



Everbridge Open User Guide

Everbridge Suite

July 2023

Everbridge Suite
2023
Printed in the USA

Copyright © 2023. Everbridge, Inc, Confidential & Proprietary. All rights are reserved. All Everbridge products, as well as NC4, xMatters, Techwan, Previstar, one2many, SnapComms, Nixle, RedSky, and Connexient, are trademarks of Everbridge, Inc. in the USA and other countries. All other product or company names mentioned are the property of their respective owners. No part of this publication may be reproduced, transcribed, or transmitted, in any form or by any means, and may not be translated into any language without the express written permission of Everbridge.

Limit of Liability/Disclaimer of Warranty: Everbridge makes no representations or warranties of any kind with respect to this manual and the contents hereof and specifically disclaims any warranties, either expressed or implied, including merchantability or fitness for any particular purpose. In no event shall Everbridge or its subsidiaries be held liable for errors contained herein or any damages whatsoever in connection with or arising from the use of the product, the accompanying manual, or any related materials. Further, Everbridge reserves the right to change both this publication and the software programs to which it relates and to make changes from time to time to the content hereof with no obligation to notify any person or organization of such revisions or changes.

This document and all Everbridge technical publications and computer programs contain the proprietary confidential information of Everbridge and their possession and use are subject to the confidentiality and other restrictions set forth in the license agreement entered into between Everbridge and its licensees. No title or ownership of Everbridge software is transferred, and any use of the product and its related materials beyond the terms on the applicable license, without the express written authorization of Everbridge, is prohibited.

If you are not an Everbridge licensee and the intended recipient of this document, return to Everbridge, Inc., 155 N. Lake Avenue, Pasadena, CA 91101.

Export Restrictions: The recipient agrees to comply in all respects with any governmental laws, orders, other restrictions ("Export Restrictions") on the export or re-export of the software or related documentation imposed by the government of the United States and the country in which the authorized unit is located. The recipient shall not commit any act of omission that will result in a breach of any such export restrictions.

Everbridge, Inc.
155 N. Lake Avenue, 9th Floor
Pasadena, California 91101 USA
Toll-Free (USA/Canada) +1.888.366.4911

Visit us at www.everbridge.com

Everbridge software is covered by US Patent Nos. 6,937,147; 7,148,795; 7,567,262; 7,623,027; 7,664,233; 7,895,263; 8,068,020; 8,149,995; 8,175,224; 8,280,012; 8,417,553; 8,660,240; 8,880,583; 9,391,855. Other patents pending.

Overview	4
Everbridge Open.....	5
Email Ingestion.....	6
Setting Up an Integration	7
Viewing Emails	17
Response Subscriptions	20
Setting Up Response Subscription Profiles	20
Enabling Response Subscriptions in Your Incident Templates	22
Reviewing the Usage Logs of Your Response Subscriptions.....	24
Safety iPaaS Connectors.....	25
IT Alerting iPaaS Connectors.....	26
Other Safety Connectors	27
Risk Events.....	28

Overview

Everbridge Open offers an extensive suite of integration options for our Critical Event Management (CEM) platform. The Everbridge Open two-way capabilities allow third-party systems to create powerful closed-loop integrations with our platform. Everbridge Open is used by partners to build integrations for our mutual customers and by our customers for their own proprietary use cases.

Everbridge Open

Everbridge Open consists of the following four types to build your integrations. Depending on the integration, you can use the integration type that best meets your needs:

- Risk Event Interface (REI)
- iPaaS (integration Platform as a Service)
- Public REST API
- Email Ingestion

Email Ingestion

Email Ingestion functionality provides Administrators with the capability to set up an integration between Everbridge Suite and a third-party alerting application. Everbridge Suite ingests an email from a third-party application, parses the email, and launches an Incident.

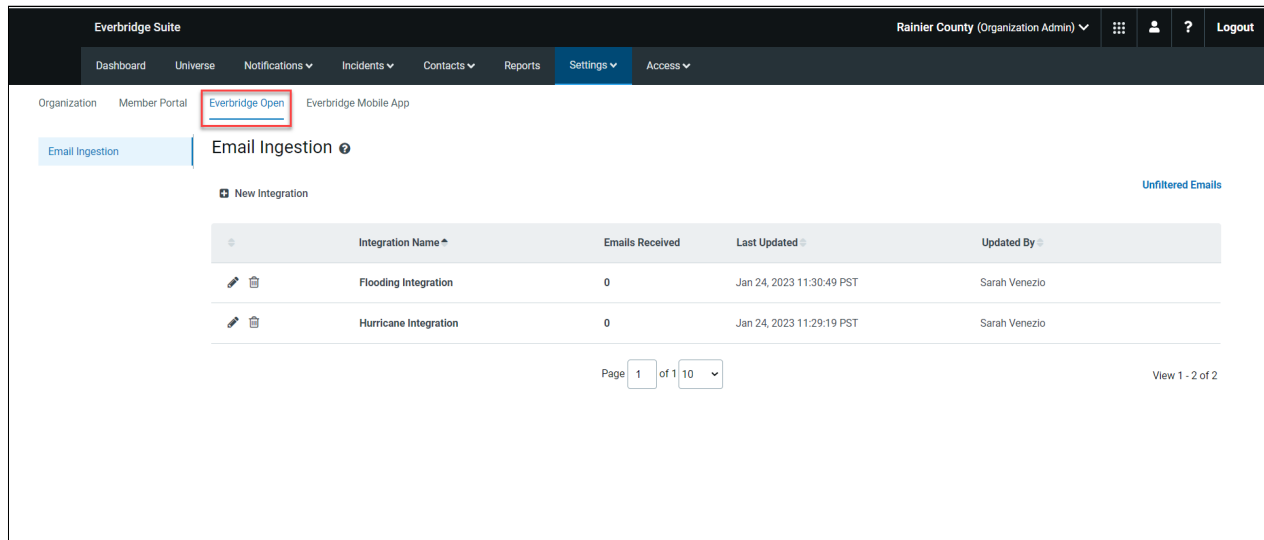
The Administrator determines the parsing criteria. The user selects certain words from the email that can be mapped to a specific variable in the Incident template. For example, the user can indicate that the phrase "Affected Area" from the email be mapped to a custom variable in the template called "Location" or the "Severity-p2" from the email be mapped to a variable called "Severity."

NOTE:

1. In this version of Email Ingestion, the integration can launch a new Incident when an email trigger has been received by Everbridge. Currently, "Update" and "Close" of an Incident via Email Ingestion is not supported.
2. For incoming emails, Everbridge Email Ingestion functionality supports Plain Text mode. If emails are sent to Everbridge Email Server (MailGun) in HTML mode, MailGun strips all HTML tags and generates a plain text body for Everbridge Suite. In this process, MailGun converts all smart characters into their plain counterparts, such as - becomes -, o becomes *, and so forth.

Setting Up an Integration

From the **Settings** tab, select the **Everbridge Open** tab. Then select **Email Ingestion** from the left-hand pane. The Email Ingestion list of existing integrations is displayed.



To add an integration:

1. From the **Settings** tab, select the **Everbridge Open** tab.
2. From the Everbridge Open tab, select **Email Ingestion**.
3. Click **New Integration**. The New Integration dialog is displayed.

4. Type an Integration Name and press TAB.
5. Fill in the fields for **When an email is...**:
 - Sent from: Type a case-sensitive email address from which the email will be sent to Everbridge. You can use the wild card character (*) in the account/username part of the email address. For example, *@everbridge.com, 12223345*@domain.com, or *12234@domain.com. The domain (in this example, "domain.com", never changes
 - And received at: Type the case-sensitive *username-880038799094@everbridge.com*. (The *username* can be any custom text. The *username* and 12-digit number will be different for your Organization.)
 - Click Copy to copy this email address to the Clipboard.
6. Define the conditions for the incoming email. You can define only the conditions that meet ALL requirements, or only conditions that meet ANY requirements, or meets both ALL and ANY requirements.
7. Meets ALL of these requirements (using 0-10):
 - From the left-most drop-down list, select Email Subject, Email Body, or Text Attachments.
 - From the center drop-down list, select the condition: Contains, Exactly Matches, Starts With, or Ends With.
 - From the right-most text box, type the value of the condition.
 - Optionally, select the link: Add another to add another requirement.
 - Meets ANY of these requirements (using 0-10):

- From the left-most drop-down list, select Email Subject, Email Body, or Text Attachments.
 - From the center drop-down list, select the condition: Contains, Exactly Matches, Starts With, or Ends With.
 - From the right-most text box, type the value of the condition.
 - Optionally, select the link: Add another to add another requirement.
8. From **Launch the Incident...**, select the link: Select an Incident template. The Select an Incident Template dialog appears.

Select an incident template ✕

Name	Category	
<input type="radio"/> Ad Hoc Incident Template	--	Select an incident template
<input type="radio"/> Ad-Hoc IPAWS Template	IPAWS Alert	
<input type="radio"/> Wildfire Evacuation IPAWS Alert - WEA & EAS	IPAWS Alert	
<input type="radio"/> IPAWS Monthly Test - WEA ONLY	IPAWS Alert	
<input type="radio"/> IPAWS Monthly Test - WEA & EAS	IPAWS Alert	
<input type="radio"/> Planned Outage	Scheduling	
<input type="radio"/> Hurricane Alert	Severe Weather	
<input type="radio"/> Hurricane Evacuation	Severe Weather	
<input type="radio"/> Flooding	Severe Weather	
<input type="radio"/> Hurricane Warning	Severe Weather	

Page of 2 > >>

9. Select the radio button indicating the desired Incident template from the list in the left-hand pane. The selected Incident template is displayed on the

right-hand pane.

Select an incident template
✕

Name	Category
<input type="radio"/> Ad Hoc Incident Template	---
<input type="radio"/> Ad-Hoc IPAWS Template	IPAWS Alert
<input type="radio"/> Wildfire Evacuation IPAWS Alert - WEA & EAS	IPAWS Alert
<input type="radio"/> IPAWS Monthly Test - WEA ONLY	IPAWS Alert
<input type="radio"/> IPAWS Monthly Test - WEA & EAS	IPAWS Alert
<input type="radio"/> Planned Outage	Scheduling
<input checked="" type="radio"/> Hurricane Alert	Severe Weather
<input type="radio"/> Hurricane Evacuation	Severe Weather
<input type="radio"/> Flooding	Severe Weather
<input type="radio"/> Hurricane Warning	Severe Weather

Page of 2 > >>
View 1 - 10 of

Cancel
OK

Hurricane Alert

Created On: Jul 01, 2022 02:53:18 PDT

Last Updated: Jul 01, 2022 02:53:18 PDT

Updated By: John Smith

PREVIEW: TITLE

Hurricane Alert

BODY

This is a test {Category}

Category:

Body - English:

- Click **OK**. The selected Incident Template will appear at the bottom of the page under the **Launch Incident** header.

Everbridge Suite Rainier County (Organization Admin) ? Logout

Dashboard Universe Notifications Incidents Contacts Reports Settings Access

Organization Member Portal Everbridge Open Everbridge Mobile App

Email Ingestion | Email Ingestion > New Integration

*Integration Name: Hurricane Integration

WHEN AN EMAIL IS

*Sent from: no-reply@everbridge.net

*And received at: customerlearning@453003085616326@integration.everbridge.us Copy

AND MEETS

ALL of these requirements:

Email Subject Contains Hurricane

+ Add another (Using 1 of 10)

AND

ANY of these requirements:

+ Add (Using 0 of 10)

LAUNCH THE INCIDENT

Hurricane Alert: [Change](#)

Map Incident Variables

Indicate where the variable's value should go within the email source.

Variable Name	Incoming Source	Regular Expression	Location in Source
<input type="checkbox"/> Category	-Select	<input type="checkbox"/>	Text before (Category) Text after
<input type="checkbox"/> Body - English	-Select	<input type="checkbox"/>	Text before (Body - English) Text after

Override template contact selections with the ones selected below.

[> Override Template Options](#)

[> Test Variables](#)

Automatically close the incident after successful launch

Save Cancel

11. As needed, select the following for each desired Incident variable:

Variables that are required in the Incident template must be mapped. You cannot clear the checkbox. The checkboxes of optional variables can be cleared. You do not have to map optional variables. You can map an optional variable by selecting the checkbox.

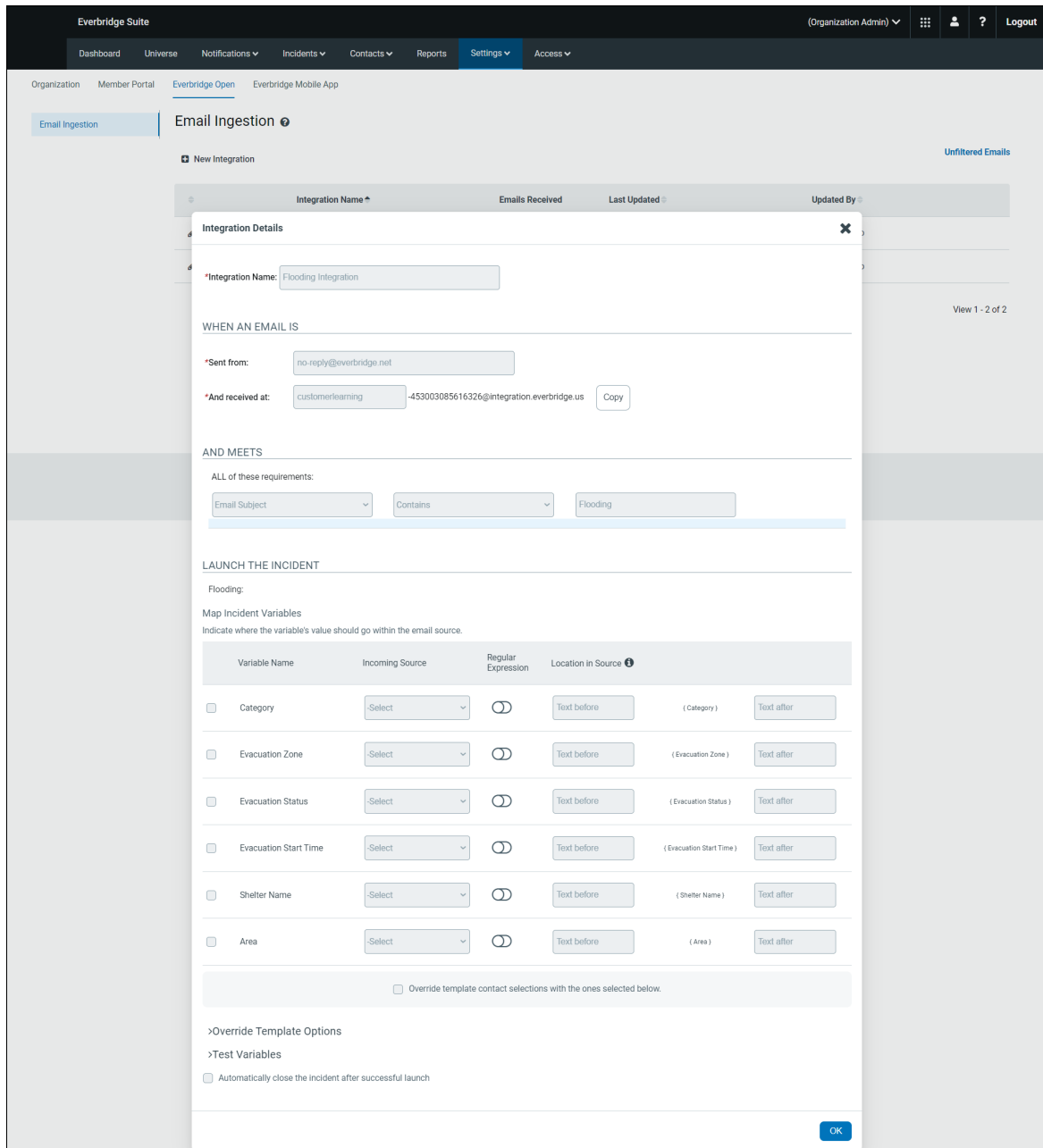
- Select the checkbox if you want to use the variable to the right of the checkbox.
- From the drop-down list, the Incoming Source: Email Subject, Email Body, or Text Attachments.
- If your Incoming Source field is "To" (an email address), check the format of the field and craft your Regular Expressions accordingly to match the desired text section. Alternatively, you can use an exact "contains" match.
- Toggle ON to Use a Regular Expression. Then, in the Location in Source field, enter the regular expression.

- Location in Source (Text before and Text after): Refers to the text that surrounds the variable information in the email. You can use words as well as punctuation to specify the location. The more specific the “before” and “after” text, the easier to pull the variable from the source.
- Optionally, select the checkbox: Override template contact selections with the ones selected below and fill in as needed.
 - When parsing contacts, the External ID is used. In other words, you can parse contacts by providing the External ID in the email.
 - When parsing groups, the Group Name is used. In other words, you can parse groups by providing the Group Name in the email.
 - When parsing rules, the Rule Name is used. In other words, you can parse rules by providing the Rule Name in the email.
- Test Variables: Select the Test Variables link to test your Regular Expressions. See the following **Regular Expression** considerations.
 - A Regular Expression match uses Case Sensitive mode.
 - A Regular Expression match uses MultiLine mode. The match is done within one line so ^ and\$ can be used to match the beginning and end of a line rather than the whole input.
 - Regular Expression uses DOTALL mode, which makes dot (.) to match new lines. This allows multiline chunks of text to be grabbed.
 - A Regular Expression match matches the first group if at least one group exists. Otherwise, it matches the whole text. This is done to be able to extract chunks of text.
- Optionally, select the checkbox: **Automatically close the Incident after a successful launch.**

12. Click **Save** when done.

To view an existing integration:

1. From the Everbridge Open tab, select **Email Ingestion**.
2. From the table, select the desired integration by clicking its name. (Or, if this integration is triggered as an Incident, click the integration name on the Incident Details page.) The Integration Details dialog is displayed.



3. Review the fields of the selected integration.
4. Click **OK**.

To modify an existing integration:

1. From the Everbridge Open tab, select **Email Ingestion**.
2. From the table, select the desired integration by clicking the **Pencil** icon. The Edit Integration dialog is displayed.

Everbridge Suite (Organization Admin) ? Logout

Dashboard Universe Notifications Incidents Contacts Reports Settings Access

Organization Member Portal Everbridge Open Everbridge Mobile App

Email Ingestion > Edit Integration

*Integration Name: Flooding Integration

WHEN AN EMAIL IS

*Sent from: no-reply@everbridge.net

*And received at: customerlearning -453003085616326@integration.everbridge.us Copy

AND MEETS

ALL of these requirements:

Email Subject Contains Flooding

Add another (Using 1 of 10)

AND

ANY of these requirements:

Add (Using 0 of 10)

LAUNCH THE INCIDENT

Flooding: [Change](#)

Map Incident Variables

Indicate where the variable's value should go within the email source.

Variable Name	Incoming Source	Regular Expression	Location in Source
<input type="checkbox"/> Category	-Select	<input type="radio"/>	Text before (Category) Text after
<input type="checkbox"/> Evacuation Zone	-Select	<input type="radio"/>	Text before (Evacuation Zone) Text after
<input type="checkbox"/> Evacuation Status	-Select	<input type="radio"/>	Text before (Evacuation Status) Text after
<input type="checkbox"/> Evacuation Start Time	-Select	<input type="radio"/>	Text before (Evacuation Start Time) Text after
<input type="checkbox"/> Shelter Name	-Select	<input type="radio"/>	Text before (Shelter Name) Text after
<input type="checkbox"/> Area	-Select	<input type="radio"/>	Text before (Area) Text after

Override template contact selections with the ones selected below.

[> Override Template Options](#)

[> Test Variables](#)

Automatically close the incident after successful launch

Save Cancel

3. Optionally, change the Integration Name.
4. As needed, change the fields for **When an email is...**
 - **Sent from:** Type a case-sensitive email address. You can use the wild card character (*) in the account/username part of the email address. For example, *@domain.com, 12223345*@domain.com, or *12234@domain.com. The domain (in this example, "domain.com", never changes.
 - **And received at:** This is a read-only field. To update this field with a different case-sensitive email address, create a new integration.
 - Click **Copy** to copy this email address to the Clipboard.

5. Define the conditions for the incoming email. You can define only the conditions that meet ALL requirements, or only conditions that meet ANY requirements, or meets both ALL and ANY requirements.
 - Meets ALL of these requirements (using 0-10):
 - From the left-most drop-down list, select Email Subject, Email Body, or Text Attachments.
 - From the center drop-down list, select the condition: Contains, Exactly Matches, Starts With, or Ends With.
 - From the right-most text box, type the value of the condition.
 - Optionally, select the link: Add another to add another requirement.
 - Meets ANY of these requirements (using 0-10):
 - From the left-most drop-down list, select Email Subject, Email Body, or Text Attachments.
 - From the center drop-down list, select the condition: Contains, Exactly Matches, Starts With, or Ends With.
 - From the right-most text box, type the value of the condition.
 - Optionally, select the link: Add another to add another requirement.
 6. From **Launch the Incident...**, click **Select an Incident template**. The Select an Incident Template dialog appears.
 7. Select the radio button indicating the desired Incident template from the list in the left-hand pane. The selected Incident template is displayed on the right-hand pane.
 8. Click **OK**.
 9. As needed, select the following for each desired Incident variable:
 - Select the checkbox if you want to use the variable to the right of the checkbox.
 - From the drop-down list, the Incoming Source: Email Subject, Email Body, or Text Attachments.
 - If your Incoming Source field is "To" (an email address), check the format of the field and craft your Regular Expressions accordingly to match the desired text section. Alternatively, you can use an exact "contains" match.
 - Toggle ON to Use a Regular Expression. Then, in the Location in Source field, enter the regular expression.
 - Location in Source (Text before and Text after): Refers to the text that surrounds the variable information in the email. You can use words as well as punctuation to specify the location. The more specific the "before" and "after" text, the easier to pull the variable from the source.
 - Optionally, select the checkbox: Override template contact selections with the ones selected below and fill in as needed.
 10. Test Variables: Select the Test Variables link to test your Regular Expressions. See the following **Regular Expression** considerations.
-
-
-

- A Regular Expression match uses Case Sensitive mode.
- A Regular Expression match uses MultiLine mode. The match is done within one line so ^ and\$ can be used to match the beginning and end of a line rather than the whole input.
- Regular Expression uses DOTALL mode, which makes dot (.) to match new lines. This allows multiline chunks of text to be grabbed.

NOTE: A Regular Expression match matches the first group if at least one group exists. Otherwise, it matches the whole text. This is done to be able to extract chunks of text.

11. Optionally, select the checkbox: Automatically close the Incident after a successful launch.
12. Click **Save**.

To delete an integration:

1. From the list of integrations, click the **a** of the integration to be deleted.
2. Click **Yes** to confirm the deletion.

Viewing Emails

To view unfiltered emails:

1. From the **Email Ingestion** page, select **Unfiltered Emails**. The Unfiltered Emails dialog is displayed, showing the list of the ingestion times.

Ingestion Time	View Raw Email
2015-07-23 12:10:10 PDT	2:11
2015-07-07 11:26:33 PDT	<no subject>
2015-03-26 10:28:44 PDT	Fire emergency and smoke

Page 1 of 10 View 1 - 3 of 3

OK

2. Click the link under the View Raw Email column next to the desired ingestion time. The individual View Raw Email dialog is displayed. (See also [step 3](#) of the procedure [To view email received: All/Successes/Failures.](#))

View Raw Email

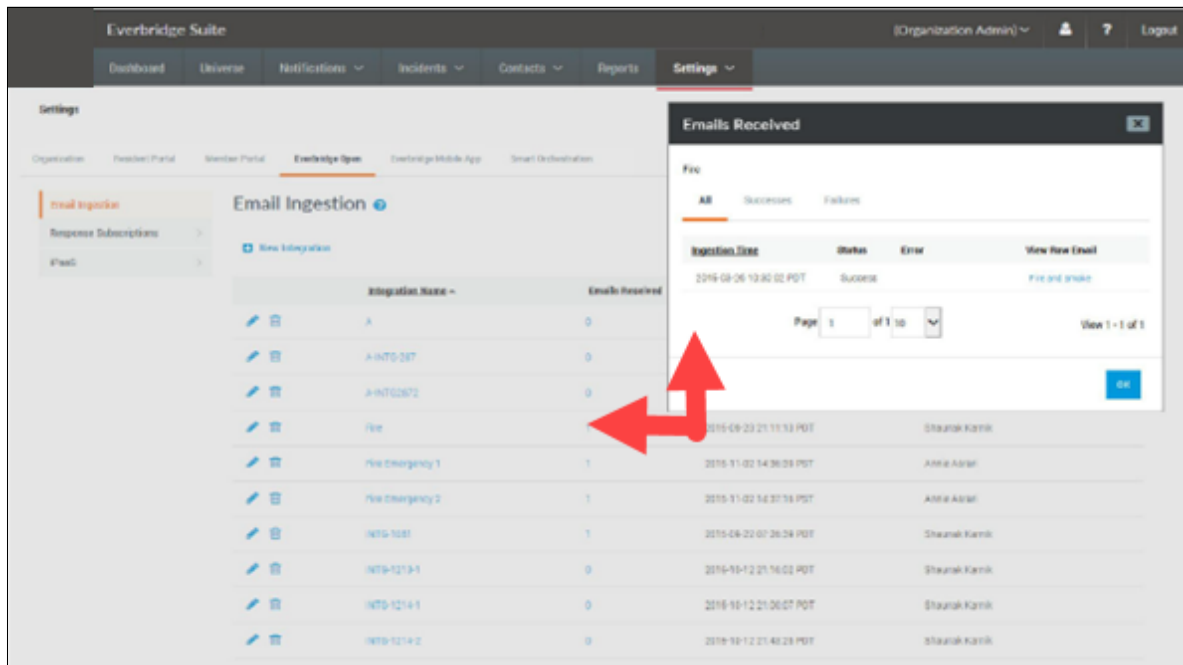
From: Annie Asrari <annie.asrari@everbridge.com>
To: annie-448605039099909@qa1.everbridge.us
Subject: Fire emergency and smoke
Location: Natick, MA.

OK

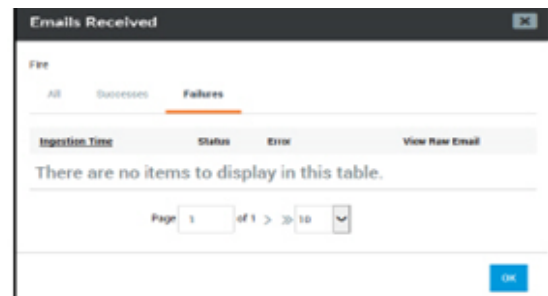
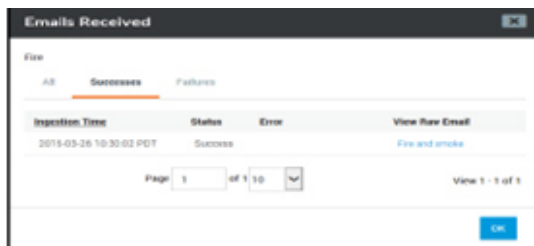
3. Review the email, then click **OK**. You are returned to the Unfiltered Emails dialog.
4. Click **Close**.

To view email received: All/Successes/Failures:

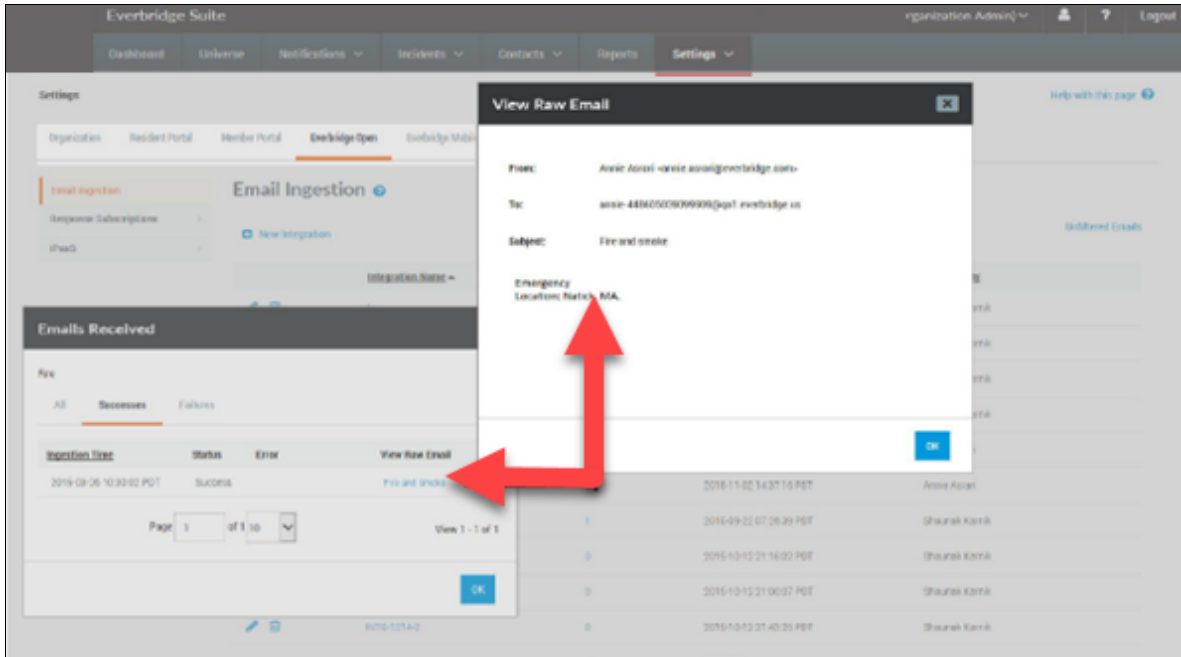
1. From the Email Ingestion page, select the number next to the desired Integration Name. This number indicates the number of emails that have been received regarding an integration. The Emails Received dialog is displayed with the All sub-tab in focus.



2. Optionally, select the Successes and/or Failures sub-tabs to see those lists.



3. Click the link: View Raw Email next to the desired ingestion time. The individual View Raw Email dialog is displayed. (See also [Step 2](#) of the procedure [To view unfiltered emails.](#))



4. Review the email, then click OK.

Response Subscriptions

Setting Up Response Subscription Profiles

From the Settings tab, select the **Everbridge Open** tab. Then select **Profiles** from the left-hand pane. The list of Response Subscriptions: Profiles is displayed.

Each profile must include at least one webhook.

Add a Response Subscription: Profile

To add a Response Subscription: Profile

1. From the **Settings** tab, select the **Everbridge Open** tab.
2. From the **Everbridge Open** tab, select **Response Subscriptions: Profiles**.
3. Click **New Profile**. The **Response Subscriptions: Create/Edit Profile** dialog is displayed.
4. Type a profile name.
 - If they exist, a list of available webhooks is displayed.
 - Click **Add** if you have not yet created any webhooks.
5. Select the check boxes of the webhooks you want used in this profile.
6. Click **Save**.

Edit a Response Subscription: Profile

To edit a Response Subscription: Profile

1. From the **Settings** tab, select the **Everbridge Open** tab.
2. From the **Everbridge Open** tab, select **Response Subscriptions: Profiles**.
3. Click the Pencil icon next to the Profile you want to modify.
4. Perform the steps in the procedure [To add a Response Subscription: Profile](#).

Delete a Response Subscription: Profile

To delete a Response Subscription: Profile

1. From the **Settings** tab, select the **Everbridge Open** tab.
 2. From the **Everbridge Open** tab, select **Response Subscriptions: Profiles**.
 3. Click the Trash Bin of the profile you want to delete.
 4. Confirm the deletion.
-
-
-

Add a Response Subscription: Webhook

To add a Response Subscription: Webhook

1. From the **Settings** tab, select the **Everbridge Open** tab.
2. From the **Everbridge Open** tab, select **Response Subscriptions: Webhooks**.
The list of webhooks is displayed.
 - Each webhook displays its webhook name, URL, username, and password (secured).
3. Click **New Webhook**. The **Create/Edit Webhook** dialog is displayed.
4. Type a name for your webhook and press TAB.
5. Type a Callback URL for the webhook and press TAB.
6. Select either of the **Callback Format** radio buttons:
 - **JSON**
 - **XML**.
 - Everbridge can send the responses to the webhook in either JSON or XML format.
7. Optionally, type a Username and Password for the webhook.
8. Click **OK**. Each webhook that you create becomes available for use in the Profiles.

Edit a Response Subscription: Webhook

To edit a Response Subscription: Webhook

1. From the **Settings** tab, select the **Everbridge Open** tab.
2. From the **Everbridge Open** tab, select **Response Subscriptions: Webhooks**.
3. Click the Pencil icon next to the webhook you want to modify.
4. Perform steps 3-8 of the procedure [To add a Response Subscription: Webhook](#).

Delete a Response Subscription: Webhook

To delete a Response Subscription: Webhook

1. From the **Settings** tab, select the **Everbridge Open** tab.
 2. From the **Everbridge Open** tab, select **Response Subscriptions: Webhooks**.
 3. Click the Trash Bin of the webhook you want to delete.
 4. Confirm the deletion.
-
-
-

Enabling Response Subscriptions in Your Incident Templates

After you set up your Webhooks and Profiles, you can receive full Incident details, confirmations, and polling responses by subscribing profiles in your Incidents. On the **Settings** page of an Incident Template, the default is **Response Subscriptions: No**.

Perform the respective procedure, below, to subscribe profiles to your standard Incident templates and polling Incident templates.

Standard Incident Templates

To specify response subscriptions for a standard Incident template:

1. From the **Incidents** tab, **Incident Templates** sub-tab, select **Settings** from either a new Incident template or an existing Incident template.
2. Click the **Edit** link.
3. Scroll to the **Response Subscriptions** section.
4. Select the **Enabled** check box.
5. In the **Profile** field, select one profile of all profiles listed.
6. Select the **First confirmation only** or **Every confirmation** radio button.

Polling Incident Templates

To specify response subscriptions for a polling Incident template:

1. From the **Incidents** tab, **Incident Templates** sub-tab, select **Settings** from either a new Incident template or an existing Incident template.
2. Click the **Edit** link.
3. Scroll to the **Response Subscriptions** section.
4. Select the **Enabled** check box.
5. In the **Profile** field, select one profile of all profiles listed.
6. Select the desired radio button: **Specific response** or **Any response** radio button.
7. From the dynamic drop-down list, select the desired response (depending on the poll).
8. Select the **First time only** or **Every time** radio button.
9. Select the **First time only** or **Every time** radio button.

You see your selections in the upper right-hand corner of the Response Subscriptions pane.

NOTE: The Incident JSON gets posted as soon as the first confirmation or polling response has been received.

Reviewing the Usage Logs of Your Response Subscriptions

You can review the usage of your Response Subscriptions. You can also view the Notification response details.

View Response Subscription: Profile Usage Log

To see the Usage Log of a Response Subscription: Profile:

1. From the **Settings** tab, select the **Everbridge Open** tab.
2. From the **Everbridge Open** tab, select **Response Subscriptions: Profiles**.
3. Click the **Usage** link of the profile you want to see. The **Usage Log** appears.
4. Click **OK** when done.

View Response Subscription: Profile Details

To see the Details of a Response Subscription: Profile:

1. From the **Settings** tab, select the **Everbridge Open** tab.
2. From the **Everbridge Open** tab, select **Response Subscriptions: Profiles**.
3. Click the **Usage** link of the profile you want to see.
4. Click the hyperlink in the **Total Responses** column to display the details. The **Notification Response Details** page appears.
5. Click **OK** when done.

Safety iPaaS Connectors

Safety Connection offers out-of-the-box connectors Safety Connectors built on iPaaS to update the Last Known Location of contacts based on their badging activity. These connectors capture access events, and optionally security events, from client badging systems like OnGuard or C-CURE 9000.

You will find the following related connector information in the Everbridge Support Center:

- Everbridge Access Control
- OnGuard
- Tyco C-CURE 9000

IT Alerting iPaaS Connectors

iPaaS enables enterprise IT organizations to easily build their own integrations with the tools and solutions they already use. You can find out more about ITA connectors built on iPaaS in the Everbridge Support Center.

You will find the following related connector information in the Everbridge Support Center:

- BigPanda
- BMC Remedy
- BMC Remedyforce
- Cherwell
- HP Service Manager
- IBM QRadar
- IBM Resilient
- IBM Tivoli Netcool/OMNibus
- ITA API Connector
- Jira Service Desk
- Jira Software
- Micro Focus (HP) Service Manager
- New Relic
- Red Hat Ansible Tower
- ServiceNow
- SolarWinds
- Splunk
- Zabbix
- Zendesk

Other Safety Connectors

You will find the following related connector information in the Everbridge Support Center:

- CT - Harald
- SAP Concur
- International SOS
- Microsoft Office 365
- Travel Itinerary Connector by Magnatech
- RiskBand

Risk Events

In addition to the many risk feeds that Everbridge offers, **Self-Service Risk Events** provides the ability to send your exclusive risk data or data from a third-party to your Everbridge organization using a RESTful API.

You will find Self-Service Risk Events information in the Everbridge Support Center.

