Auto Launch Critical Event from Polling Package Incident Administrators Guide

Everbridge Suite

September 1

Auto Launch Critical Event from Polling Package User Guide.
Everbridge Suite
September 1, 2021
Printed in the USA.

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 revision 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, please 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.

Contents

Related Documentation and Training ... 4
Related Everbridge Documentation ... 4
Related training ... 4
Smart Orchestration Training ... 4
Critical Event Management ... 5
Incident Communications ... 5
IT Alerting ... 6
Overview ... 6
Workflow ... 7
Features ... 7
Set up the package ... 8
Import the package ... 8
Set up the REST Connector ... 9
Set Environment Values ... 10
Set up a Response Subscription ... 11
Select Critical Event Templates and Task Lists ... 11
Variables ... 11
Use Cases ... 14
Severe Weather ... 14
IT Outage ... 14

Related Documentation and Training

Documentation and training are provided to help you implement and run the Everbridge Critical Event Management Suite of products.

Related Everbridge Documentation

Documentation for Everbridge products is available from:

- Online Help. Selecting Online Help provides help for the Everbridge Suite system. In addition, select (?) on a page to access context-sensitive help.
- Everbridge Support Center. Guides are available as PDFs. You can either:
  - go to Home > Documents, click tab that you want, and select the guide you want.
  - in Search, type the name of the desired guide.

Related training

The Auto Launch Critical Event from Polling package encompasses three different parts of the Everbridge Platform: Smart Orchestration, Incident Communication, and Critical Event Management. We also recommend that you be familiar with IT Alerting.

Training for each of these is available in Everbridge University, Everbridge's self-service, online training resource for the Everbridge Platform.

Smart Orchestration Training

Training course	Description
Smart Orchestration	This course is aimed at enabling IT and engineering teams to create custom workflows, integrating different tools with Everbridge platform. In this course, you will learn how to create workflows to orchestrate various processes as part of a solution to meet your needs. The intended audience for this course is Engineers and IT team members with the following responsibilities: 1. Responsible for building system integrations for their organization. 2. Responsible for building, customizing, managing and monitoring workflow automation. Lessons are taught using a combination of images, text, and videos, with a Knowledge Check at the end.

Critical Event Management

Training course	Description
Critical Event Management Platform Overview	This course contains the information needed to obtain your Critical Event Management Short Deck Certification. It includes a video that introduces Critical Event Management and a presentation activity. Lessons are taught using a combination of images, text, and videos, with a Knowledge Check at the end.

Incident Communications

Training course	Description
Introduction to Incident Communications	This course covers key concepts of Incident Communications and its place in a critical response plan. Specifically, within the lessons, you will: 1. Gain familiarity with the navigation of Incident Communications. 2. Learn how Incident Communications align with Notifications. 3. Explore the phases of Incident Notifications Workflow. Lessons are taught using a combination of images, text, and videos, with a Knowledge Check at the end.
Incident Communications Administrator Certification	This certification prepares Incident Communication Administrators to ensure that all of the appropriate variables, templates and scenarios are in place when emergencies arise. Specifically, these courses cover how to: 1. Create and manage Incident templates and Scenarios. 2. Use variables and set up Incident Operators for success. 3. Generate, read, and use reports in Everbridge. Courses are taught using a combination of images, text, and videos, with a Knowledge Check at the end.
Incident Communications Operator Certification	This certification prepares learners to launch, update and close Incidents as a part of that process. Specifically, these courses will cover how to: 1. Launch Scenarios and Incidents. 2. Adjust Variables within an Incident. 3. Monitor Incidents and Scenarios through their life cycles.

	Courses are taught using a combination of images, text, and videos, with a Knowledge Check at the end.

IT Alerting

Training course	Description
Introduction to IT Alerting	This course covers key concepts of IT Alerting and its place in a critical response plan. IT Alerting involves the smooth routing of Incidents to appropriate contacts as well as the reporting of data collected during that process. Lessons are taught using a combination of images, text, and videos, with a Knowledge Check at the end.
IT Alerting Administrator Certification	This certification covers the concepts and navigation essential for an IT Alerting Administrator to master after an initial set-up. It covers how to: 1. Create and maintain Variables and Incident Templates. 2. Navigate the IT Alerting Dashboards. 3. Identify the components available for Incident routing. Courses are taught using a combination of images, text, and videos, with a Knowledge Check at the end.
IT Alerting Operator Certification	This certification prepares IT Operators to monitor and analyze critical events, as well as navigate the Dashboard. Specifically, these courses will teach you: 1. What IT Alerting is and how to navigate the dashboard. 2. How to open Incidents and filter details. 3. How to monitor trends and review graphs. Courses are taught using a combination of images, text, and videos, with a Knowledge Check at the end.

Overview

This guide describes the Everbridge Auto Launch Critical Event from Polling package for Smart Orchestration. When an Incident's severity or priority is upgraded and requires a cohesive response across multiple teams, this package allows you to automatically create a Critical Event from the Incident.

You can use this guide to download the package and set up the workflow that automatically creates a Critical Event from an Incident.

IMPORTANT: Your Organization Administrator must enable the Create, edit, and monitor workflows permission for you to install and configure this package.

Workflow

When you create or update an Incident, you can propose that the Incident be promoted to a Critical Event. When you do this, select a Critical Event Template to use and add related tasks to the Template.

When the proposal to promote the Incident to a Critical Event is reviewed and approved, a workflow begins that creates a Critical Event using the Template, including:

- Setting main and properties according to the ones specified in the Template.
- Launching the Task Lists that are defined in the Templates.
- Launching the Incidents that are defined in the Templates.
- Moving the Incident to the Critical Event communication.

When the Critical Event launches, all relevant stakeholders will receive notifications and tasks.

Features

The Auto Launch Critical Event from Polling package includes the following features:

Feature	Description
Create a Critical Event from a response subscription	When a user creates or updates an incident that contains a Polling message type, selecting a specific option will begin the Critical Event creation workflow.
Select and launch a Critical Event Template	Users can specify the Critical Event Template, and when a user creates the Critical Event, that Critical Event Template launches. The Template includes its tasks, Incidents, and documents. Auto launch uses the definition specified in the Critical Event Template at the time of the Critical Event's creation.

Select and Add Ad Hoc Task Lists to the Critical Event	Users can specify the list of Ad Hoc Task Lists to add to the Critical Event when they create it. When a user creates the Critical Event, the system automatically adds and launches additional Task Lists to the Critical Event.
Set Critical Event default parameters and custom attributes values	When a user creates the Critical Event, the system sets the values of the Title, Description, and Location Name main properties and additional custom fields based on the latest values of the matching Incident Variables from the Incident used to create the Critical Event.

Set up the package

This section explains how to set up the Auto Launch Critical Event from Polling package to function on your account. You will need to use the Smart Orchestration Cockpit to import the package and configure a connection between your account and the package.

IMPORTANT: If you do not have access to the Smart Orchestration Cockpit, contact your Everbridge Implementation Specialist and ask them to set up the package for you.

Import the package

To begin, import the package. To do this:

1. Navigate to the Settings > Smart Orchestration > Package Manager page.
2. Select the package's type from the Package Type menu.
3. Select the package's name from the Package Name menu.
4. Click Import Package.

Package contents

The Auto Launch Critical Event from Polling package contains the following:

- Environment Values
  - IC_CEM_CONFIGURATION
- WorkflowFunctions

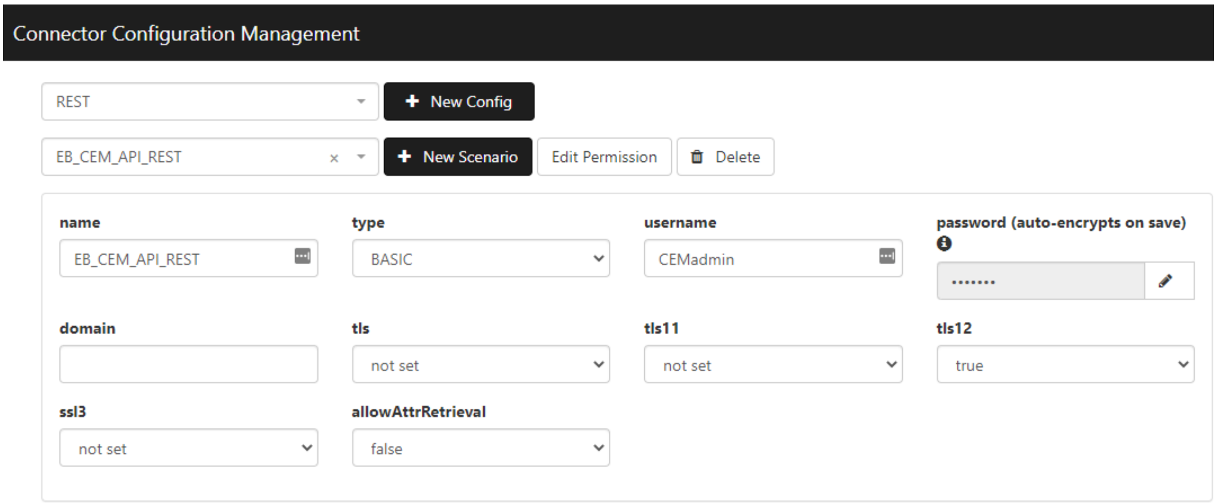
    - IC CEM Add Additional Tasks
    - IC CEM Add CE Template Vars
    - IC CEM Add Notification Vars
    - IC CEM Add Template Documents
    - IC CEM Add Template Incidents
    - IC CEM Add Template Tasks
    - IC CEM Create Critical Event
    - everbridge/ic/cem
    - IC_CEM_Response_Subscription
- Workflows
    - IC CEM Add Additional Tasks
    - IC CEM Add CE Template Vars
    - IC CEM Add Notification Vars
    - IC CEM Add Template Documents
    - IC CEM Add Template Incidents
    - IC CEM Add Template Tasks
    - IC CEM Create Critical Event
    - IC CEM Response Subscription
    - IC CEM Resp Subscription Async

Set up the REST Connector

After you download the package, you must configure the REST API connector. This will integrate the package into your Incident Communication and Critical Event Management suites.

To configure the REST API Connector:

1. Navigate to the Settings > Smart Orchestration > Workflow Designer page.
2. Select Connector Configuration > REST. The Connector Configuration Management page will appear.
3. Select REST from the New Config menu.
4. Click New Scenario.
5. Enter the following information in the corresponding fields:
    - **name** - `EB_CEM_API_REST`
    - type - `BASIC`
    - username - An Account Administrator or Organization Administrator's username. This user must have API access.
    - password - The user's password.
    - tls12 - `true`
6. Click Save.



Connector Configuration Management

REST

EB_CEM_API_REST

name: EB_CEM_API_REST
type: BASIC
username: CEMadmin
password (auto-encrypts on save): •••••••
domain:
tls: not set
tls11: not set
tls12: true
ssl3: not set
allowAttrRetrieval: false

Set Environment Values

Launching the Critical Event occurs when you create or update an incident. You will create a specific Incident Template for this effect.

In the Incident Template, you will use Incident Variables to do the following:

- Select the Critical Event Template.
- Specify Ad Hoc task lists to be added and launched.
- Set the values of the Critical Event Title, Description and Location name.

You can configure the Incident Variable names and specify them in a Workflow Environment Variable. You will do this on the Workflow Designer page.

After you configure the REST API connection for the package, configure the API Environment Variables. To do this:

1. In the Workflow Designer page, select Manage > **Environment Values**. The **Environment Values** page will appear.
2. Edit the IC_CEM_Configuration variable and click **Save** and Close.

```
{
"cemBaseURL": "https://api.everbridge.net/rest",
"ebCemRestScenario" : "EB_CEM_API_REST",
"cemTemplateNameVarName": "<incident variable name 1>",
"cemTaskTemplatesVarName": "<incident variable name 2>",
"cemTitleVarName" : "<incident variable name 3>",
"cemDescriptionVarName" : "<incident variable name 4>",
"cemLocationNameVarName" : "<incident variable name 5>"
}
```

In this configuration, the environment values represent the following:

- `cemBaseURL` - The URL for the Everbridge Swagger REST API.
- `ebCemRestScenario` - The scenario name specified on the Connector **Configuration Management** page.
- `cemTemplateNameVarName` - The Incident Variable name you will use to select the Critical Event.

- `cemTaskTemplatesVarName` - The Incident Variable name you will use to specify Ad Hoc task lists.
- `cemTitleVarName` - The Incident Variable name from which the Critical Event Title will be set.
- `cemDescriptionVarName` - The Incident variable name from which the Critical Event Description will be set.
- `cemLocationNameVarName` - The Incident variable name from which the Critical Event Location name will be set.

Set up a Response Subscription

After you download and configure the Auto Launch Critical Event from Polling package, you mustcontact your Implementation Specialist or Organization Administrator and request that they set up and enable a response subscription. Response subscriptions allow you to receive confirmations and polling responses from notification recipients and put those responses into your third-party systems.

The package uses a response subscription to trigger the workflow.

Select Critical Event Templates and Task Lists

After you set up your response subscription, you can create Incident Variables to associate with Critical Event Templates and Ad Hoc Task Lists. You will add these Variables to your Incident Templates, which will allow you to manually create a Critical Event directly from an Incident.

The Variable names must match the ones that you configured on the Workflow Designer page.

Variables

To manually select Critical Event Templates and Task Lists when launching an Incident, you will set two Environment Variables. You must specify a Critical Event Template as one of these variables. If you do not, the workflow will fail.

The table below contains the available environment variables.

> NOTE: Title and Description are mandatory default properties when you create a Critical Event. Make certain that the values exist on the template you allow for selection or are made mandatory variables in the Incident Template.

Purpose	Variable Type	Mandatory	Format
Select a Critical Event Template	Single Selection	Yes	Text string. The value must match an existing Critical Event Task List name.

Select and auto launch task lists	• Multi selection
	• Existing object name
		No	Text string. The value must match an existing Critical Event Task List name.
			`name1,true`
			`name2,false`
			• `true`- The Task List launches automatically
			• `false`- The Task List does not launch automatically.
			Everbridge recommends that you create at least two values per task list, one with `true` and the other with `false`. All values are case-sensitive.

Specify Title	• Single selection • Multi selection • Textarea • Textbox	No	Text string. Values specified in this variable will set the Title of the newly-created Critical Event.
Specify Location name	• Single selection • Textarea • Textbox	No	Text string. Values specified in this variable will set the Location name of the newly-created Critical Event.
Specify Description	• Single selection • Textarea • Textbox	No	Text string. Values specified in this variable will set the Description of the newly-created Critical Event.

You can also add additional Incident Variables to your Template. Custom properties are automatically created to the Critical Event and the value specified when you use the Template.

When the Critical Event launches, the workflow checks to see if any custom properties exist in the Critical Event Template. If so, it looks for any Incident Notifications that include a Variable with the same name.

If the workflow finds one, it sets the value of the property with the value found in the most recent Incident Notification. If the workflow does not find one, it keeps the value of the property as set in the Critical Event Template.

Use Cases

Severe Weather

An Incident Administrator is preparing for the impact of a Tropical Storm on their area. They launch an Incident for the storm that notifies the relevant stakeholders. 24 hours later, the National Hurricane Center (NHC) upgrades the Tropical Storm to a Category 1 Hurricane, predicting stronger winds and more rain in the area.

Incident Administrator decides to update the Incident and proposes promoting it to a Critical Event. They open the Update Incident page and select the Hurricane template. After that, they select the related tasks to include with the Critical Event and click Send. A review board receives the notification and approves the proposal, creating a Critical Event. Senior management and regulators receive event notifications and all relevant stakeholders receive notifications and tasks.

The Incident Administrator monitors the progress of the tasks in the task list, updates the Situation Report and Executive Summary as needed, and launch the Impact Tracker to collect information on the Critical Event's progress in real-time.

The Incident Administrator also shares current updates throughout the hurricane and subsequent recovery efforts with stakeholders via communications and the Dashboard.

After the Hurricane moves through the area, the Incident Administrator verifies that all related tasks from the list are complete and closes the Critical Event.

IT Outage

A financial services company receives reports from their end users about their services being unavailable. A high priority ticket is created in the ITSM system, which automatically creates an Incident. The Incident contains a Conference Bridge message type, which patches all of the relevant Support Analysts into a conference call to analyze the outage and attempt to restore the service. All relevant stakeholders also receive an SMS message that informs them of the service outage.

An analysis of the issue reveals that all of their end-users are no longer receiving service. The Incident Administrator decides to update the Incident and proposes promoting it to a Critical Event. They open the Update Incident page and select the IT Outage Critical Event template. After that, they select the related tasks to include with the Critical Event, set the necessary information, and click Send. The Crisis Management team receives the notification and approves the proposal, creating a Critical Event. Senior management and regulators receive event notifications and all relevant stakeholders receive notifications and tasks.

The Incident Administrator monitors the progress of the service restoration tasks, updates the Situation Report and Executive Summary as needed, and launch the Impact Tracker to collect information on the Critical Event's progress in real-time.

The Incident Administrator also shares current updates throughout the outage and repair efforts with stakeholders via communications and the Dashboard.

After the company confirms that their end users have their service restored, the Incident Administrator closes the Critical Event.