Everbridge PACS Connector Guide

Everbridge Suite

May 2024

Everbridge Suite
2024
Printed in the USA

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

Before Installing

PACS Prerequisites

Communication between the PACS Importer and the PACS Exporter utilizes HTTP. If the components are running on different servers, ensure connectivity and that the firewall allows access to the server on (default) port 43366.

Supported PACS Systems

C-CURE 9000

- **License required:** CC9WS-EVERBDG
- The agent cannot be installed on the MAS server as it doesn't support any type of integration.
- Supports version 2.7 through 3.0 via Victor Web Services
- Supports C-CURE 9000 Enterprise
- Ensure Victor WebServices is installed and accessible by navigating to:
  - *http://SERVERNAME/victorwebservice/api/Generic/version*
    - NOTE: Replace "servername" with localhost or the correct server name for your installation.

OnGuard

- **License required:** EPC-311-xxx SKU (based on system size)
- **License required:** Partner Integration (IPC-311-EVRBG01)
- Supports version 8.0 to 8.2 via OpenAccess
- Ensure OpenAccess WebServices is installed and accessible by navigating to:
  - https://SERVERNAME:8080/api/access/onguard/openaccess/swagger/
    - NOTE: Replace "servername" with localhost or the correct server name for your installation.

PACS Exporter and Importer Installation

- The agent requires .NET (4.5.2 or higher). It will be installed with the agent if it does not already exist.
- If Installation fails or is unable to retrieve the required dependencies, they can be downloaded and installed manually:
  - https://www.microsoft.com/net/download/windows

Everbridge Suite Configuration

- Add the appropriate Location Source for your PACS integration to Location Sources. For details, see **Location Sources** in the *Safety Connection User Guide*.
- Supported Location sources:
  - OnGuard
  - C-CURE 9000

Choose the location source based on the PACS system you are integrating with.

Everbridge Prerequisites

> **NOTE:** If the client integration will utilize Everbridge External IDs, proceed to Step 3.

Do the following in Everbridge:

1. Create an **Additional Information** field to hold the identifying attribute that will correlate badge holders with Everbridge contacts. For details on creating an Additional Information field, see the **Additional Information** section of the *Organization Administrator Guide*.
   - NOTE: Only Text/Textbox and Number data types can hold Badge IDs.
2. Set the value of that Additional Information field for the reach of your contacts.
3. Add or upload your buildings. For details, see the **Uploading Buildings** section of the *Safety Connection User Guide*.
4. Add the name of your Access Control Integration to Location Sources. The name must match the “source” that is sent in the payload.
5. Perform the procedures in the iPaaS Configuration section. As needed, the steps to modify agents, delete agents, or search for a specific agent are provided in the iPaaS Usage section.

Connectivity

External connections to Everbridge servers are made via HTTPS/SSL on port 443 (using TLS 1.1+).

Overview

The Everbridge Connector is designed to integrate Everbridge's Critical Event Management system with events from **Physical Access Control Systems** (PACS).

The Connector is available on **iPaaS** (integration Platform as a Service). iPaaS is the middle layer between the third-party system and Everbridge. iPaaS simplifies the installation and configuration of integrations built to work with the Everbridge platform.

Enable iPaaS

Ask your Everbridge representative to enable Everbridge Open iPaaS for your Account and Organization.

> **NOTE:** Dynamic Locations must also be enabled.

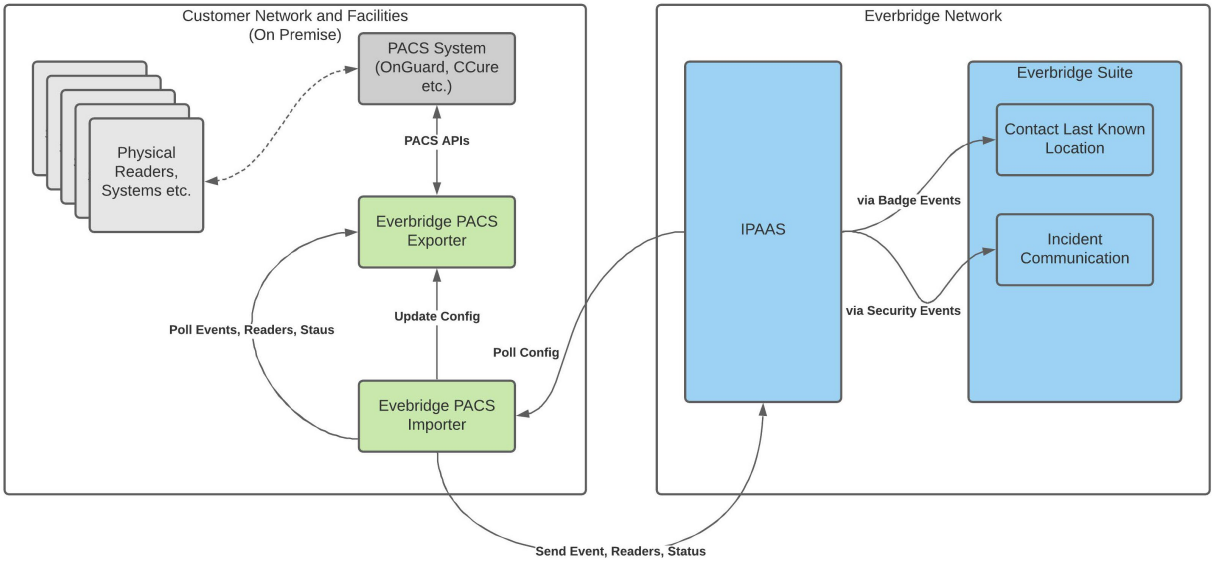
Use Case

The Connector is designed to update the **Last Known Location** of contacts based on their badging activity. The connector captures Access Events, and optionally security events, from the client system. Access Events will update the dynamic location of contacts to reflect the building they have entered.

By automatically updating the dynamic location of contacts, message senders can view the location of contacts on the Everbridge **Universe** map. Message senders can also use polygons or rules to notify all contacts who may be affected by a location-based emergency in a specific building or area.

If supported and configured, the connector can also integrate with security events, such as fire alarm or door forced open. You can create rules and conditions in iPaaS so that incoming events will be evaluated against the predefined criteria to launch Everbridge Incidents and Scenarios if a match is found.

System Architecture



Client Network

The Everbridge PACS client integration consists of three components:

- PACS Exporter
- PACS Importer
- Third-party PACS (e.g., OnGuard)

These components run inside the client network. The two Everbridge components provide an asynchronous connection between PACS (OnGuard, C-CURE, etc.) data and events and the core Everbridge platform. The Exporter handles all interaction with the PACS and provides a normalized data format for all integrated systems. The Importer is a bridge between the core Everbridge platform and the Exporter. The Importer performs queuing, filtering, and validation of events before they are passed into the core Everbridge system for further processing.

Everbridge Network

Within the Core Everbridge Platform, multiple subsystems are utilized:

- Integration Platform as a Service (iPaaS)
- Contacts (Last Known Location)
- Incident Communication

iPaas is the interface and API integration point for all messages received from the PACS Importer. iPaaS dispatches both badging events (to the Contacts system) and security events (to the Incident Communication system). Badging events will update a configured user's Last Known Location based on the mapping association between a badge reader and an existing building configuration. Security events, if configured, and if they match user-defined conditions, will result in an Incident being created. An Incident can send various forms of communication, including SMS and phone calls, as well as accept responses and acknowledgments from those communications.

Network Connections

PACS Client External Communication

All communication between the PACS client system and the Core Everbridge Platform occurs over HTTPS (port 443). All external connections are initiated by the PACS Importer and communicate only with the Everbridge iPaaS API.

PACS Client Internal Communication

Within the client system, communication occurs over HTTP between the Importer and Exporter. The default port is 43366. Communication between the Exporter and the PACS itself varies based on the integrated system; refer to the appropriate documentation for that system for specific information. In most installations, the Importer and Exporter components will be installed on the same system. If these components are installed on separate systems and an HTTPS connection is required, a certificate must be configured within IIS.

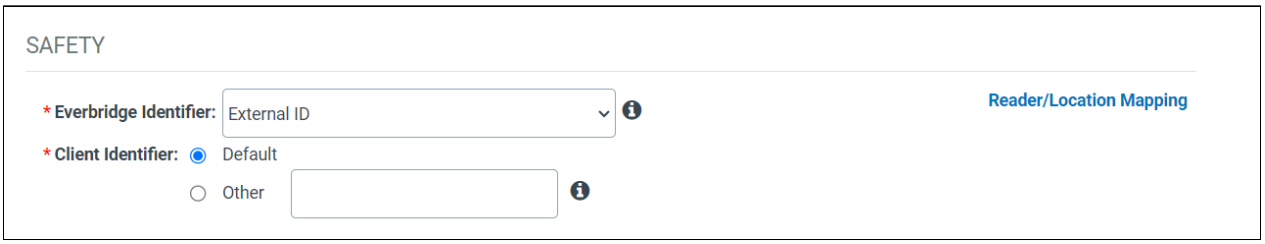
A self-signed certificate can also be creaated use using steps similar to: https://aboutssl.org/how-to-create-a-self-signed-certificate-in-iis/

iPaaS Configuration

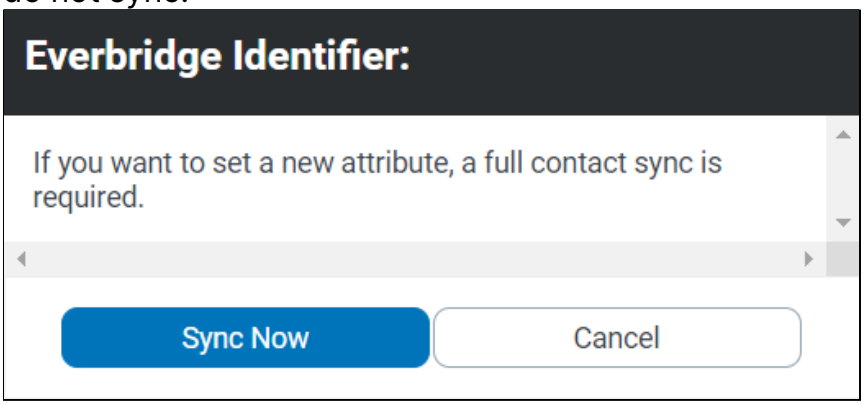
At the Organization level, you can configure shared agent settings from **Settings** > **Everbridge Open** > **iPaaS** > **Settings**.

Everbridge Identifier

If your people records contain Everbridge External IDs, select **External ID** in the Everbridge identifier drop-down list and skip to the **Reader/Location Mapping** section; otherwise, you will need to use an **Additional Information** field to hold the identifying attribute that will be used to correlate client users with Everbridge contacts.



- After you create an Additional Information field, you will see it in the Everbridge Identifier drop-down list.
- Select the correct attribute from the drop-down list.
- You are then prompted to do a full contact sync. This is required to update all your synced contacts to point to the new Additional Information field. If you click **Cancel**, the attribute reverts to the previous selection and the contacts do not sync.



Client Identifier

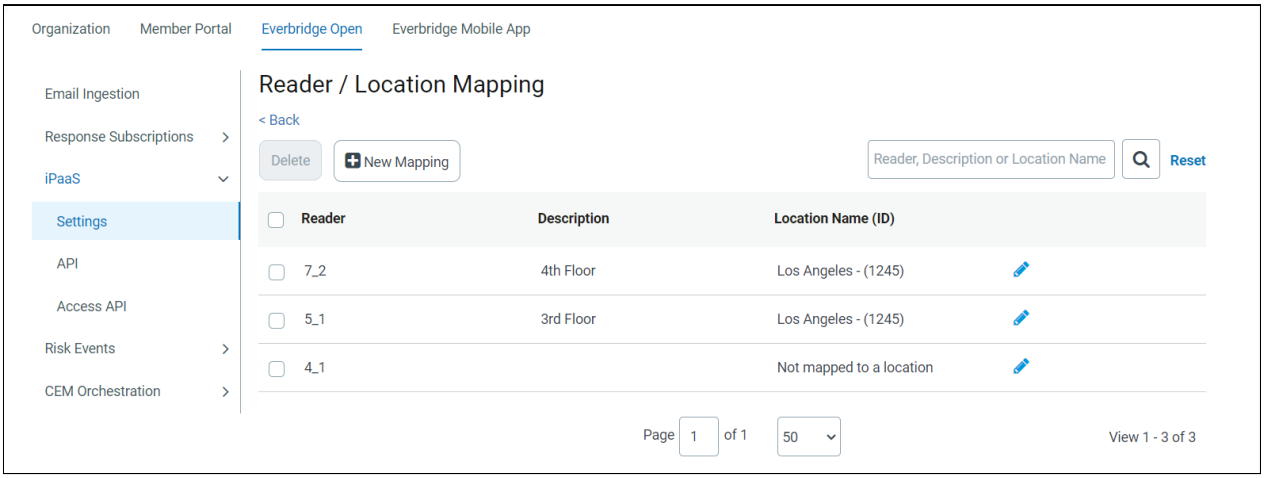
The **Client Identifier** is the field in client integration used to identify people.

Select one of the following two choices:

- **Default** - This is the Badge ID.
- **Other** - Enter the name of the field in the client integration that will be used to correlate people with Everbridge contacts.

Reader/Location Mapping

After you upload your buildings, you will need to map your Readers to Everbridge locations. Once the Everbridge client agent is running, the badge readers will automatically be sent to Everbridge every hour. You will then need to map each of these readers to Locations. Navigate to the Reader/Location Mapping page by selecting the **Reader/Location Mapping** link on the **Settings** page. Here you can add, modify, and delete badge Reader to Location mappings:



You can also map readers to Locations without using the UI by making use of a couple of API endpoints in iPaaS (useful if you have a lot of readers and buildings):

1. Ensure the readers are sent over to Everbridge.
2. Retrieve your list of readers with an HTTPS GET call to: https://ipaas-ingestion.everbridge.net/swagger-ui/index.html#/Access%20Control/getInternalReaderesUsingGET
    - You will need to authorize with the header name “Authorization” and use your iPaaS API key for the value.
    - For each reader entry in the JSON response, inject the Everbridge Building ID into the ‘assetId’ field. This matches the ‘Location Id’ for the building found at **Everbridge Open** > **Organization** > **Map** > **Manage Buildings** > **Buildings**.
    - The ‘assetName’ field is not used during updates. All other fields should not be edited.

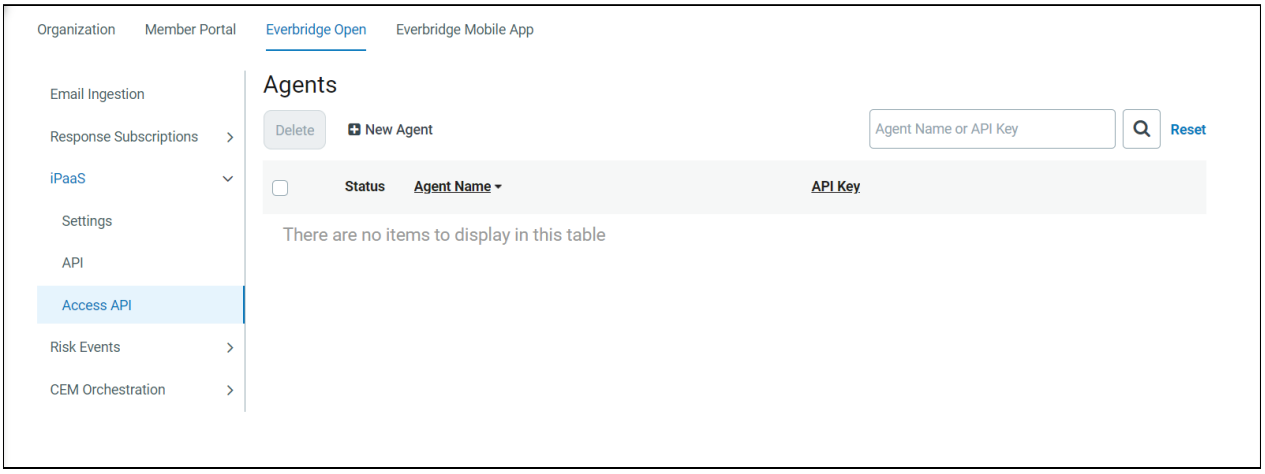
3. Map your readers to buildings with an HTTPS POST call to: https://ipaasingestion.everbridge.net/swagger-ui/#/Access%20Control/postReadersUsingPOST/.

Refresh Everbridge Identifier

Refresh Everbridge Identifier will sync all contacts. You may want to do this if you have changed or added many users. Every hour modified contacts will sync automatically. This is not needed if your badge identifiers are the same as your Everbridge External IDs.

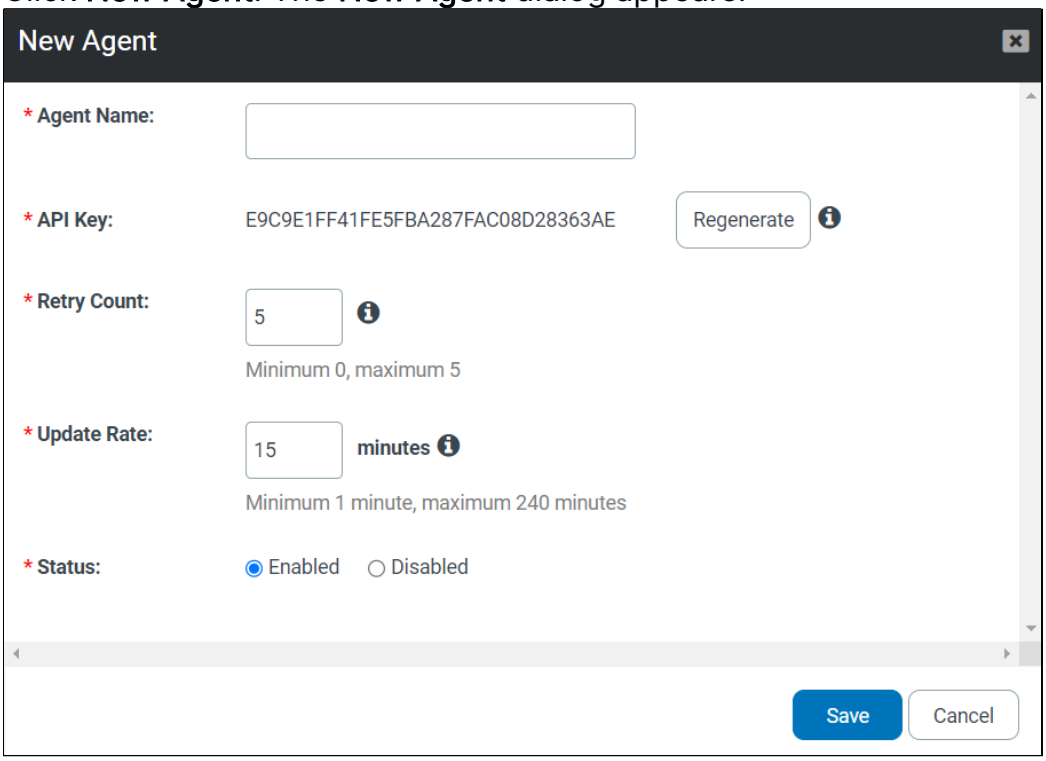
Adding Agents to Your Organization

The **Agent Configuration** is the group of settings that will be used to configure all of the agents used in your Organization. It can be configured from **Settings** > **Everbridge Open** > **iPaaS** > **Access API**.



To create a new Agent Configuration:

1. Click **New Agent**. The **New Agent** dialog appears.



2. Se the following fields:
   - **Agent Name** - Display name used to refer to the agent.
   - **API Key** - A code used by iPaaS to identify the connector/agent. This will be automatically generated when creating a new agent configuration in iPaaS.
   - **Retry Count** - If a message fails, this is the number of retries that will be made. The value can be between 0 and 5.
   - **Update Rate** - The frequency of sending data to Everbridge Suite via iPaaS. The value must be between 1 minute and 240 minutes.
   - **Status**
     - *Enabled* - Turns on the connection between the connector and iPaaS so that iPaaS can receive messages.
     - *Disabled* - Turns off the connection between the connector and iPaaS so that no messages will be received.
   - Click **Save**.

Resolving an Access Event to a Contact

In order to maintain consistency of Cardholder/Contact data between your PACS and Everbridge, user information in both systems must be regularly updated. The integration relies on a shared field. This field is usually an Employee ID or Email Address.

Typical values are:

- OnGuard: SSNO, EMAIL
- C-Cure: Text1-Text14, EmailAddress

Other values may be supported, depending on your configuration.

This information must remain synchronized by a **separate process** between your user repository system of record (e.g., Human Resource database) and both your PACS system and Everbridge.

The only information sent between the iPaaS and the PACS Agent and Importer is a field resolving the badge ID to the user identity. The field used for user identity must match (including case and formatting) in both systems. For example, if one system trims leading zeros or spaces, and presents the field with a different format or capitalization, the correct user may not be resolved.

PACS Exporter

This section describes the PACS Exporter installation process. The installer ensures that additional dependencies are present, or it installs them. This installation applies to a connection to the Physical Access Control System (PACS). A separate section will cover the PACS Importer, which sends collected data to the Everbridge system.

Download

The Importer (Agent) and Exporter are available for download via the Everbridge Support Center in the CEM Connectors section. Please select the appropriate system (C-Cure 9000 or OnGuard). The Agent/Importer should be installed on the same system or on a system that can access the PACS Exporter via HTTP.

Installation

To install:

1. Launch **Setup.exe**.
    - If the .NET Framework 4.7.2 is not installed, you'll be prompted to install it first. You may be prompted to reboot your system before proceeding with further installation.
2. Read and agree to the License Agreement.
3. Choose the folder to install the Service. By default, the folder is: **C:\Program Files (x86)\Everbridge\Everbridge PACS Exporter**
4. To install into a different folder, click **Browse**.
5. Complete the installation.
6. You are prompted to fill in the following values:

Label	Type	Purpose/Action
PACS Type	Drop-down	The PACS type. E.g., LenelOnGuard
PACS API Server	Text Field	The URL of the PACS system web service. E.g., https://localhost:8080/api/openaccess/
PACS API Event Server	Text Field	The URL of the PACS system event web service. Not required for all PACS types.
PACS API Username	Text Field	The username used to authenticate with the PACS web service.

PACS API Password	Text Field	The password used to authenticate with the PACS web service.

IMPORTANT: These values are the connection to the Physical Access Control System (PACS), not to the Everbridge system.

Configure the Windows Service Log On

To configure the Windows Service Log On:

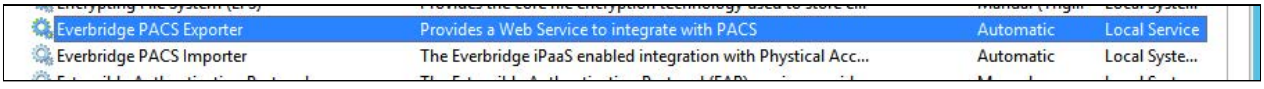
1. Select **Windows** > **Run**.
2. Enter services.msc
3. Select **OK**.
4. Browse to **Everbridge PACS Exporter Service**.
5. Right-click and select **Properties**.
6. Select the **Log On** tab.
7. Change the account information to a Windows account that has the necessary read/write permissions.
8. Select **OK**.
    - If the **Log On As A Service right granted dialog** appears, select **OK**.
9. Confirm that the service now has the correct user account listed.
10. Right-click on the service and select **Start**.

Service

It is possible to check whether the Connector was properly installed and started through the Computer Management Console:

1. **Computer** > [**Right Click**] > **Manage** > **Services and Applications** > **Services** > **Everbridge PACS Exporter**.

The service can be stopped or started as a standard Windows Service.



Information Logging

To view logging:

1. Navigate to the folder where you installed the Everbridge PACS Exporter.

2. A logs directory exists in the root directory and contains a file called **Everbridge.Service.log**. All log entries are stored in this file.

Increase Logging Output

To increase the logging output:

1. Navigate to the folder where you installed the **Everbridge Plugin** agent.
2. Open **StandardLogging.config** in a text editor.
3. Change the following line: *<level value="INFO" />* To: *<level value="DEBUG" />*
4. Restart the **Everbridge PACS Exporter** agent.

PACS Importer

The PACS Exporter should be installed and configured before installing the PACS Agent (this component). The Exporter provides an interface to various PACS systems including OnGuard and C-Cure 9000. This component relays the data gathered by the PACS Exporter and makes it available in the Everbridge system.

Download

The Importer (Agent) and Exporter are available for download via the Everbridge Support Center in the CEM Connectors section. Please select the appropriate system (C-Cure 9000 or OnGuard). The Agent/Importer should be installed on the same system or on a system that can access the PACS Exporter via HTTP.

Installation

This section describes the PACS Agent installation process. The installer ensures that additional dependencies are present or it installs them.

1. Launch **Setup.exe**.
   - If the .NET Framework 4.5 is not installed, you will be prompted to install it first. You may be prompted to reboot your system before proceeding with further installation.
2. Read and agree to the License Agreement.
3. Choose the folder to install the Service. By default, the folder is: **C:\Program Files (x86)\Everbridge\Everbridge PACS Importer**
4. To install into a different folder, click **Browse**.
5. You are prompted to fill in the following values:

Label	Type	Purpose/Action
PACS Exporter URL	Text Field	The URL of the PACS Exporter; by default, http://localhost:43366/ if installed on the same server.
PACS Exporter Username	Text Field	The username you have previously configured for the PACS Exporter.
PACS Exporter Password	Text Field	The password you have previously configured for the PACS Exporter.

Proxy server configuration is optional. The proxy configuration should be set if you require accessing the Everbridge server via a proxy connection. Connections to the PACS Exporter do not utilize the proxy connection as they are expected to be internal connections that are usually running on the same host. If you do not use a proxy server, these items should be left blank.

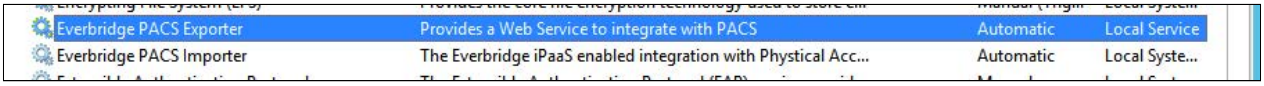
Label	Type	Purpose/Action
Proxy Server URL	Text Field	The URL of the proxy server used to access the Everbridge API
Proxy Server Username	Text Field	The username of the proxy server user (optional).
Proxy Server Domain	Text Field	The domain of the proxy server user (optional).
Proxy Server Password	Text Field	The password of the proxy server user (optional).

6. Complete the installation.
7. Navigate to Windows Services.
8. Manually start the E**verbridge PACS Importer**.

Service

The service is automatically started after successful configuration completion. It is possible to check whether the Connector was properly installed and started through the **Computer Management Console**.

1. **Computer** > [**Right Click**] > **Manage** > **Services and Applications** > **Services** > Everbridge **PACS Importer**.
The service can be stopped or started as a standard Windows Service.



Information Logging

To view logging:

1. 1. Navigate to the folder where you installed the Everbridge Plugin agent.
2. A logs directory exists in the root directory and contains a file called **everbridgeAgent.log**. All log entries are stored in this file.

Increase Logging Output

To increase logging output:

1. Navigate to the folder where you installed the Everbridge Plugin agent.
2. Open **log4net.config** in a text editor.
3. Change the following line: *<level value="INFO" />* To: *<level value="DEBUG" />*

4. Restart the Everbridge Plugin agent.

Additional iPaaS Configuration

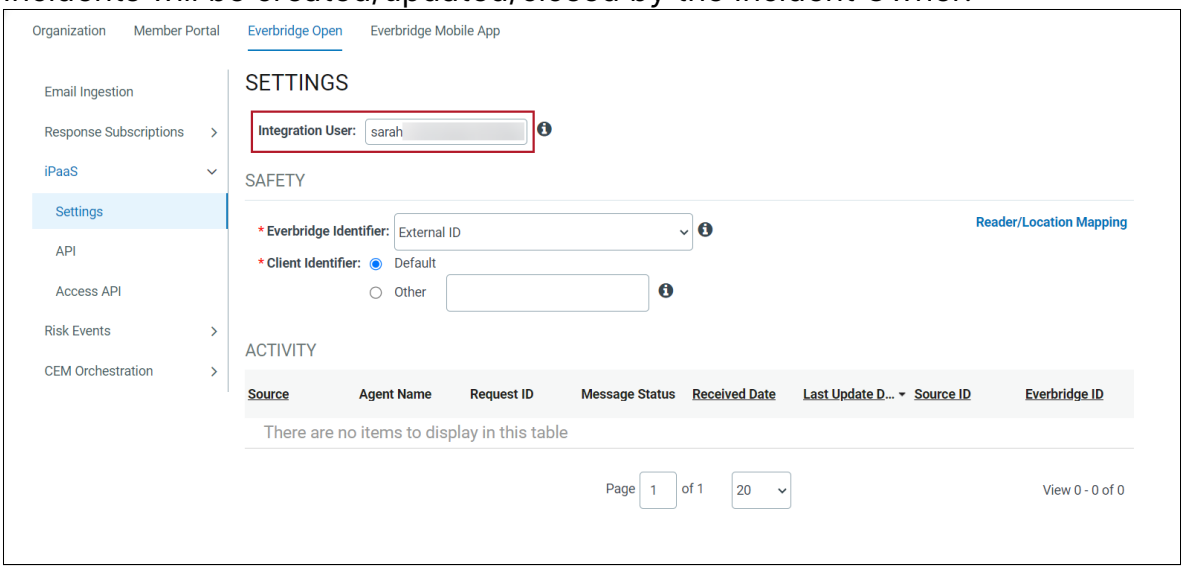
After completing the initial setup of iPaaS and the PACS Client, additional configuration is required to map readers, configure security events and optionally specify an integration user.

Integration User

The **Integration User** can be set in **iPaaS Settings** and is shown as the user for all iPaaS actions. The selected user must be an Account Administrator or Organization Administrator with API Access.

To set the Integration User:

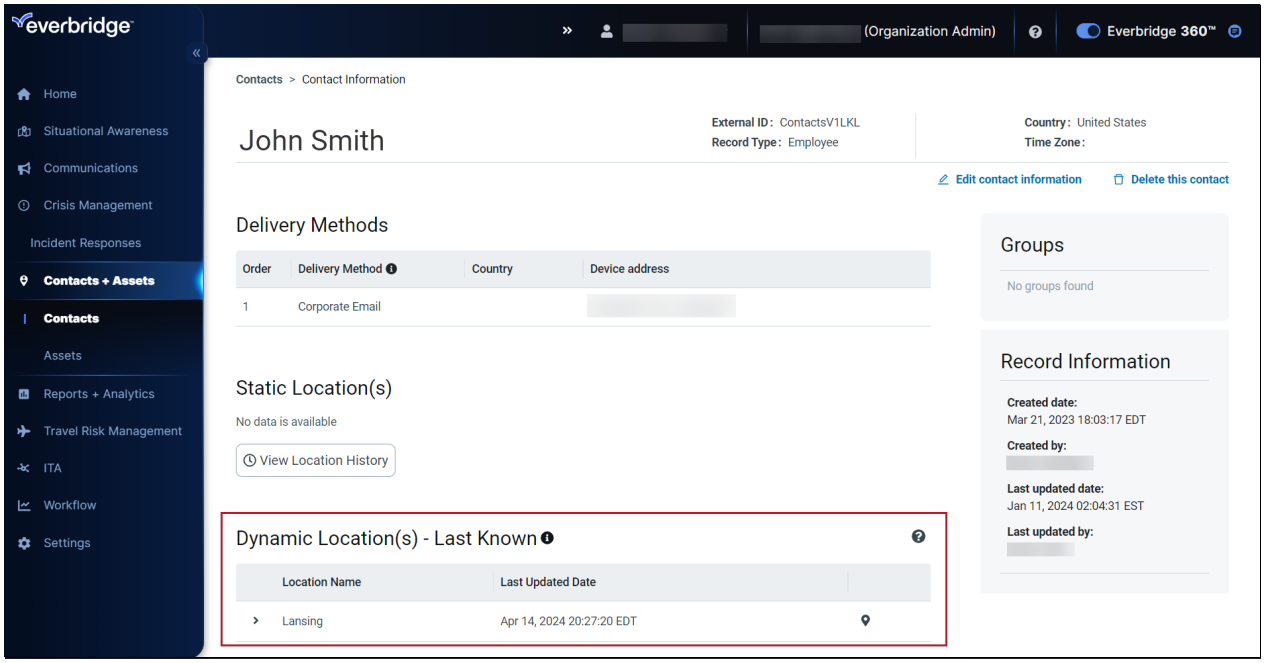
1. Click the **Settings** tab under **iPaaS**.
2. Set the **Integration User** field to the Everbridge Username that will be shown for all iPaaS actions. If both the Incident Owner and Integration User are set, Incidents will be created/updated/closed by the Incident Owner.



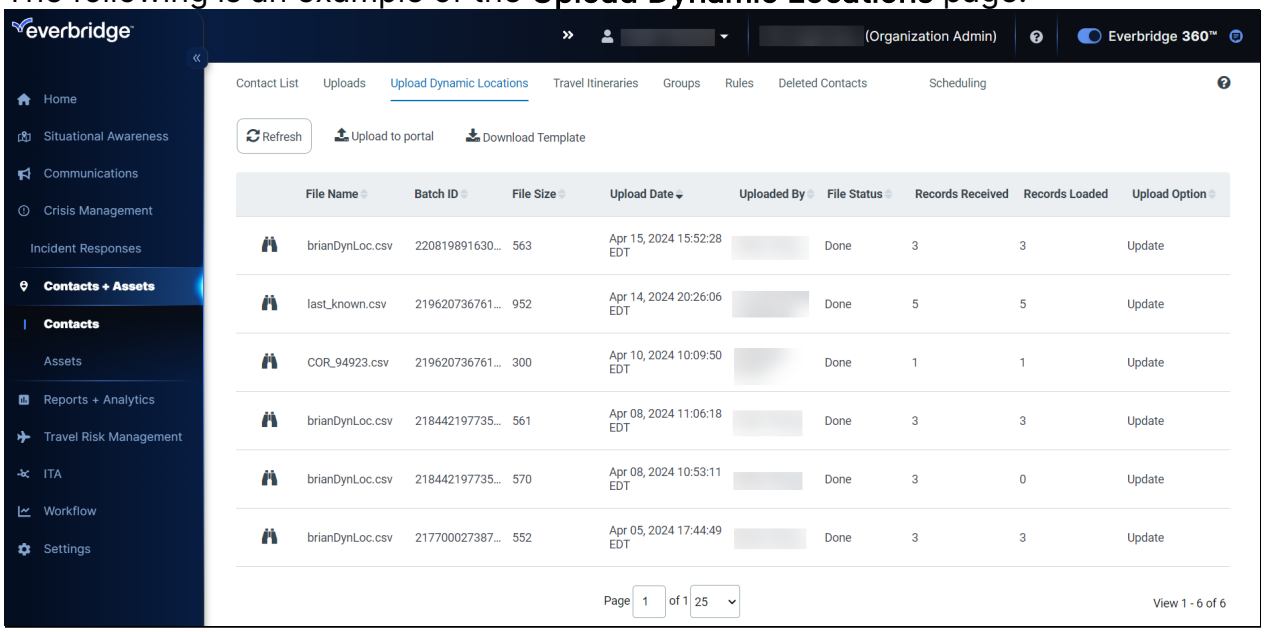
Viewing Updated Locations in Everbridge

When integrating with access control systems, the Last Known Locations of contacts will be updated in Everbridge. This is shown in **Upload Dynamic Locations** page and the the **Dynamic - Last Known Locations** section on the **Contact Information** page, which is accessed by clicking on the contact's name

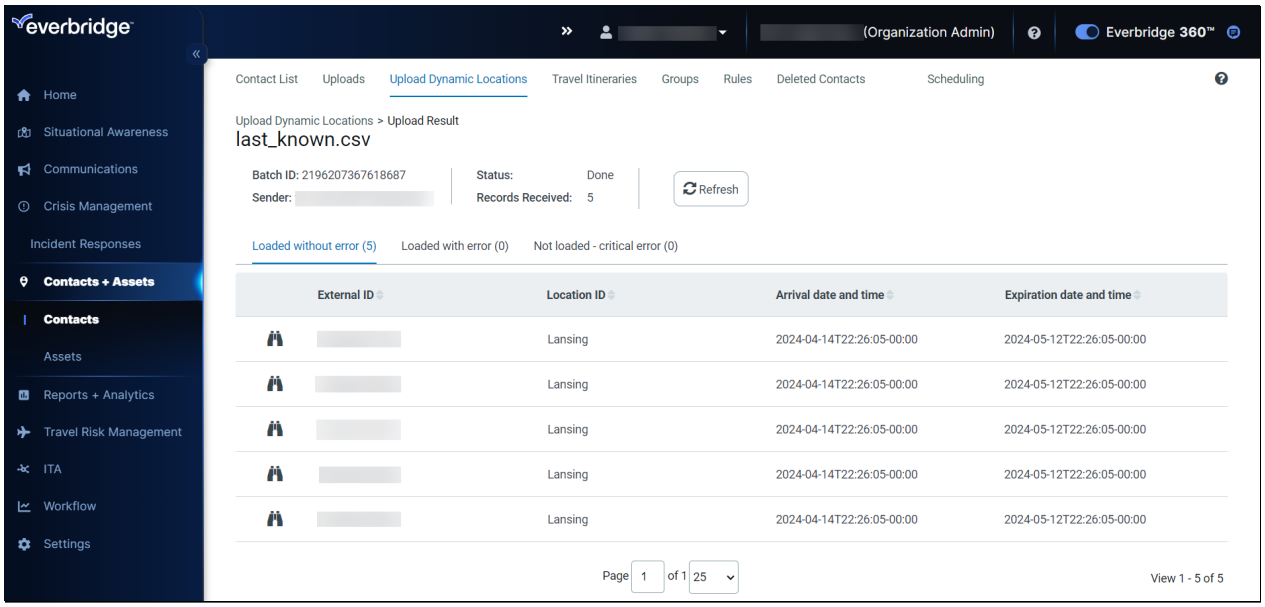
from the **Contact List**.



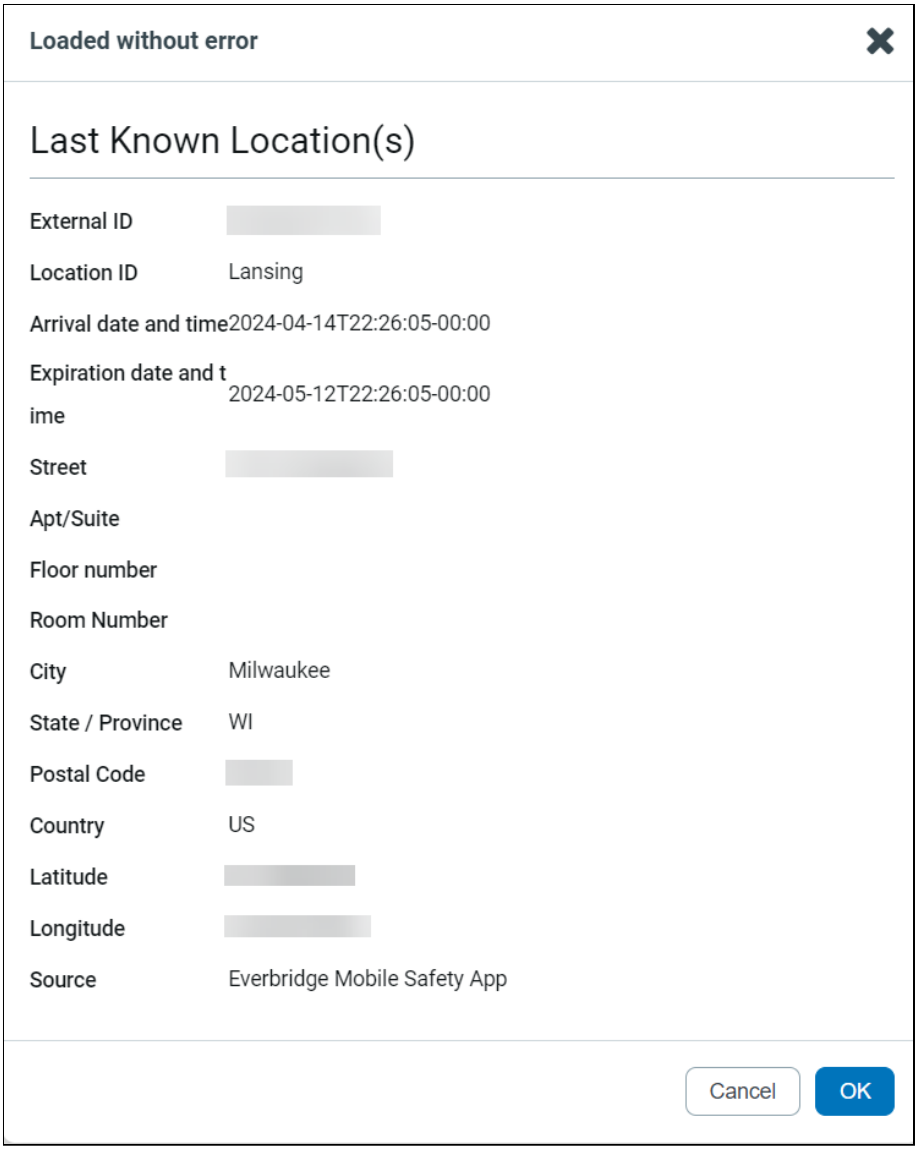
The following is an example of the **Upload Dynamic Locations** page:



Click on the magnifying glass next to an upload to view the **Upload Results** page, which details the records that were loaded with and without errors, and those that weren't loaded due to a critical error.



Clicking on the magnifying glass next to an External ID will open the details of the Last Known Location:


Loaded without error
Last Known Location(s)
External ID
Location ID
Lansing
Arrival date and time
2024-04-14T22:26:05-00:00
Expiration date and time
2024-05-12T22:26:05-00:00
Street
Apt/Suite
Floor number
Room Number
City
Milwaukee
State / Province
WI
Postal Code
Country
US
Latitude
Longitude
Source
Everbridge Mobile Safety App
Cancel
OK

iPaaS Security Event Configuration

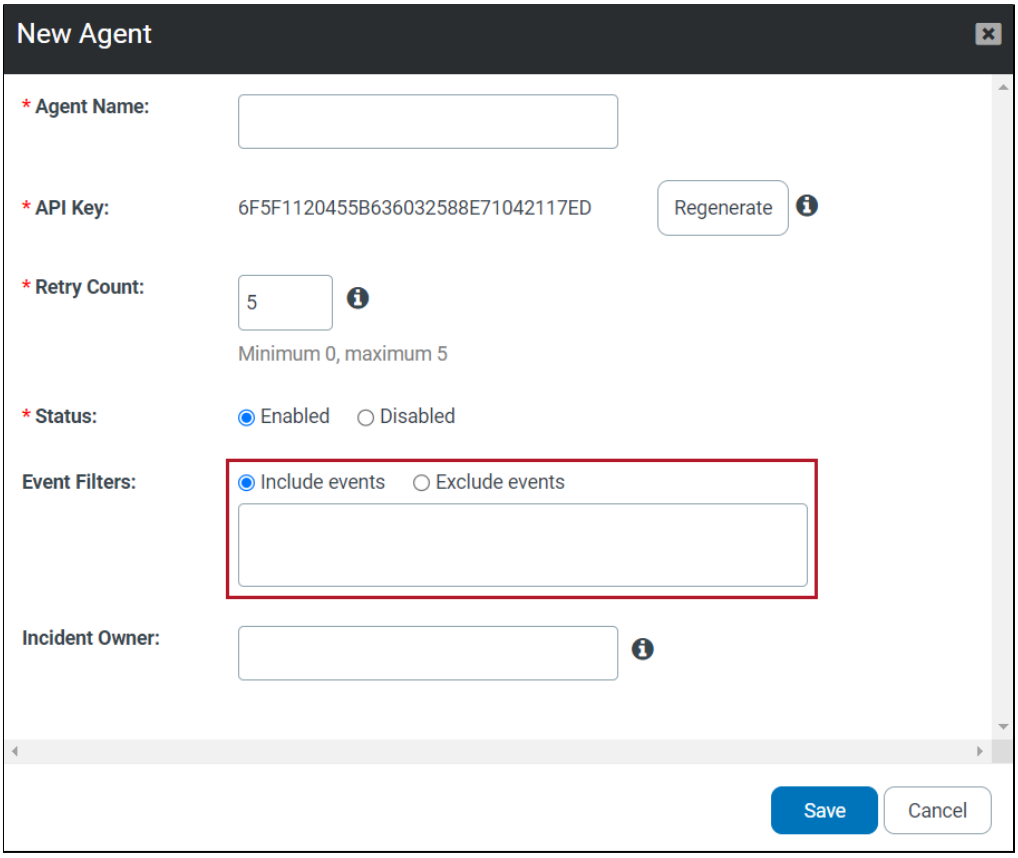
The Everbridge connector supports integration with security events, such as fire alarms or doors forced open. You can create rules and conditions in iPaaS so that incoming events will be evaluated against these predefined criteria to launch Everbridge Incidents and Scenarios if a match is found.

Enabling Security Events

Integration with Security events is disabled by default.

To enable security event integration:

1. Set the Event filters to **Include events** or **Exclude events**.



2. Specify the events that you would like to include or exclude in the text area below Event Filters. If the field is left blank, no security events will be sent. To include all events, you must add an asterisk (*). You may use an asterisk as a wildcard. In many cases, including all events will create an excess of events and should be avoided. Simple wildcards can be used as the beginning or end of the string. For example, if you want to include or exclude all door events, you would enter “door” into this field.

- Multiple events can be included by separating events with a comma. For example, duress*,LNL_Access*. The configuration is case-sensitive.

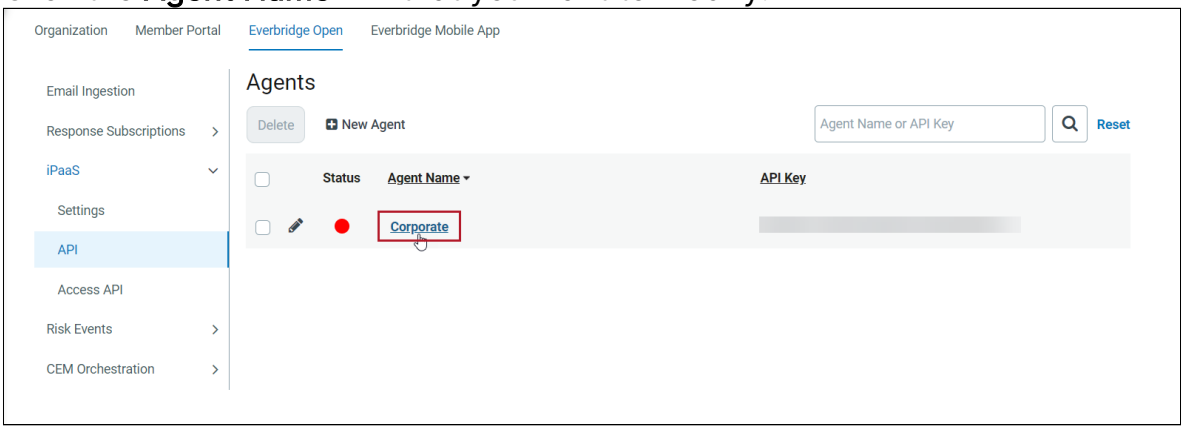
Incident Owner

The **Incident Owner** can be set per Agent Configuration and will appear in the Everbridge interface as the person who has created, updated, and closed Incidents and Scenarios.

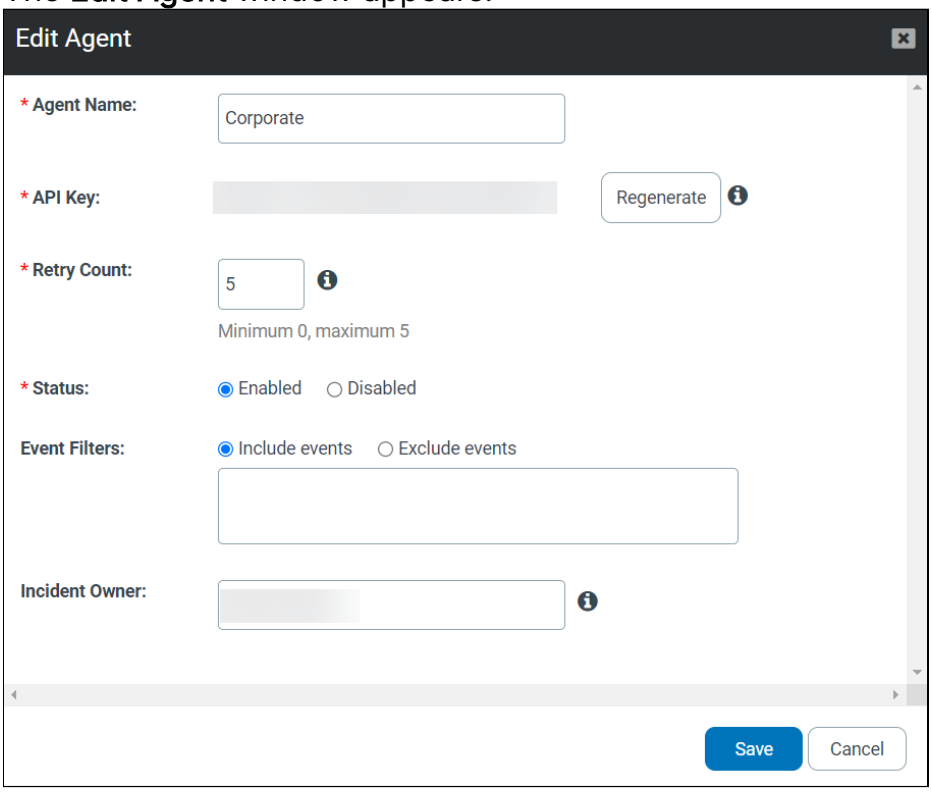
> **IMPORTANT:** If the Incident Owner or Integration User is invalid or removed, all processing in iPaaS will fail. All users must match exactly and are case-sensitive.

To set the Incident Owner:

1. Click the **Agent Name** link that you want to modify.



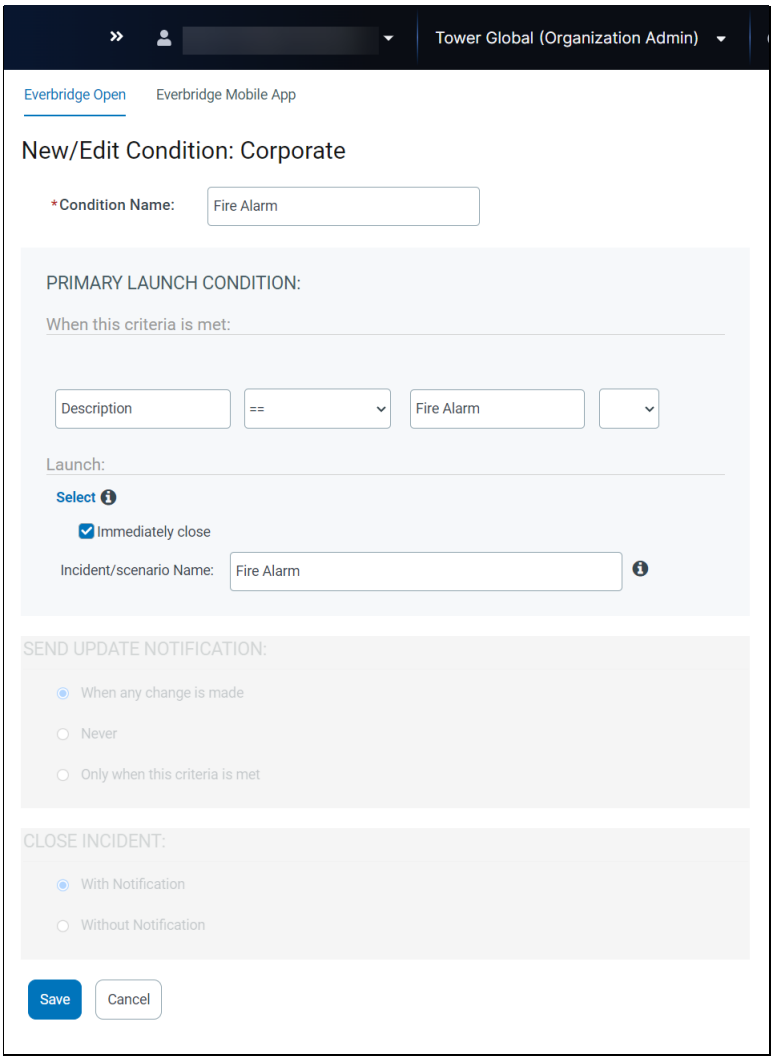
The **Edit Agent** window appears.



2. Set the **Incident Owner** field to the Everbridge Username that will appear as the Incident Owner for all Incidents created under this Agent Configuration. The selected user must be an Incident Operator or Incident Administrator.
3. Click **Save**.

Adding Conditions to Agent Configurations

Conditions contain the criteria for creating Everbridge Incidents and Scenarios, as well as Notification Templates. For instance, you might want to alert a certain group of people when fire alarm events occur. In this example, you would add a new condition that may look something like the following.



Launching Notifications

When this alarm is received by Everbridge, the security event details will be evaluated against all conditions until a match is found. The order of the evaluation is reflected in the order specified in the user interface. Once a matching condition is found, an Incident or Scenario is created and further evaluation ceases. If all conditions are evaluated and no condition matches the event received, no action is performed.

Add a Condition

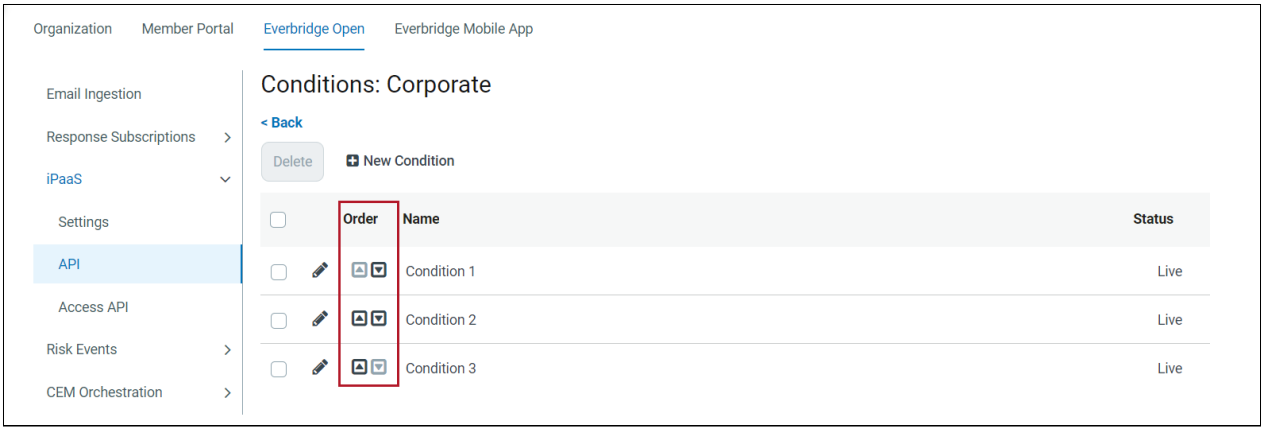
To add a condition:

1. Click the Pencil icon next to the agent configuration, or environment, in which you want to add criteria to monitor events.
2. On the **Conditions** page, click the **New Condition** button.

3. On the **New/Edit Condition** page, fill out the following fields:
    - **Condition Name** - Required field. This can be any string used to reference a set of criteria.
    - **Launch** - Required field. Select the template that will be used in the notification that will be sent when the condition is met. Only Live templates with the category “ITA” will appear in the list.
    - **Immediately close** - Select this option if only one notification will be needed. An incident will be created, the notification will be sent, and the incident will be immediately closed.
    - **The key-value pairs for fields and field values** - Valid characters are:
        - a-z
        - A-Z
        - 0-9
        - Underscore
        - Hyphen
    - **Update Incident**
        - **When any change is made** - Any time an update is received, a Notification will be sent.
        - **Never** - Updates received will not send Notifications.
    - Close Incident
        - **With Notification** - A Notification will be sent when the Incident is closed.
        - **Without Notification** - A Notification will not be sent when the Incident is closed.
4. Click **Save**.

Ordering of Conditions

The order in which conditions are displayed is the order in which they will be executed. Once a match is found, an Incident or Scenario will be created using the Template or Scenario in the corresponding condition. No other condition will be evaluated until another message is received by iPaaS. You can change the priority order of conditions in the list by using the arrow buttons to move the conditions up and down the list.


Organization
Member Portal
Everbridge Open
Everbridge Mobile App
Email Ingestion
Response Subscriptions
iPaaS
Settings
API
Access API
Risk Events
CEM Orchestration
Conditions: Corporate
< Back
Delete
New Condition
Order
Name
Status
Condition 1
Live
Condition 2
Live
Condition 3
Live

iPaaS Usage

Settings

The **Settings** tab will show a list of all the messages received by iPaaS from the client agent. This will help you troubleshoot issues when things are not working as expected.

The information displayed includes:

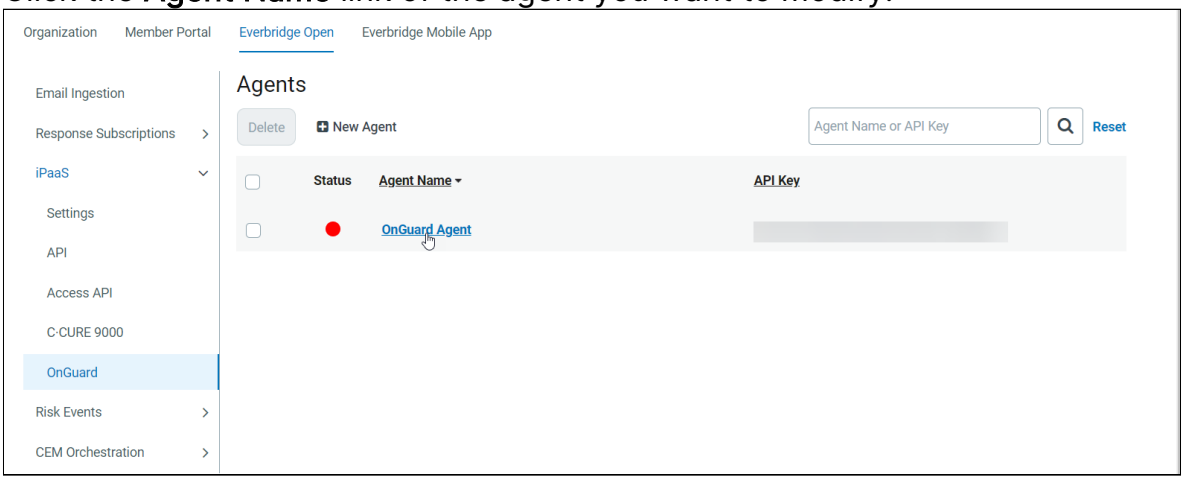
Field	Description
Source	This is the sourceSystemType field passed in the message.
Agent Name	The name of the agent configuration.
Request ID	Unique identifier that is automatically generated.
Message Status	One of the following values: SUCCESS, FAIL, or INPROGRESS.
Received Date	The date that the message was received.
Source ID	Unique identifier from client message.
Everbridge ID	The Incident/Scenario ID if one has been created.

To get message details, click the **Request ID** link.

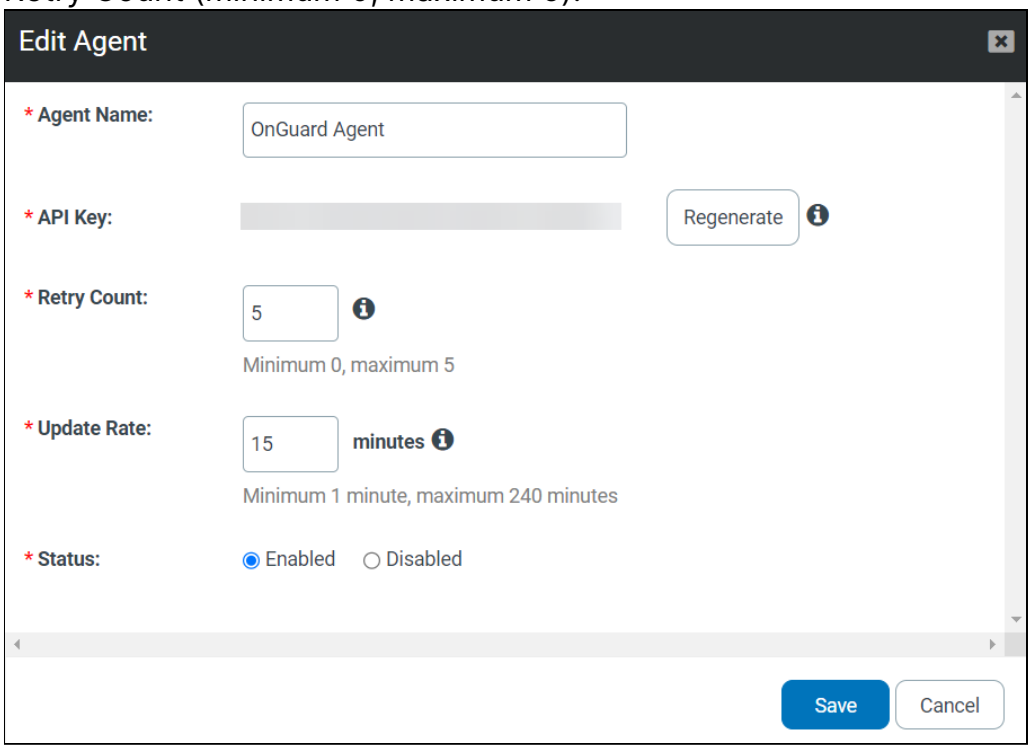
Modifying Agent Configurations

To modify agent configurations:

1. Click the **Agent Name** link of the agent you want to modify.



2. The **Edit Agent** dialog appears. Make your desired changes.
   - If you need a new API key, click the **Regenerate** button.
   - Optionally, change the Update Rate (minimum 1 minute, maximum 240 minutes) or the Retry Count (minimum 0, maximum 5).

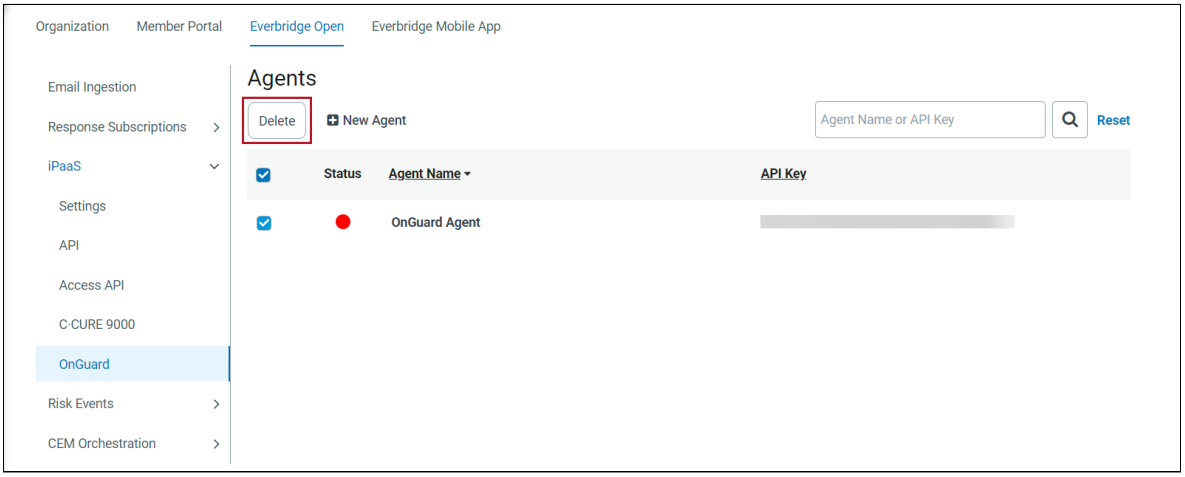


3. Click **Save**.

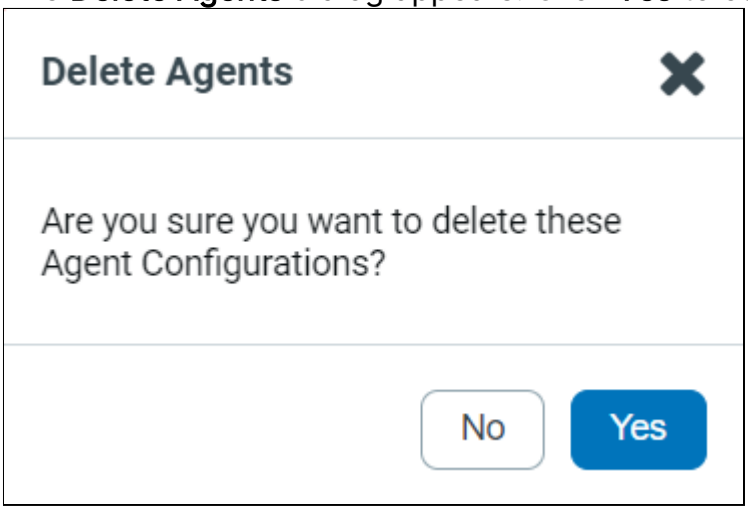
Deleting Agent Configurations

To delete agents:

1. Select the checkbox of each agent you would like to delete from the agent list view. If you would like to delete all agents, select the checkbox above the list to select all.
2. Click the **Delete** button.

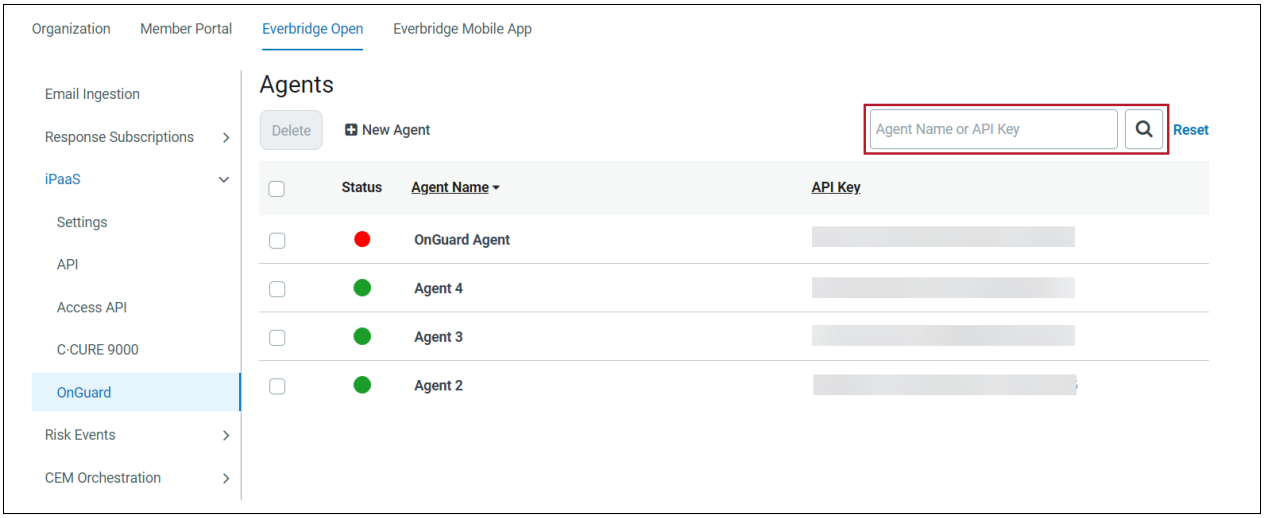


3. The **Delete Agents** dialog appears. Click **Yes** to confirm the deletions.

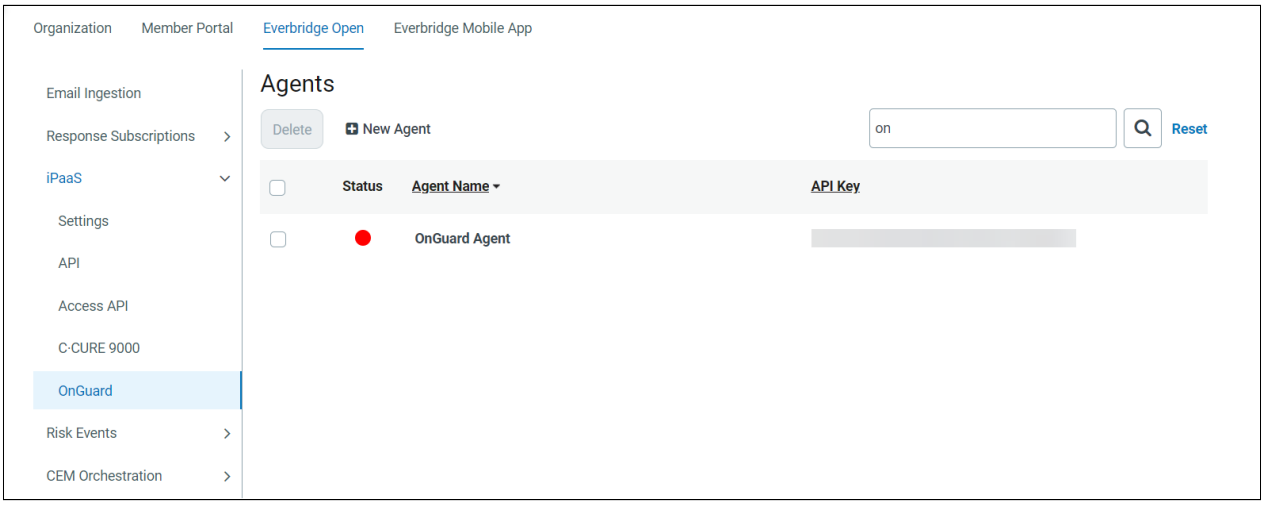


Searching

You can search for agent configurations based on API key or agent name. Type the API key, agent name (or partial name) and click the magnifying glass icon.

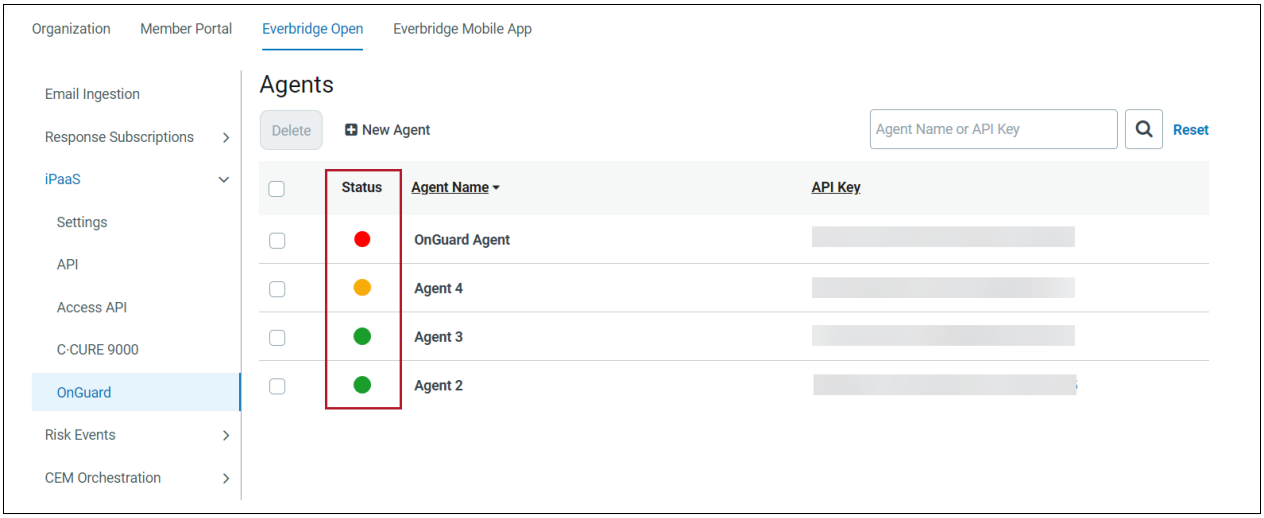


The item is displayed for you to view or modify.



Agent Health Check

The agent will be checked for a heartbeat every minute. If there is no response for two consecutive checks, a red status icon will be displayed in the agent list. If the connector is having issues communicating with the client, an orange status icon is shown.



Using the Heartbeat API to Alert on Connector Errors

The Heartbeat API can be used to integrate with an alert monitoring tool (such as AlertSite, Dynatrace, Sentry, etc) to be notified of any errors in the Importer, Exporter, or PACS system.

To get the last heartbeat, use the following endpoint:

```
GET https://ipaas-ingestion.everbridge.net/ipaas/v1/agent/heartbeat
```

The following is an example response:

```
{
  "dateTime": 1559849757,
  "currentState": "RUNNING",
  "targetConnectionIsHealthy": true,
  "errors": [
    {
      "type": "string",
      "title": "string",
      "message": "string"
    }
  ]
}
```

The expected result is an HTTP 200/OK response with the payload. An HTTP 404/ NOT FOUND response will also be returned if there has not been a heartbeat sent. Any other response is considered an error.

Using Wachete with the Heartbeat API

To receive email notifications when there is an error in the PACS Importer or Exporter, an external monitoring tool is required. Wachete is a website monitoring tool that will allow you to freely monitor up to five pages or endpoints and requires minimal setup. We recommend using your internal tools first, as Wachete requires a paid subscription to poll more often than every 24 hours. Your engineering or IT staff can provide guidance on the appropriate tool to use.

You will first need to sign up here:
https://www.wachete.com/sign-up

1. Create a new "wachet" by visiting this page and clicking **Create new watchet**: https://www.wachete.com/wachets
2. Enter the following for the URL: https://ipaas-ingestion.everbridge.net/ipaas/v1/agent/heartbeat
3. Click **Show advanced options** at the bottom right of the page. Under **HTTP request headers** enter: "Authentication:API_KEY" using the API key configured during the setup for the PACS Importer.
4. Click **Next**. You should see the above-mentioned JSON response on this page. Click on the value for "currentState", then click **Monitor**.
5. To add a notification, click **Next** and scroll down to the **Notifications** section.
6. The default notification settings will send an email to the user's email address when this value has changed. More advanced notification settings can be configured under **Show advanced options**.
7. Click **Add watchet** to finish the setup.

Resolving an Access Event to a Contact

In order to maintain consistency of Cardholder/Contact data between your PACS and Everbridge, user information in both systems must be regularly updated. The integration relies on a shared field. This field is usually an Employee ID or Email Address.

Typical values are:

- **OnGuard**: SSNO, EMAIL
- **C-CURE**: Text1-Text14, EmailAddress

Other values may be supported, depending on your configuration. This information must remain synchronized by a separate process between your user repository system of record (e.g., Human Resource database) and both your PACS system

and Evrerbridge. The only information sent between the iPaaS and the PACS Agent and Importer is a field resolving the badge ID to the user identity. The field used for user identity must match (including case and formatting) in both systems. For example, if one system trims leading zeros or spaces, and presents the field with a different format or capitalization, the correct user may not be resolved.

Upgrading From Legacy PACS Connector

This section provides the installation process for the PACS Exporter and PACS Importer when upgrading from a legacy install for OnGuard and C-CURE, as well as rollback instructions to avoid service interruptions. This upgrade should not affect any existing reader location mappings configured in iPaaS. Any configured contacts and Last Known Locations should still be updated as normal after this installation. Additionally, you will need to update your Location Source from “LENEL” to “OnGuard” and “TYCO” to “CCure9000”.

Upgrading OnGuard

To upgrade OnGuard:

1. Open **Services** and stop the Everbridge OnGuard Agent.
    - **NOTE**: We recommend stopping the old service instead of removing it in case an error occurs during this upgrade process.
2. Download Everbridge **PACS Exporter** and run the *setup.exe* installer.
3. Follow the installation instructions described in the PACS Exporter section of this guide. Verify your configuration values are correct by viewing the *Everbridge.PacsEventExport.Service.exe.config* file in the install directory.
4. Download Everbridge **PACS Importer** and run *setup.exe*.
5. Follow the installation instructions described in the PACS Importer section of this guide. Verify your configuration values are correct by viewing the *EverbridgeAgent.exe.config* file in the install directory.
6. Launch the PACS Exporter (can be started as a standard Windows Service).
7. Launch the PACS Importer (can be started as a standard Windows Service).
8. A logs directory exists in the root directory of the PACS Exporter and PACS Importer where you can view any output in case the services do not start correctly.
9. If you need to roll back, stop the PACS Exporter and PACS Importer and restart the Everbridge OnGuard Agent.

Upgrading C-CURE

To upgrade C-CURE:

1. Open **Server Configuration Application** and stop *Everbridge.NextGenConnectedProgram.Generic.Server* under the **Server Components** tab. Stop the *CrossFire Framework Service* and *CrossFire Server Component Framework Service* under the **Services** tab.

- We recommend stopping the old service instead of removing it in case an error occurs during this upgrade process.

2. Download **Everbridge PACS Exporter** and run the *setup.exe* installer.
3. Follow the installation instructions described in the PACS Exporter section of this guide. Verify your configuration values are correct by viewing the *Everbridge.PacsEventExport.Service.exe.config* file in the install directory.
4. Restart the Server components listed in Step 1 in the Server Configuration Application (except for *Everbridge.NextGenConnectedProgram.Generic.Server,* which is unused now).
5. Download **Everbridge PACS Importer** and run *setup.exe*.
6. Follow the installation instructions described in the PACS Importer section of this guide. Verify your configuration values are correct by viewing the *EverbridgeAgent.exe.config* file in the install directory.
7. Launch the PACS Exporter (can be started as a standard Windows Service).
8. Launch the PACS Importer (can be started as a standard Windows Service).
9. A logs directory exists in the root directory of the PACS Exporter and PACS Importer where you can view any output in case the services do not start correctly.
10. If you need to roll back, stop the PACS Exporter and PACS Importer and restart *Everbridge.NextGenConnectedProgram.Generic.Server* in the Server Configuration Application.

Troubleshooting

Issue Type	Possible Cause	Details
Service Does Not Start	PACS Exporter Connection	Ensure the PACS Exporter can be reached. To test connectivity, you can open a browser to: *http://SERVERNAME:PORT/api/Version* and ensure a value is returned. By default, this is: *http://localhost:43366/api/Version*
Service Does Not Start	Firewall	If installing on a remote system, work with your IT staff to ensure that the appropriate ports are open to reach the PACS collector. You can open a browser to: *http://SERVERNAME:PORT/api/Version* and ensure a value is returned.
Events Not Sent	Everbridge Connection	Manually test that you are able to still reach the Everbridge server from the server where the connector is installed. Check that the API key remains valid. Contact Everbridge support to ensure the IPAAS service is not experiencing issues.
Events Not Sent	PACS Connection	Ensure the PACS (C-Cure or OnGuard) web service is accessible. C-Cure: *http://SERVERNAME/*

		victorwebservice/ api/Generic/version. OnGuard: *https:// SERVERNAME:8080/api/ access/ onguard/openaccess/ swagger/*
Events Not Sent	PACS Connection	Ensure the PACS (C-Cure or OnGuard) web service credentials are correct. Try to manually execute a web service call to ensure your credentials are correct. Refer to the PACS vendor documentation for specific details.
Locations Not Updated in Everbridge	Badge Configuration	Check the Activity View and Badge Configuration in IPAAS to ensure that messages are received. If messages are received but not resolved to a user, ensure the badge mapping is appropriately configured.
A License Error Occurs	License is missing or invalid	Review the prerequisites section and ensure the correct license and additional associated steps have been executed. NOTE: If you are a user of the “legacy connector” a different license is required.
License Not Found in C-CURE	Older version of C-CURE	The user must have appropriate DBA permissions to inject a batch script, edit a file,

		and access logs. Permissions tend to be different across environments. Open a command prompt. Go to the directory: *Tyco**CrossFire**Tools*. Execute the following command: `InsertLicenseOption /U /V /S:" LOCALHOST" /N:"Everbridge - Webservice Suite Connection - Integration" /A:"Everbridge" /G:5bd51800-77b8-49cd -8164-0230942fb827 /C:2 /P:0`