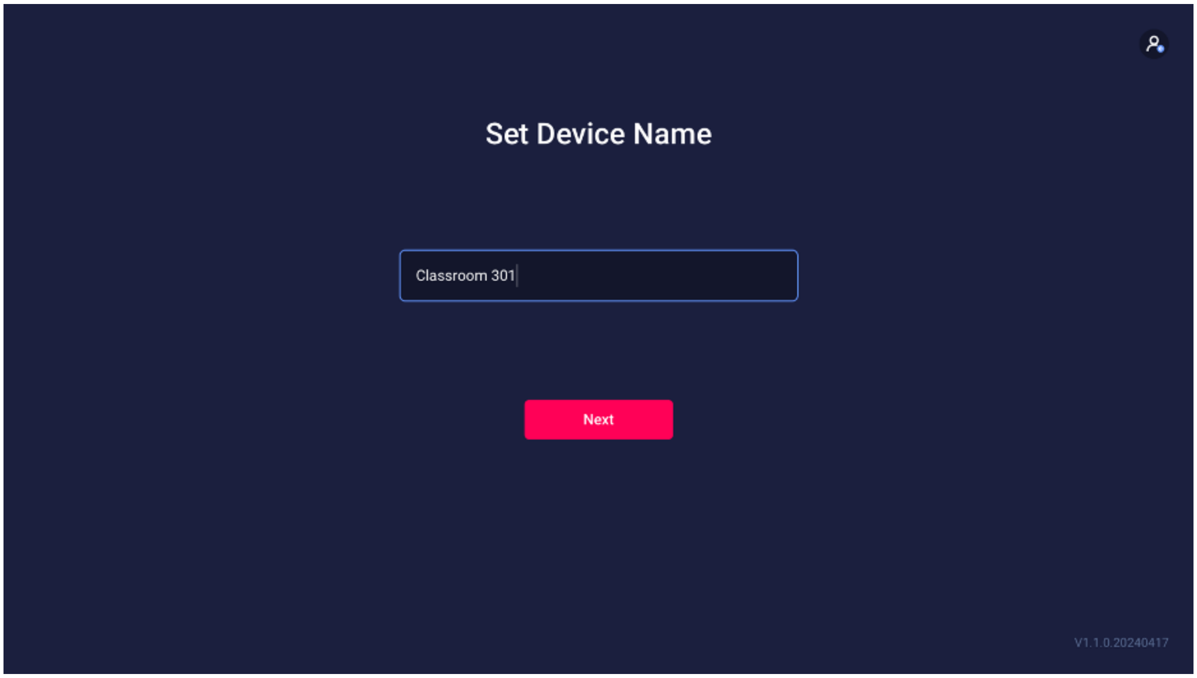
2 Supports batch upload in Excel file format

2.2 Registration via the Newline Secure Android Application (Method 3)

- Open the ‘Newline Secure’ application on your display
- Tap ‘Account Binding’
- Login with your Newline Secure account information

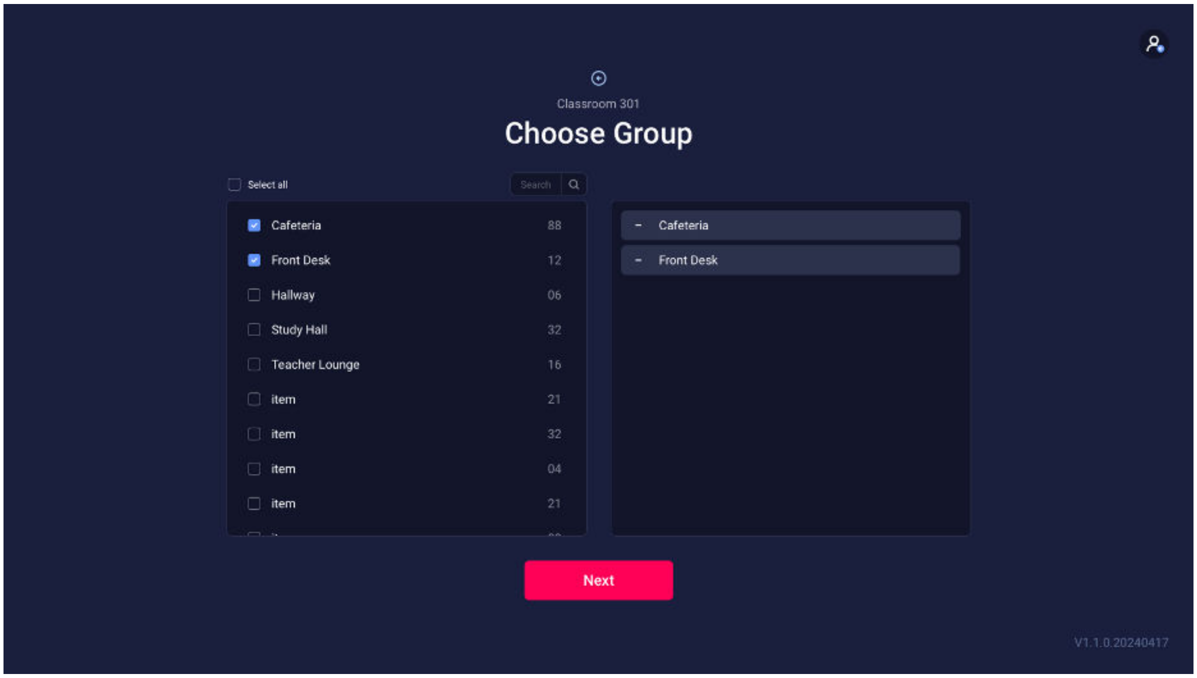


- Enter a device name for this display



Classroom 301

- Select at least one group for this display to be registered to



Classroom 301

Choose Group

□ Select all

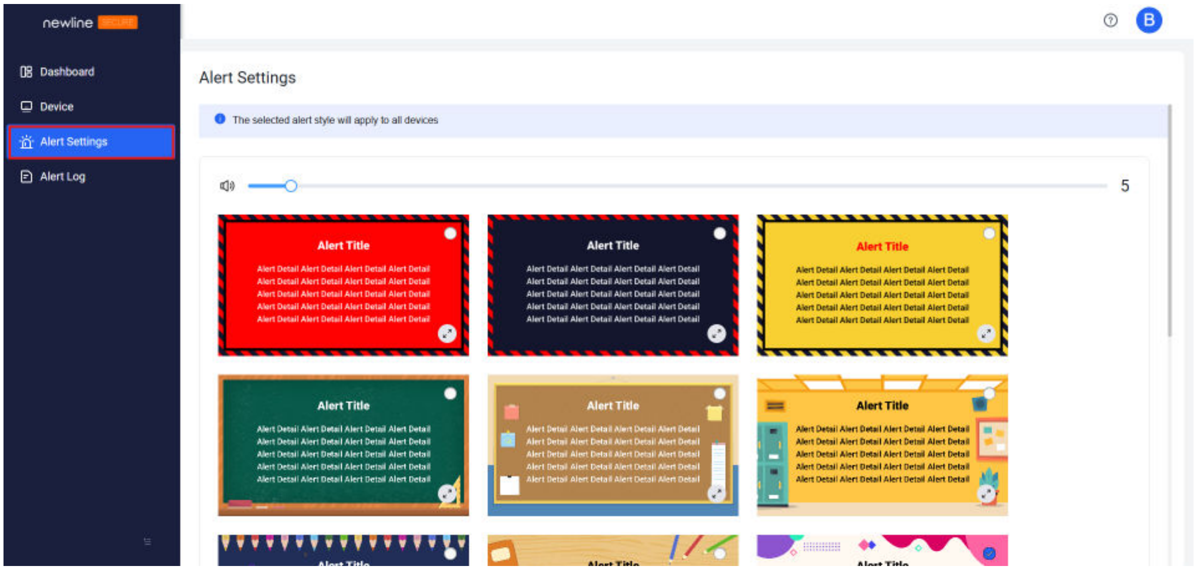
Search

☑ Cafeteria	88
☑ Front Desk	12
□ Hallway	06
□ Study Hall	32
□ Teacher Lounge	16
□ item	21
□ item	32
□ item	04
□ item	21

- Cafeteria
- Front Desk

Step 3: Customize your global alert settings

- On the ‘Alert Settings’ tab, you can customize the alert background image and audio level for your Newline Secure alerts:



Alert Settings

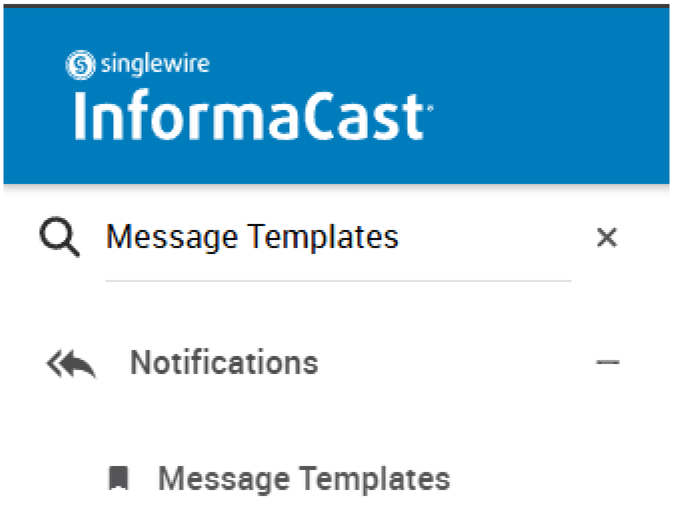
The selected alert style will apply to all devices

5

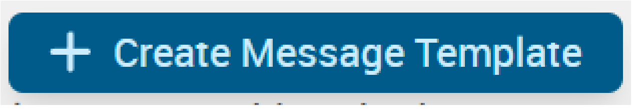
- Note: These settings automatically apply **globally** across all Newline Secure groups and devices

Step 4: Create your Singlewire InformaCast Message Template

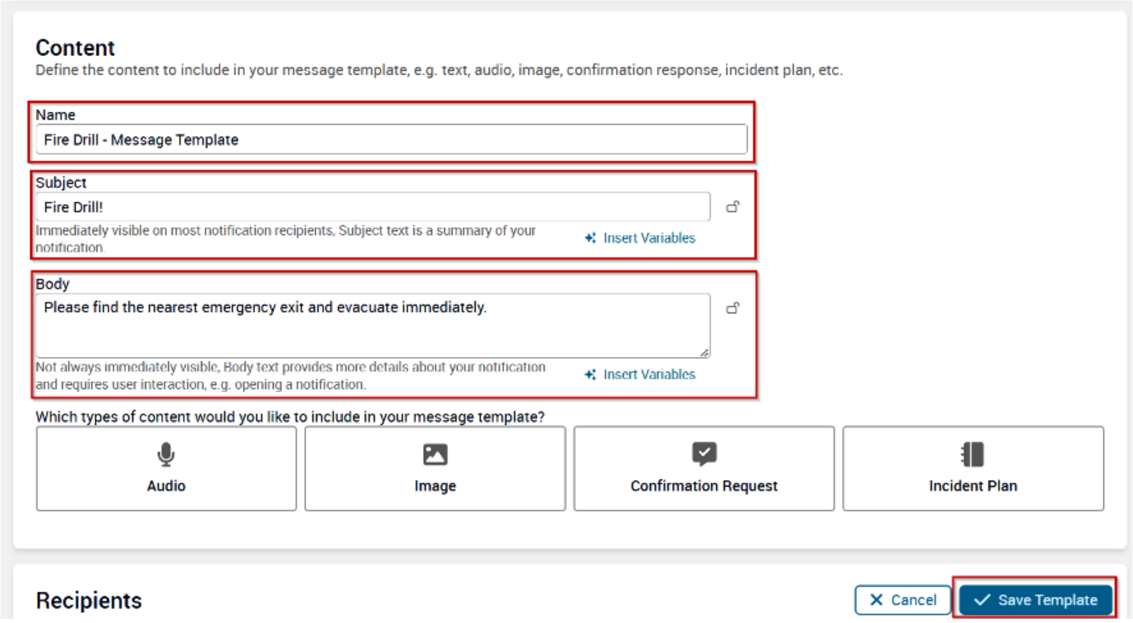
- Inside of your Singlewire InformaCast console, navigate to **'Notifications'** ⇒ **'Message Templates'**



- Click the **'Create Message Template'** button in the top right



- Add the following items into the message template, then click the **'Save Template'** button in the bottom right corner
  - Template Name
  - Alert Subject
  - Alert Body (Description)



Content

Define the content to include in your message template, e.g. text, audio, image, confirmation response, incident plan, etc.

Name: Fire Drill - Message Template

Subject: Fire Drill!

Immediately visible on most notification recipients, Subject text is a summary of your notification

Body: Please find the nearest emergency exit and evacuate immediately.

Not always immediately visible, Body text provides more details about your notification and requires user interaction, e.g. opening a notification.

Which types of content would you like to include in your message template?

- You will also have to add in a recipient to save this template, feel free to add any external systems (that are not Newline Secure) or email addresses for notifications.
- **Note: Custom Audio & Images are not currently supported by Newline Secure.**

Step 5: Create your Singlewire InformaCast Scenario(s)

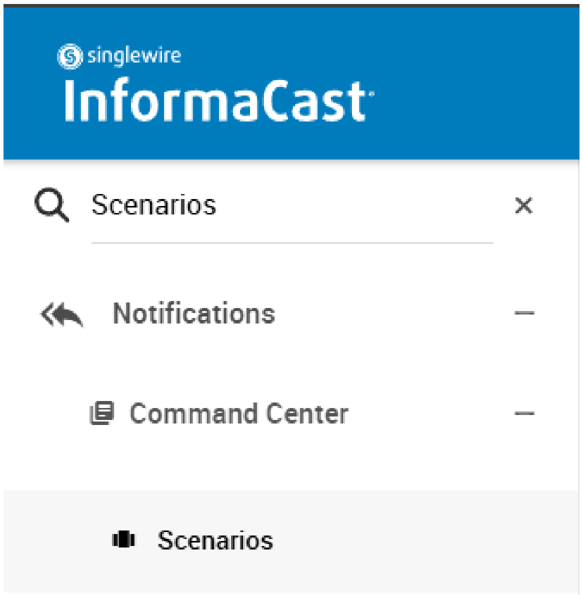
In this guide we will be creating two different scenarios, an ‘Alert’ scenario, and an ‘All Clear’ scenario:

- The ‘Alert’ scenario will activate the Newline Secure application on a group of devices and display the subject and description of a **Singlewire InformaCast Message Template**.
- The ‘Clear’ scenario will clear out any existing alerts that are being displayed on a group of devices, returning them to normal functionality.

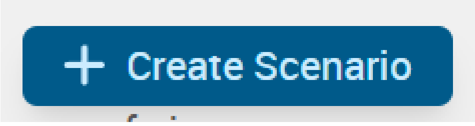
If you have existing scenarios in your console you are welcome to move forward to Step 6, otherwise please follow the below guide to create your **Alert** and **Clear** scenarios:

Creating an Alert scenario

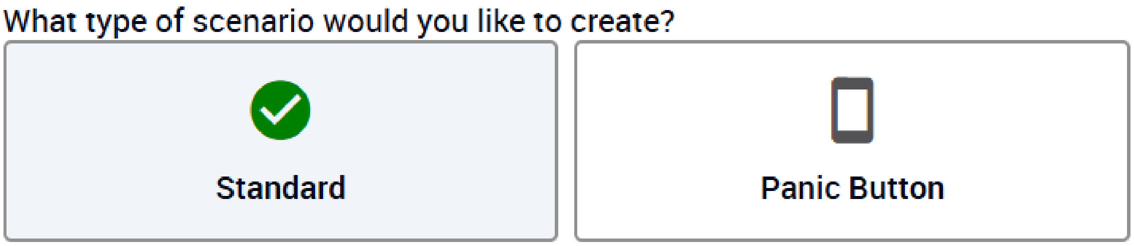
- Inside of your Singlewire InformaCast console, navigate to **'Notifications'** ⇒ **'Command Center'** ⇒ **'Scenarios'** on the side toolbar



- Click the **'Create Scenario'** button in the top right

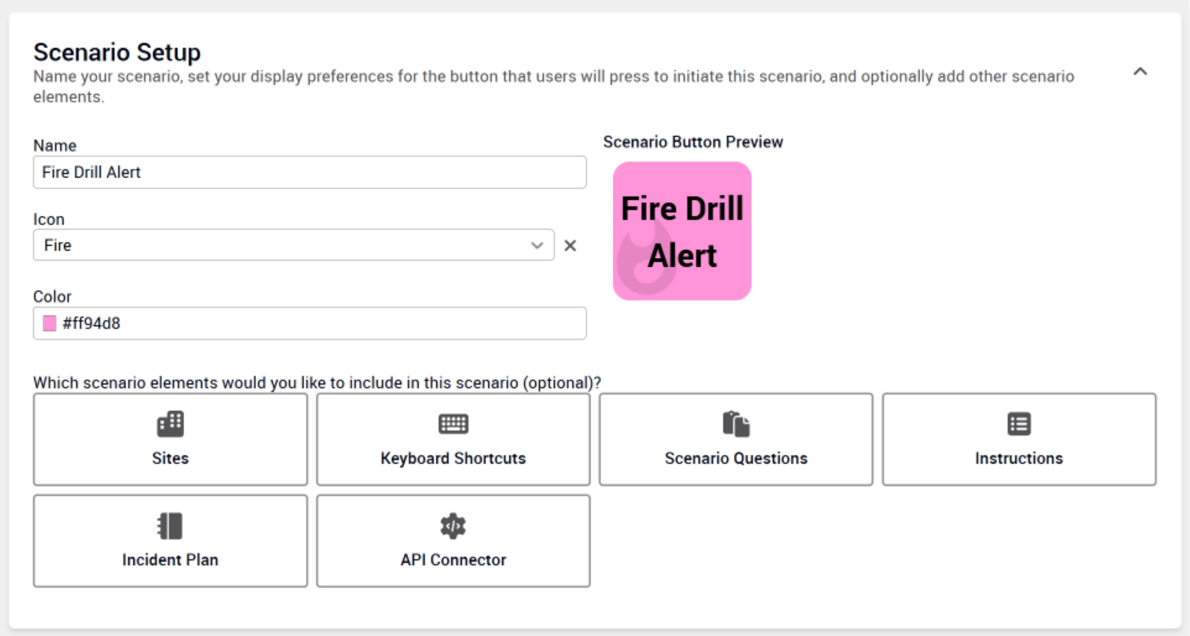


- Select your preferred **Scenario Type** and click **'Continue'**


What type of scenario would you like to create?

  - For this guide we will be using the **Standard** scenario type

- Enter the scenario name, and choose an icon / color for your alert button



Scenario Setup

Name your scenario, set your display preferences for the button that users will press to initiate this scenario, and optionally add other scenario elements.

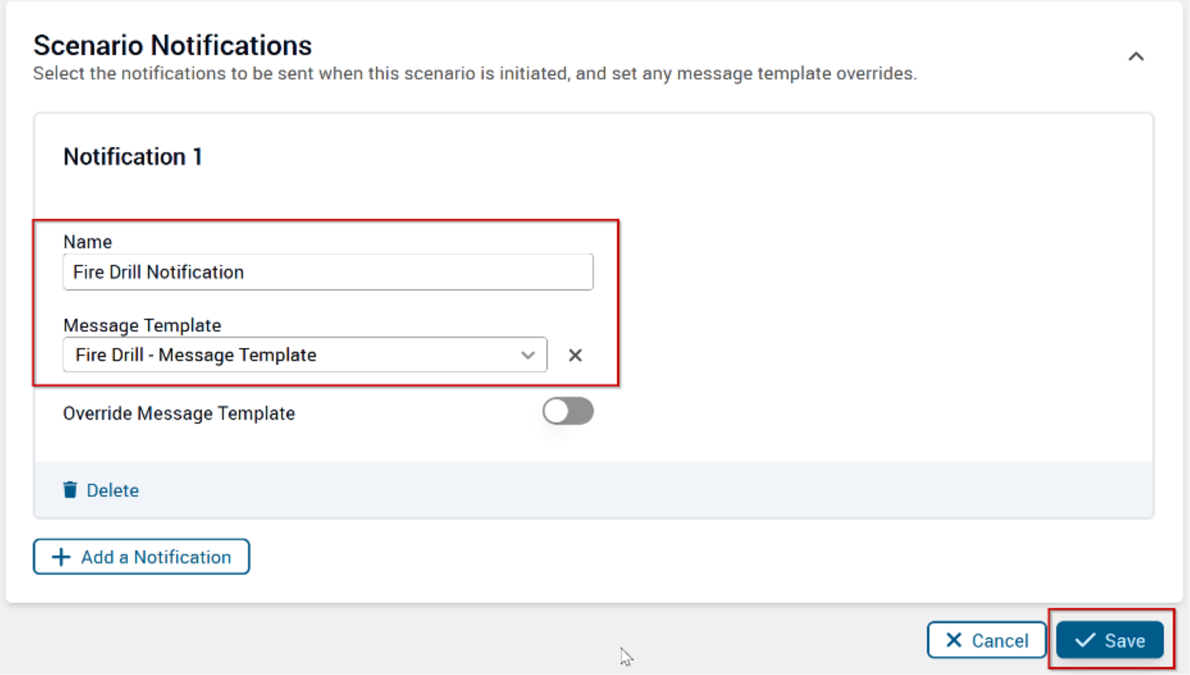
Name: Fire Drill Alert

Icon: Fire

Color: #ff94d8

Which scenario elements would you like to include in this scenario (optional)?

- Set a name for your scenario notification, then using **‘Message Template’** dropdown menu select the **Message Template** that was created earlier in this guide (Step 5).
  - After your scenario is customized, be sure to click the **‘Save’** button



Scenario Notifications

Select the notifications to be sent when this scenario is initiated, and set any message template overrides.

Notification 1

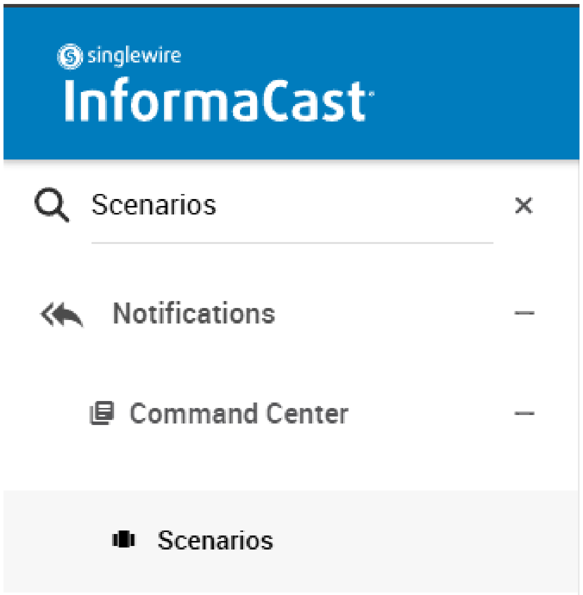
Name: Fire Drill Notification

Message Template: Fire Drill - Message Template

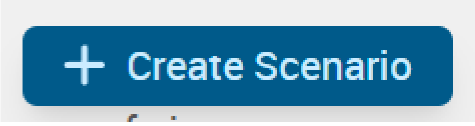
Override Message Template

Creating a Clear scenario

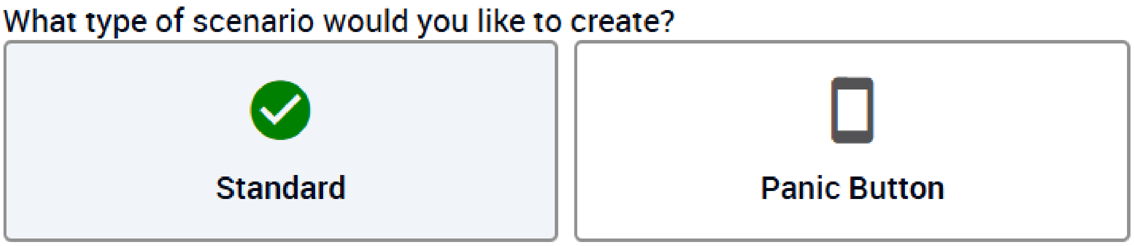
- Inside of your Singlewire InformaCast console, navigate to **'Notifications'** ⇒ **'Command Center'** ⇒ **'Scenarios'** on the side toolbar



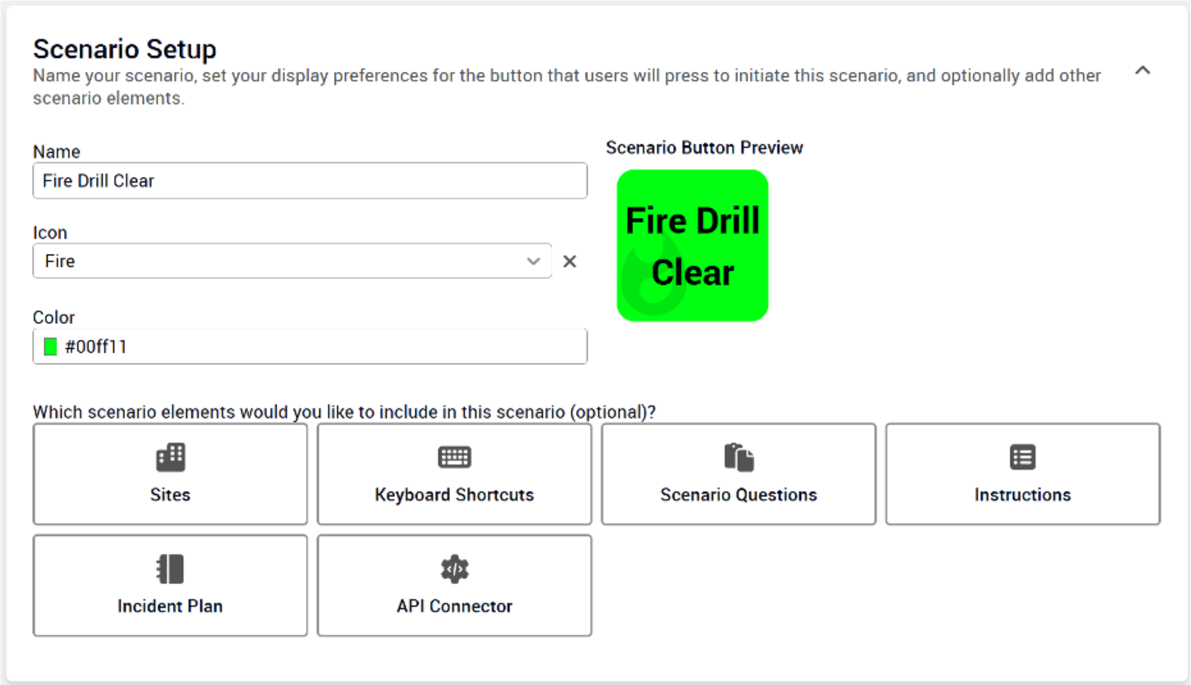
- Click the **'Create Scenario'** button in the top right



- Select your preferred **Scenario Type** and click **'Continue'**


What type of scenario would you like to create?

  - For this guide we will be using the **Standard** scenario type
- Enter the scenario name, and choose an icon / color for your alert button



Scenario Setup

Name your scenario, set your display preferences for the button that users will press to initiate this scenario, and optionally add other scenario elements.

Name: Fire Drill Clear

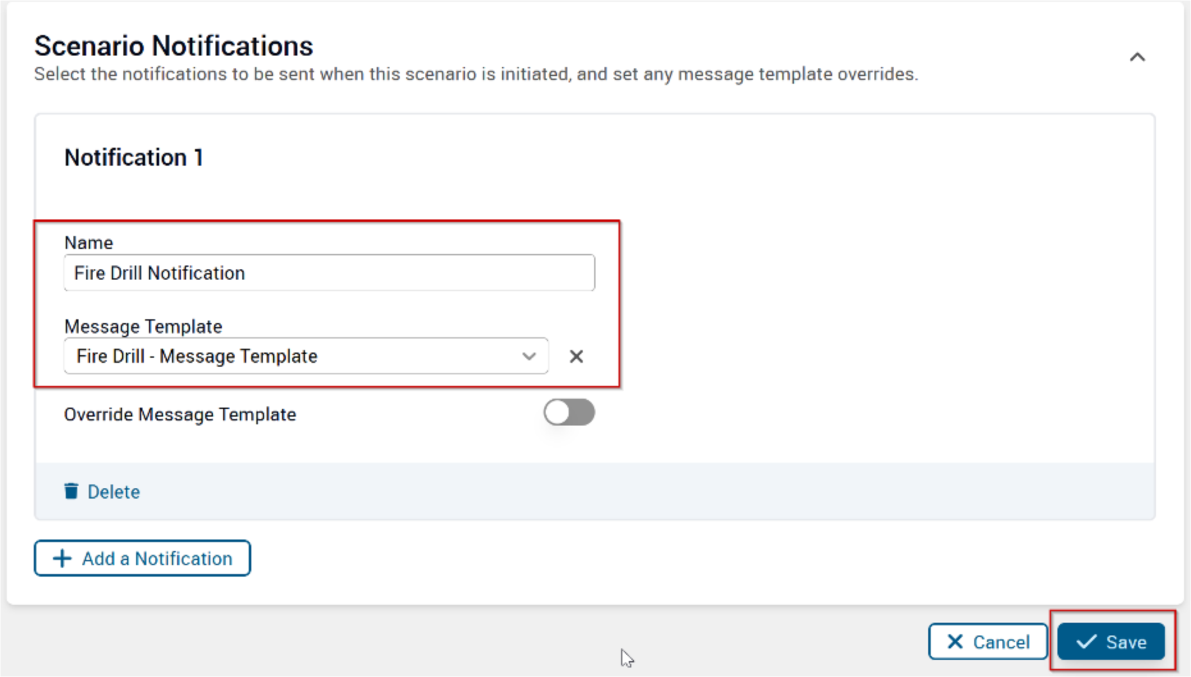
Icon: Fire

Color: 🟩 #00ff11

Scenario Button Preview

Which scenario elements would you like to include in this scenario (optional)?

- Set a name for your scenario notification, then using **'Message Template'** dropdown menu select the **Message Template** that was created earlier in this guide (Step 5).
    - After your scenario is customized, be sure to click the **'Save'** button



Scenario Notifications

Select the notifications to be sent when this scenario is initiated, and set any message template overrides.

Notification 1

Name: Fire Drill Notification

Message Template: Fire Drill - Message Template

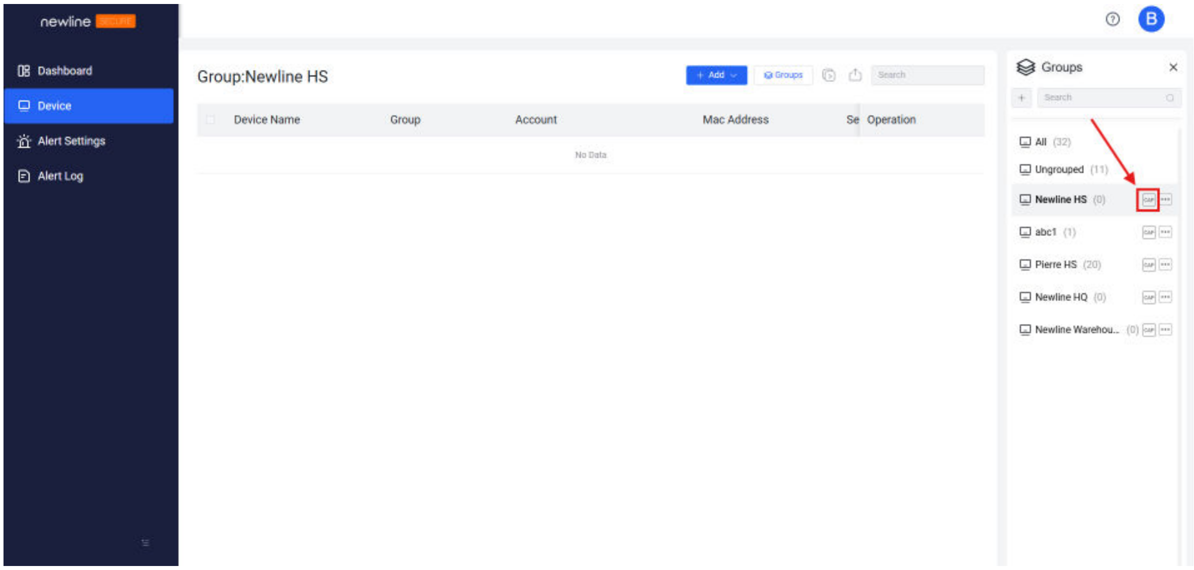
Override Message Template

Step 6: Add the Newline Secure API Connectors to each scenario

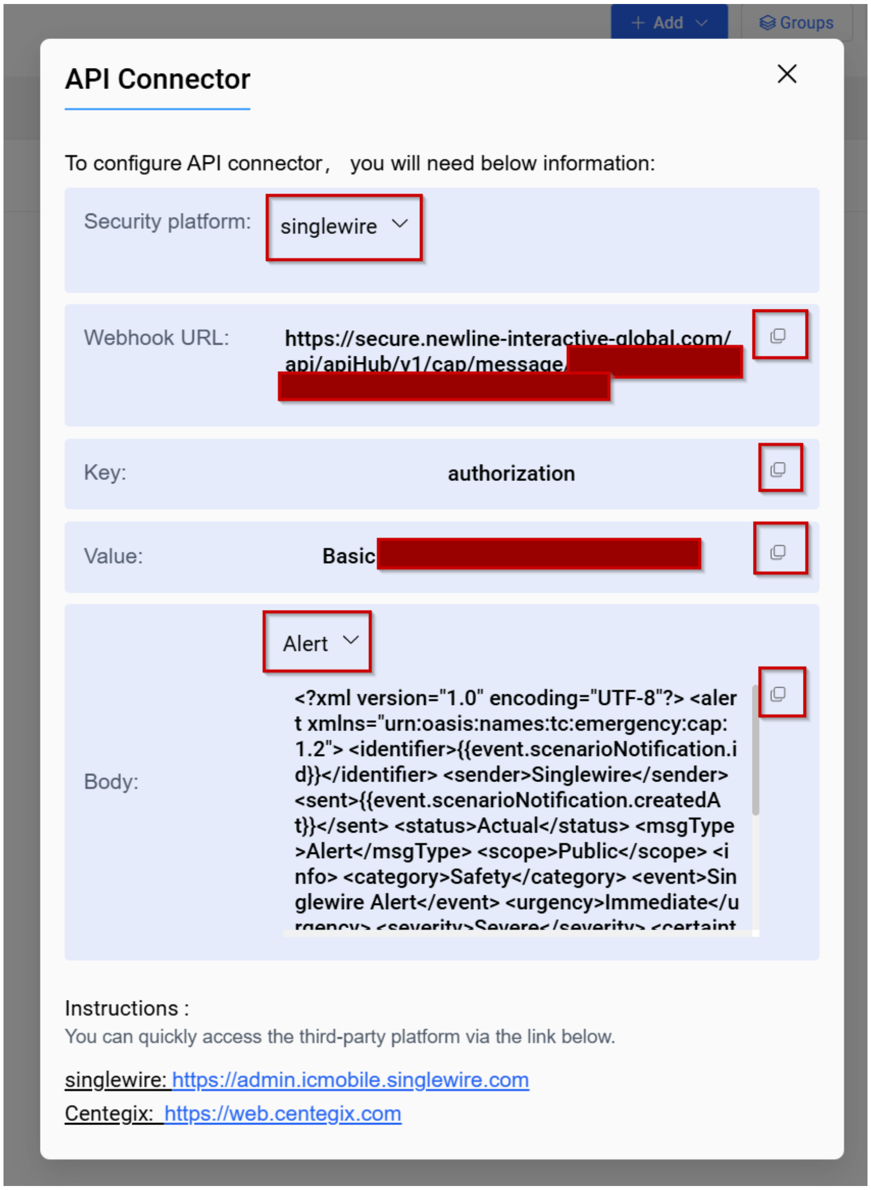
Generate CAP 'Alert' Information from Newline Secure

To create a **Singlewire API Connector** to attach to a **Singlewire Scenario**, we first need to generate the Common Alerting Protocol (CAP) endpoint information for each Newline Secure group:

- Click the 'CAP' button in the device group list to generate CAP integration information



- Now you should see a window appear that contains the API endpoint information for your Newline Secure group. Keep this window open as we will need to copy this information over to the Singlewire InformaCast console.



API Connector

To configure API connector， you will need below information:

Security platform: singlewire

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Key: authorization

Value: Basic [redacted]

Body: Alert

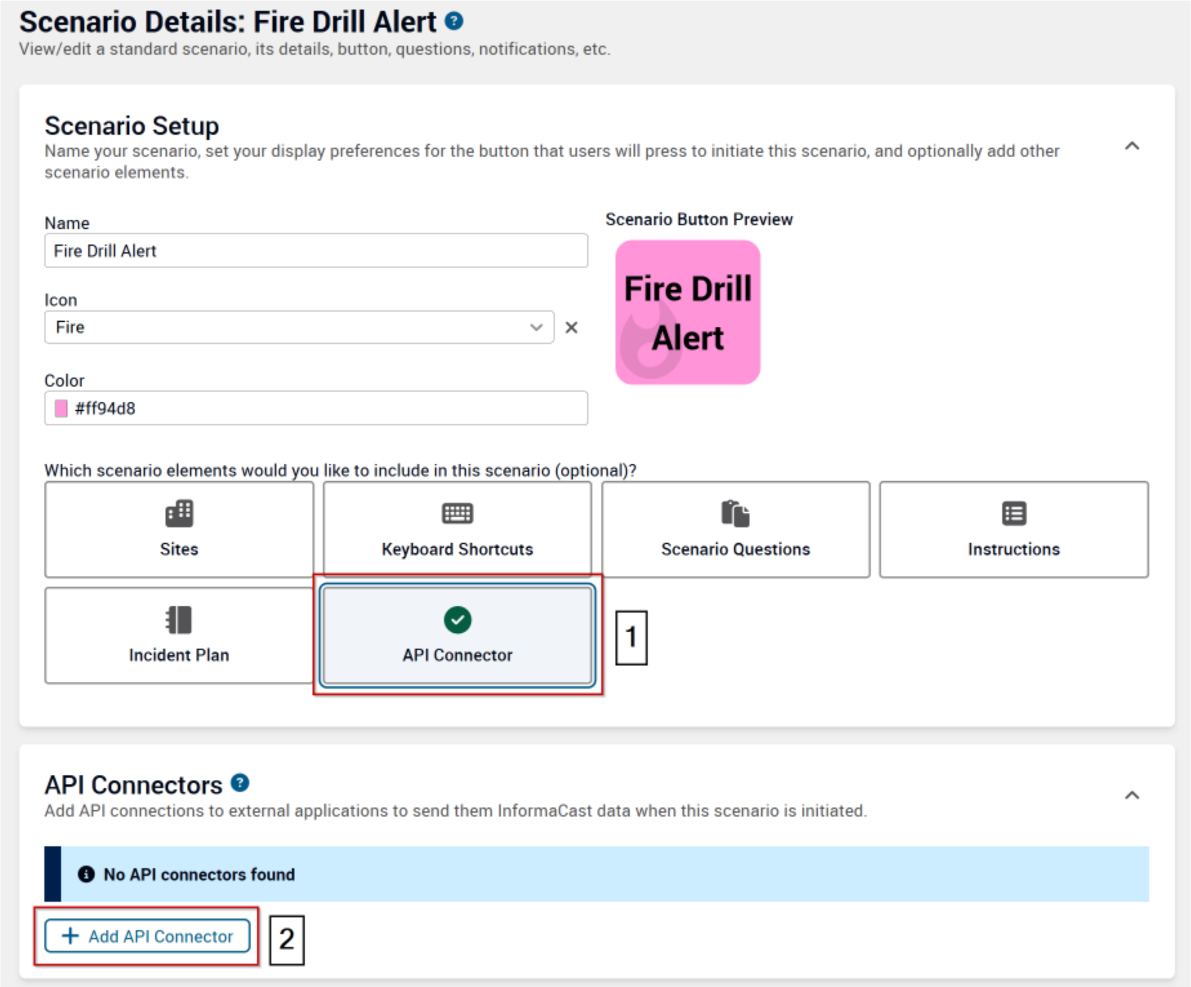
```
<?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier>{{event.scenarioNotification.id}}</identifier> <sender>Singlewire</sender> <sent>{{event.scenarioNotification.createdAt}}</sent> <status>Actual</status> <msgType>Alert</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Singlewire Alert</event> <urgency>Immediate</urgency> <severity>Severe</severity> <certaint
```

Instructions :
You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com
Centegix: https://web.centegix.com

- ◦ Ensure that **'Security Platform'** is set to **Singlewire**
- ◦ Ensure that **'Body'** is set to **Alert**

- In the Singlewire InformaCast console, navigate back to **Scenarios** and re-open the **'Alert'** scenario that was created in **Step 6**



Scenario Details: Fire Drill Alert

View/edit a standard scenario, its details, button, questions, notifications, etc.

Scenario Setup

Name your scenario, set your display preferences for the button that users will press to initiate this scenario, and optionally add other scenario elements.

Name: Fire Drill Alert

Icon: Fire

Color: #ff94d8

Scenario Button Preview: Fire Drill Alert

Which scenario elements would you like to include in this scenario (optional)?

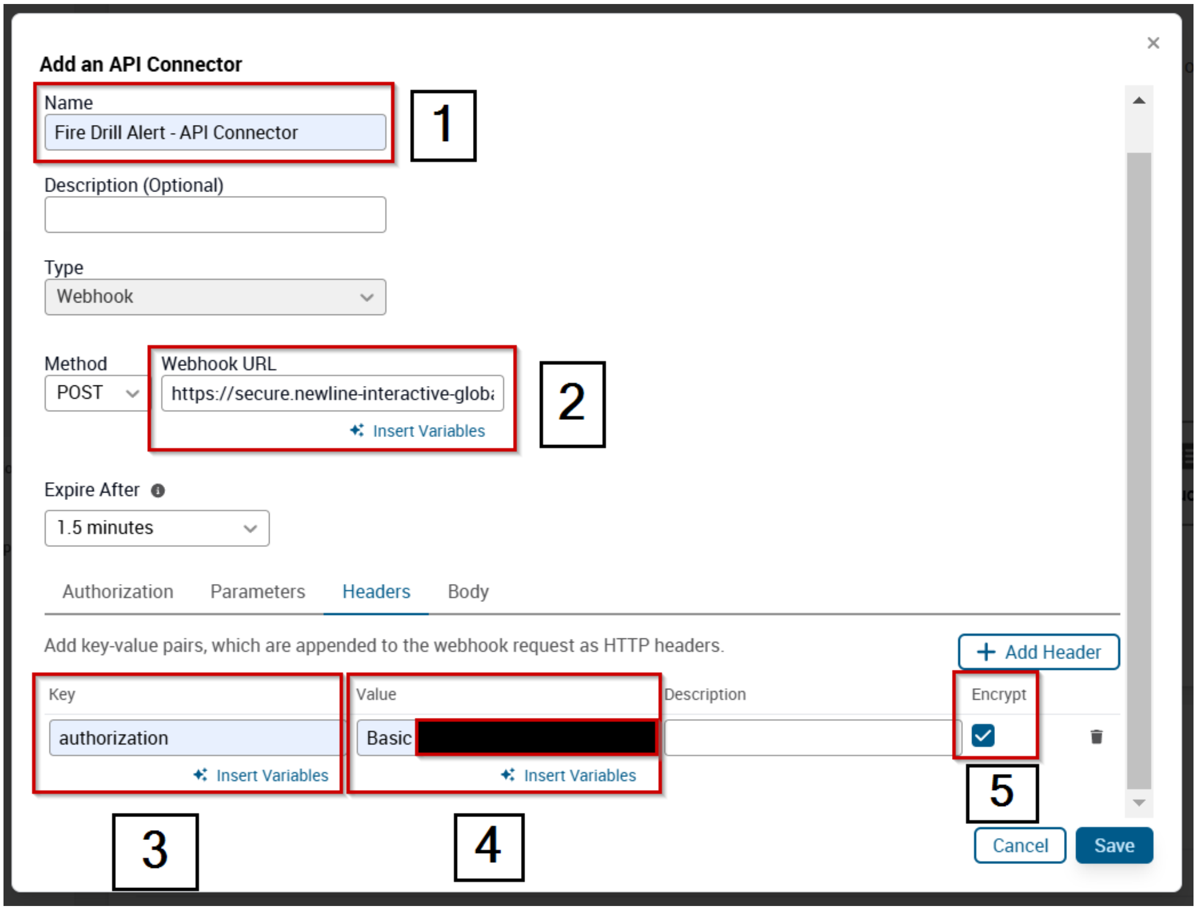
API Connectors

Add API connections to external applications to send them InformaCast data when this scenario is initiated.

No API connectors found

- Click on **API Connector**
- Click on **Add API Connector**

- A new window should appear titled **'Add an API Connector'**, use the **CAP Alert** information we have just gathered from **Newline Secure** to create this connector and navigate to the **Headers** tab:



Add an API Connector

Name: Fire Drill Alert - API Connector

Description (Optional):

Type: Webhook

Method: POST

Webhook URL: https://secure.newline-interactive-globa

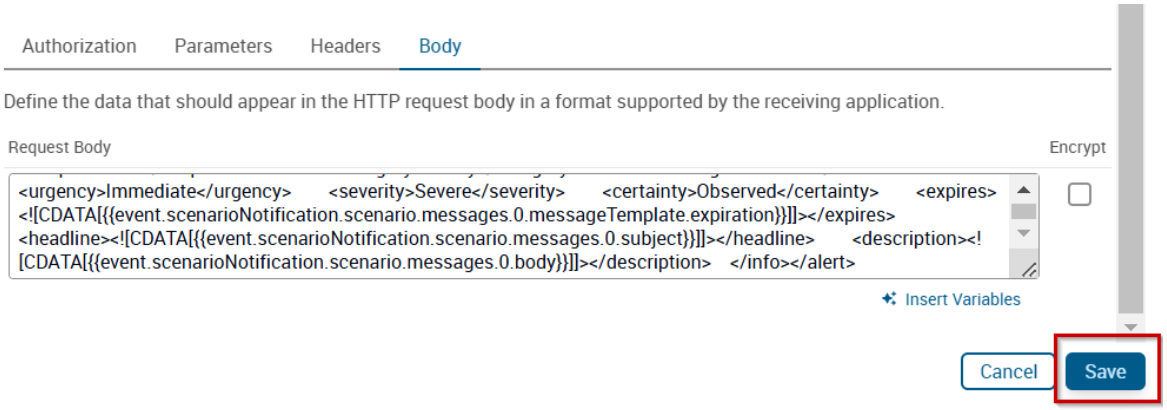
Expire After: 1.5 minutes

Add key-value pairs, which are appended to the webhook request as HTTP headers.

Key	Value	Description	Encrypt
authorization	Basic [redacted]		☑

- 1 - Create a name for your API connector
- 2 - Copy over the **Webhook URL** from your Newline Secure Group's CAP information window
- 3 - Copy over the **Key** from your Newline Secure Group's CAP information window
- 4 - Copy over the **Value** from your Newline Secure Group's CAP information window
- 5 - Ensure you **check the Encrypt box**.

- Then, click on the **'Body'** tab and copy over the **Body** from your Newline Secure Group's CAP information window and click **Save**



Define the data that should appear in the HTTP request body in a format supported by the receiving application.

Request Body

```
<urgency>Immediate</urgency>      <severity>Severe</severity>      <certainty>Observed</certainty>      <expires>
<![CDATA[{{event.scenarioNotification.scenario.messages.0.messageTemplate.expiration}}]]></expires>
<headline><![CDATA[{{event.scenarioNotification.scenario.messages.0.subject}}]]></headline>      <description><!
[CDATA[{{event.scenarioNotification.scenario.messages.0.body}}]]></description>    </info></alert>
```

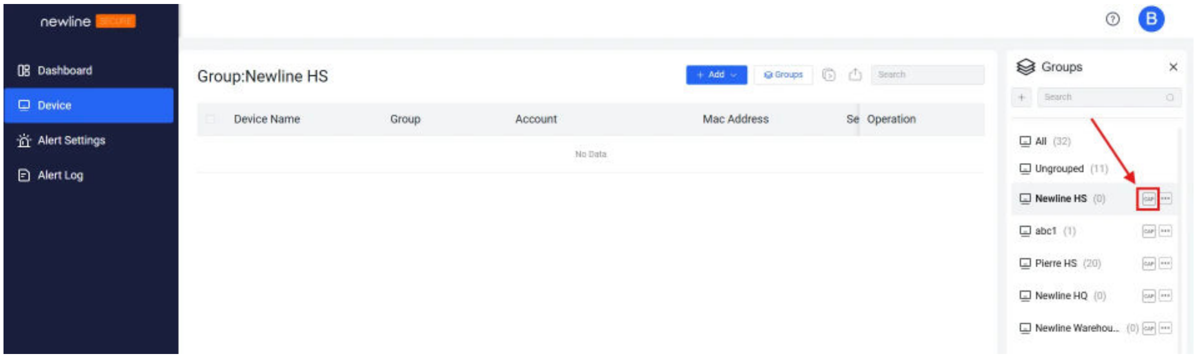
Encrypt □

- This will navigate you back to the **Scenario Edit Screen** where you can now see that the API connector has been added. **ENSURE THAT YOU CLICK SAVE ONCE MORE TO FINISH ADDING YOUR API CONNECTOR TO THE SCENARIO.**

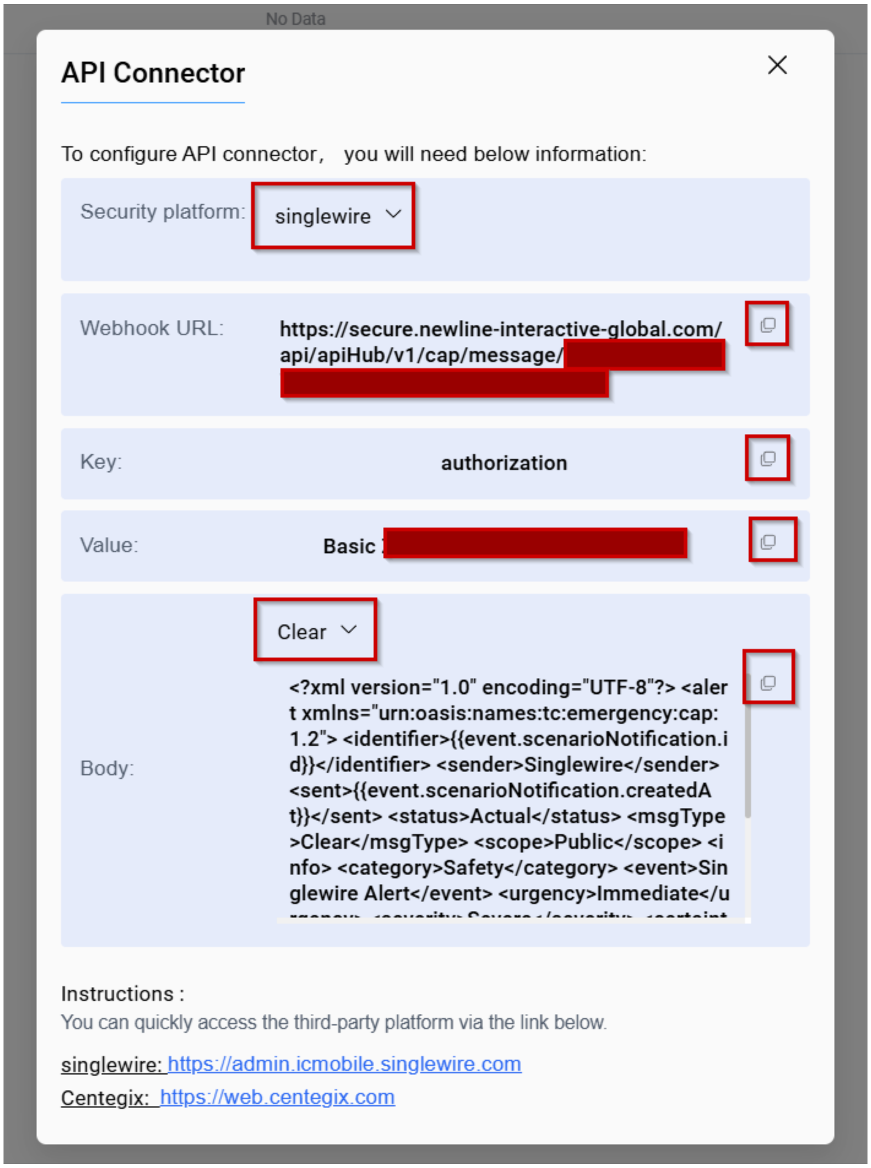
Generate CAP 'Clear' Information from Newline Secure

To create a **Singlewire API Connector** to attach to a **Singlewire Scenario**, we first need to generate the Common Alerting Protocol (CAP) endpoint information for each Newline Secure group:

- Click the 'CAP' button in the device group list to generate CAP integration information



- Now you should see a window appear that contains the API endpoint information for your Newline Secure group. Keep this window open as we will need to copy this information over to the Singlewire InformaCast console.



No Data

API Connector

To configure API connector， you will need below information:

Security platform: singlewire

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Key: authorization

Value: Basic [redacted]

Body: Clear

```
<?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier>{{event.scenarioNotification.id}}</identifier> <sender>Singlewire</sender> <sent>{{event.scenarioNotification.createdAt}}</sent> <status>Actual</status> <msgType>Clear</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Singlewire Alert</event> <urgency>Immediate</u
```

Instructions :

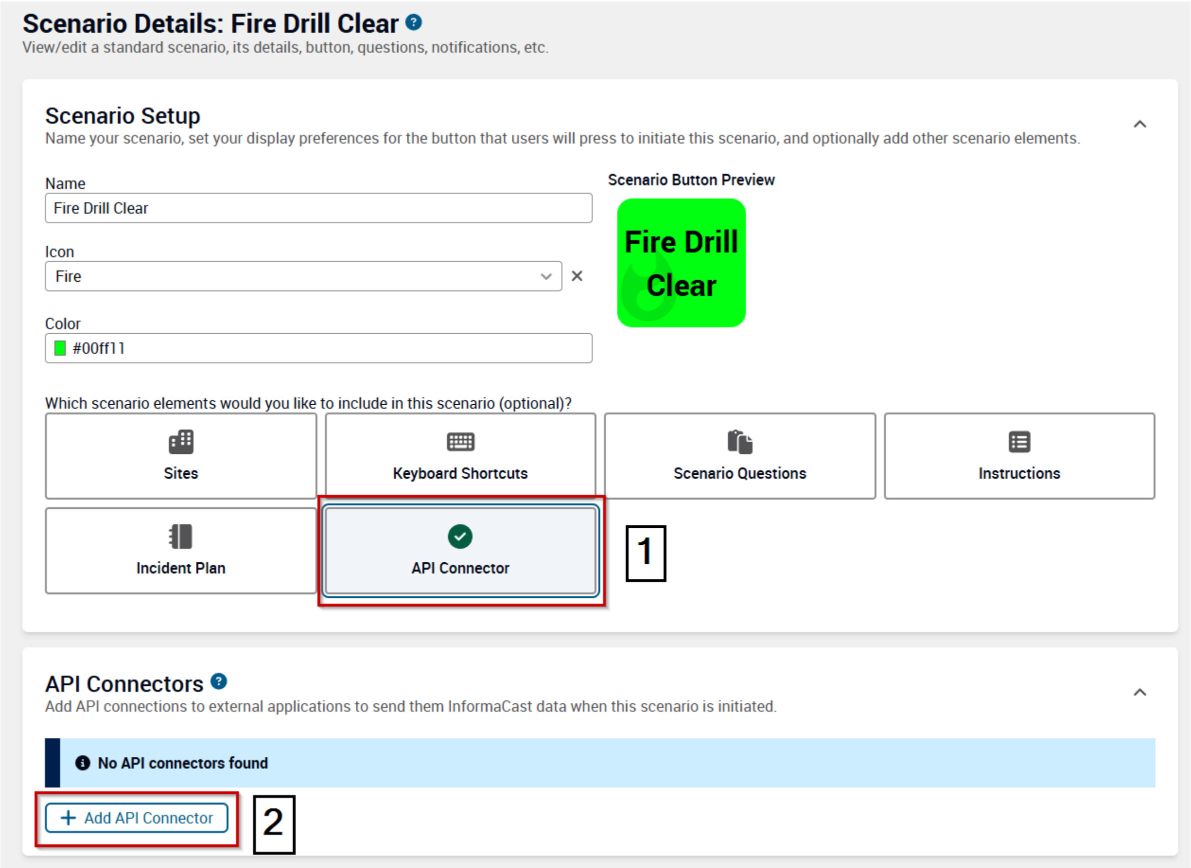
You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com

Centegix: https://web.centegix.com

- Ensure that **‘Security Platform’** is set to **Singlewire**
- Ensure that **‘Body’** is set to **Clear**

- In the Singlewire InformaCast console, navigate back to **Scenarios** and re-open the **‘Alert’** scenario that was created in **Step 6**



Scenario Details: Fire Drill Clear

View/edit a standard scenario, its details, button, questions, notifications, etc.

Scenario Setup

Name your scenario, set your display preferences for the button that users will press to initiate this scenario, and optionally add other scenario elements.

Name: Fire Drill Clear

Icon: Fire

Color: 🟩 #00ff11

Scenario Button Preview

Which scenario elements would you like to include in this scenario (optional)?

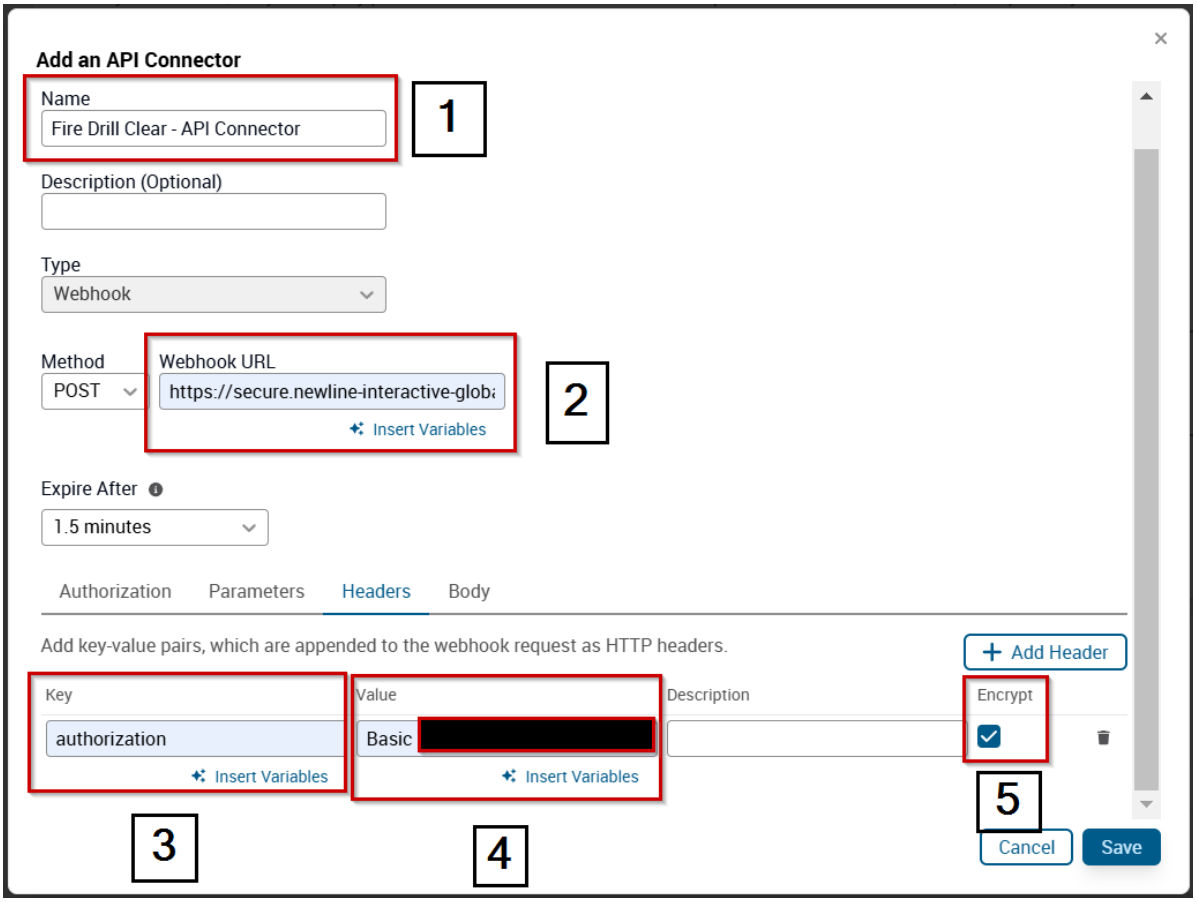
API Connectors

Add API connections to external applications to send them InformaCast data when this scenario is initiated.

No API connectors found

- Click on **API Connector**
- Click on **Add API Connector**

- A new window should appear titled **'Add an API Connector'**, use the **CAP Alert** information we have just gathered from **Newline Secure** to create this connector and navigate to the **Headers** tab:



Add an API Connector

Name: Fire Drill Clear - API Connector

Description (Optional):

Type: Webhook

Method: POST

Webhook URL: https://secure.newline-interactive-glob…

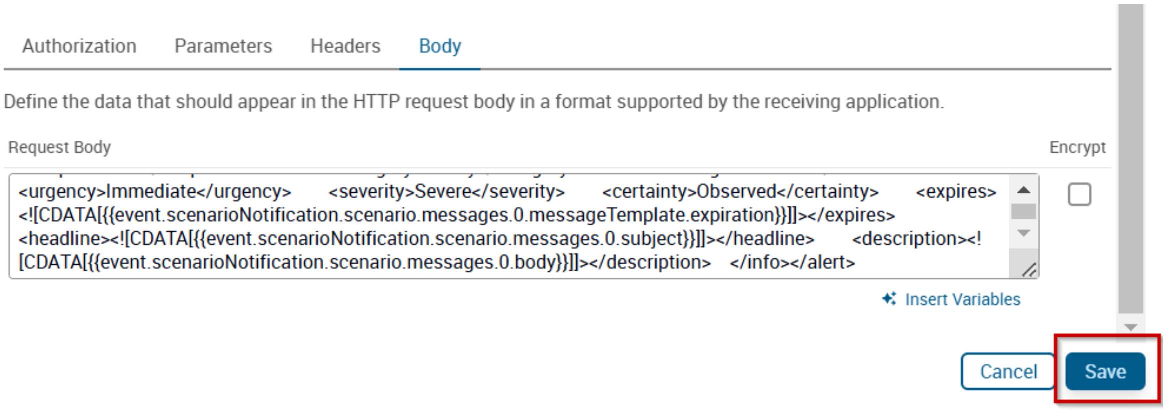
Expire After: 1.5 minutes

Add key-value pairs, which are appended to the webhook request as HTTP headers.

Key	Value	Description	Encrypt
authorization	Basic [redacted]		☑

- 1 - Create a name for your API connector
- 2 - Copy over the **Webhook URL** from your Newline Secure Group’s CAP information window
- 3 - Copy over the **Key** from your Newline Secure Group’s CAP information window
- 4 - Copy over the **Value** from your Newline Secure Group’s CAP information window
- 5 - Ensure you **check the Encrypt box**.

- Then, click on the **‘Body’** tab and copy over the **Body** from your Newline Secure Group’s CAP information window and click **Save**



Define the data that should appear in the HTTP request body in a format supported by the receiving application.

Request Body

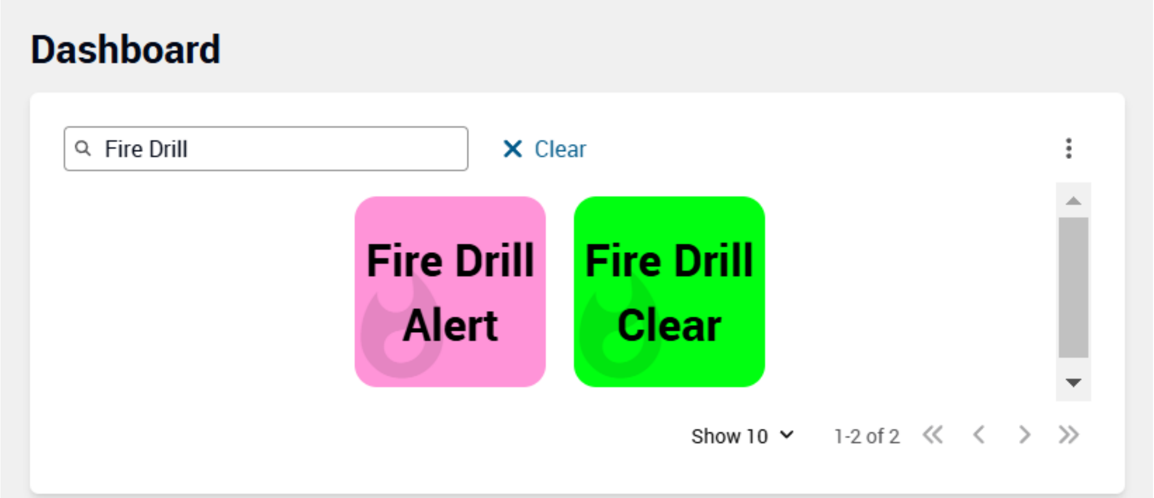
```
<urgency>Immediate</urgency>      <severity>Severe</severity>      <certainty>Observed</certainty>      <expires>
<![CDATA[{{event.scenarioNotification.scenario.messages.0.messageTemplate.expiration}}]]></expires>
<headline><![CDATA[{{event.scenarioNotification.scenario.messages.0.subject}}]]></headline>      <description><!
[CDATA[{{event.scenarioNotification.scenario.messages.0.body}}]]></description>    </info></alert>
```

Encrypt □

- This will navigate you back to the **Scenario Edit Screen** where you can now see that the API connector has been added. **ENSURE THAT YOU CLICK SAVE ONCE MORE TO FINISH ADDING YOUR API CONNECTOR TO THE SCENARIO**.

Congratulations!

You've successfully created Alert and Clear scenarios. These are now available on your InformaCast console and ready to integrate into existing workflows.



If you have questions or need assistance with the Newline Secure portal, please contact Newline Technical Support:

- Submit a ticket here!
- Give us a call at +1 (833)-469-9520

If you have questions or need assistance with the Singlewire Portal, please contact Singlewire Support by submitting a ticket using the link below:

- https://support.singlewire.com/s/contactsupport

Centegix Integration Guide

Integrating Newline Secure with Centegix CrisisAlert

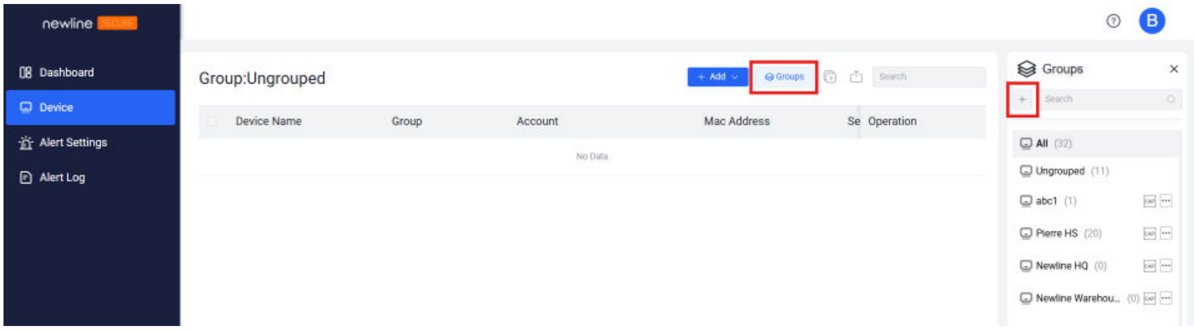
This guide will walk you through integrating Newline Secure with Centegix CrisisAlert using the Centegix IP Integrations feature.

Before proceeding with this guide, please ensure that you have followed the Portal Sign-Up Guide **in order to create your account!**

Note: Only Newline Q Pro Series Panels are currently supported. For best performance and stability, please ensure that your Q Pro is on firmware v1.0.75 or higher.

Step 1: Create a Device Group

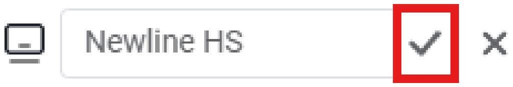
- On the ‘Device’ tab, look for the ‘Groups’ sidebar and click the ‘+’ icon



Group:Ungrouped

Device Name	Group	Account	Mac Address	Se	Operation
No Data					

  - If you do not see the ‘Groups’ sidebar, then you can click the ‘Groups’ button to open it.
- Type in a name for your group in the text box that appears, and click the ‘✓’ icon



Step 2: Register Your Devices

Note: Only Newline Q Pro Series Panels are currently supported. For best performance and stability, please ensure that your Q Pro is on firmware v1.0.75 or higher.

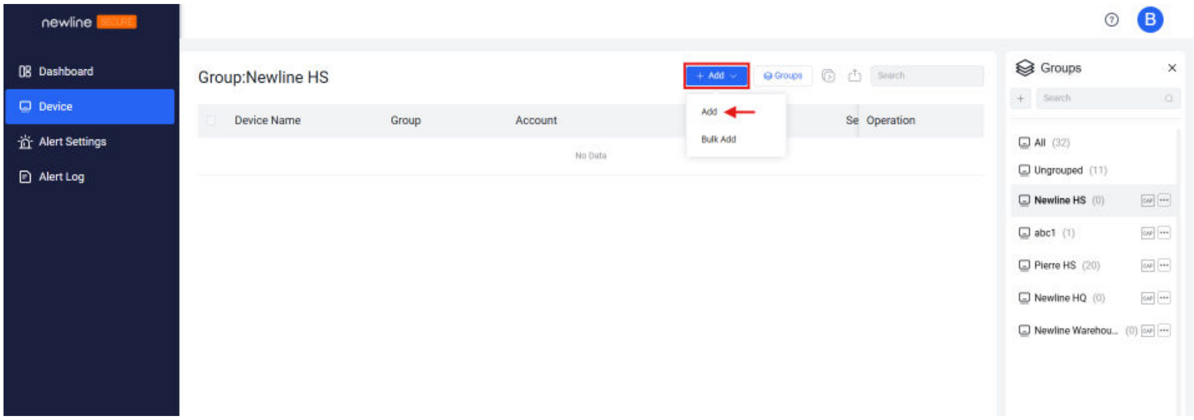
There are three methods for registering your devices to a Newline Secure Device Group:

- Single Device Registration via the Web Console
- Bulk Device Registration via the Web Console
- Registration via the Newline Secure Android Application on the Display

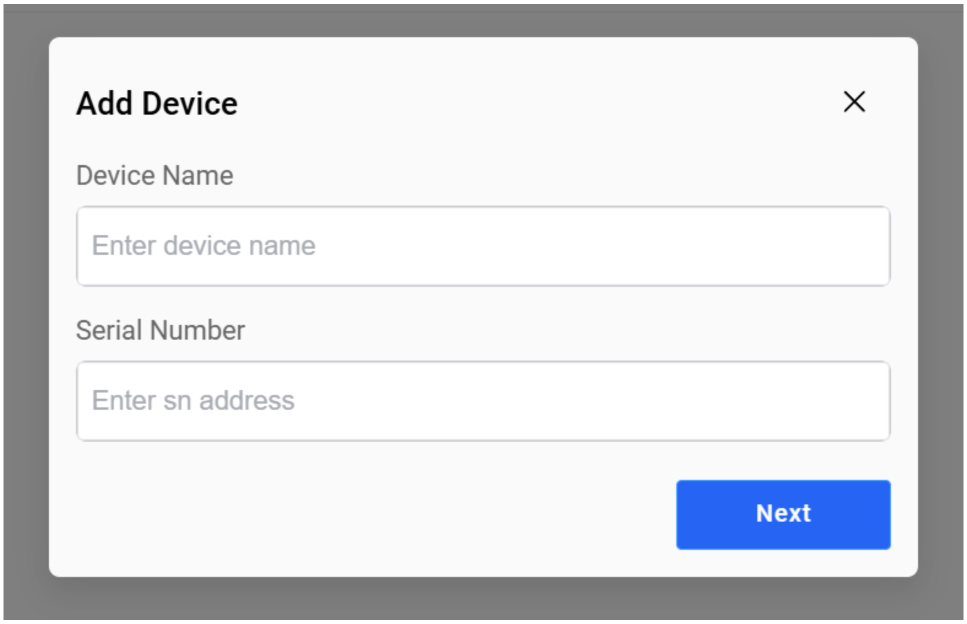
2.1 Register Your Device on the Newline Secure Web Console

2.1.1 Single Device Registration (Method 1)

- On the 'Device' tab, navigate to and click the blue 'Add' button, then select 'Add'



- Input the device's serial number and set a name for the device, then click 'Next'



Add Device

Device Name

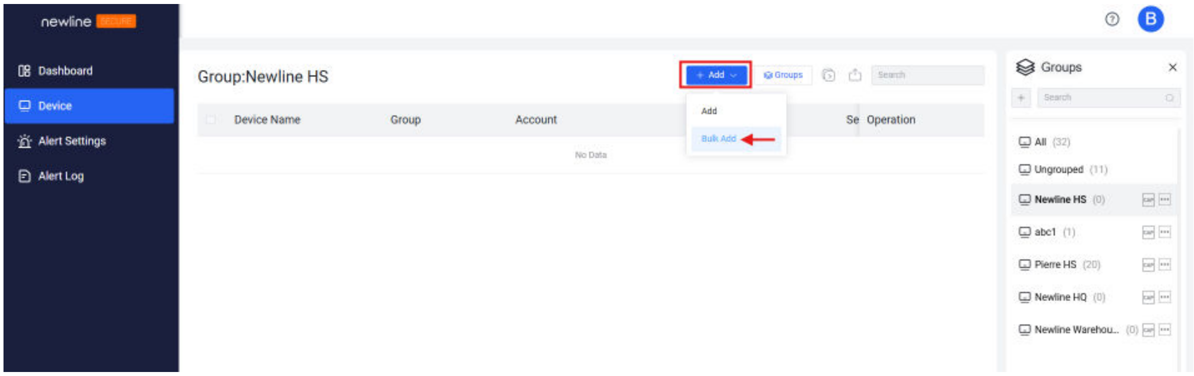
Enter device name

Serial Number

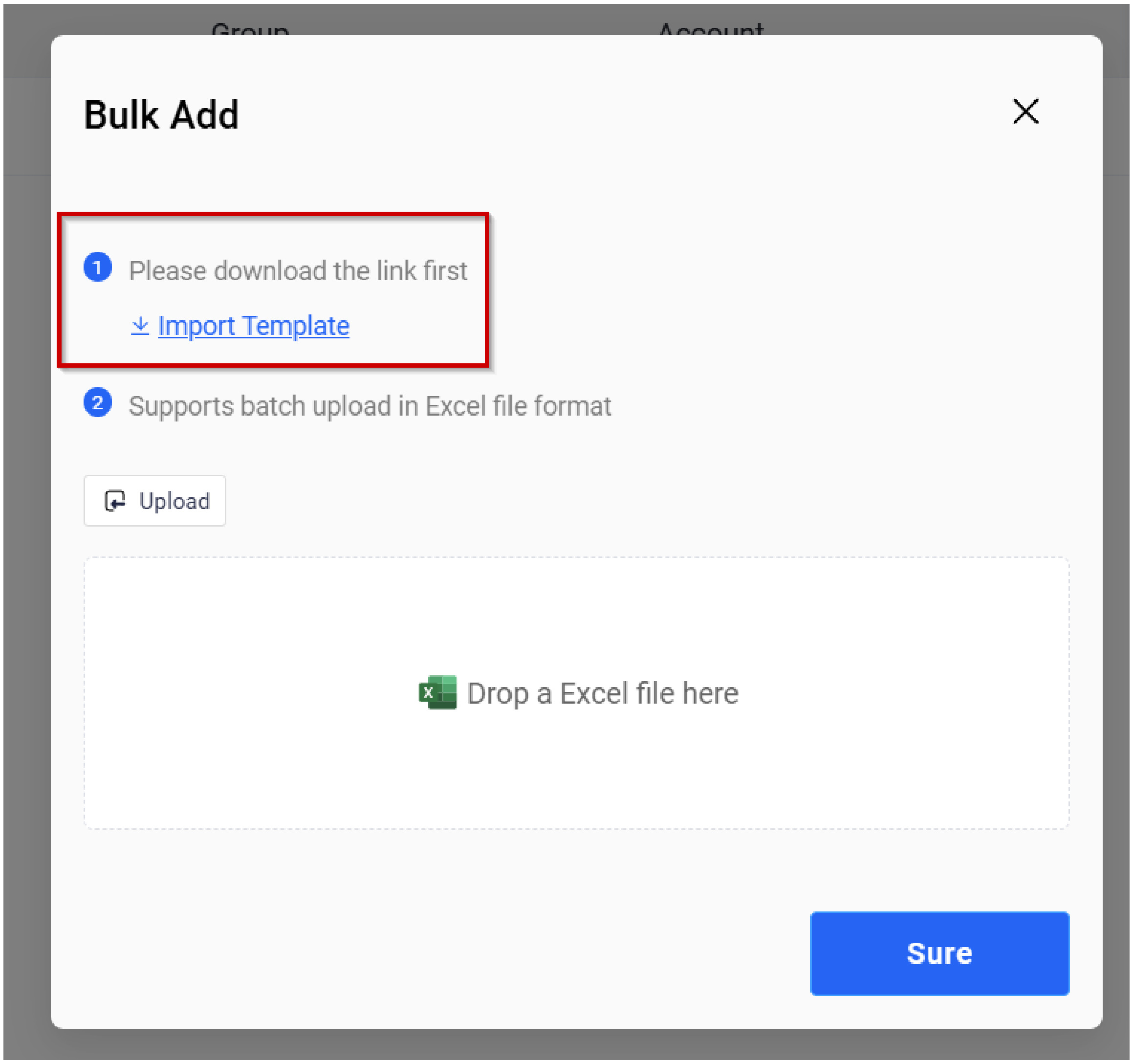
Enter sn address

2.1.2 Bulk Device Registration (Method 2)

- On the ‘Device’ tab, navigate to and click the blue ‘Add’ button, then select ‘Bulk Add’



- Download the import template using the provided link

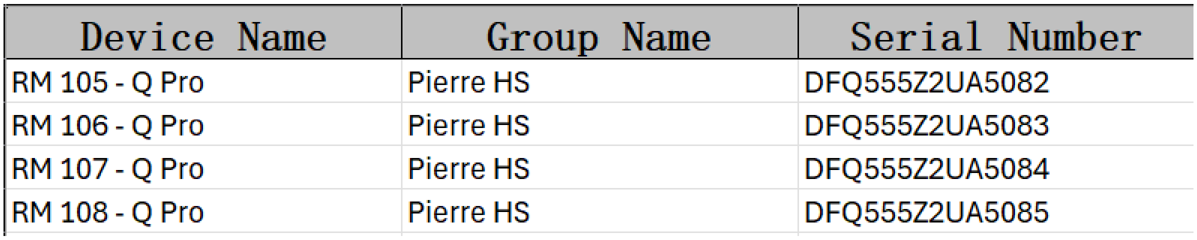


1 Please download the link first

2 Supports batch upload in Excel file format

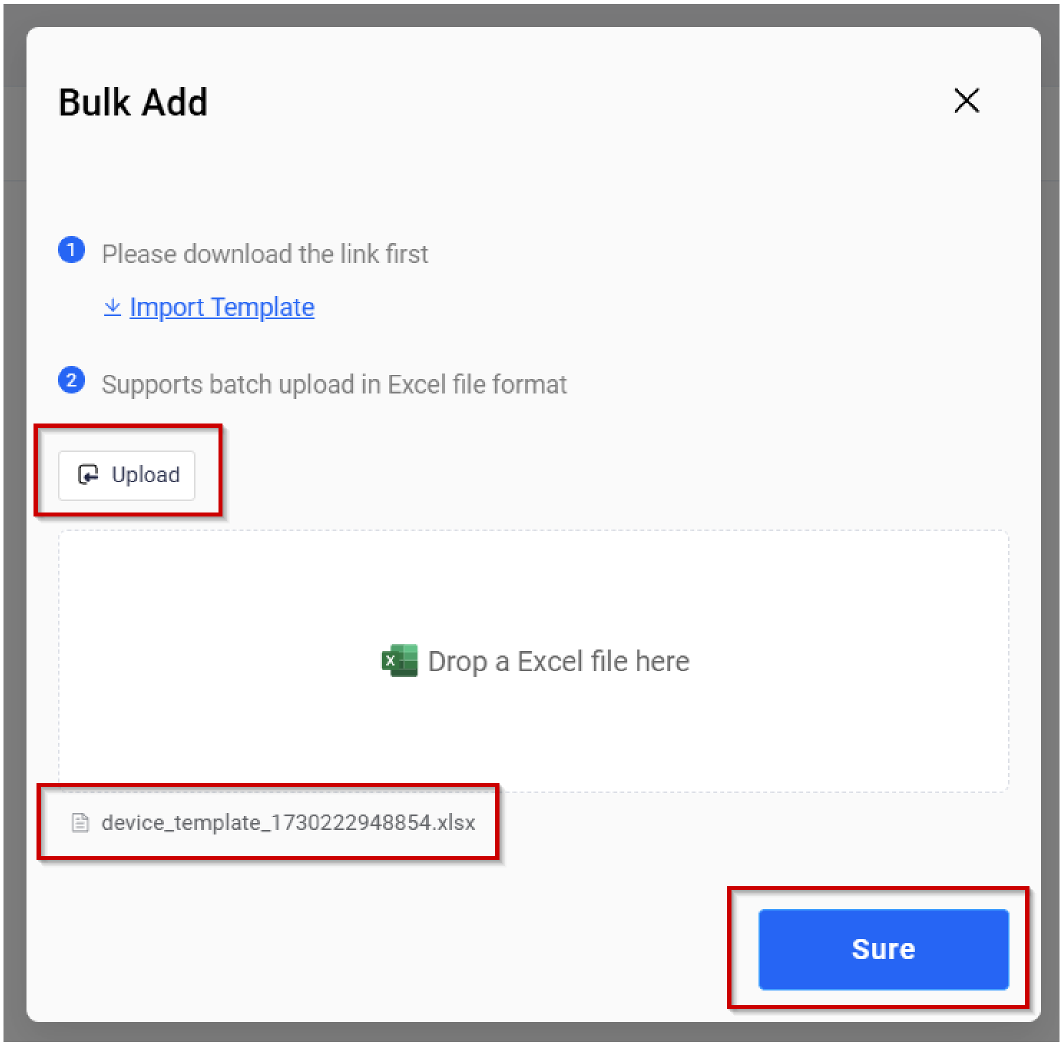
Drop a Excel file here

- Enter your devices into the Excel table and save the import template to your computer (.xlsx format)



Device Name	Group Name	Serial Number
RM 105 - Q Pro	Pierre HS	DFQ555Z2UA5082
RM 106 - Q Pro	Pierre HS	DFQ555Z2UA5083
RM 107 - Q Pro	Pierre HS	DFQ555Z2UA5084
RM 108 - Q Pro	Pierre HS	DFQ555Z2UA5085

- Select ‘Upload’ or drag and drop the Excel file into the designated area, then click the confirmation button to complete bulk-registration



Bulk Add

1 Please download the link first

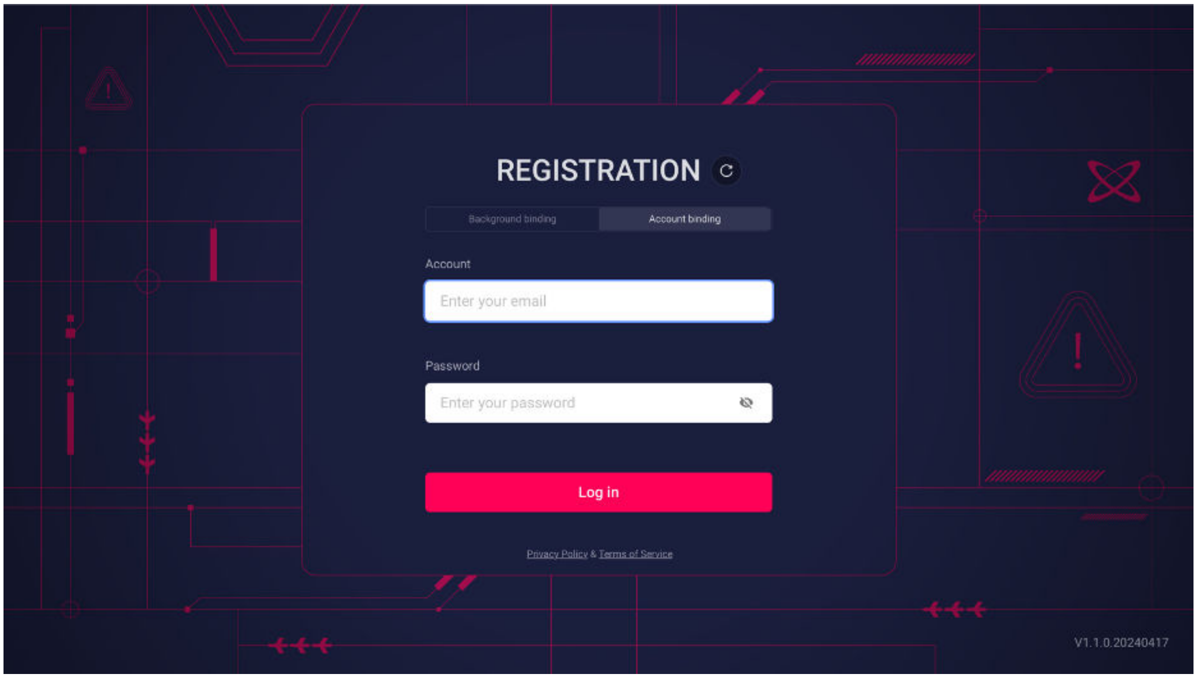
Import Template

2 Supports batch upload in Excel file format

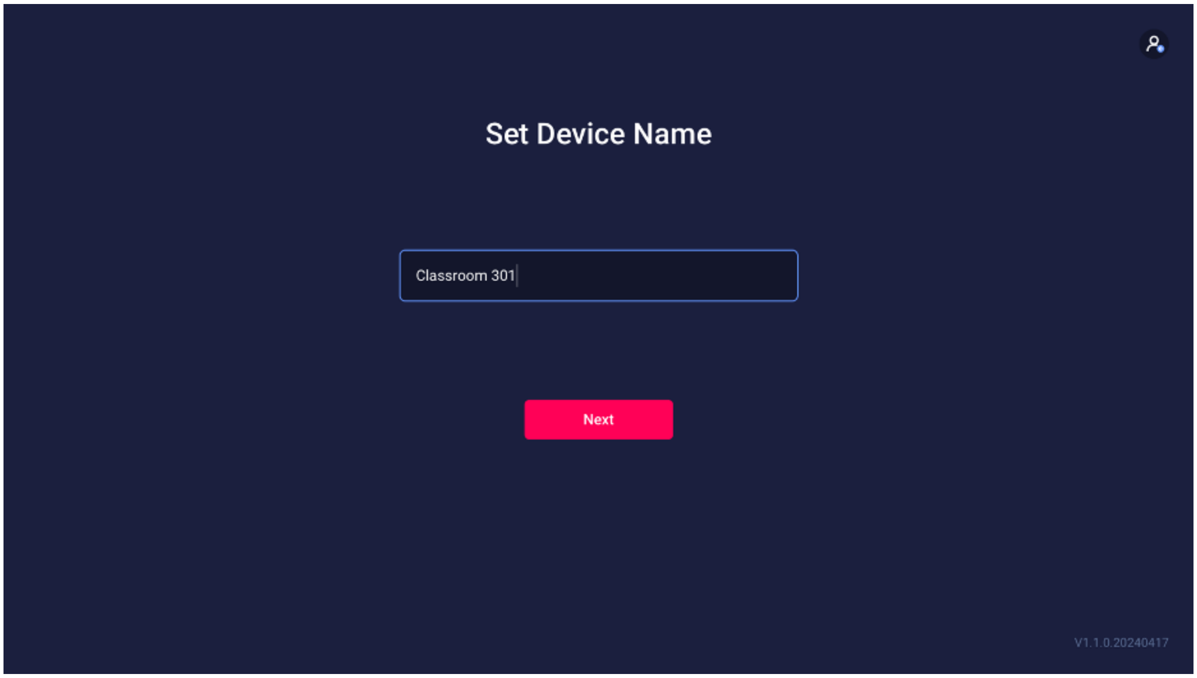
device_template_1730222948854.xlsx

2.2 Registration via the Newline Secure Android Application (Method 3)

- Open the ‘Newline Secure’ application on your display
- Tap ‘Account Binding’
- Login with your Newline Secure account information



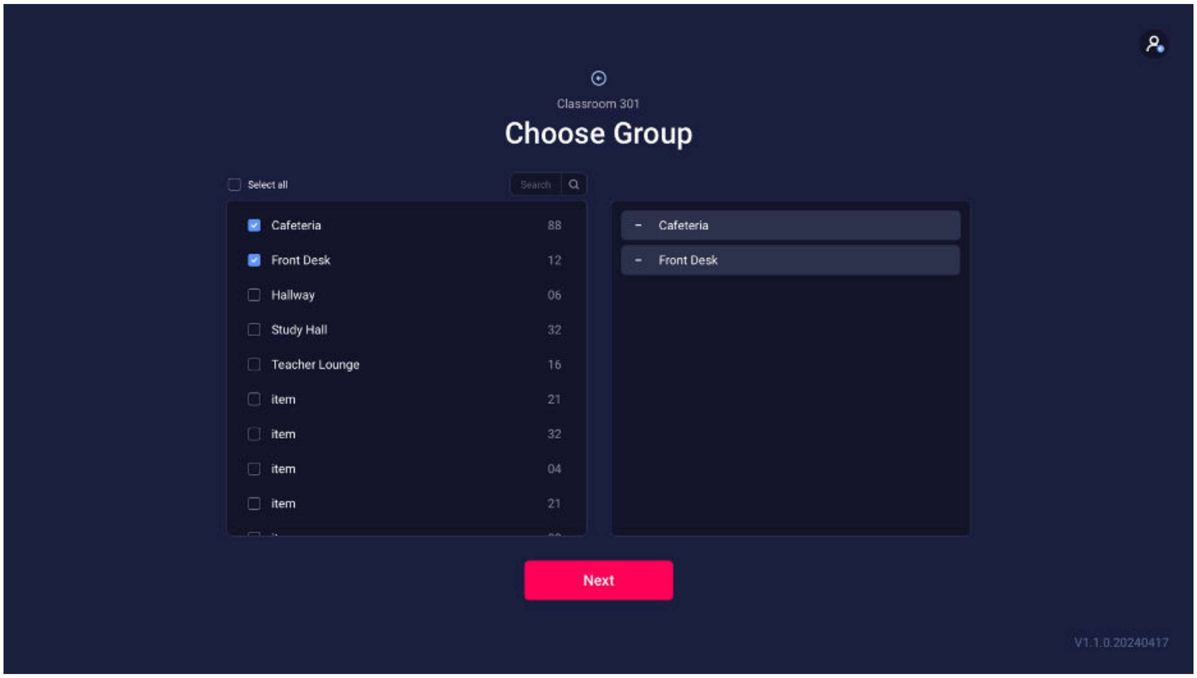
- Enter a device name for this display



Set Device Name

Classroom 301

- Select at least one group for this display to be registered to



Classroom 301

Choose Group

□ Select all   Search

☑	Cafeteria	88
☑	Front Desk	12
□	Hallway	06
□	Study Hall	32
□	Teacher Lounge	16
□	item	21
□	item	32
□	item	04
□	item	21

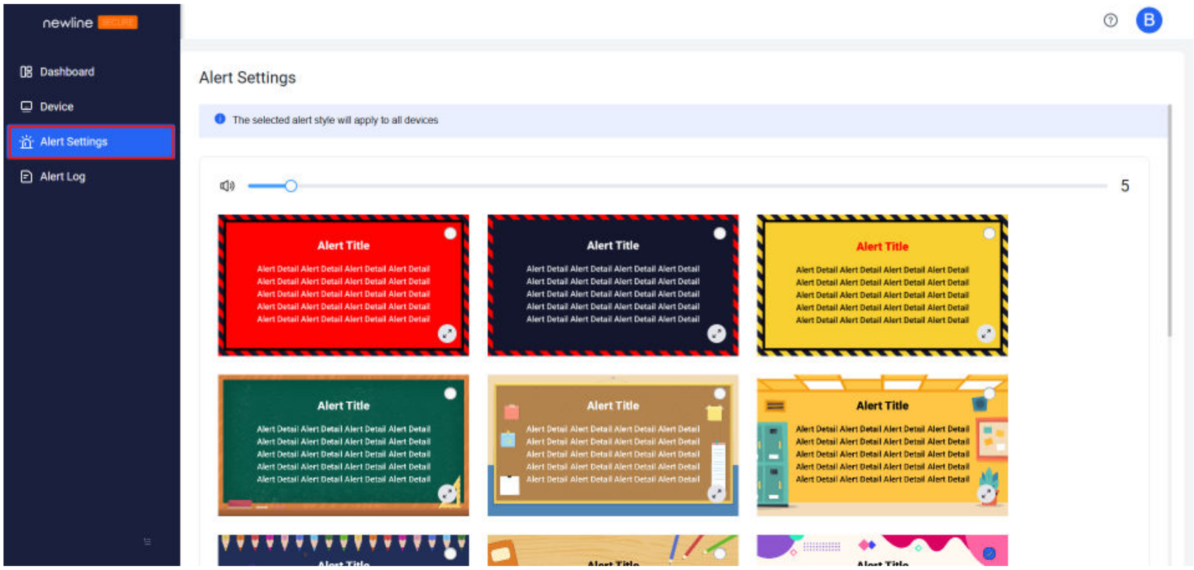
- Cafeteria
- Front Desk

Next

V1.1.0.20240417

Step 3: Customize Your Global Alert Settings

- On the 'Alert Settings' tab, you can customize the alert background image and audio level for your Newline Secure alerts:



newline SECURE
Dashboard
Device
Alert Settings
Alert Log

Alert Settings

The selected alert style will apply to all devices

Volume: 5

Alert Title
Alert Detail Alert Detail Alert Detail Alert Detail
Alert Title
Alert Detail Alert Detail Alert Detail Alert Detail
Alert Title
Alert Detail Alert Detail Alert Detail Alert Detail
Alert Title
Alert Detail Alert Detail Alert Detail Alert Detail
Alert Title
Alert Detail Alert Detail Alert Detail Alert Detail
Alert Title
Alert Detail Alert Detail Alert Detail Alert Detail

  - Note: These settings automatically apply **globally** across all Newline Secure groups and devices

Step 4: Create your Centegix Alerts

- Centegix provides a brief tutorial on how to create and edit alert types

https://www.youtube.com/watch?v=kvZUy_gjwR8&t

Note: Custom Audio & Images are not currently supported by Newline Secure.

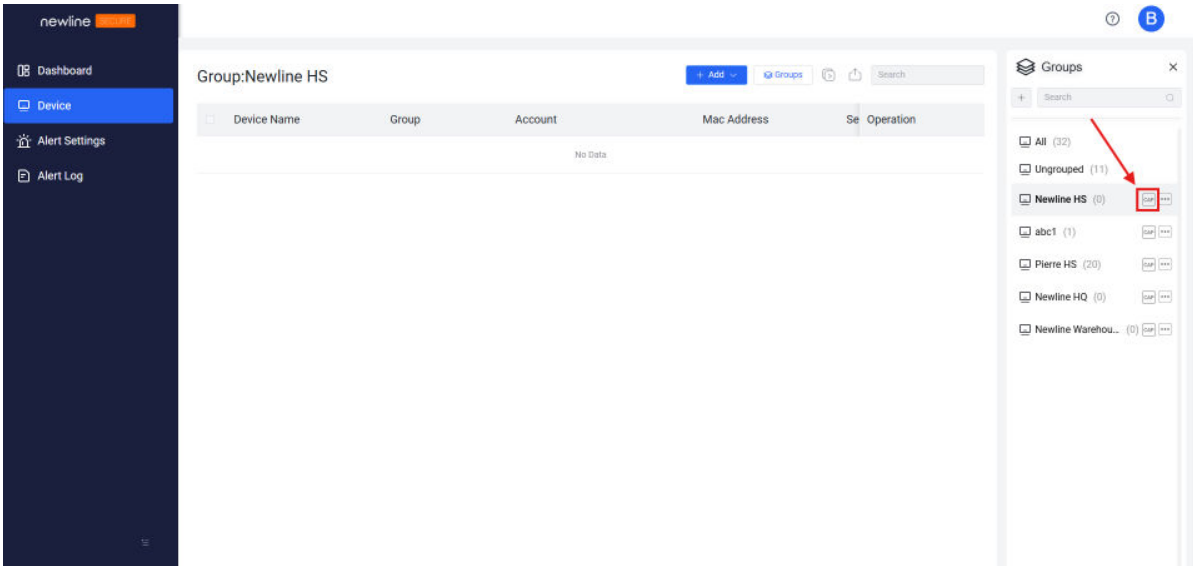
Step 5: Add the Newline Secure API Connectors to the IP Integrations

Now that you have created an alert, we will need to use the API Connectors created by the Newline Secure Portal and setup the IP Integrations in the Centegix CrisisAlert portal

Generate CAP ‘Alert’ Information from Newline Secure

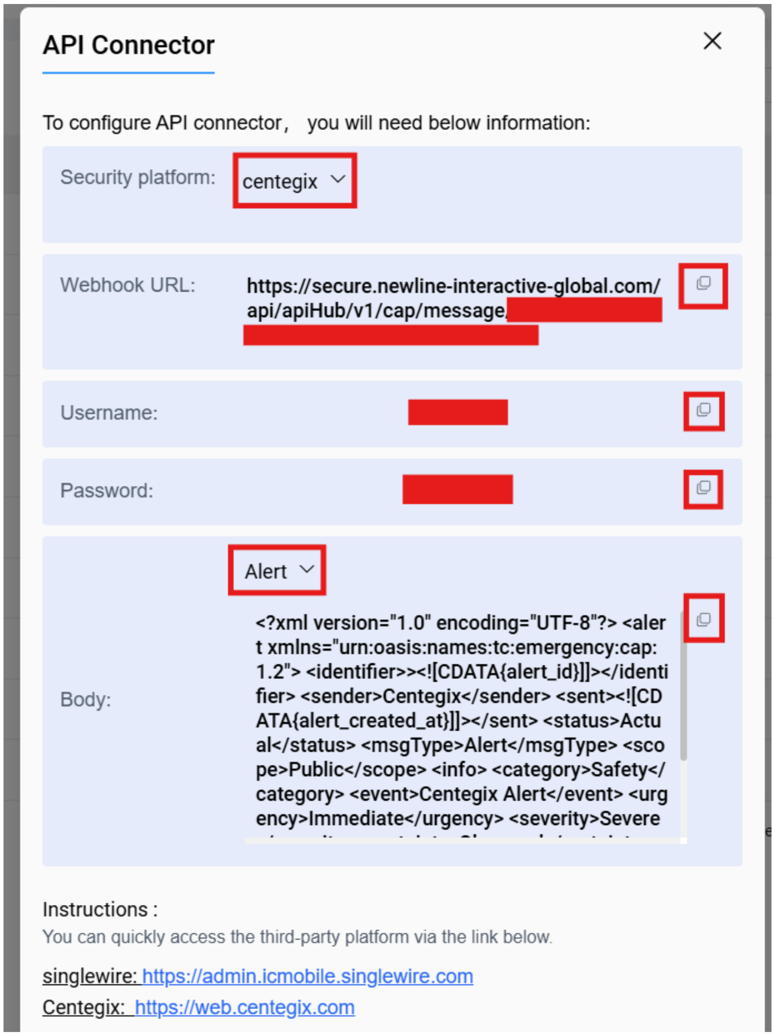
To create a **Centegix API Connector** to attach to a **Centegix IP Integration**, we first need to generate the Common Alerting Protocol (CAP) endpoint information for each Newline Secure group:

- Click the ‘CAP’ button in the device group list to generate CAP integration information



Device Name	Group	Account	Mac Address	Se	Operation
No Data					

- Now you should see a window appear that contains the API endpoint information for your Newline Secure group. Keep this window open as we will need to copy this information over to the Centegix CrisisAlert console.



API Connector

To configure API connector， you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

Password: [redacted]

Body: Alert

```
<?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier>><![CDATA{alert_id}]]></identifier> <sender>Centegix</sender> <sent><![CDATA{alert_created_at}]]></sent> <status>Actual</status> <msgType>Alert</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Alert</event> <urgency>Immediate</urgency> <severity>Severe
```

Instructions :

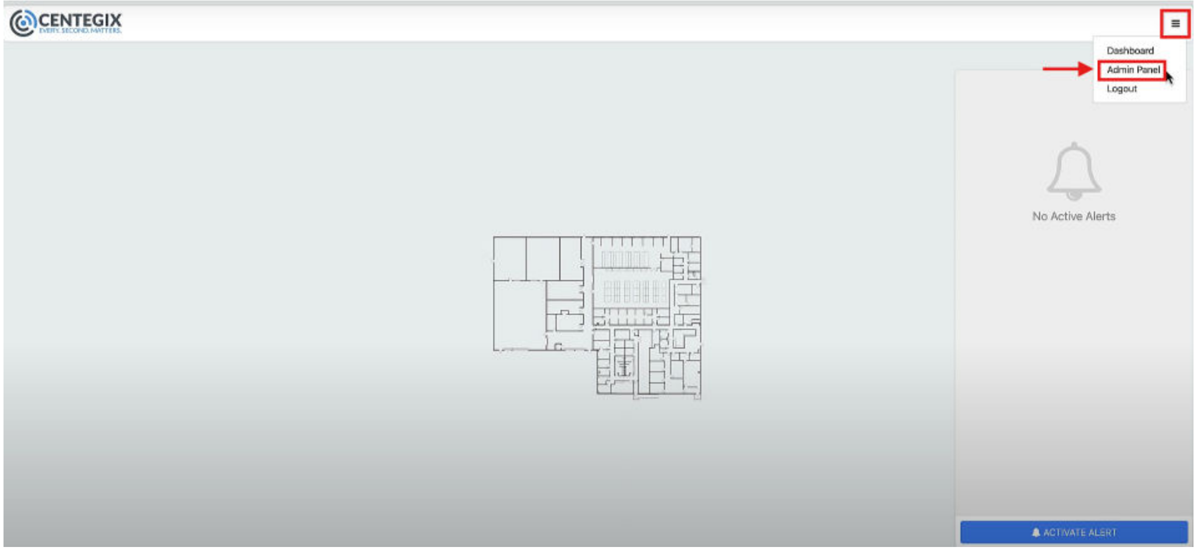
You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com

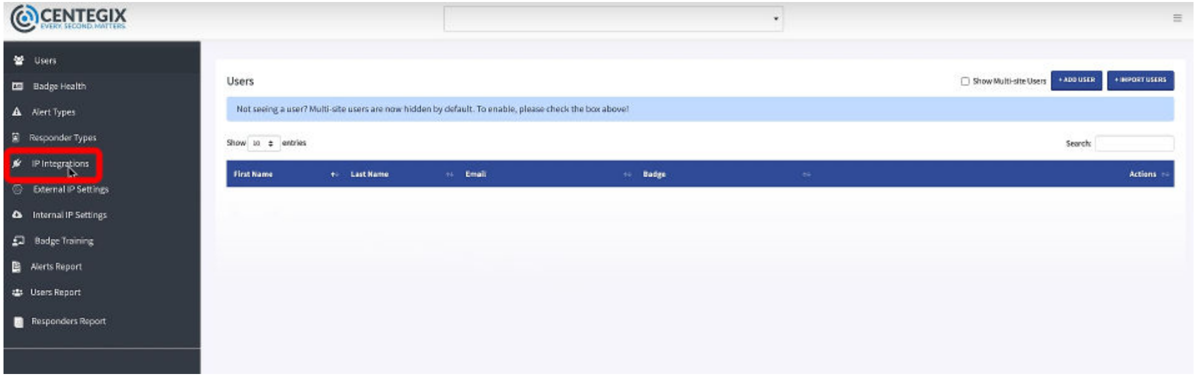
Centegix: https://web.centegix.com

- Ensure that **'Security Platform'** is set to **Centegix**
- Ensure that **'Body'** is set to **Alert**

- In the Centegix CrisisAlert dashboard, click the 'Menu' icon on the top right
- Then select 'Admin Panel'



- Once in the ‘Admin Panel’, navigate to and click on the ‘IP Integrations’ option on the left side.

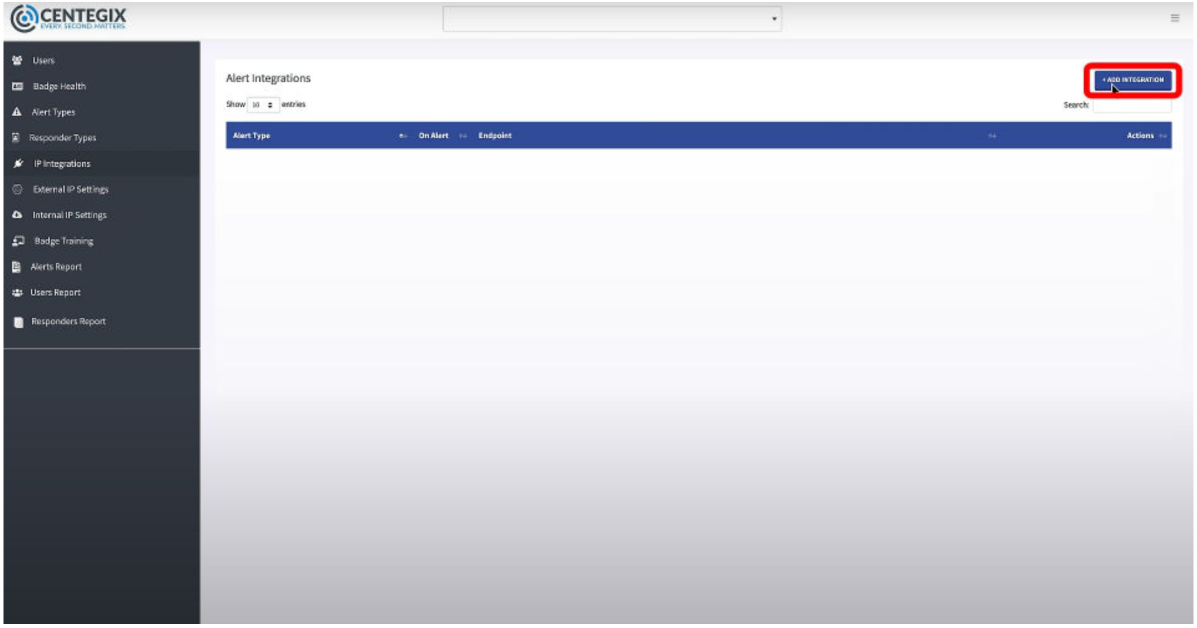


Users

Not seeing a user? Multi-site users are now hidden by default. To enable, please check the box above!

First Name	Last Name	Email	Badge	Actions

- Next on the ‘Alert Integrations’ page, select ‘+ Add Integration’ in the top right



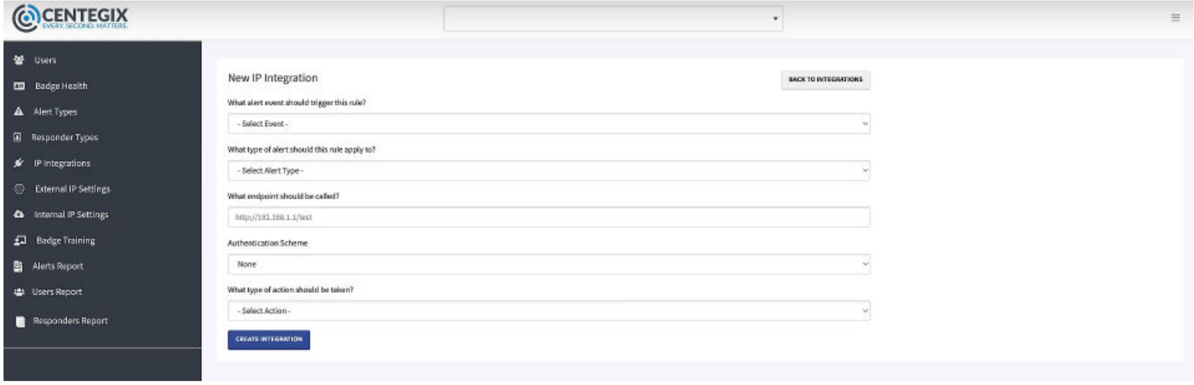
Alert Integrations

Show 10 entries

Search:

Alert Type	On Alert	Endpoint	Actions

- This is the ‘New IP Integration’ screen where we will enter the Newline Secure API Connectors information from earlier. We’ll go over each dropdown individually.



New IP Integration

What alert event should trigger this rule?

- Select Event -

What type of alert should this rule apply to?

- Select Alert Type -

What endpoint should be called?

http://192.168.1.1/test

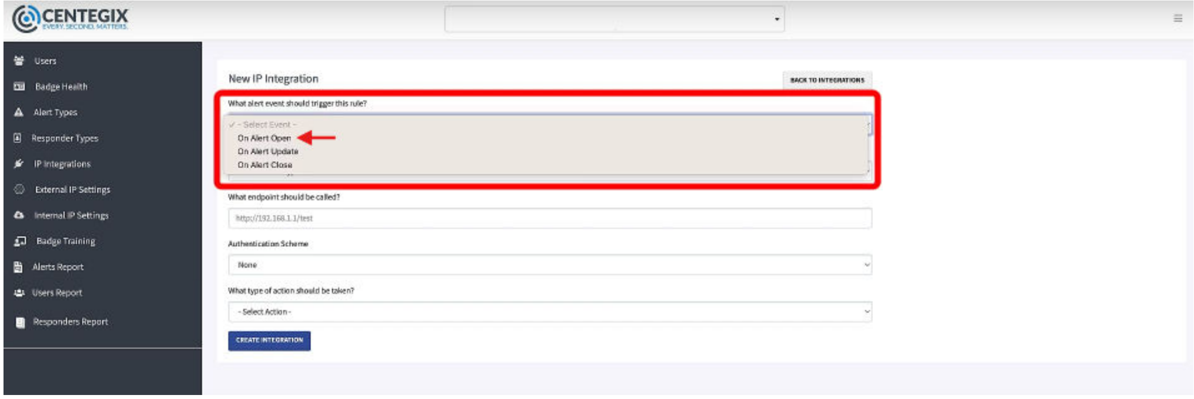
Authentication Scheme

None

What type of action should be taken?

- Select Action -

- Click on the ‘Select Event’ dropdown, in this step we will be creating an ‘Open’, so select ‘On Alert Open’



New IP Integration

What alert event should trigger this rule?

✓ - Select Event -
On Alert Open
On Alert Update
On Alert Close

What endpoint should be called?

http://192.168.1.1/test

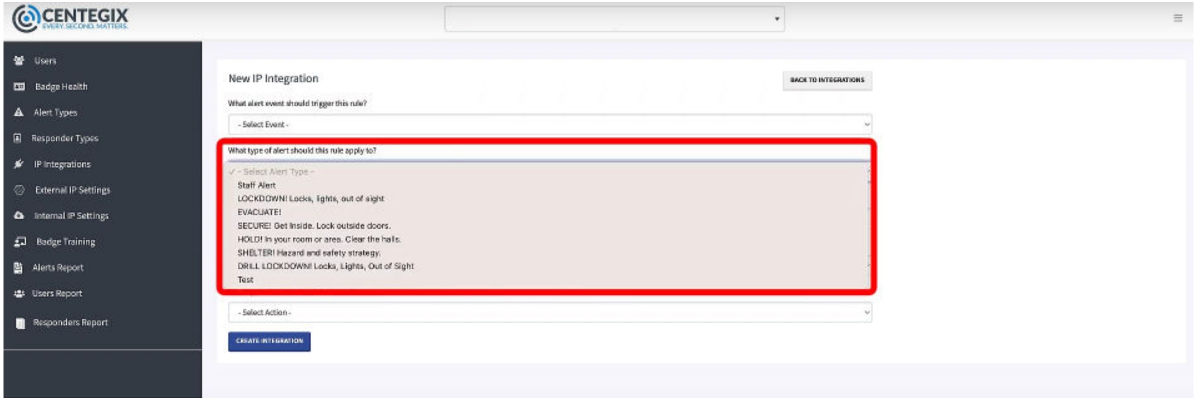
Authentication Scheme

None

What type of action should be taken?

- Select Action -

- Next, we will select the type of alert to apply, here you will select an alert type that you have created earlier



New IP Integration

What alert event should trigger this rule?

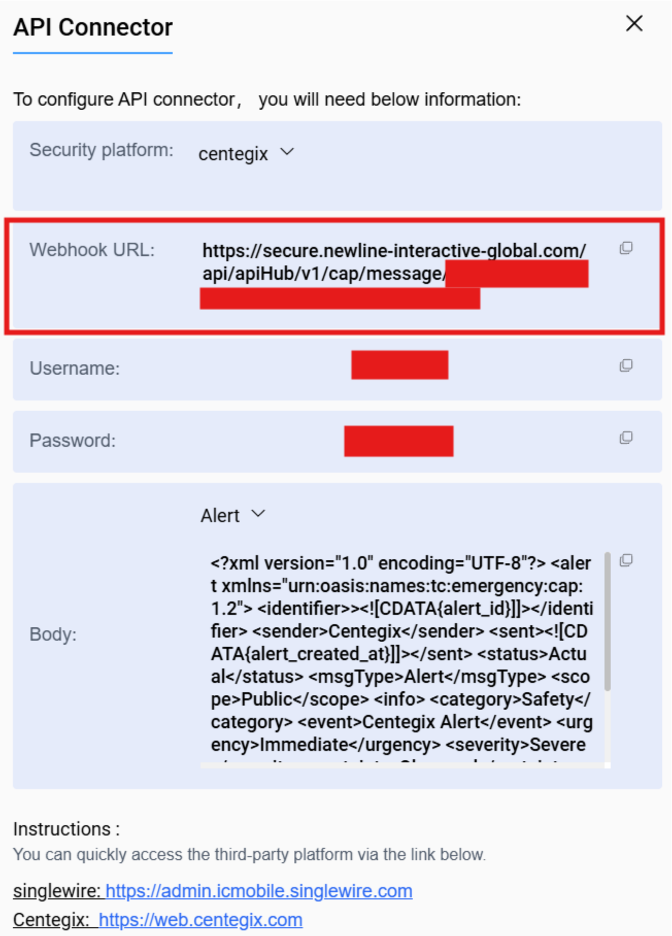
- Select Event -

What type of alert should this rule apply to?

✓ - Select Alert Type -
Staff Alert
LOCKDOWN! Locks, lights, out of sight
EVACUATE!
SECURE! Get Inside. Lock outside doors.
HOLD! In your room or area. Clear the halls.
SHELTER! Hazard and safety strategy.
DRILL LOCKDOWN! Locks, Lights, Out of Sight
Test

- Select Action -

- Next is the ‘endpoint’, for this field we will copy the ‘Webhook URL’ from the Newline Secure portal



API Connector

To configure API connector， you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

Password: [redacted]

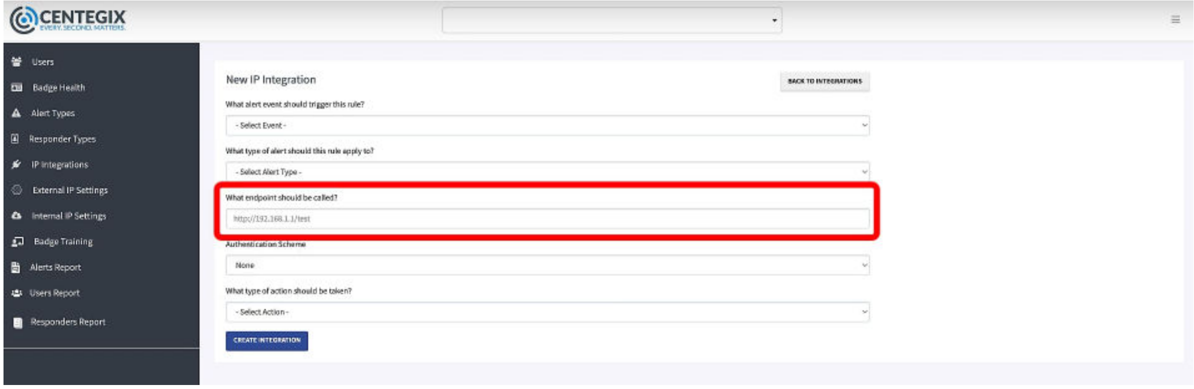
Body: Alert

```
<?xml version="1.0" encoding="UTF-8"?> <aler
t xmlns="urn:oasis:names:tc:emergency:cap:
1.2"> <identifier>><![CDATA{alert_id}]]></identi
fier> <sender>Centegix</sender> <sent><![CD
ATA{alert_created_at}]]></sent> <status>Actu
al</status> <msgType>Alert</msgType> <sco
pe>Public</scope> <info> <category>Safety</
category> <event>Centegix Alert</event> <urg
ency>Immediate</urgency> <severity>Severe
```

Instructions :
You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com
Centegix: https://web.centegix.com

- And paste it into this field



New IP Integration

What alert event should trigger this rule?
- Select Event -

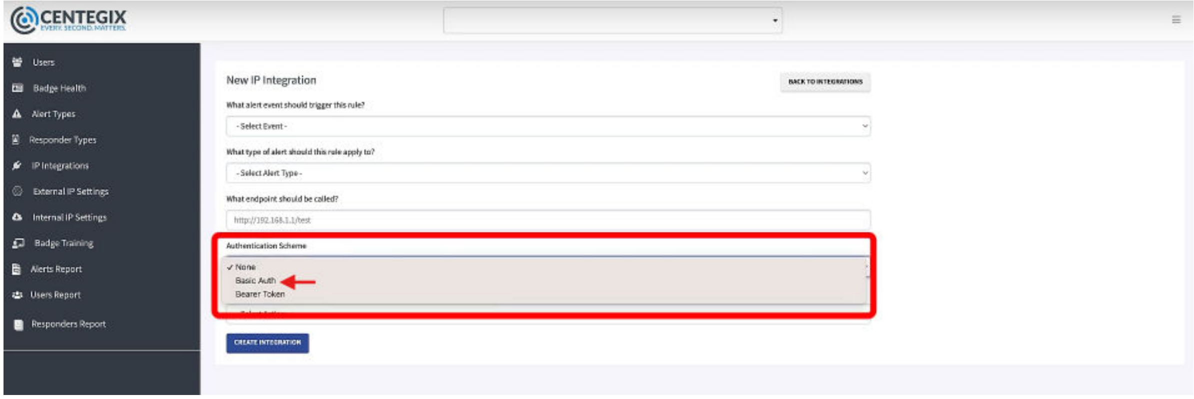
What type of alert should this rule apply to?
- Select Alert Type -

What endpoint should be called?
http://192.168.1.1/test

Authentication Scheme
None

What type of action should be taken?
- Select Action -

- Now we will choose the ‘Authentication Scheme’, please select ‘Basic Auth’ from the dropdown



New IP Integration

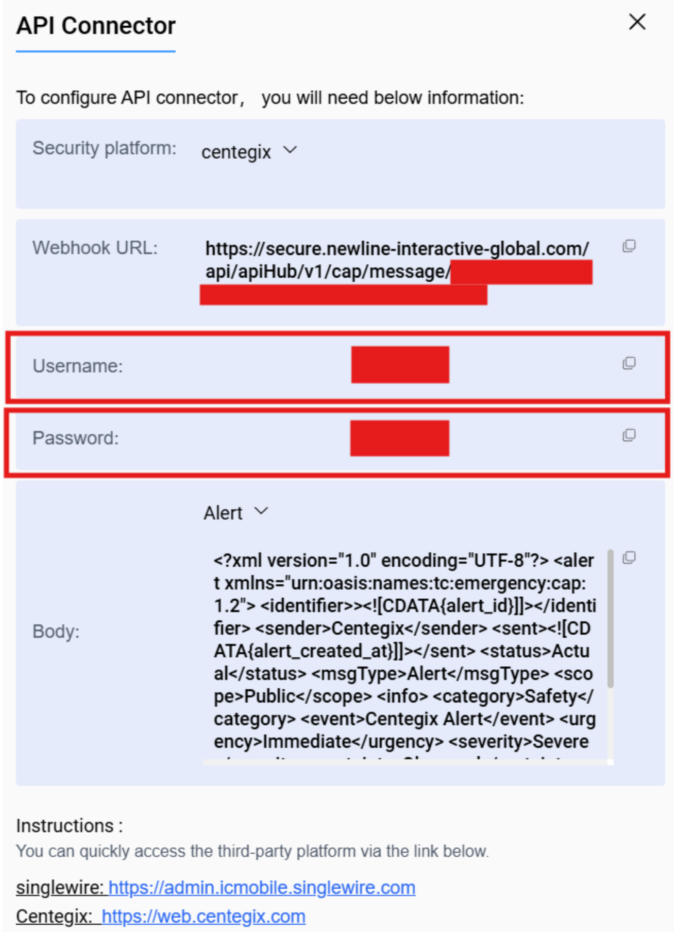
What alert event should trigger this rule?
- Select Event -

What type of alert should this rule apply to?
- Select Alert Type -

What endpoint should be called?
http://192.168.1.1/test

Authentication Scheme
✓ None
Basic Auth
Bearer Token

- For ‘Basic Auth’, copy the username and password from the Newline Secure portal and paste them in the appropriate fields in the Centegix CrisisAlert console.



API Connector

To configure API connector， you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

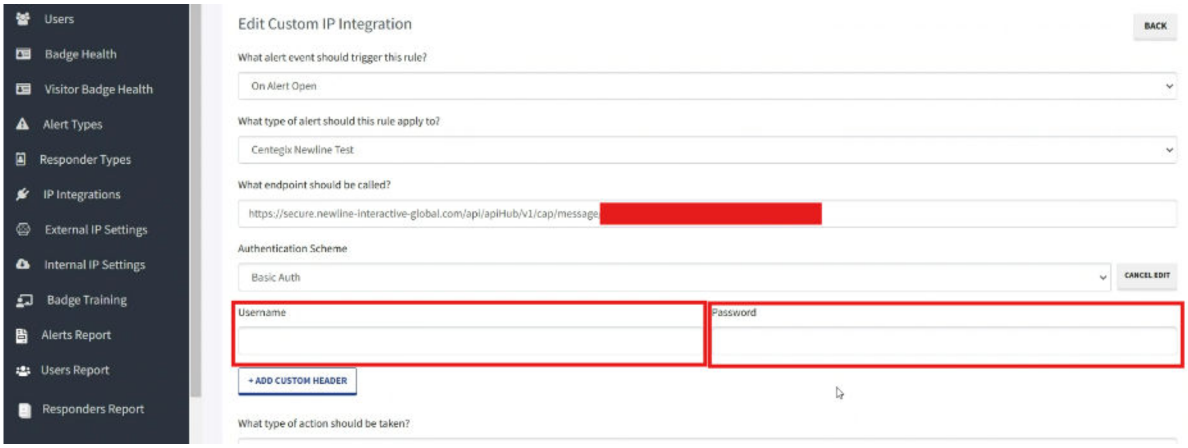
Password: [redacted]

Alert

Body: <?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier>><![CDATA{alert_id}]]></identifier> <sender>Centegix</sender> <sent><![CDATA{alert_created_at}]]></sent> <status>Actual</status> <msgType>Alert</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Alert</event> <urgency>Immediate</urgency> <severity>Severe

Instructions :
You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com
Centegix: https://web.centegix.com



Edit Custom IP Integration

What alert event should trigger this rule?
On Alert Open

What type of alert should this rule apply to?
Centegix Newline Test

What endpoint should be called?
https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message[redacted]

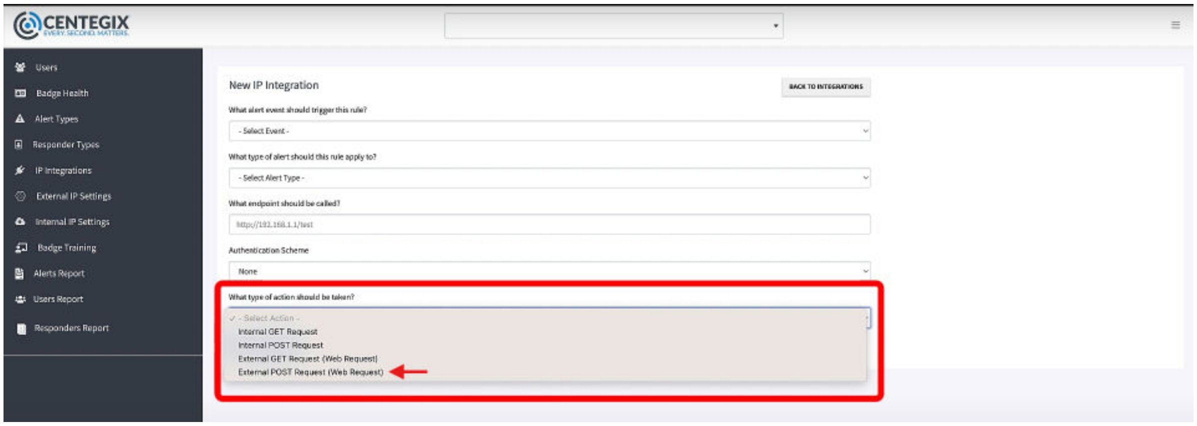
Authentication Scheme
Basic Auth

Username

Password

What type of action should be taken?

- Lastly, we will choose the action type, select ‘External POST Request’ from the dropdown



New IP Integration

What alert event should trigger this rule?
- Select Event -

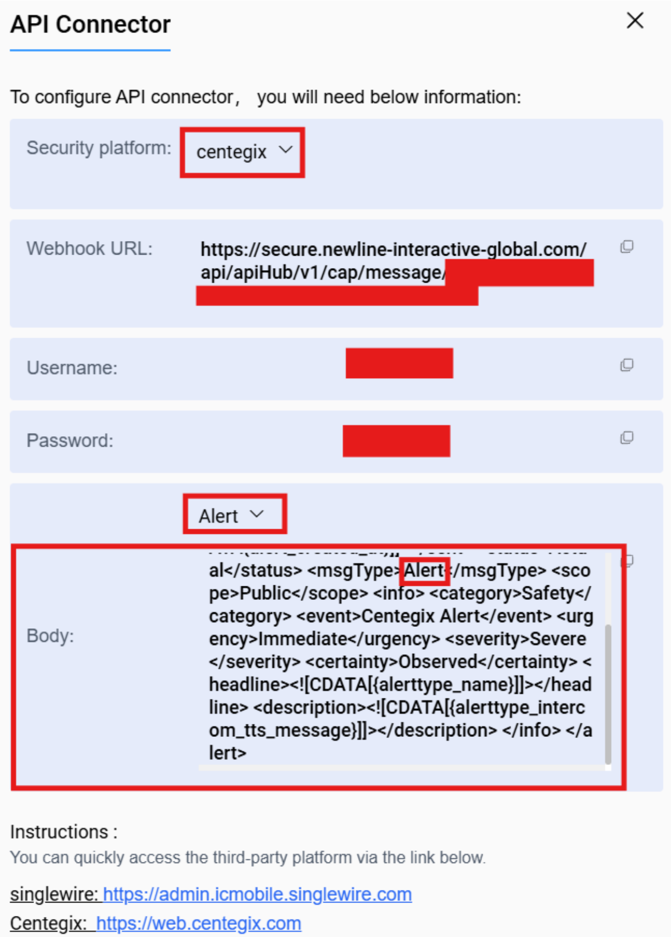
What type of alert should this rule apply to?
- Select Alert Type -

What endpoint should be called?
http://192.168.1.1/test

Authentication Scheme
None

What type of action should be taken?
✓ - Select Action -
Internal GET Request
Internal POST Request
External GET Request (Web Request)
External POST Request (Web Request)

- After that, please select ‘XML’ as the object type and paste the Alert ‘Body’ from the Newline Secure Console into the appropriate field in the Centegix console.
  (Make sure that the XML body correctly shows the msgType ‘Alert’ as shown below.)



API Connector

To configure API connector， you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

Password: [redacted]

Alert

Body:

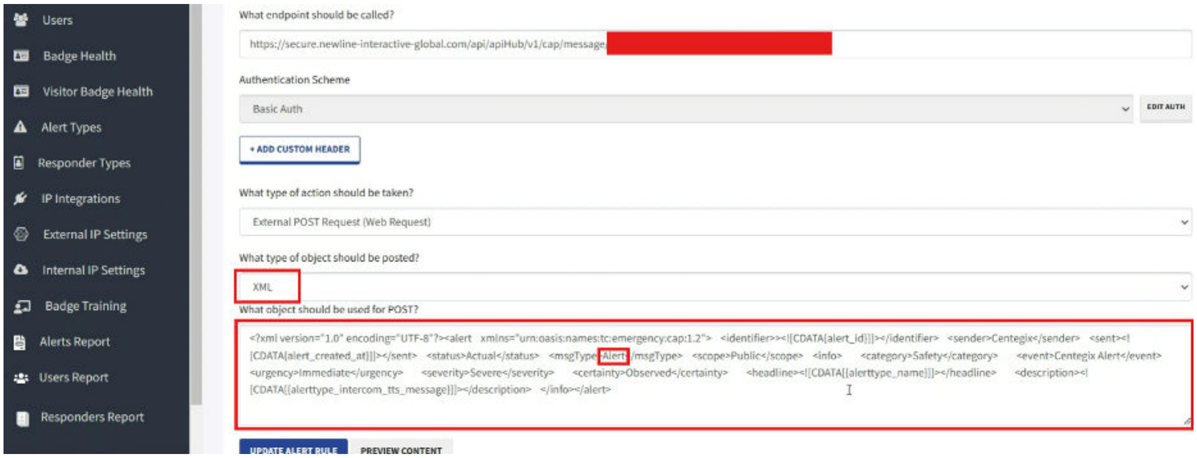
```
al</status> <msgType>Alert</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Alert</event> <urgency>Immediate</urgency> <severity>Severe</severity> <certainty>Observed</certainty> <headline><![CDATA[{alerttype_name}]]></headline> <description><![CDATA[{alerttype_intercom_tts_message}]]></description> </info> </alert>
```

Instructions :

You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com

Centegix: https://web.centegix.com



What endpoint should be called?

https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Authentication Scheme

Basic Auth

What type of action should be taken?

External POST Request (Web Request)

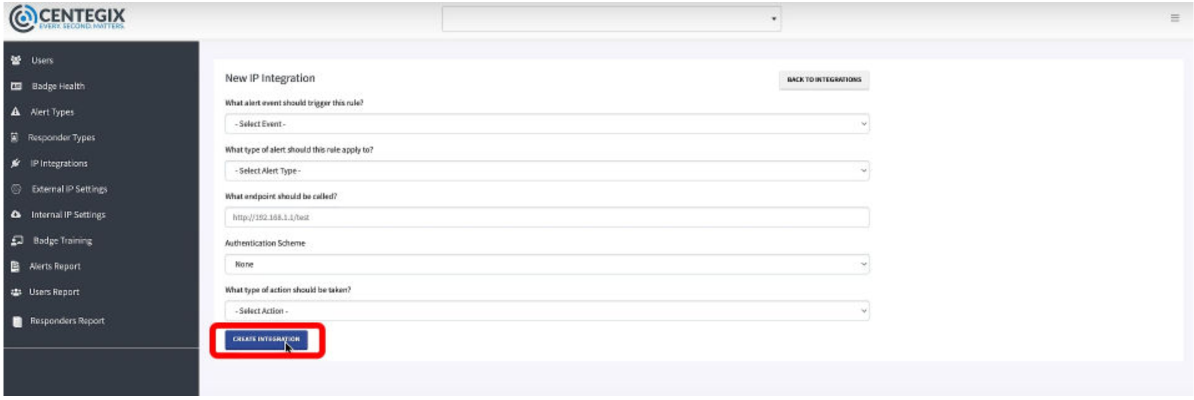
What type of object should be posted?

XML

What object should be used for POST?

```
<?xml version="1.0" encoding="UTF-8"?><alert   xmlns="urn:oasis:names:tc:emergency:cap:1.2">   <identifier><![CDATA[alert_id]]]></identifier>   <sender>Centegix</sender>   <sent><![CDATA[alert_created_at]]]></sent>   <status>Actual</status>   <msgType>Alert</msgType>   <scope>Public</scope>   <info>     <category>Safety</category>     <event>Centegix Alert</event>     <urgency>Immediate</urgency>     <severity>Severe</severity>     <certainty>Observed</certainty>     <headline><![CDATA[{alerttype_name}]]></headline>     <description><![CDATA[{alerttype_intercom_tts_message}]]></description>   </info></alert>
```

- Finally, double check that you have entered everything correctly, then select ‘Create Integration’



New IP Integration

What alert event should trigger this rule?
- Select Event -

What type of alert should this rule apply to?
- Select Alert Type -

What endpoint should be called?
http://192.168.1.1/test

Authentication Scheme
None

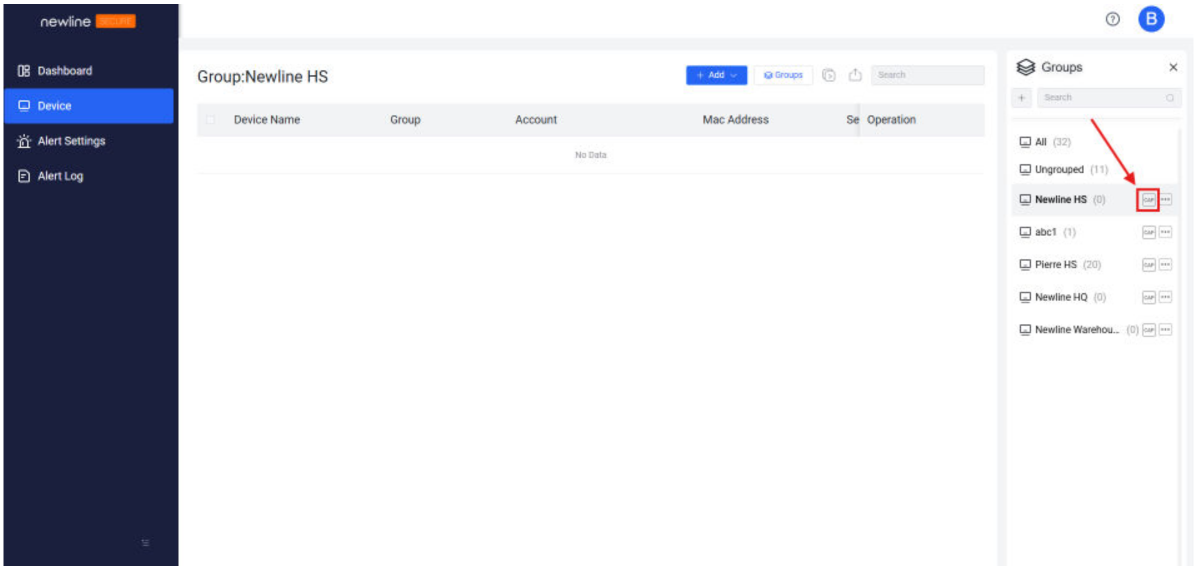
What type of action should be taken?
- Select Action -

- Now that we have created an IP Integration for the ‘Alert’, we will have to repeat the same steps for the ‘Clear’.

Generate CAP ‘Clear’ Information from Newline Secure

In order to create the ‘Clear’ we will be using the exact same steps that we used for the ‘Alert’ with a couple of changes in the process.

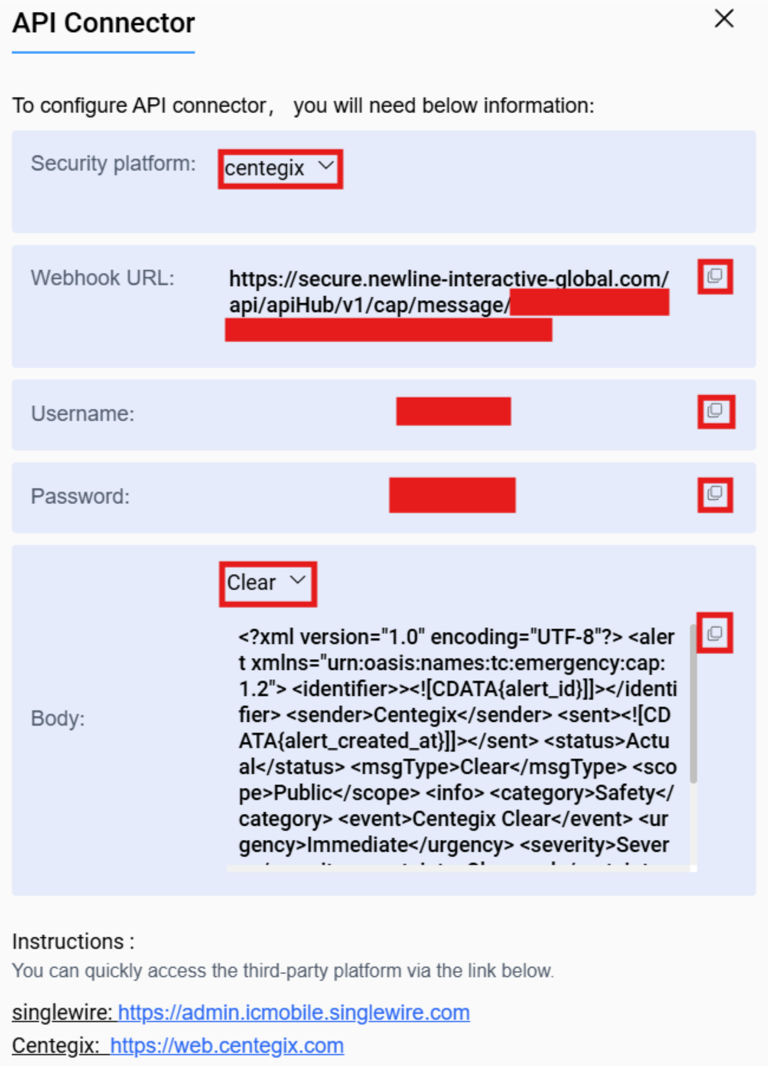
- Click the ‘CAP’ button in the device group list to generate CAP integration information



Group:Newline HS

Device Name	Group	Account	Mac Address	Se	Operation
		No Data			

- Now you should see a window appear that contains the API endpoint information for your Newline Secure group. Keep this window open as we will need to copy this information over to the Centegix CrisisAlert console.



API Connector

To configure API connector， you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

Password: [redacted]

Body: Clear

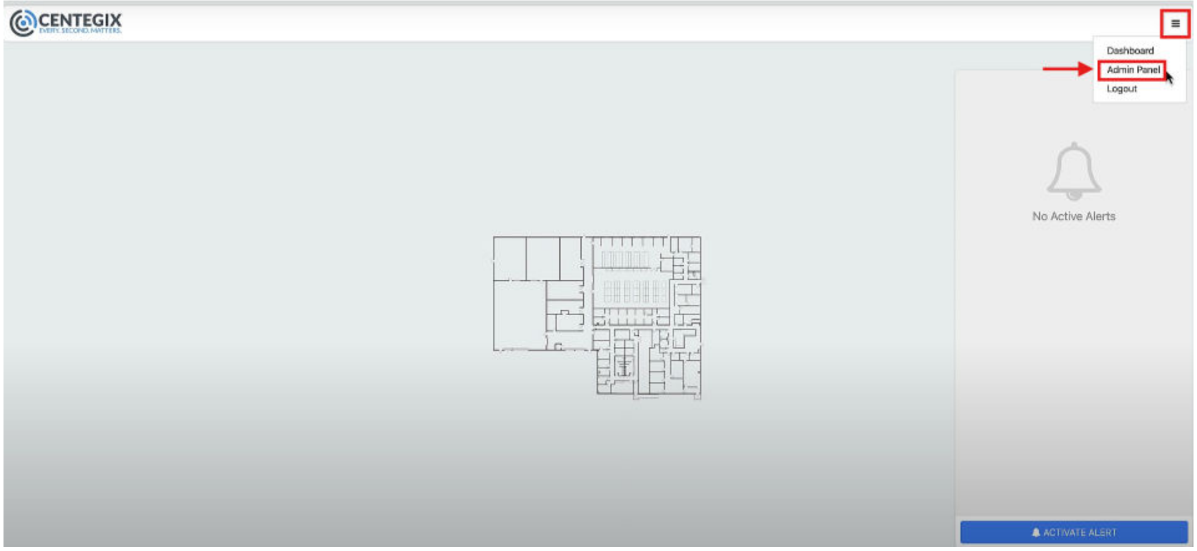
```
<?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier>><![CDATA{alert_id}]]></identifier> <sender>Centegix</sender> <sent><![CDATA{alert_created_at}]]></sent> <status>Actual</status> <msgType>Clear</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Clear</event> <urgency>Immediate</urgency> <severity>Sever
```

Instructions :
You can quickly access the third-party platform via the link below.

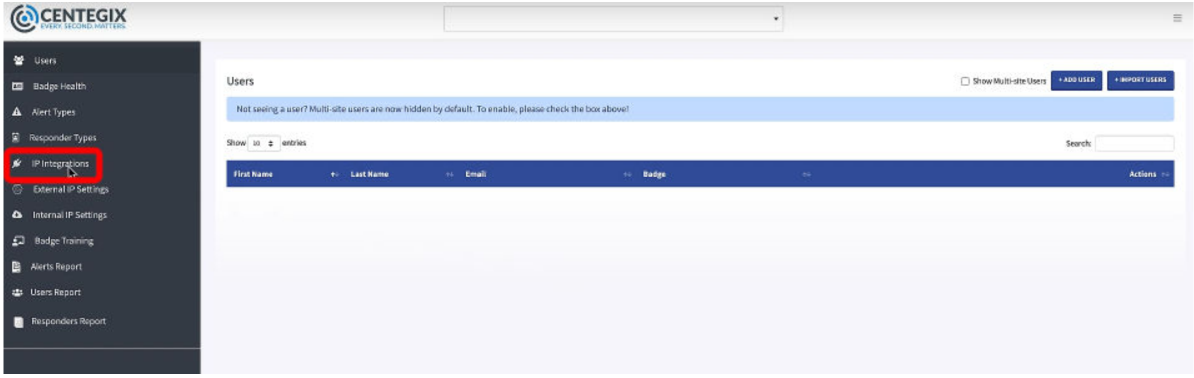
singlewire: https://admin.icmobile.singlewire.com
Centegix: https://web.centegix.com

- Ensure that **‘Security Platform’** is set to **Centegix**
- Ensure that **‘Body’** is set to **Clear**

- In the Centegix CrisisAlert dashboard, click the ‘Menu’ icon on the top right
- Then select ‘Admin Panel’

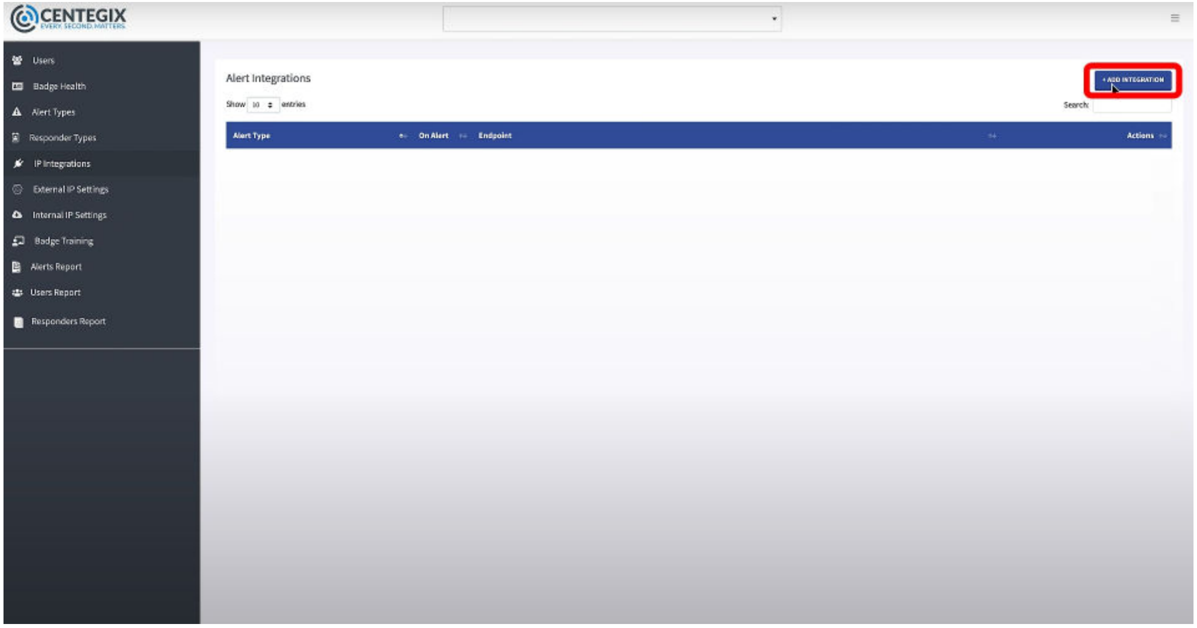


- Once in the ‘Admin Panel’, navigate to and click on the ‘IP Integrations’ option on the left side.



Not seeing a user? Multi-site users are now hidden by default. To enable, please check the box above!

- Next on the ‘Alert Integrations’ page, select ‘+ Add Integration’ in the top right

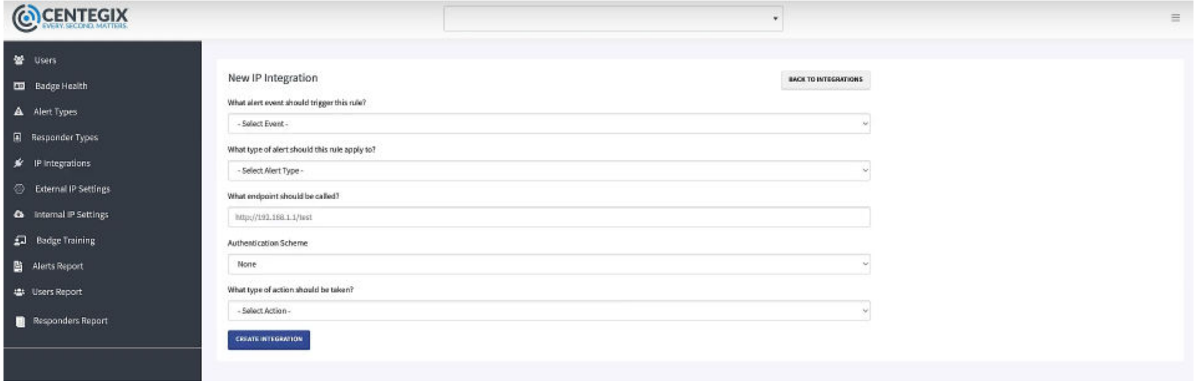


Alert Integrations

Show 10 entries

Alert Type	On Alert	Endpoint	Actions

- This is the ‘New IP Integration’ screen where we will enter the Newline Secure API Connectors information from earlier.



New IP Integration

What alert event should trigger this rule?
- Select Event -

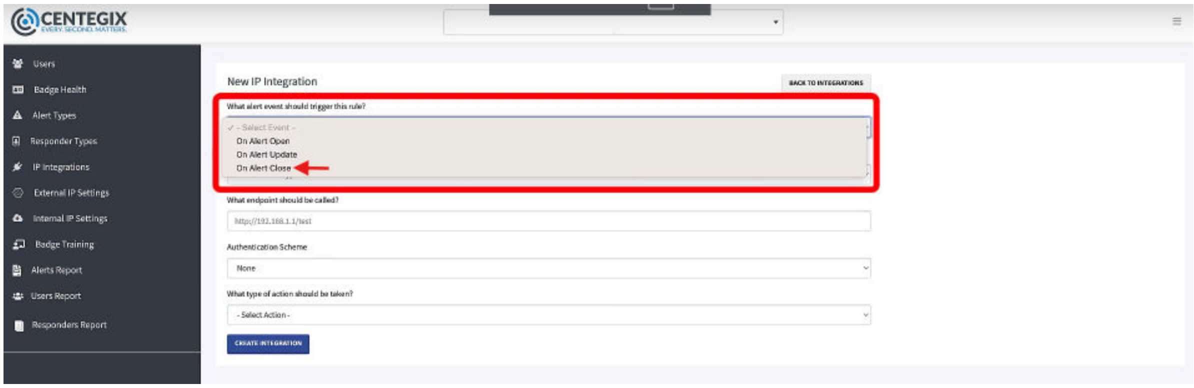
What type of alert should this rule apply to?
- Select Alert Type -

What endpoint should be called?
http://192.168.1.1/test

Authentication Scheme
None

What type of action should be taken?
- Select Action -

- Click on the ‘Select Event’ dropdown, in this step we will be creating a ‘Clear’, so select ‘On Alert Close’



New IP Integration

What alert event should trigger this rule?

✓ - Select Event -
On Alert Open
On Alert Update
On Alert Close

What endpoint should be called?

http://192.168.1.1/test

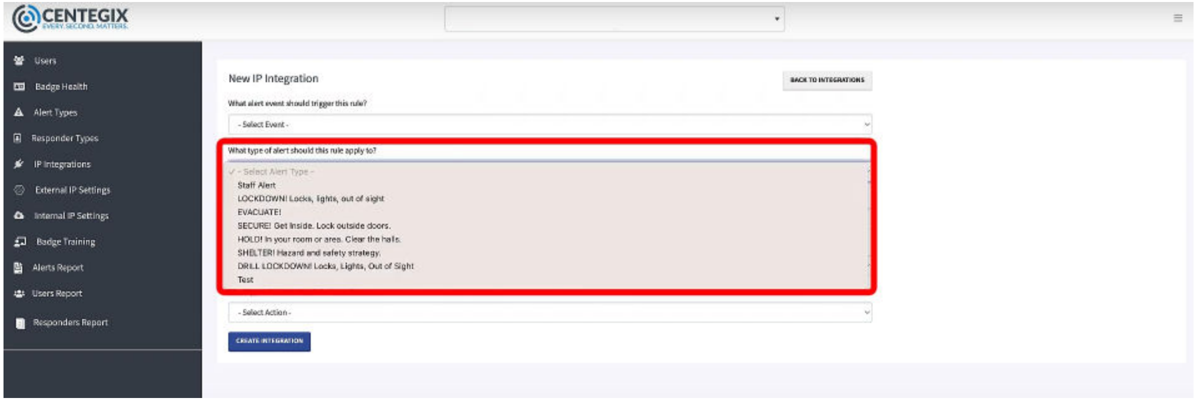
Authentication Scheme

None

What type of action should be taken?

- Select Action -

- Next, we will select the type of alert to apply, here you will select an alert type that you have created.



New IP Integration

What alert event should trigger this rule?

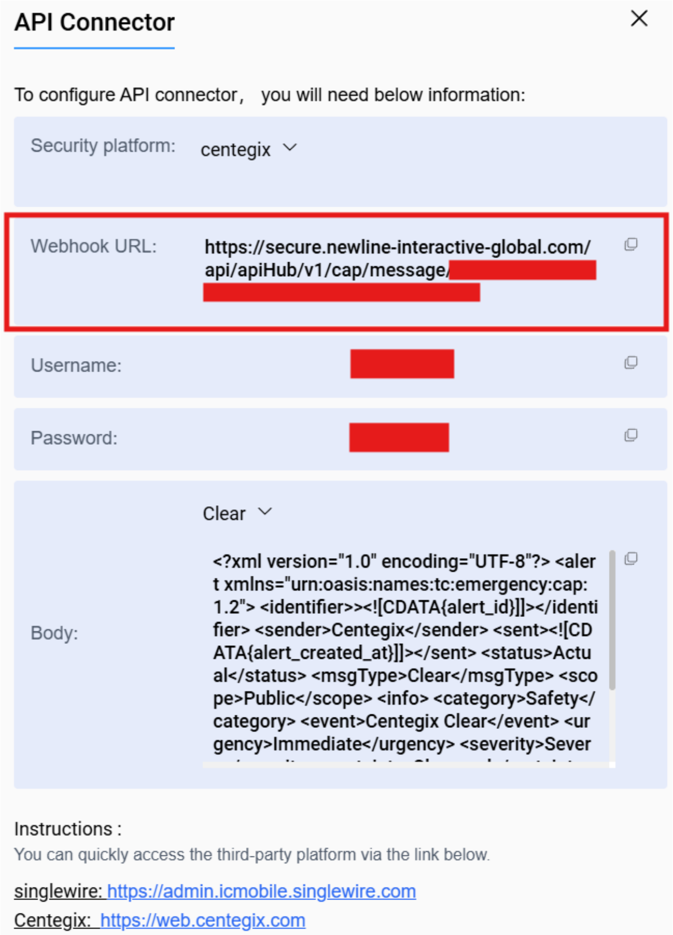
- Select Event -

What type of alert should this rule apply to?

✓ - Select Alert Type -
Staff Alert
LOCKDOWN! Locks, lights, out of sight
EVACUATE!
SECURE! Get Inside. Lock outside doors.
HOLD! In your room or area. Clear the halls.
SHELTER! Hazard and safety strategy.
DRILL LOCKDOWN! Locks, Lights, Out of Sight
Test

- Select Action -

- Next is the 'endpoint', for this field we will copy the 'Webhook URL' from the Newline Secure portal



API Connector

To configure API connector， you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

Password: [redacted]

Body: Clear

```
<?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier>><![CDATA{alert_id}]]></identifier> <sender>Centegix</sender> <sent><![CDATA{alert_created_at}]]></sent> <status>Actual</status> <msgType>Clear</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Clear</event> <urgency>Immediate</urgency> <severity>Sever
```

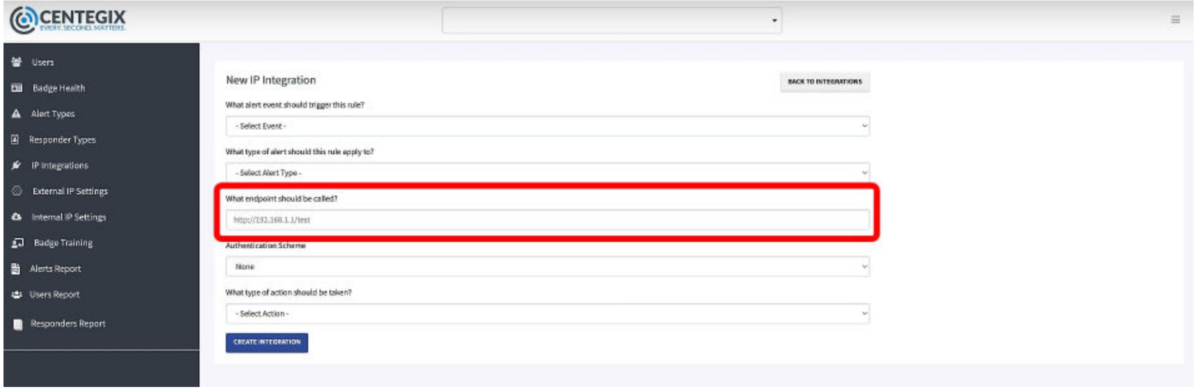
Instructions :

You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com

Centegix: https://web.centegix.com

- And paste it into this field



New IP Integration

What alert event should trigger this rule?

- Select Event -

What type of alert should this rule apply to?

- Select Alert Type -

What endpoint should be called?

http://192.168.1.1/test

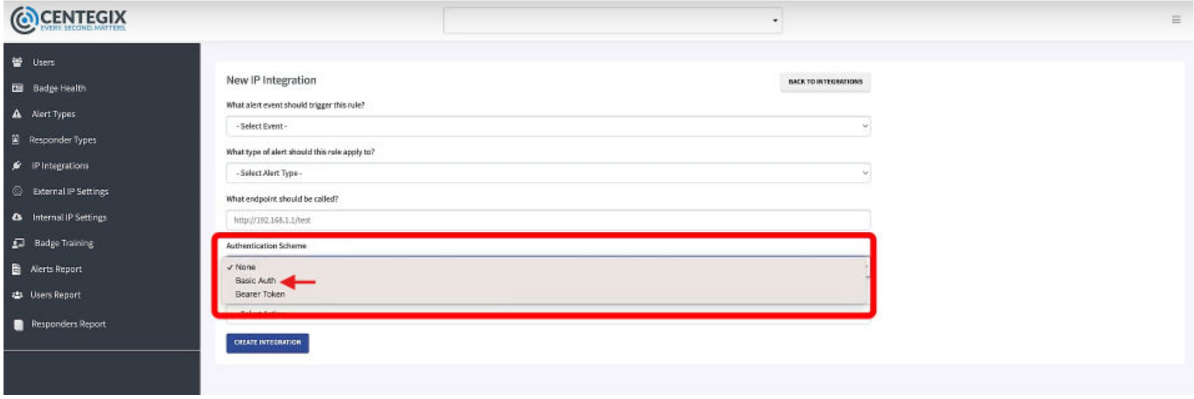
Authentication Scheme

None

What type of action should be taken?

- Select Action -

- Now we will choose the ‘Authentication Scheme’, please select ‘Basic Auth’ from the dropdown



New IP Integration

What alert event should trigger this rule?

- Select Event -

What type of alert should this rule apply to?

- Select Alert Type -

What endpoint should be called?

http://192.168.1.1/test

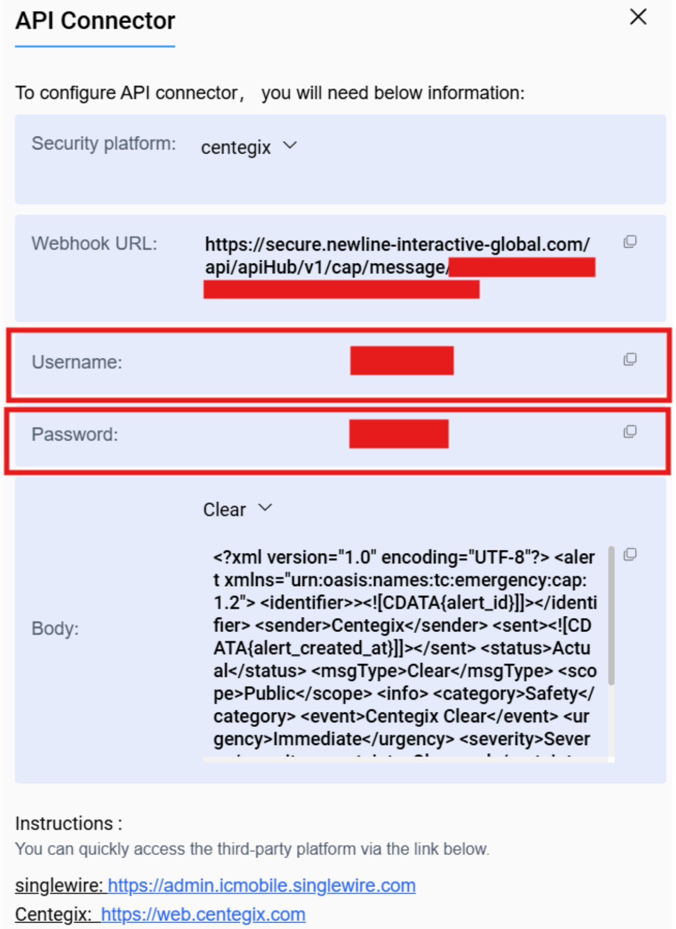
Authentication Scheme

✓ None

Basic Auth

Bearer Token

- For ‘Basic Auth’, copy the username and password from the Newline Secure portal and paste them in the appropriate fields in the Centegix CrisisAlert console.



API Connector

To configure API connector， you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

Password: [redacted]

Clear

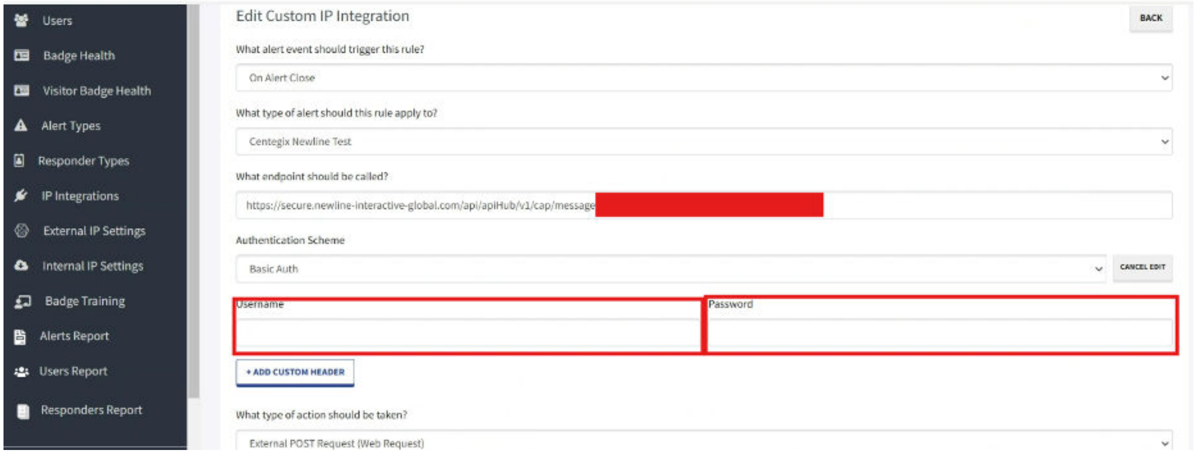
Body: <?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier>><![CDATA{alert_id}]]></identifier> <sender>Centegix</sender> <sent><![CDATA{alert_created_at}]]></sent> <status>Actual</status> <msgType>Clear</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Clear</event> <urgency>Immediate</urgency> <severity>Sever

Instructions :

You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com

Centegix: https://web.centegix.com



Edit Custom IP Integration

What alert event should trigger this rule?
On Alert Close

What type of alert should this rule apply to?
Centegix Newline Test

What endpoint should be called?
https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message[redacted]

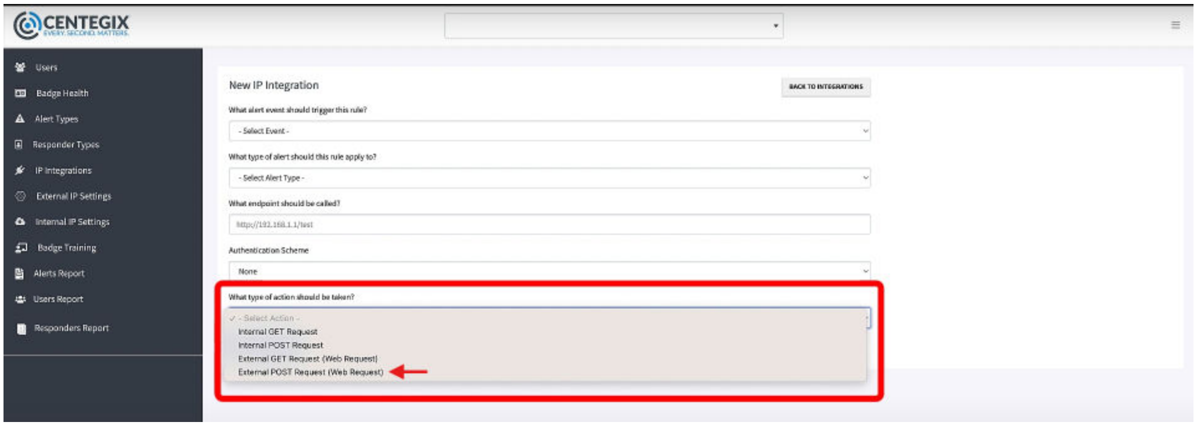
Authentication Scheme
Basic Auth

Username

Password

What type of action should be taken?
External POST Request (Web Request)

- Next, we will choose the action type, select ‘External POST Request’ from the dropdown



New IP Integration

What alert event should trigger this rule?
- Select Event -

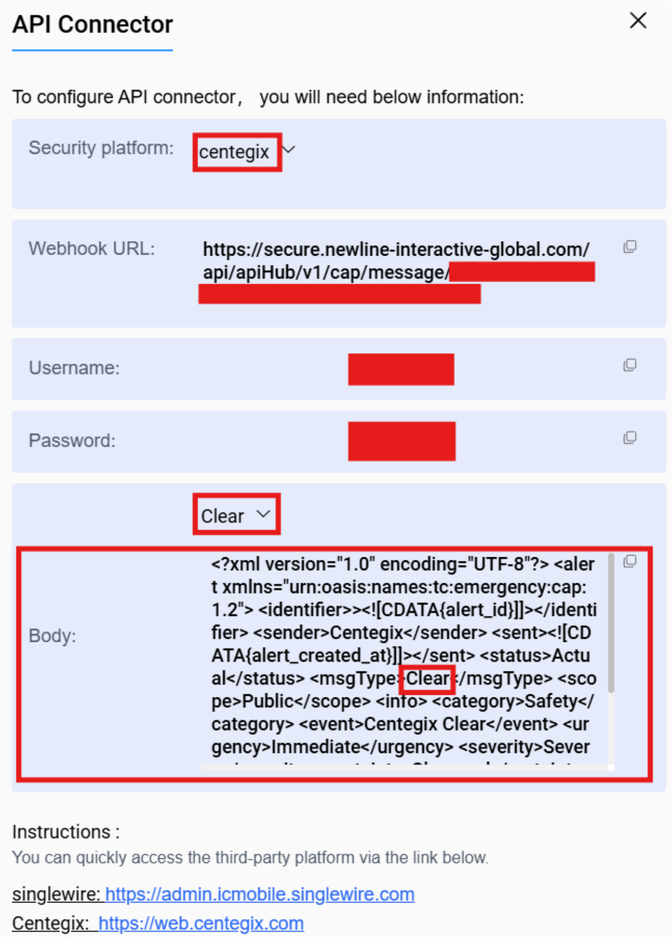
What type of alert should this rule apply to?
- Select Alert Type -

What endpoint should be called?
http://192.168.1.1/test

Authentication Scheme
None

What type of action should be taken?
✓ - Select Action -
Internal GET Request
Internal POST Request
External GET Request (Web Request)
External POST Request (Web Request)

- After that, please select ‘XML’ as the object type and paste the Clear ‘Body’ from the Newline Secure Console into the appropriate field in the Centegix console.
(Make sure that the XML body correctly shows the msgType ‘Clear’ as shown below.)



API Connector

To configure API connector, you will need below information:

Security platform: centegix

Webhook URL: https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Username: [redacted]

Password: [redacted]

Clear

Body:

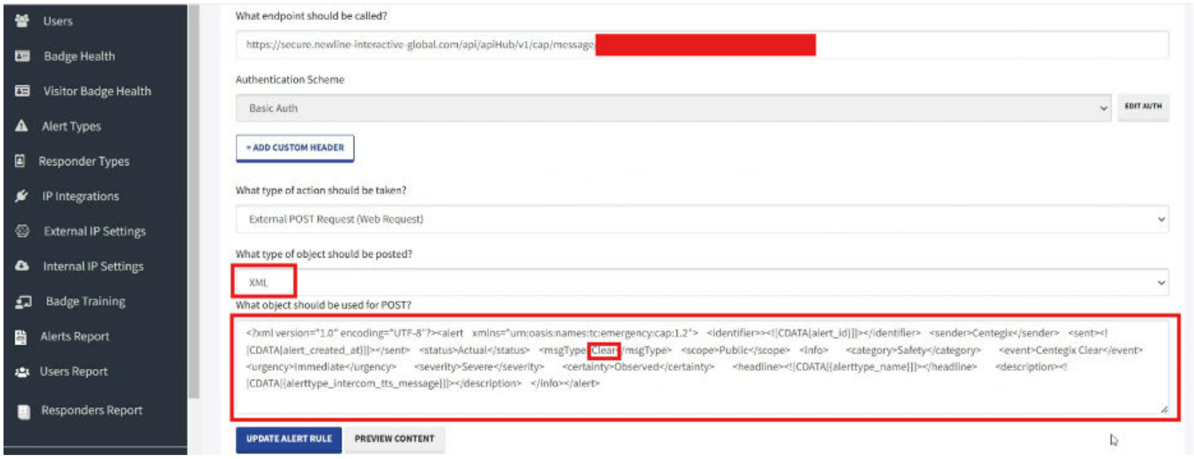
```
<?xml version="1.0" encoding="UTF-8"?> <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier><![CDATA{alert_id}]]></identifier> <sender>Centegix</sender> <sent><![CDATA{alert_created_at}]]></sent> <status>Actual</status> <msgType>Clear</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Clear</event> <urgency>Immediate</urgency> <severity>Sever
```

Instructions :

You can quickly access the third-party platform via the link below.

singlewire: https://admin.icmobile.singlewire.com

Centegix: https://web.centegix.com



What endpoint should be called?

https://secure.newline-interactive-global.com/api/apiHub/v1/cap/message/[redacted]

Authentication Scheme

Basic Auth

What type of action should be taken?

External POST Request (Web Request)

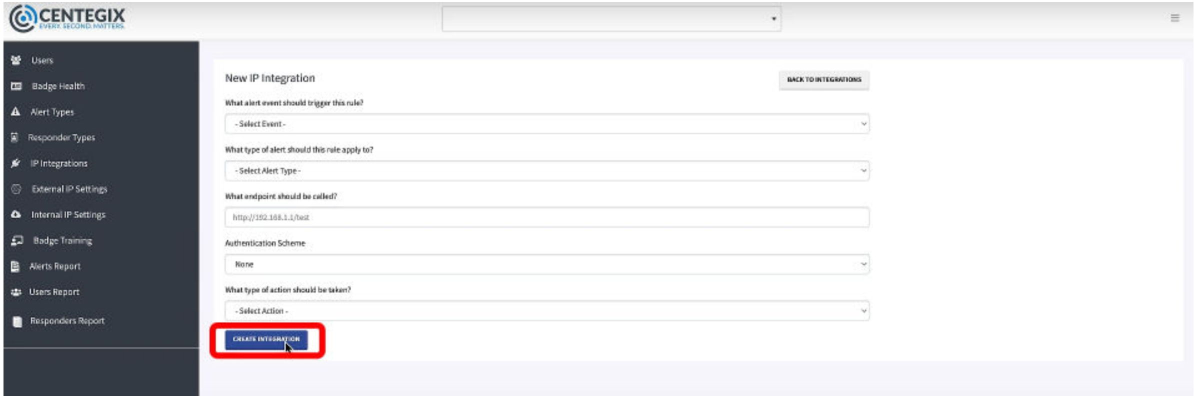
What type of object should be posted?

XML

What object should be used for POST?

```
<?xml version="1.0" encoding="UTF-8"?><alert xmlns="urn:oasis:names:tc:emergency:cap:1.2"> <identifier><![CDATA[alert_id]]></identifier> <sender>Centegix</sender> <sent><![CDATA[alert_created_at]]></sent> <status>Actual</status> <msgType>Clear</msgType> <scope>Public</scope> <info> <category>Safety</category> <event>Centegix Clear</event> <urgency>Immediate</urgency> <severity>Severe</severity> <certainty>Observed</certainty> <headline><![CDATA[{alerttype_name}]]></headline> <description><![CDATA[{alerttype_intercom_tts_message}]]></description> </info></alert>
```

- Finally, double check that you have entered everything correctly, then select 'Create Integration'



New IP Integration

What alert event should trigger this rule?

- Select Event -

What type of alert should this rule apply to?

- Select Alert Type -

What endpoint should be called?

http://192.168.1.1/test

Authentication Scheme

None

What type of action should be taken?

- Select Action -

Congratulations!

You have now created new IP Integrations that will trigger an alert, and clear out of existing alerts for a Newline Secure group of devices.

If you have any questions/issues with the Newline Secure Portal, please reach out to Newline Technical Support and we'd be glad to help you out!

- Submit a ticket here!
- Give us a call at +1 (833)-469-9520

If you have questions or need assistance with the Centegix Portal, please contact Centegix Support by sending an email:

- support@centegix.com

Mass-Deployment Guide

Installing & Mass Deploying Newline Secure

Is Newline Secure not pre-installed on your panels?

In order to obtain the Newline Secure apk file, please reach out to the Newline Tech Support Team

- Submit a ticket here!

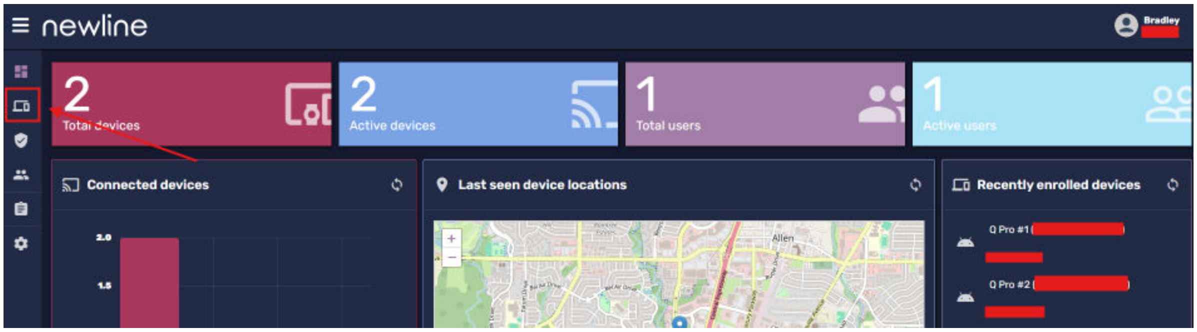
This guide will walk you through how to install and mass deploy Newline Secure across multiple panels using Newline Display Management.

Before proceeding with this guide, please ensure that you have completed the steps in the Portal Sign-Up Guide **and either the Singlewire or Centegix Integration Guide.**

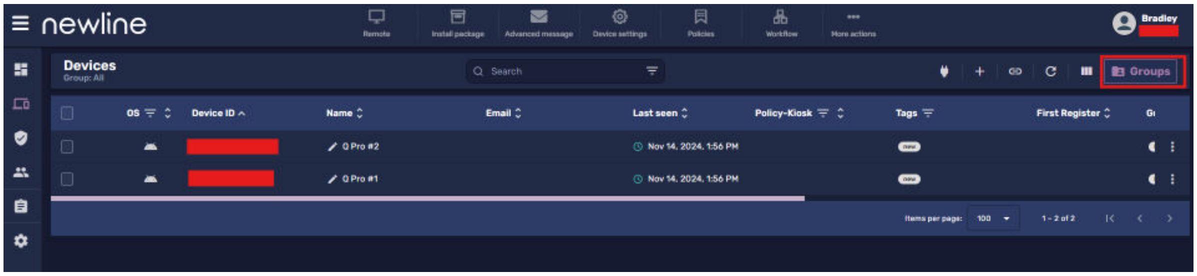
Note: Only Newline Q Pro Series Panels are currently supported. For best performance and stability, please ensure that your Q Pro is on firmware v1.0.75 or higher.

Step 1: Create a Group in NDM

- After logging into Newline Display Management, navigate to the ‘Devices’ tab.



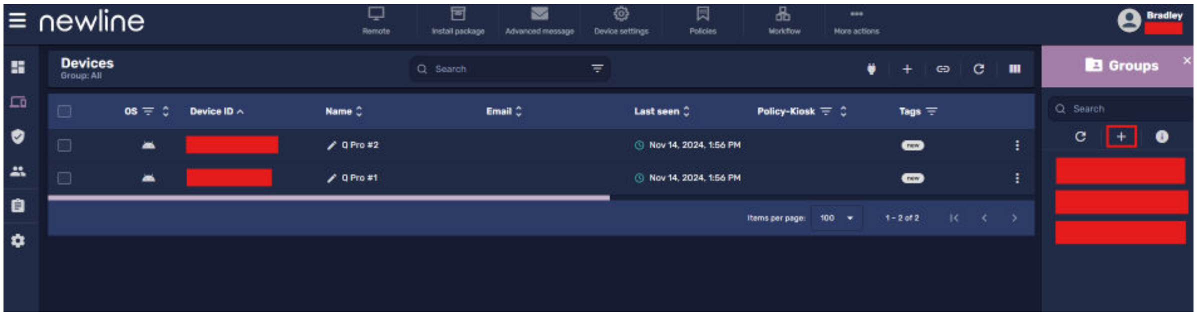
- Select the ‘Groups’ button on the right side of the screen.



[redacted]

OS	Device ID	Name	Email	Last seen	Policy-Kiosk	Tags	First Register	Gi
	[redacted]	Q Pro #2		Nov 14, 2024, 1:56 PM		new		
	[redacted]	Q Pro #1		Nov 14, 2024, 1:56 PM		new		

- This will open the ‘Groups’ tab, select the ‘+’ icon to create a new group.



[redacted]

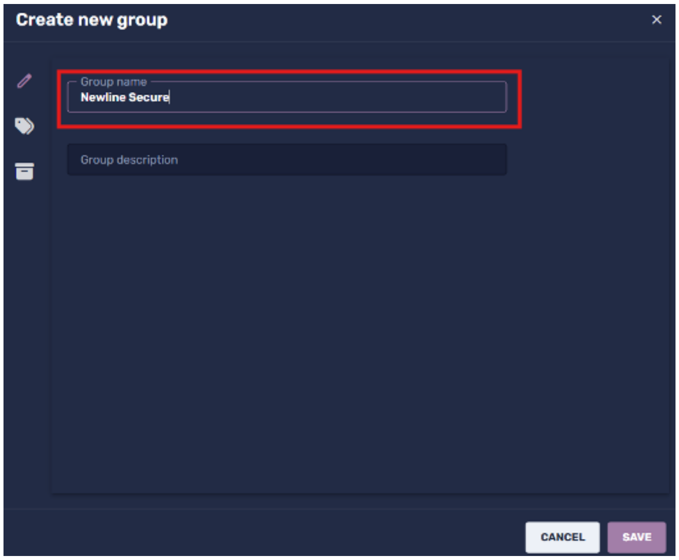
OS	Device ID	Name	Email	Last seen	Policy-Kiosk	Tags
	[redacted]	Q Pro #2		Nov 14, 2024, 1:56 PM		new
	[redacted]	Q Pro #1		Nov 14, 2024, 1:56 PM		new

[redacted]

[redacted]

[redacted]

- Type in a ‘Group Name’ (required) and a ‘Group Description’ (optional).

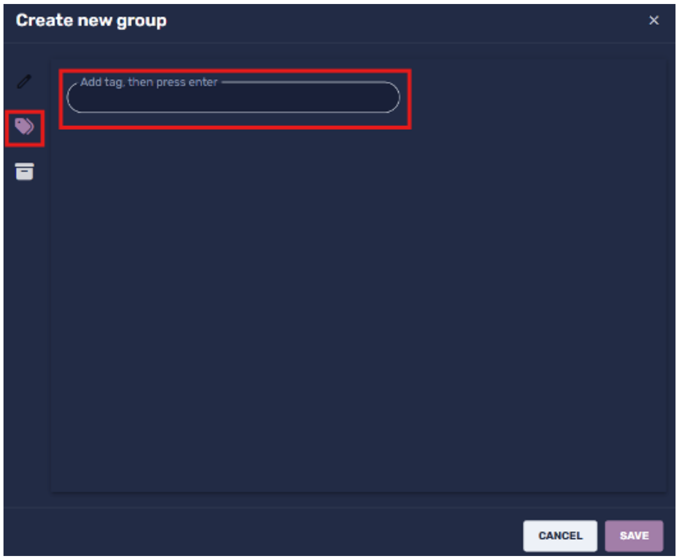


Group name: Newline Secure

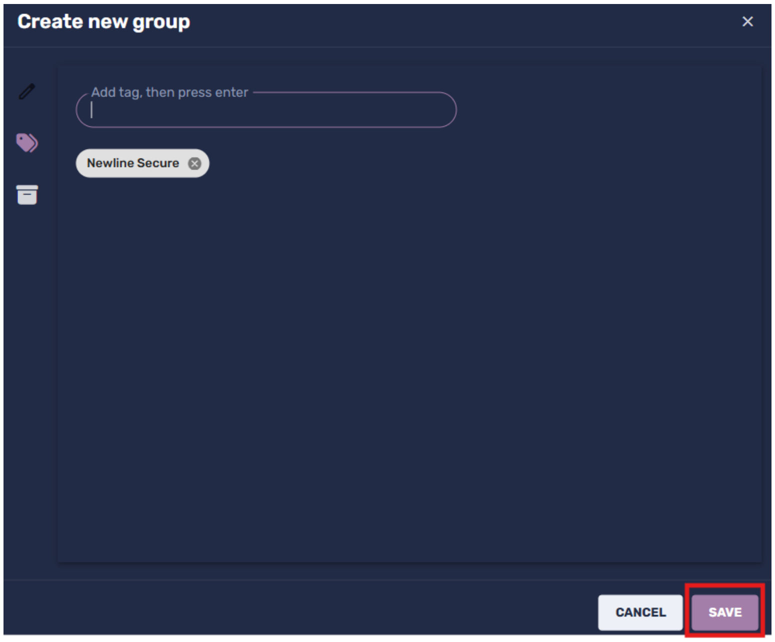
Group description

- Then navigate to the ‘Tags’ tab, from here you can create a new tag for the group or utilize an existing one.
  - If you are creating a new tag, type in a name and hit enter.

- If you are using an existing tag, select the one you would like to use.



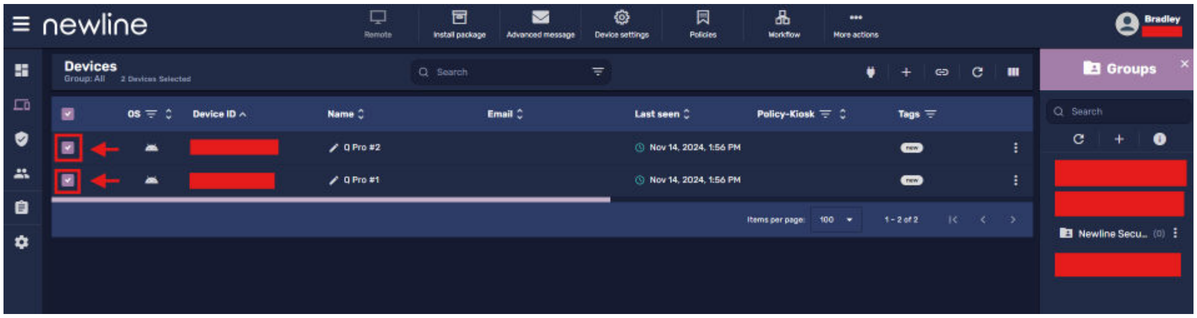
- Once you have decided on a tag to associate with your group, select Save to complete the creation of your Device Group in NDM.



Step 2: Add Devices to Your Group

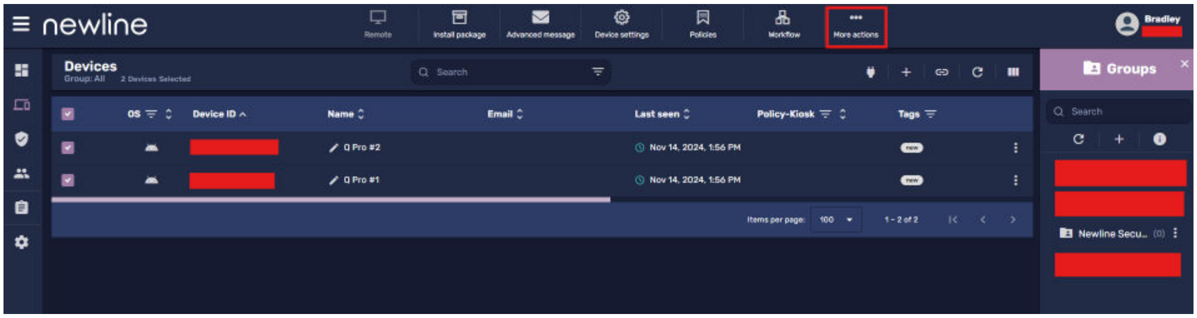
- To add devices to your newly created group, we have to add the associated tag to the devices we'd like to add.

- Start by selecting the devices from the dropdown that you'd like to add by clicking the box on the left
    - **Note: Only Newline Q Pro Series Panels are currently supported. For best performance and stability, please ensure that your Q Pro is on firmware v1.0.75 or higher.**



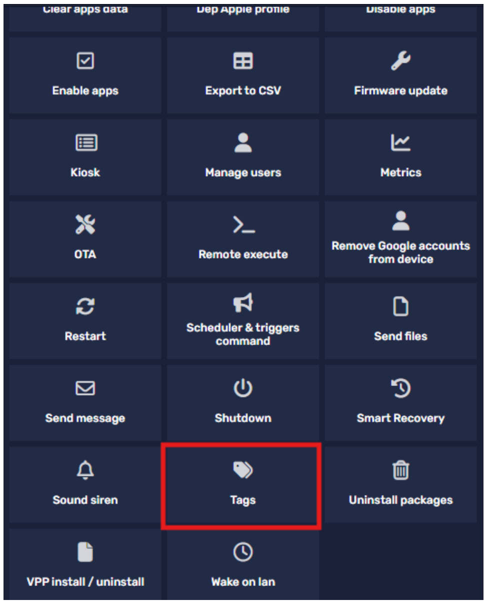
☑	OS	Device ID	Name	Email	Last seen	Policy-Kiosk	Tags
☑		[redacted]	Q Pro #2		Nov 14, 2024, 1:56 PM		new
☑		[redacted]	Q Pro #1		Nov 14, 2024, 1:56 PM		new

- After you've selected all of the devices, click the 'More Actions' button at the top

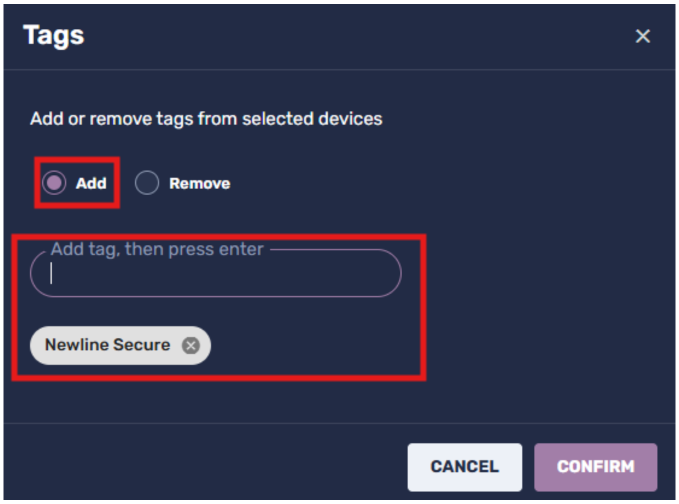


☑	OS	Device ID	Name	Email	Last seen	Policy-Kiosk	Tags
☑		[redacted]	Q Pro #2		Nov 14, 2024, 1:56 PM		new
☑		[redacted]	Q Pro #1		Nov 14, 2024, 1:56 PM		new

- Scroll down until you see the 'Tags' option and select it



- Make sure that 'Add' is selected, and input or select the tag that you associated with your Device group from the previous step.



Tags

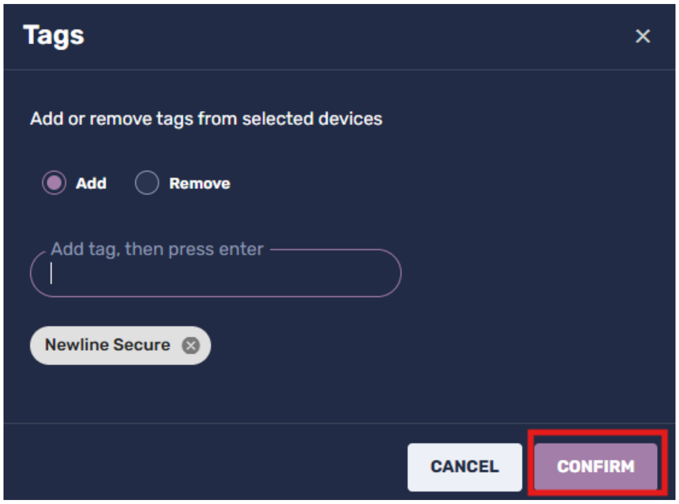
Add or remove tags from selected devices

● Add ○ Remove

Add tag, then press enter

Newline Secure

- Then select the 'Confirm' option to apply those tags.



Tags

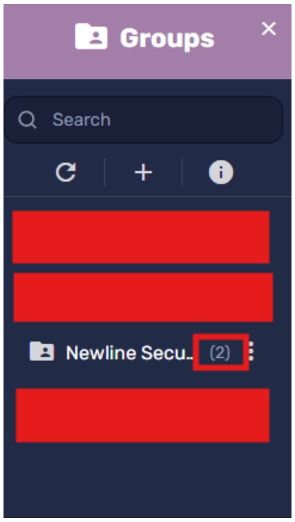
Add or remove tags from selected devices

● Add ○ Remove

Add tag, then press enter

Newline Secure

- You should see the number of devices in your group increase on the 'Groups' tab, if not, try refreshing your page to confirm that the devices were added.



[redacted]

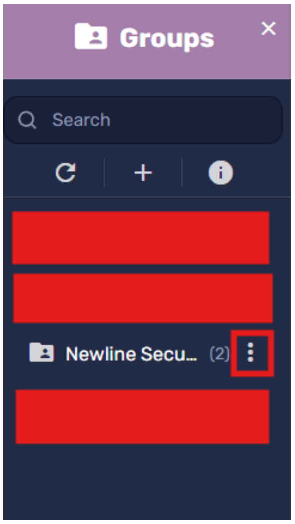
[redacted]

Newline Secu.. (2)

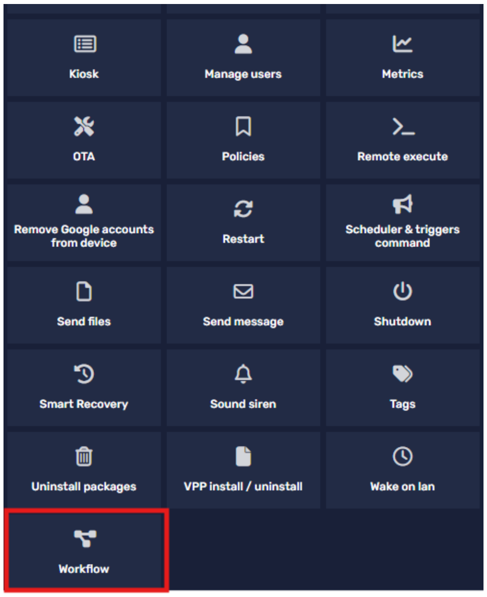
[redacted]

Step 3: Creating the Installation Workflow

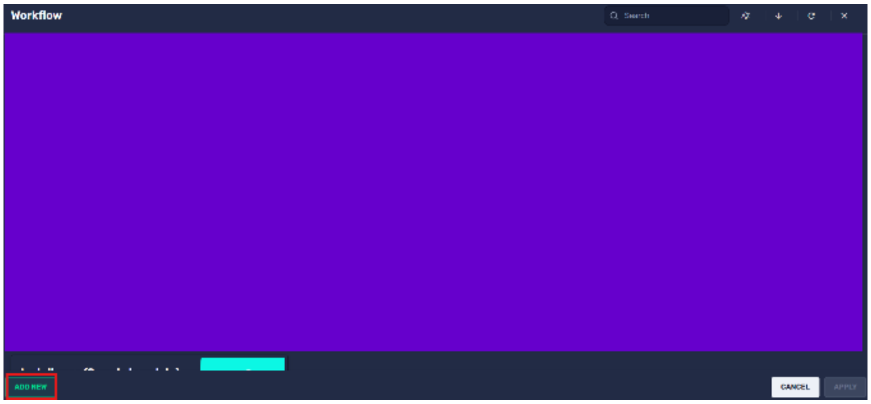
- In order to deploy Newline Secure to our newly created group, we'll need to first create a workflow.
- Select the 'Actions' button next to your 'Group' in the 'Groups' tab.



- Scroll down and select the ‘Workflow’ Option

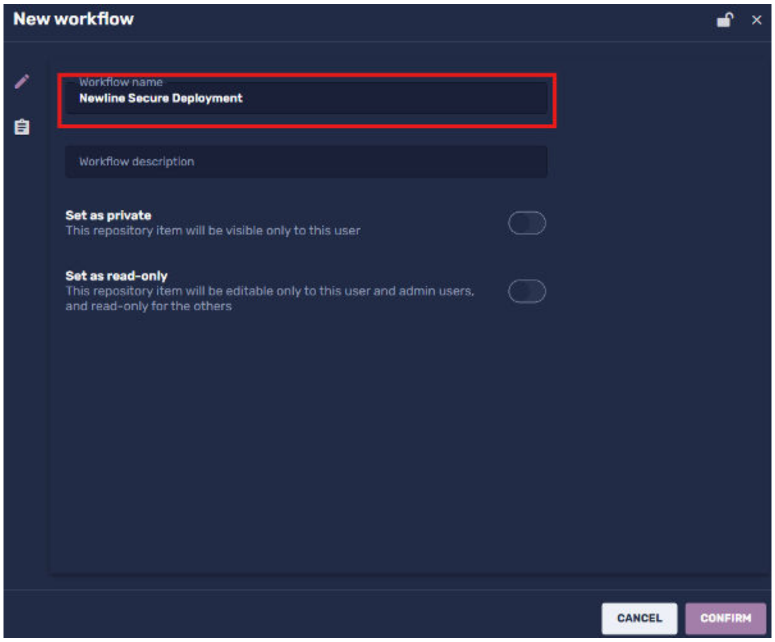


- Select ‘Add New’ in the bottom left hand corner.



[redacted]

- Start by typing a ‘Workflow Name’ (required) and a ‘Workflow Description’ (optional).



New workflow

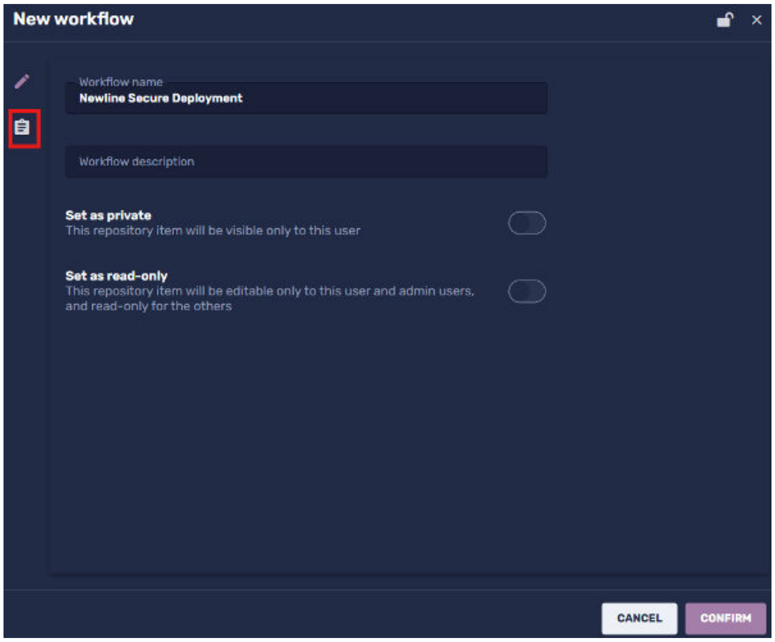
Workflow name
Newline Secure Deployment

Workflow description

Set as private
This repository item will be visible only to this user

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

- Next Select the ‘Commands” icon on the left



New workflow

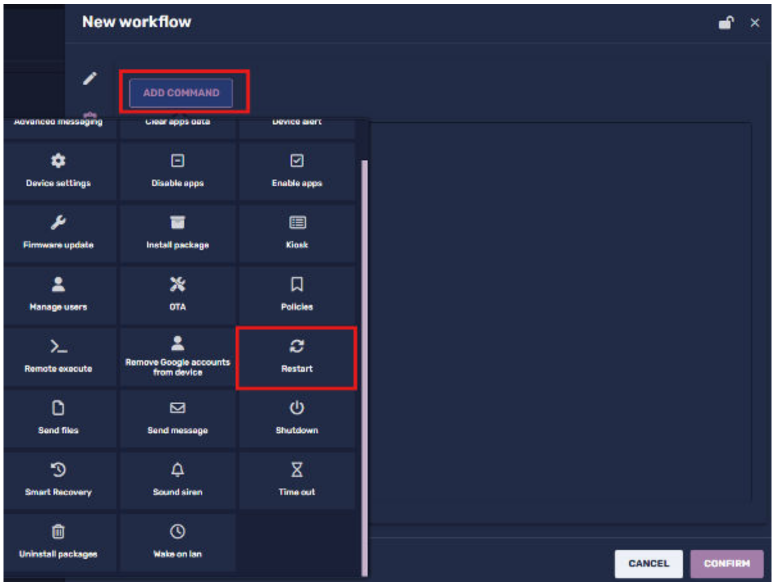
Workflow name: Newline Secure Deployment

Workflow description

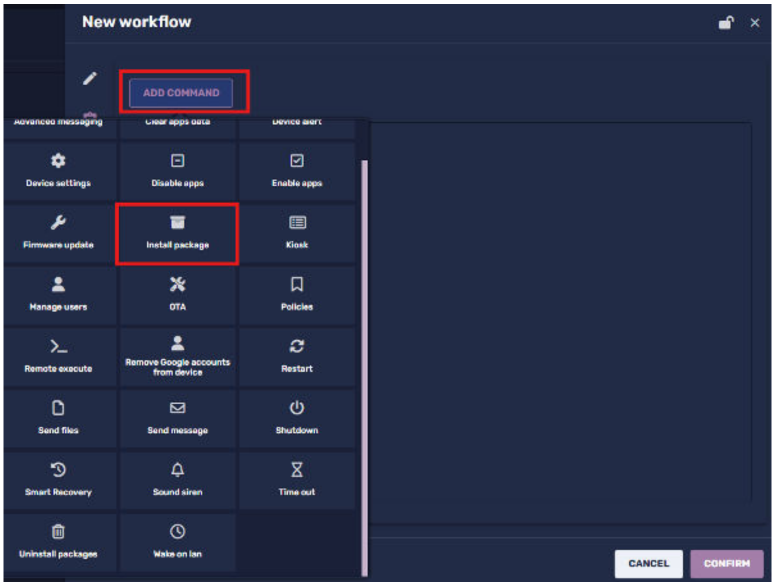
Set as private
This repository item will be visible only to this user

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

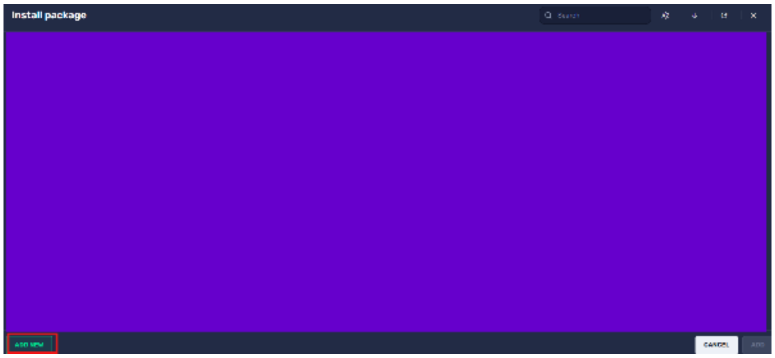
- Next select ‘Add Command’, and scroll down and select the ‘Restart’ option.



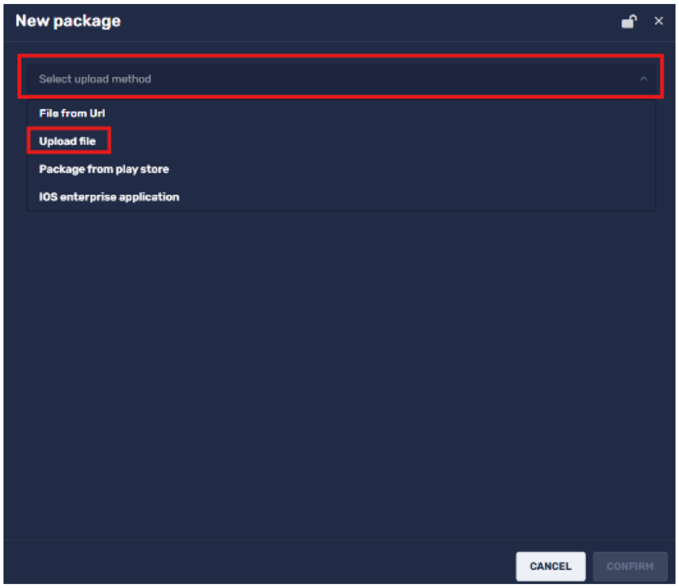
- Next select ‘Add Command’ again, and select the ‘Install Package’ option



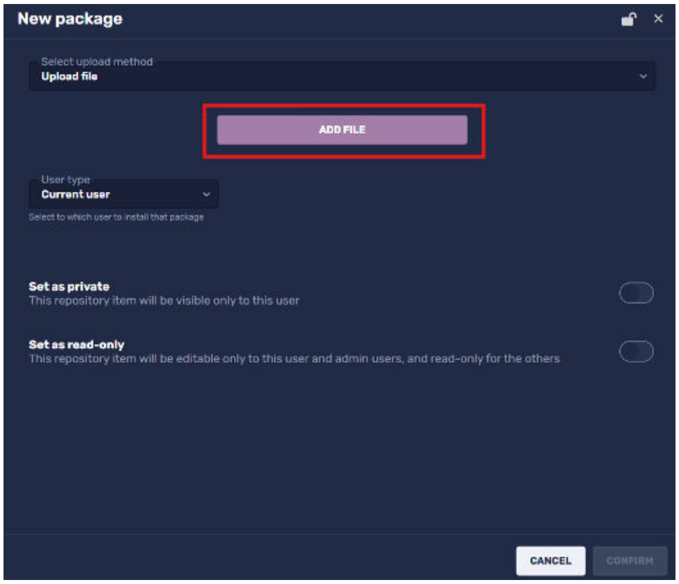
- Select 'Add New' in the bottom left corner



- Click the 'Select Upload Method' dropdown, and select 'Upload File'



- Select ‘Add File’ and choose the Newline Secure apk file that you downloaded (Note: If you don’t have the Newline Secure apk, please submit a ticket to our Newline Tech Support Team here!)
  - Once selected, it may take a moment to load the file


New package

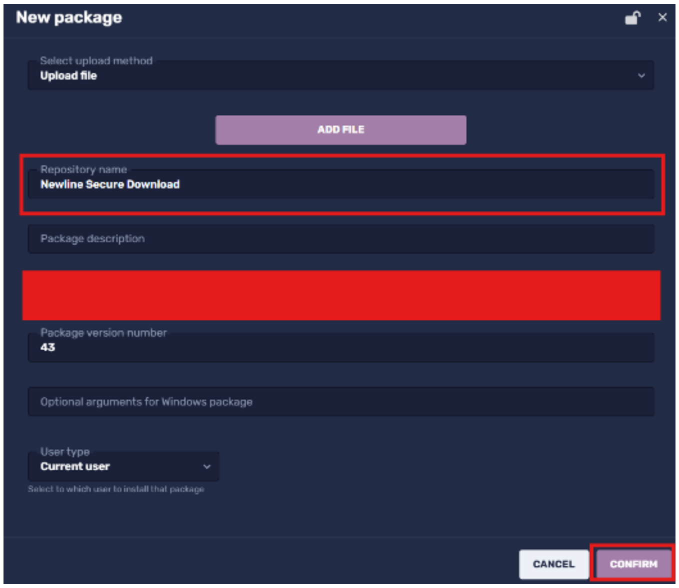
Select upload method: Upload file

User type: Current user
Select to which user to install that package

Set as private
This repository item will be visible only to this user

Set as read-only
This repository item will be editable only to this user and admin users, and read-only for the others

- Feel free to change the ‘Repository Name’ to whatever you’d like, then select ‘Confirm’


New package

Select upload method: Upload file

Repository name: Newline Secure Download

Package description

[redacted]

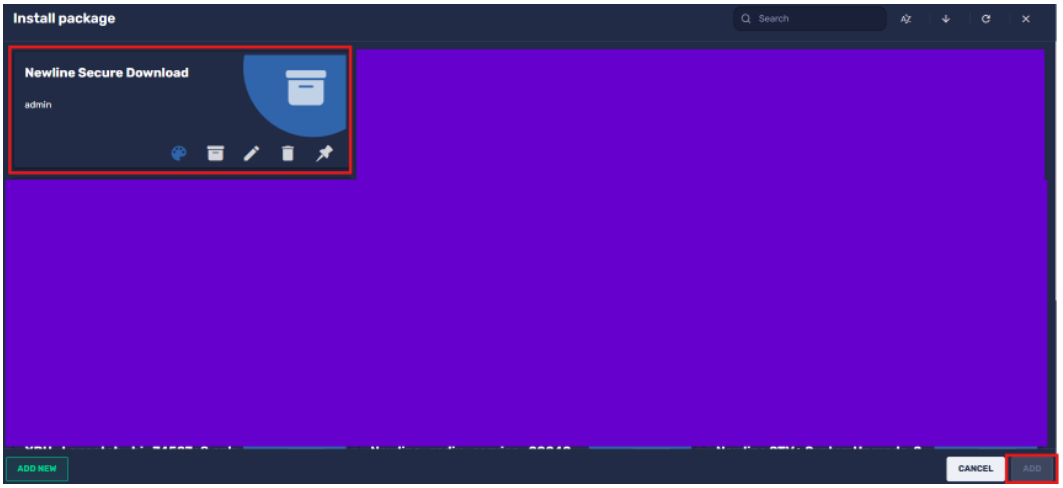
Package version number: 43

Optional arguments for Windows package

User type: Current user

Select to which user to install that package

- Now select your newly created repository and select ‘Add’ in the bottom right.

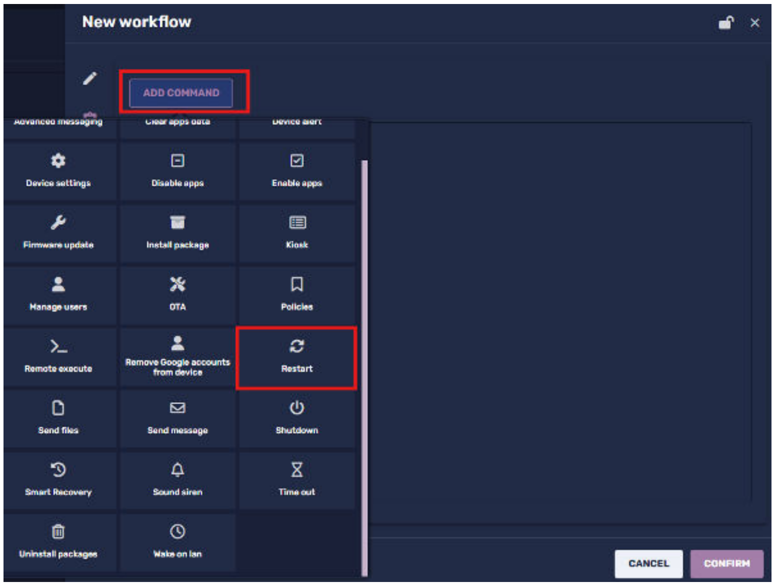

Install package

Newline Secure Download

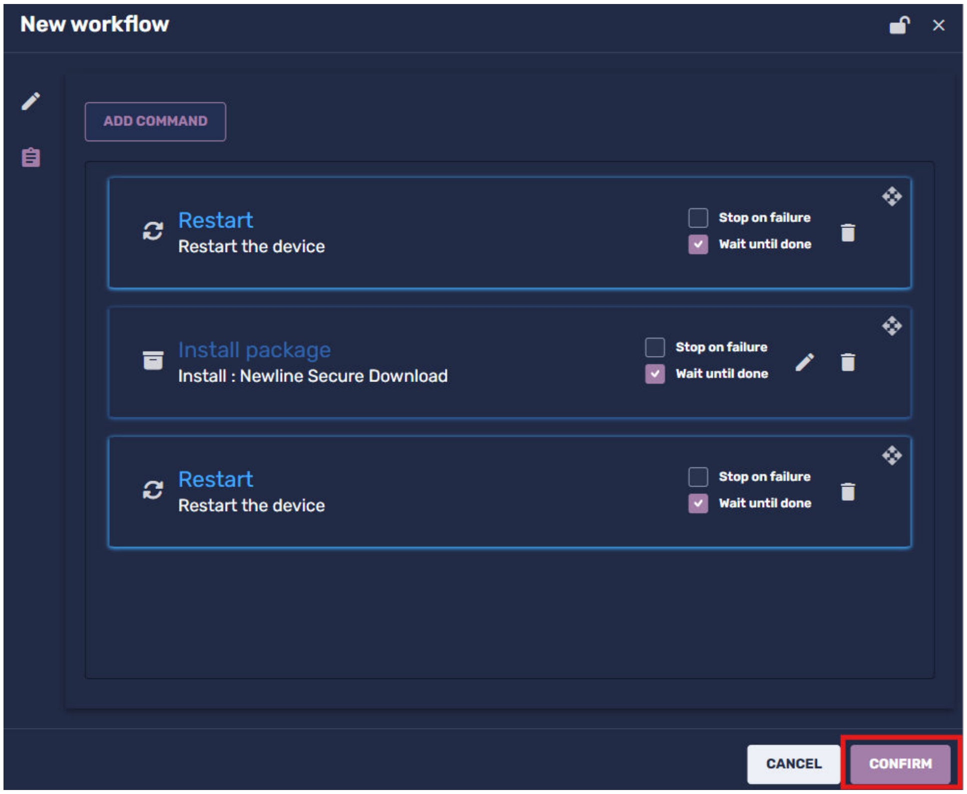
admin

[redacted]

- Finally select ‘Add Command’, and scroll down and select the ‘Restart’ option again.



- Your completed workflow should look like this:



New workflow

ADD COMMAND

Restart
Restart the device
□ Stop on failure
☑ Wait until done

Install package
Install : Newline Secure Download
□ Stop on failure
☑ Wait until done

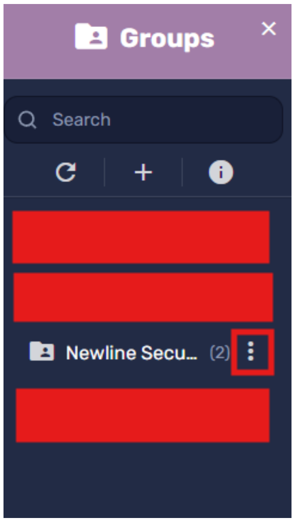
Restart
Restart the device
□ Stop on failure
☑ Wait until done

- Once you’ve double checked your ‘Workflow’, select ‘Confirm’

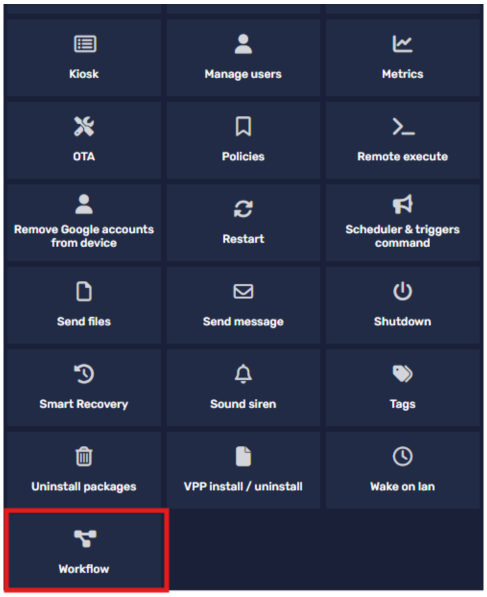
Step 4: Deploying the Workflow to Your Device Group

- Here is a brief explanation on the workflow that we just created in the previous step:
  - This workflow is designed to first restart the panel in order to ensure that the application is installed on the ‘Owner’ profile, then installs the Newline Secure apk while at the lock screen, and then restarts the panel again to complete the system registration process.
  - This workflow helps to ensure that no interaction at the panel is required in order for the mass deployment and activation of Newline Secure.

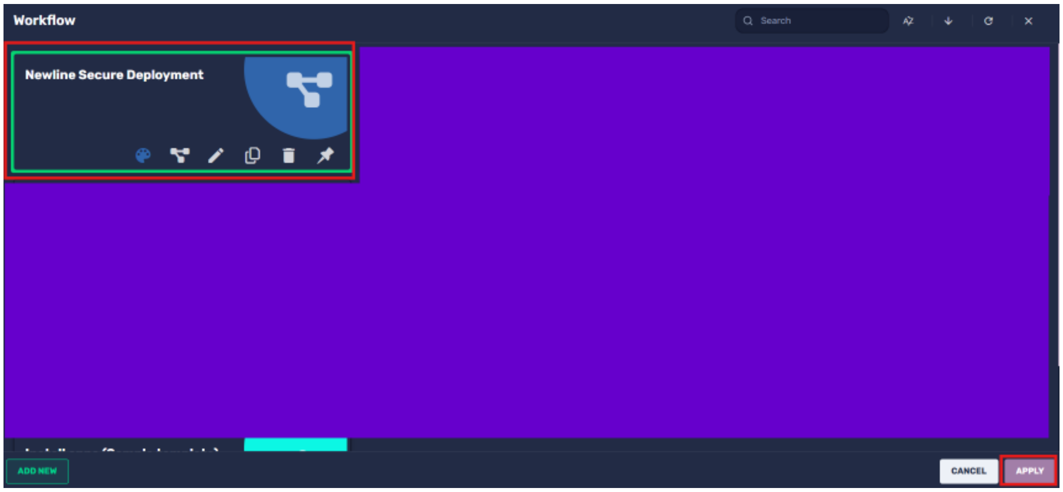
- We are now ready to deploy our Workflow to our Device Group via NDM.
- Select the ‘Actions’ button next to your ‘Group’ in the ‘Groups’ tab.



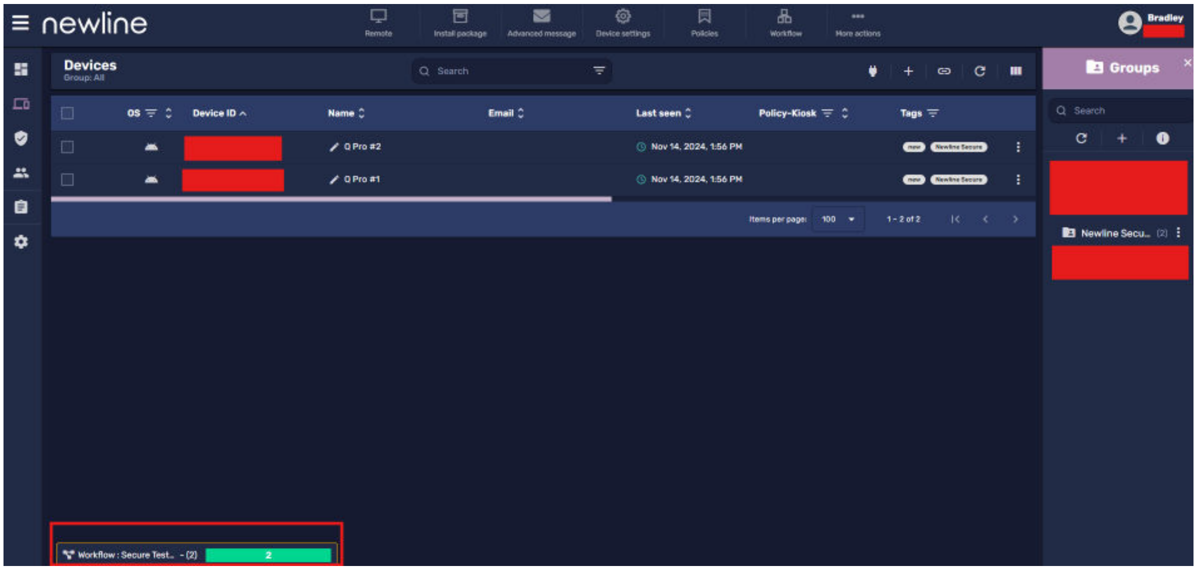
- Scroll down and select the ‘Workflow’ Option



- Select your newly created 'Workflow', and then select 'Apply'



- At the bottom left corner of the page, you can see the status of the workflow that was just sent.



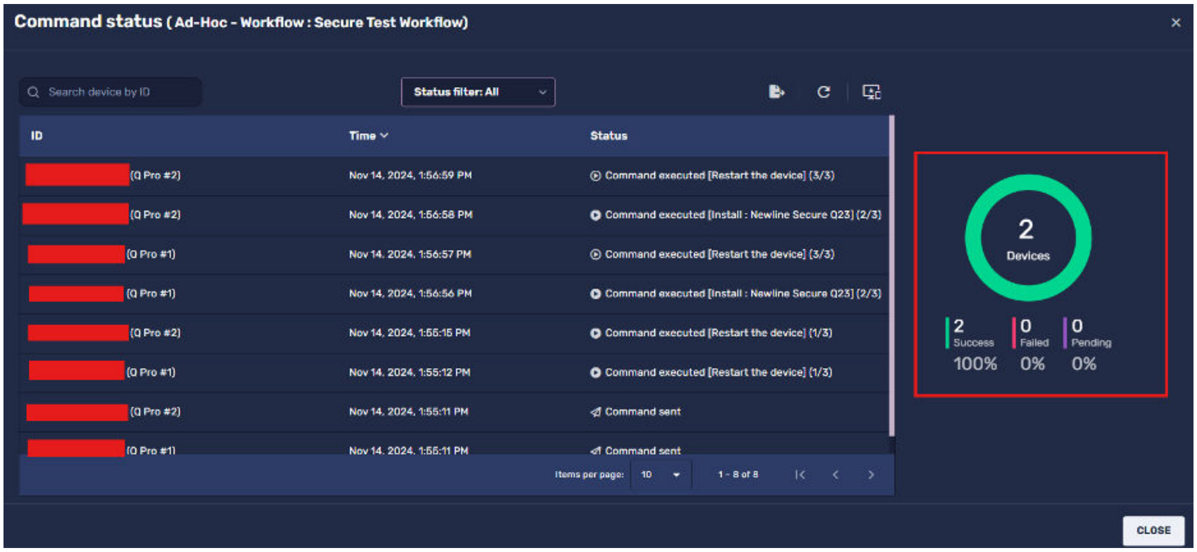
Devices
Group: All

OS	Device ID	Name	Email	Last seen	Policy-Kiosk	Tags
	[redacted]	Q Pro #2		Nov 14, 2024, 1:56 PM		new, Newline Secure
	[redacted]	Q Pro #1		Nov 14, 2024, 1:56 PM		new, Newline Secure

Items per page: 100 1 - 2 of 2

Workflow : Secure Test... - (2) 2

- Clicking on the workflow command will pull up a window showing a more detailed status
  - **Please ensure that the command is sent and reports successfully before attempting to send any alerts via Singlewire or Centegix**



Command status (Ad-Hoc - Workflow : Secure Test Workflow)

ID	Time	Status
[redacted] (Q Pro #2)	Nov 14, 2024, 1:56:59 PM	Command executed [Restart the device] (3/3)
[redacted] (Q Pro #2)	Nov 14, 2024, 1:56:58 PM	Command executed [Install : Newline Secure Q23] (2/3)
[redacted] (Q Pro #1)	Nov 14, 2024, 1:56:57 PM	Command executed [Restart the device] (3/3)
[redacted] (Q Pro #1)	Nov 14, 2024, 1:56:56 PM	Command executed [Install : Newline Secure Q23] (2/3)
[redacted] (Q Pro #2)	Nov 14, 2024, 1:55:15 PM	Command executed [Restart the device] (1/3)
[redacted] (Q Pro #1)	Nov 14, 2024, 1:55:12 PM	Command executed [Restart the device] (1/3)
[redacted] (Q Pro #2)	Nov 14, 2024, 1:55:11 PM	Command sent
[redacted] (Q Pro #1)	Nov 14, 2024, 1:55:11 PM	Command sent

Items per page: 10 1 - 8 of 8

2 Success	0 Failed	0 Pending
100%	0%	0%

- If the command reports successful, you have successfully mass-deployed and activated Newline Secure on the panels in your Device Group.

Step 5: Don’t Forget to Test Your Alerts

- Now that you’ve successfully gotten everything setup, registered, installed, and integrated, now you should test out your alerts and make sure that everything is functioning as expected.
    - Testing out your alerts will help you to ensure that all of your panels are properly receiving alerts and communicating with the Singlewire or Centegix systems.
    - This also allows you to make any changes that you may need to the Alert Background & Sound Level within the Newline Secure Console. (Remember that these backgrounds and sound levels will be applied **globally** to all of your panels.)

If you have questions or need assistance with Newline Secure or Mass Deployment via NDM, please contact Newline Technical Support:

- Submit a ticket here!
- Give us a call at +1 (833)-469-9520

If you have questions or need assistance with the Singlewire Portal, please contact Singlewire Support by submitting a ticket using the link below:

- https://support.singlewire.com/s/contactsupport

If you have questions or need assistance with the Centegix Portal, please contact Centegix Support by sending an email:

- support@centegix.com