# BridgeLink SIEM Plugin: User Guide

For BridgeLink WebAdmin

# Table of Contents

About This Guide . . . . . 3

Requirements . . . . . 4

Installation and Activation . . . . . 5

Configuration . . . . . 6

Using the SIEM Plugin . . . . . 17

Troubleshooting . . . . . 21

Support . . . . . 22

# About This Guide

The SIEM Plugin forwards BridgeLink error and event logs to one or more external Security Information and Event Management (SIEM) platforms for real-time monitoring and compliance reporting, without you leaving WebAdmin. This guide is for BridgeLink administrators who need to set up and maintain that forwarding. No SIEM expertise is required: by the end of this guide, you will be able to install and license the plugin, add and configure destinations, tune performance and alerts, and monitor delivery health from the **Statistics** tab. This guide covers SIEM Plugin version 1.0.0.

## Key Features

| Feature | Description |
|---|---|
| **Multiple Destinations** | Configure and manage several SIEM endpoints at once, each with its own protocol, address, and format. |
| **Flexible Protocols** | Send events over an HTTP/HTTPS REST API, Syslog, or write them to a local log file. |
| **Flexible Formats** | Choose **CEF**, **JSON**, or **LEEF**, so events arrive in the shape your SIEM platform expects. |
| **Independent Enable/Disable** | Turn the entire integration on or off, or enable and disable individual destinations, without deleting their configuration. |

# Requirements

- BridgeLink 26.6.0 or later.
- A SIEM Plugin license, installed on the **License Manager** tab under **Settings**. The **License Manager** plugin is a required dependency: BridgeLink will not enable the SIEM integration without a valid license on file.
- The SIEM Plugin extension itself must be installed on your BridgeLink server before it appears under **Settings**. If you do not see a **SIEM** tab after licensing, contact Innovar Healthcare support or your professional services contact to have the extension installed.
- At least one reachable SIEM destination. The plugin includes ready-made presets for **Elastic Stack**, **Splunk**, **IBM QRadar**, and **Wazuh**. Any other platform that accepts an HTTP/HTTPS REST API, Syslog, or a local log file, such as ArcSight, connects using the **Other / Custom** option.
- Network connectivity from the BridgeLink server to each SIEM destination (the appropriate outbound port, such as 514 for Syslog, must be reachable).

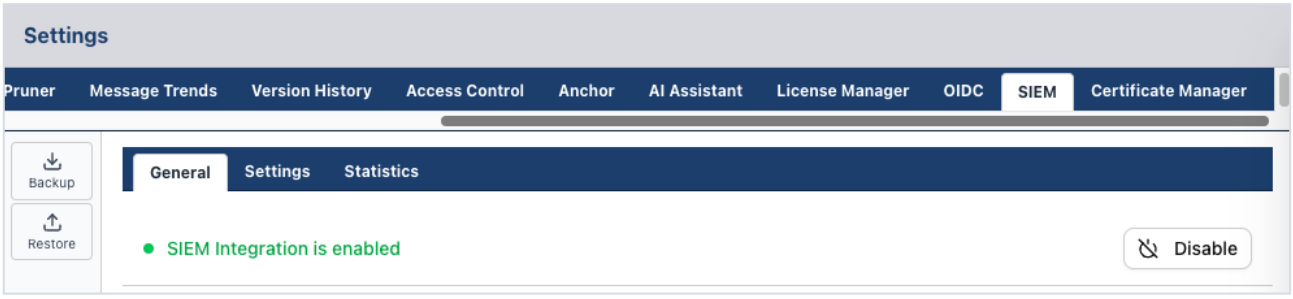
# Installation and Activation

1. Sign in to **WebAdmin** as an administrator.
2. Open **Settings**, then click the **SIEM** tab. If the tab is not listed, the SIEM Plugin extension is not yet installed; contact Innovar Healthcare support or your professional services contact.
3. Click the **License Manager** tab, then the **Installed Licenses** sub-tab.
4. Click **Install License** and choose the SIEM Plugin license file, a `.json` file supplied by Innovar Healthcare.
5. Review the **Install License** dialog, which previews the license's **Customer**, **Products**, **Issued**, **Expires**, and **Server match**, then click **Install**. A confirmation toast reads "License installed."
6. Restart BridgeLink when prompted; a banner reads "License changes will take effect after restarting BridgeLink."
7. Click the **License Status** sub-tab and confirm the **SIEM Plugin** row shows **Active** under **Status**.
8. Click the **SIEM** tab to begin configuration.

# Configuration

## General Tab: Enabling and Disabling SIEM Integration

The **General** tab is the default view when you open the **SIEM** tab, and it shows the current status of the integration at the top of the screen.




SIEM tab, General sub-tab, showing the SIEM Integration is enabled status and Disable button

- When SIEM integration is turned on, the screen shows a green **SIEM Integration is enabled** message and a **Disable** button.
- When it is turned off, the screen shows an orange **SIEM Integration is disabled** message and an **Enable** button.

To turn the integration off:

1. Click **Disable**.
2. Confirm in the **Disable SIEM Integration** dialog. Event forwarding stops immediately across all destinations, even if individual destinations are still configured and enabled.

To turn the integration back on:

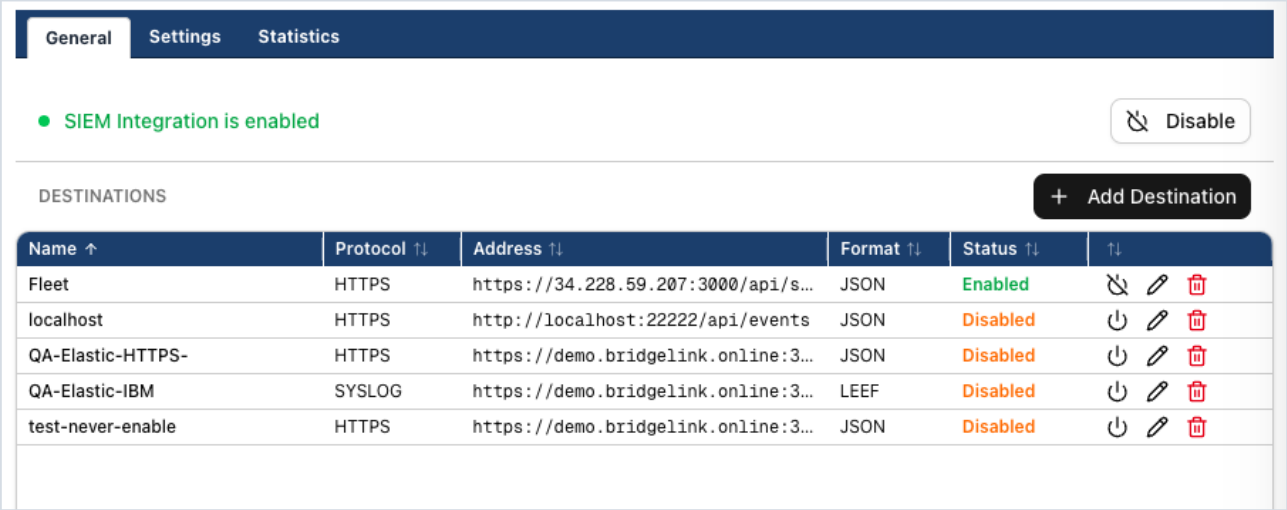
1. Click **Enable**. Forwarding resumes immediately to every destination that is itself enabled; no confirmation is required.

This is a master switch: disabling it here stops all SIEM forwarding at once, without needing to disable each destination individually.

The **General** tab also has its own action panel, on the left, with **Backup** and **Restore** buttons for exporting and importing the SIEM configuration as a file.

## Destinations Table

Below the master switch, the **Destinations** table lists every SIEM endpoint you have configured. Each row shows one destination's connection details at a glance, and you can click the sort arrows in any column header to sort the table by that column.




Destinations table listing configured SIEM endpoints with their protocol, address, format, and status

| Column | Description |
|---|---|
| **Name** | A friendly label you give the destination, so it is easy to identify (for example, `Fleet` or `QA-Elastic-IBM`). |
| **Protocol** | The transport method used to send events: **HTTP/HTTPS REST API**, **Syslog** (UDP or TCP, with optional TLS), or **Log File** (writes events to a local file, with optional automatic rotation and compression). |
| **Address** | The destination URL or `host:port` where events are sent. |
| **Format** | The event format sent to this destination: **CEF**, **JSON**, or **LEEF**. |
| **Status** | Whether this destination is currently **Enabled** or **Disabled**. |

Protocol determines how events are transmitted; Format determines how the event data is structured once it reaches your SIEM. You can mix and match, for example an HTTP/HTTPS REST API destination with JSON, or a Syslog destination with LEEF, depending on what your SIEM platform expects. A **Log File** destination writes raw output and typically pairs with a log shipper (such as Filebeat) rather than a SIEM-specific format.

Each destination row has three action icons on the right:

| Icon | Action |
|---|---|
| Power | Enable or disable this specific destination, without affecting others. |
| Pencil | Open the **Edit Destination** dialog for this destination's configuration. |
| Trash | Permanently delete the destination. A confirmation dialog warns that this cannot be undone and will immediately stop forwarding events to it. |

A destination's individual status only matters if the master **SIEM Integration** switch on the **General** tab is also enabled. If the master switch is off, all destinations stop forwarding

regardless of their individual status.

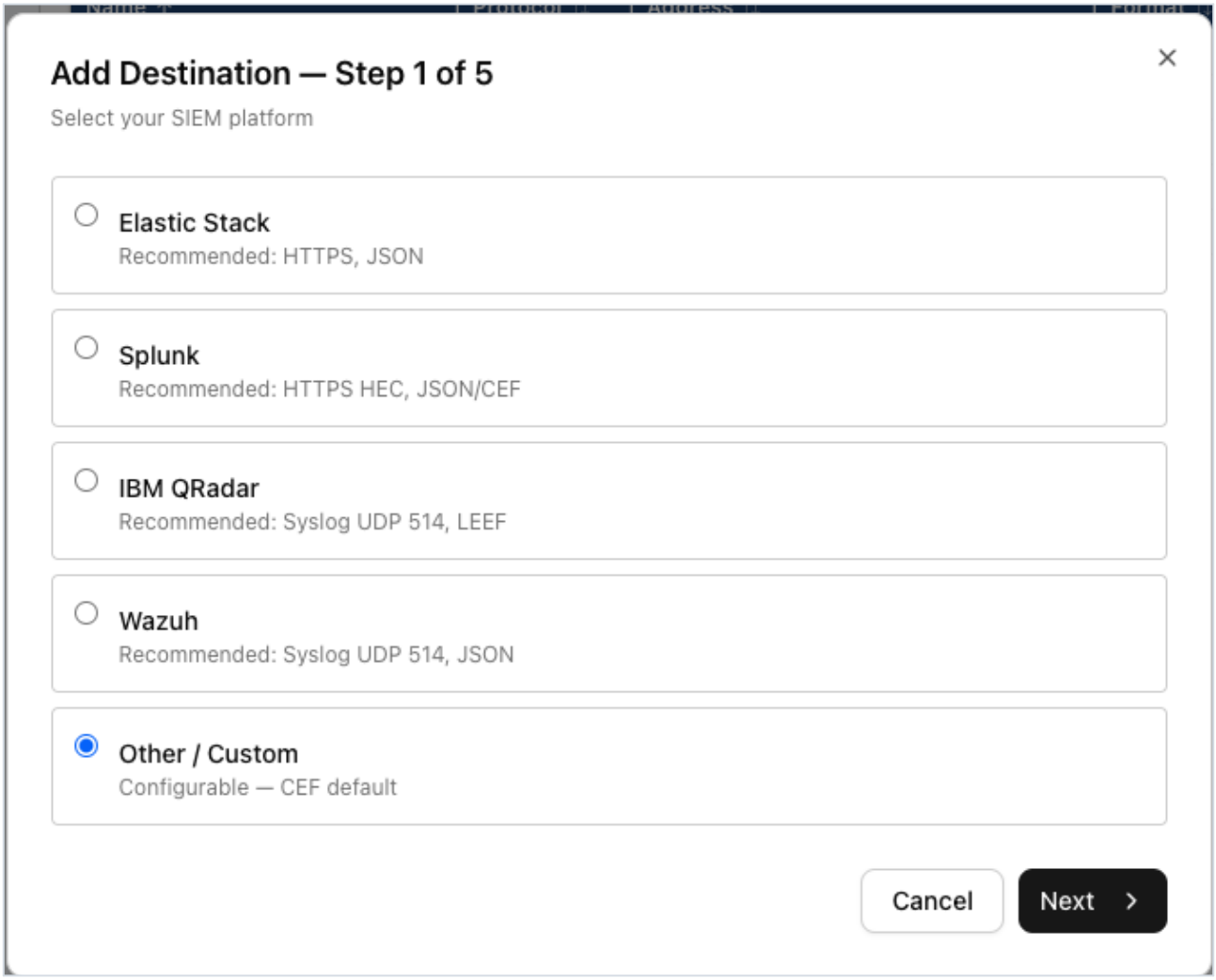
To add a new SIEM destination, click **Add Destination** in the top-right corner of the table. See **Adding a Destination** below for the setup steps.

## Adding a Destination

Clicking **Add Destination** opens a five-step wizard.

1. Click **Add Destination** in the **Destinations** table. The **Add Destination** wizard opens on **Step 1 of 5**.
2. Select your SIEM platform, then click **Next**. Each preset fills in a recommended **Protocol** and **Format** so you do not have to configure them manually.

| Platform | Recommended protocol and format |
|---|---|
| **Elastic Stack** | HTTP/HTTPS REST API, JSON |
| **Splunk** | HTTP/HTTPS REST API (HEC), JSON or CEF |
| **IBM QRadar** | Syslog, UDP port 514, LEEF |
| **Wazuh** | Syslog, UDP port 514, JSON |
| **Other / Custom** | Fully configurable; CEF by default |

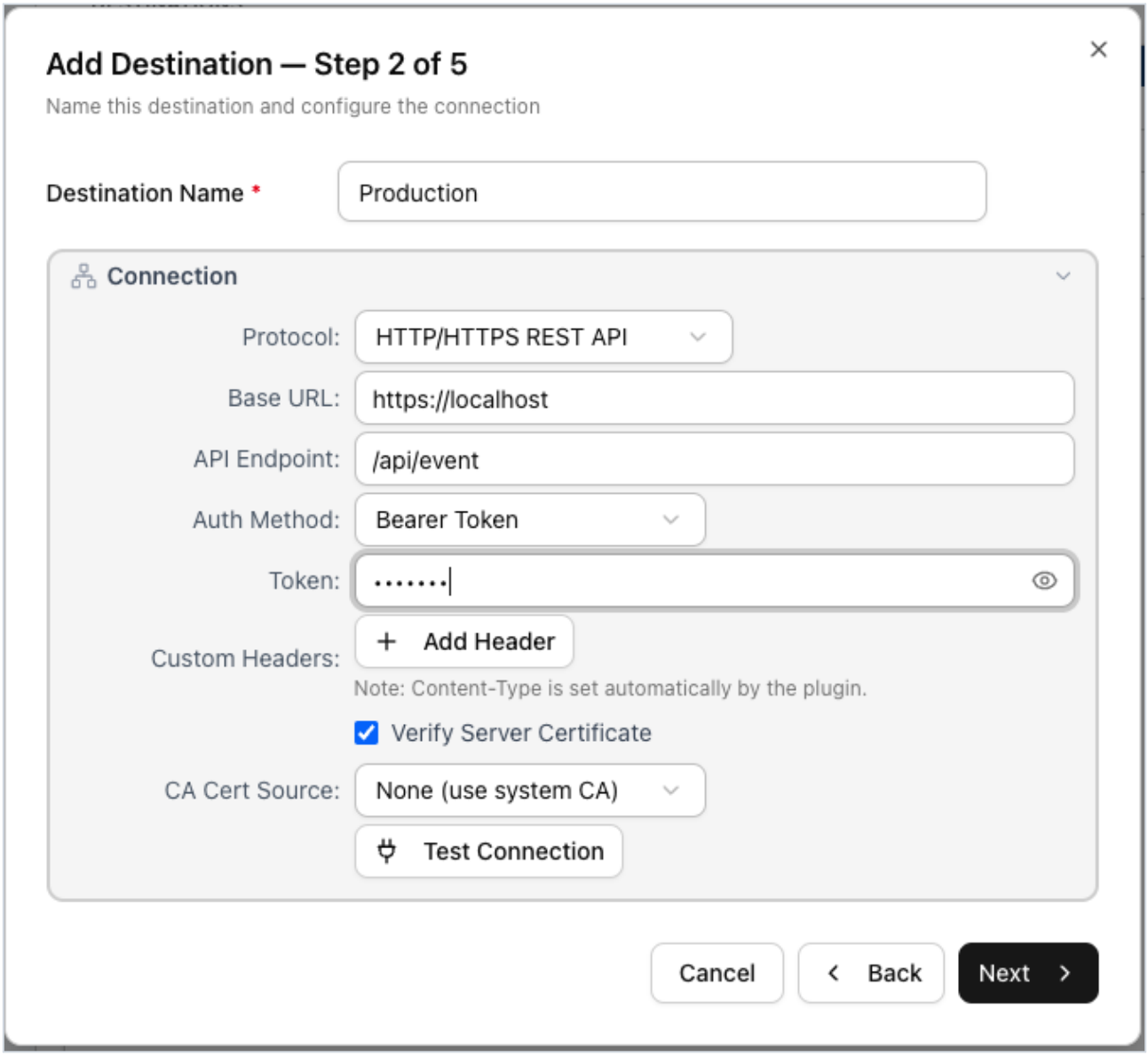



Add Destination wizard, Step 1 of 5, selecting the SIEM platform

If your platform is not listed, select **Other / Custom** and configure the connection manually.

3. On **Step 2 of 5**, enter a **Destination Name** to identify this destination later (for example, `Production` or `QA-Elastic-IBM`), then fill in the connection fields shown for the selected **Protocol**.




Add Destination wizard, Step 2 of 5, naming the destination and configuring the connection

| Protocol | Fields |
|---|---|
| **HTTP/HTTPS REST API** | **Base URL**, **API Endpoint**, **Auth Method** (**Bearer Token**, **API Key**, or **Basic Auth**), a token or credential field that changes with the selected **Auth Method** (**Token** for Bearer Token, **API Key** for API Key, or **Username**/**Password** for Basic Auth), **Custom Headers** (add more with **Add Header**), **Verify Server Certificate**, **CA Cert Source** (**None (use system CA)**, **Custom CA file path**, or **SSL plugin store**). |

| Protocol | Fields |
|---|---|
| **Syslog** | **Transport** (**UDP** or **TCP**), **Destination Host**, **Port** (default `514`), and when **TCP** is selected, a **TLS/SSL** checkbox followed by **Verify Server Certificate** and **CA Cert Source** (same three options as above). Then **Framing** (**RFC 5424** or **RFC 3164 (legacy)**) and **Facility** (`local0` through `local7`, default `local0`). |
| **Log File** | **Path**, **Enable automatic rotation**, and when rotation is enabled: **Max Size** (default `100` MB), **Max Files** (default `10`), **Compression** (**None** or **GZIP**, default **GZIP**), and **Rotation Type** (**Size-based** or **Time-based (daily)**). |

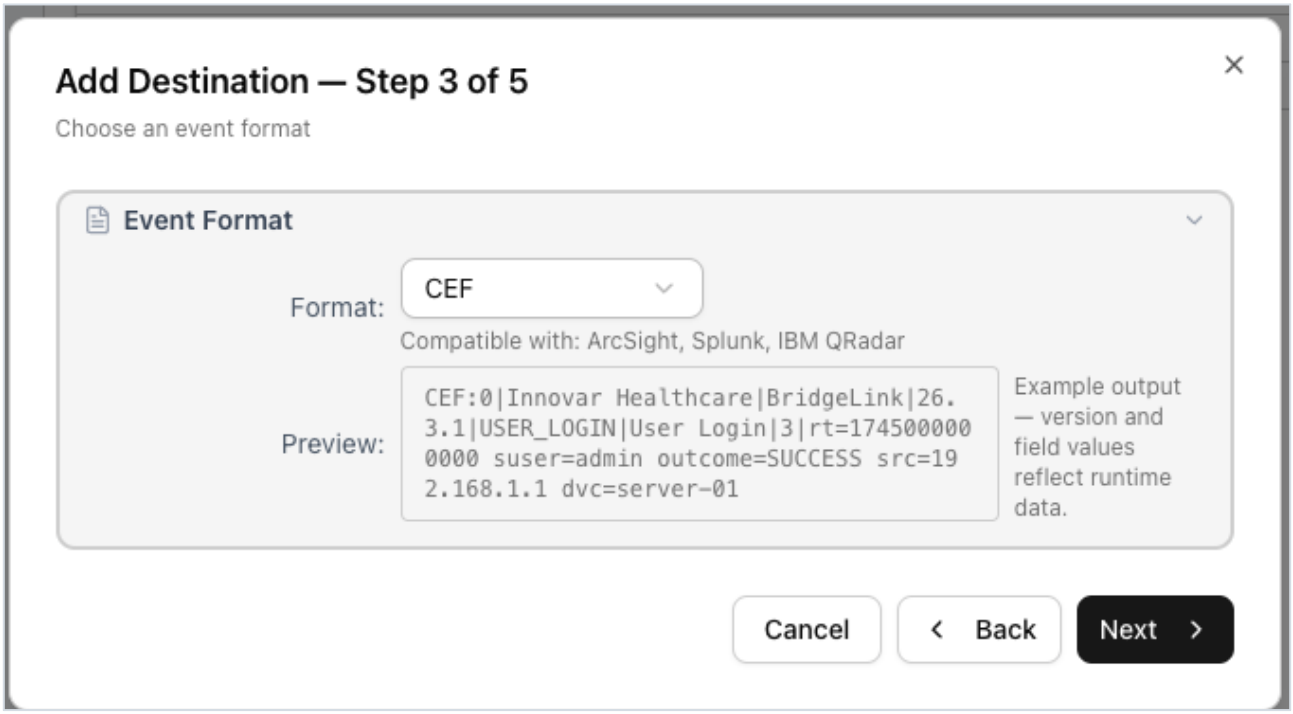
Selecting **SSL plugin store** for **CA Cert Source** requires a certificate store already configured in the SSL plugin.

Click **Test Connection** (or **Test Write Access** for a **Log File** destination) to confirm the destination is reachable, then click **Next**.

When a preset platform was chosen in Step 1, **Protocol** is locked to the recommended value. Selecting **Other / Custom** in Step 1 lets you choose the **Protocol** yourself.

4. On **Step 3 of 5**, select an **Event Format**, then click **Next**. The available options depend on the platform chosen in Step 1: **Elastic Stack** and **Wazuh** offer JSON only, **IBM QRadar** offers LEEF only, **Splunk** offers JSON or CEF, and **Other / Custom** offers all three. A compatibility hint and a live preview of sample output are shown below the dropdown.

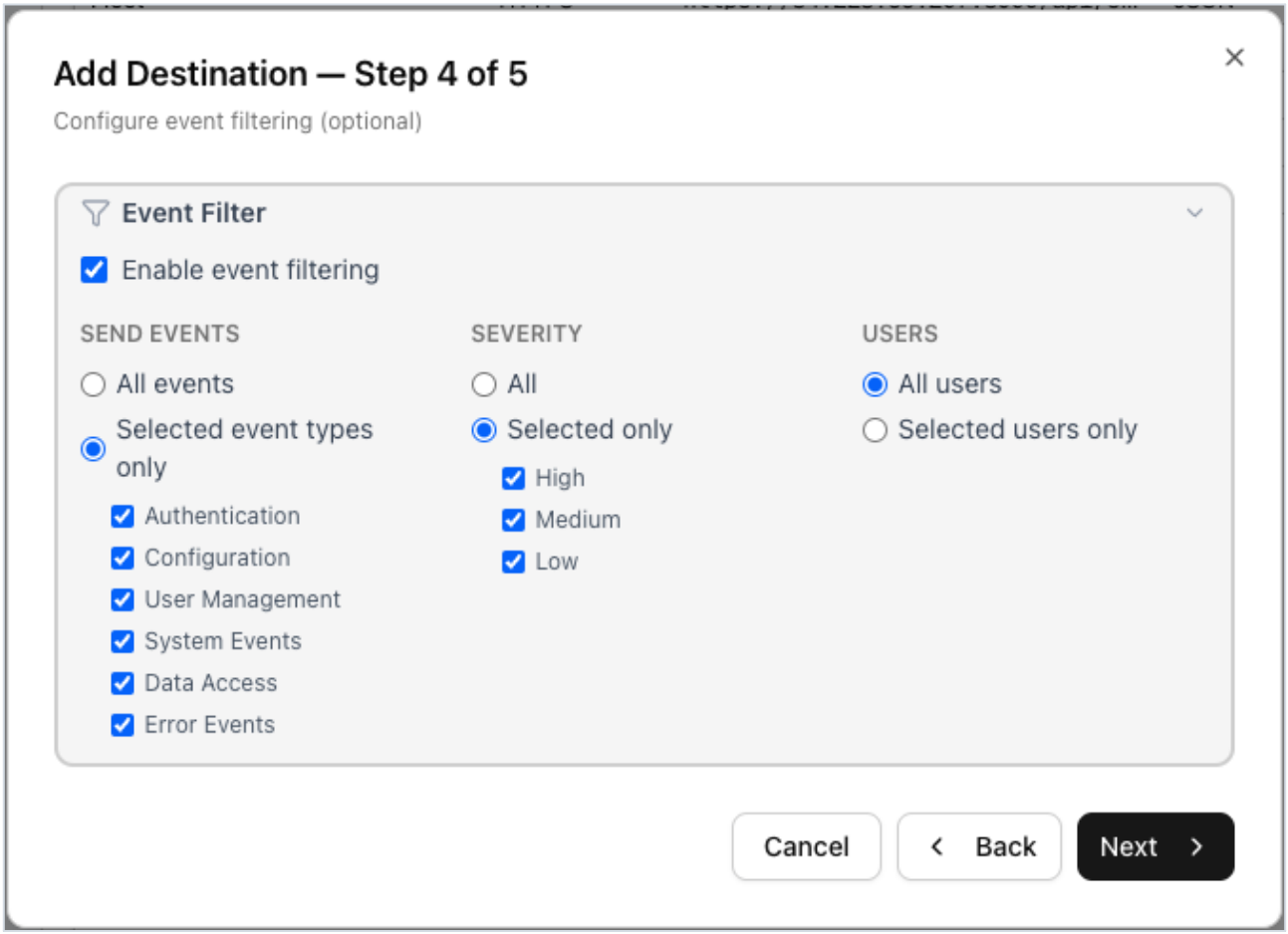
| Format | Compatible with |
|---|---|
| **CEF** | ArcSight, Splunk, IBM QRadar |
| **JSON** | Splunk, Elastic Stack, most modern SIEMs |
| **LEEF** | IBM QRadar |




Add Destination wizard, Step 3 of 5, choosing the event format

5. On **Step 4 of 5**, optionally check **Enable event filtering** to narrow down what is forwarded, then click **Next**. By default, all events are sent.

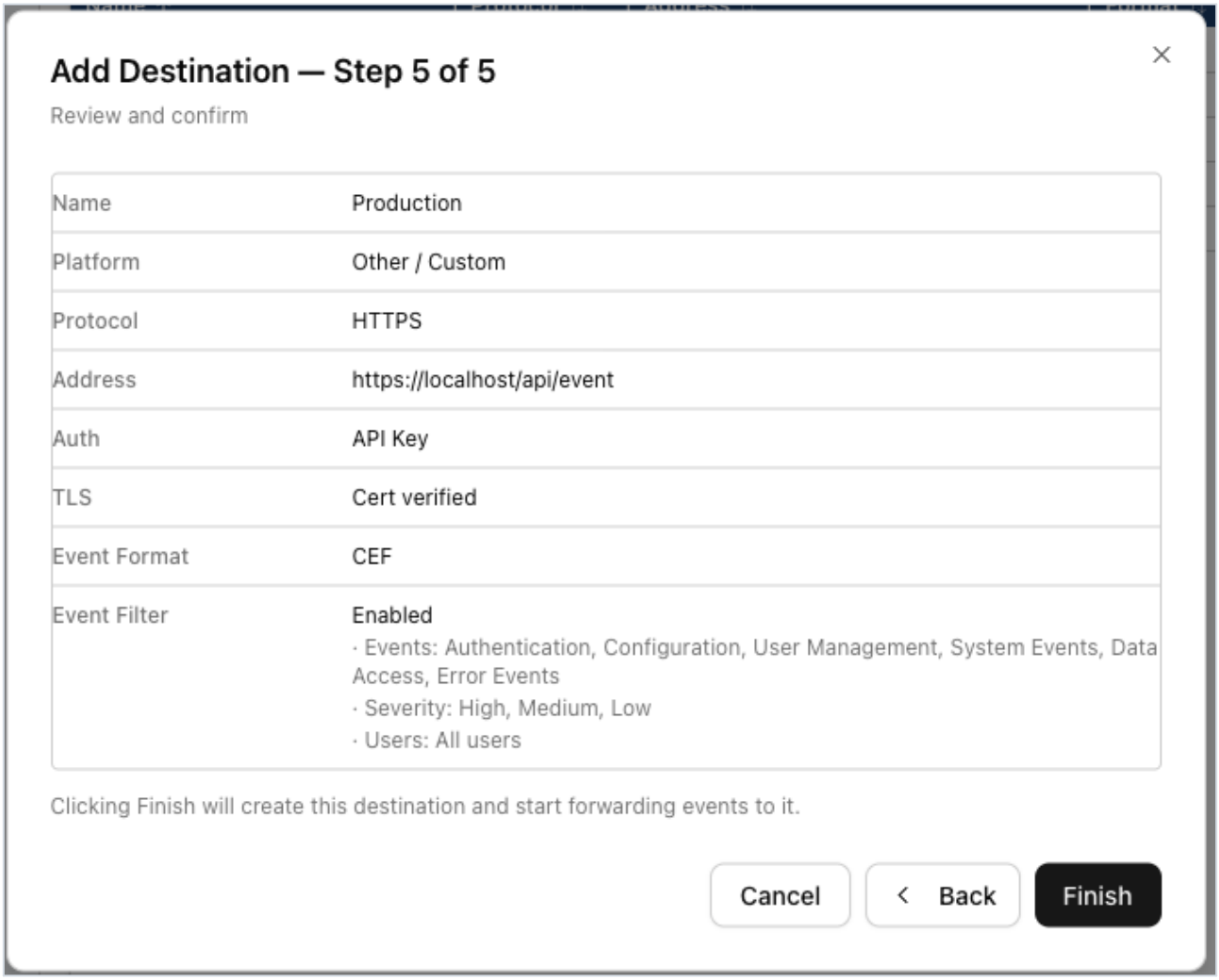



Add Destination wizard, Step 4 of 5, configuring optional event filtering

| Group | Options |
|---|---|
| **Send Events** | **All events**, or **Selected event types only**: **Authentication**, **Configuration**, **User Management**, **System Events**, **Data Access**, **Error Events**. |
| **Severity** | **All**, or **Selected only**: **High**, **Medium**, **Low**. |
| **Users** | **All users**, or **Selected users only** (searchable list). |

Filtering reduces the volume of events sent to your SIEM, which can lower ingestion costs. Consider starting with **All events** to confirm the integration is working, then narrowing the filter afterward.

6. On **Step 5 of 5**, review the summary of your configuration (**Name**, **Platform**, **Protocol**, **Address**, **Auth**, **TLS**, **Event Format**, and **Event Filter**), then click **Finish**.

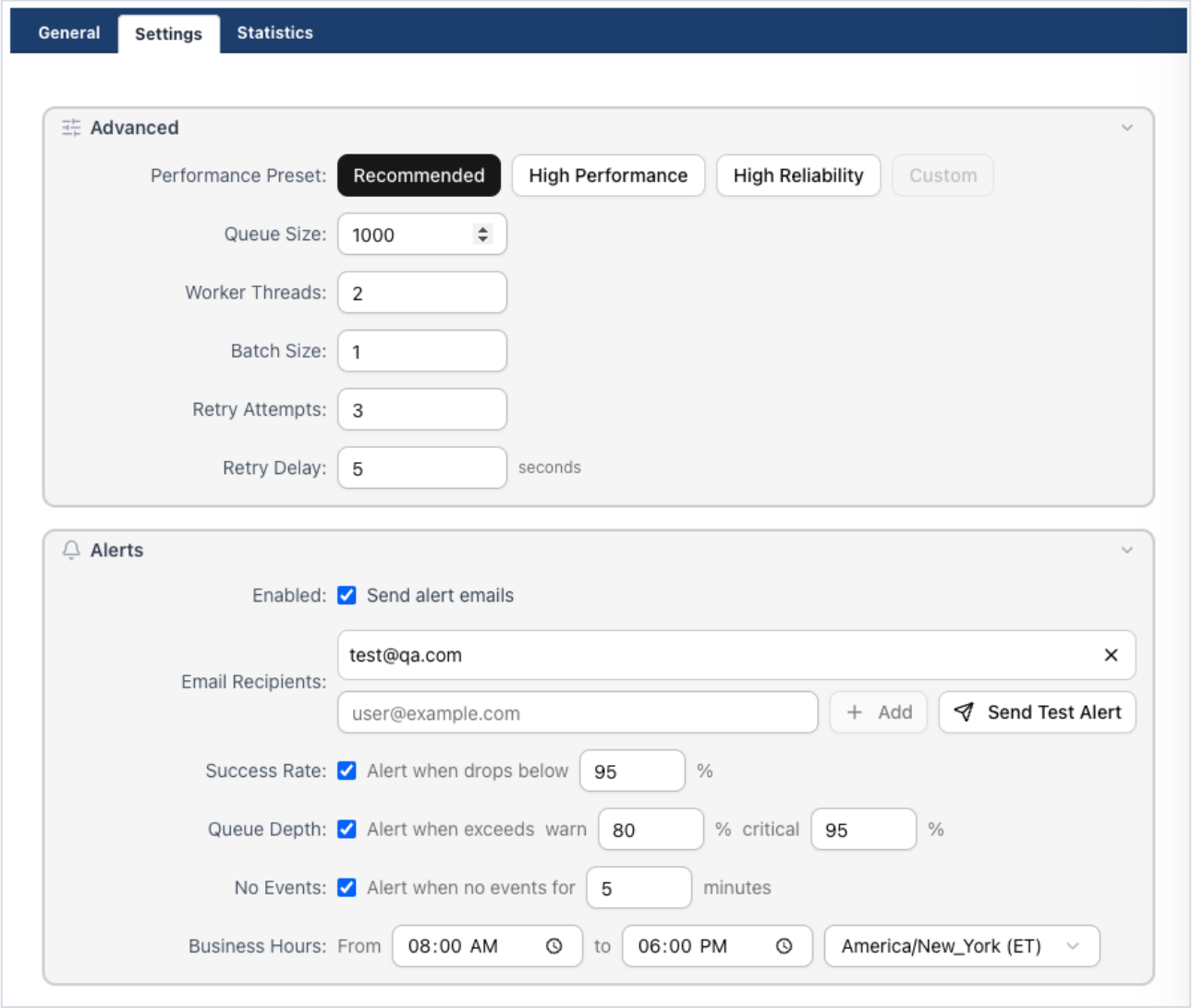



Add Destination wizard, Step 5 of 5, reviewing and confirming the new destination

BridgeLink creates the destination and immediately starts forwarding events to it based on this configuration.

## Settings Tab

The **Settings** tab lets you fine-tune performance and set up alerts that apply across all destinations.




Settings tab showing the Advanced performance tuning and Alerts sections

### Advanced (Performance Tuning)

Click a **Performance Preset** button (**Recommended**, **High Performance**, or **High Reliability**) to fill in the fields below with matching values. **Custom** is not a button you click; it appears automatically as soon as you edit any of the fields directly.

| Field | What it does | Default |
|---|---|---|
| **Performance Preset** | Quick presets that adjust the fields below. | `Recommended` |
| **Queue Size** | Number of events buffered before older ones are dropped. | `1000` |
| **Worker Threads** | Number of threads processing the send queue; more threads increase throughput. | `2` |

| Field | What it does | Default |
|---|---|---|
| **Batch Size** | Number of events sent per batch; 1 sends in real time, higher values improve efficiency. | 1 |
| **Retry Attempts** | How many times to retry sending an event after a failure. | 3 |
| **Retry Delay** | Seconds to wait between retry attempts. | 5 |

| Preset | Queue Size | Worker Threads | Batch Size | Retry Attempts | Retry Delay |
|---|---|---|---|---|---|
| **Recommended** | 1000 | 2 | 1 | 3 | 5 |
| **High Performance** | 5000 | 4 | 100 | 1 | 1 |
| **High Reliability** | 10000 | 2 | 1 | 5 | 10 |

### Alerts

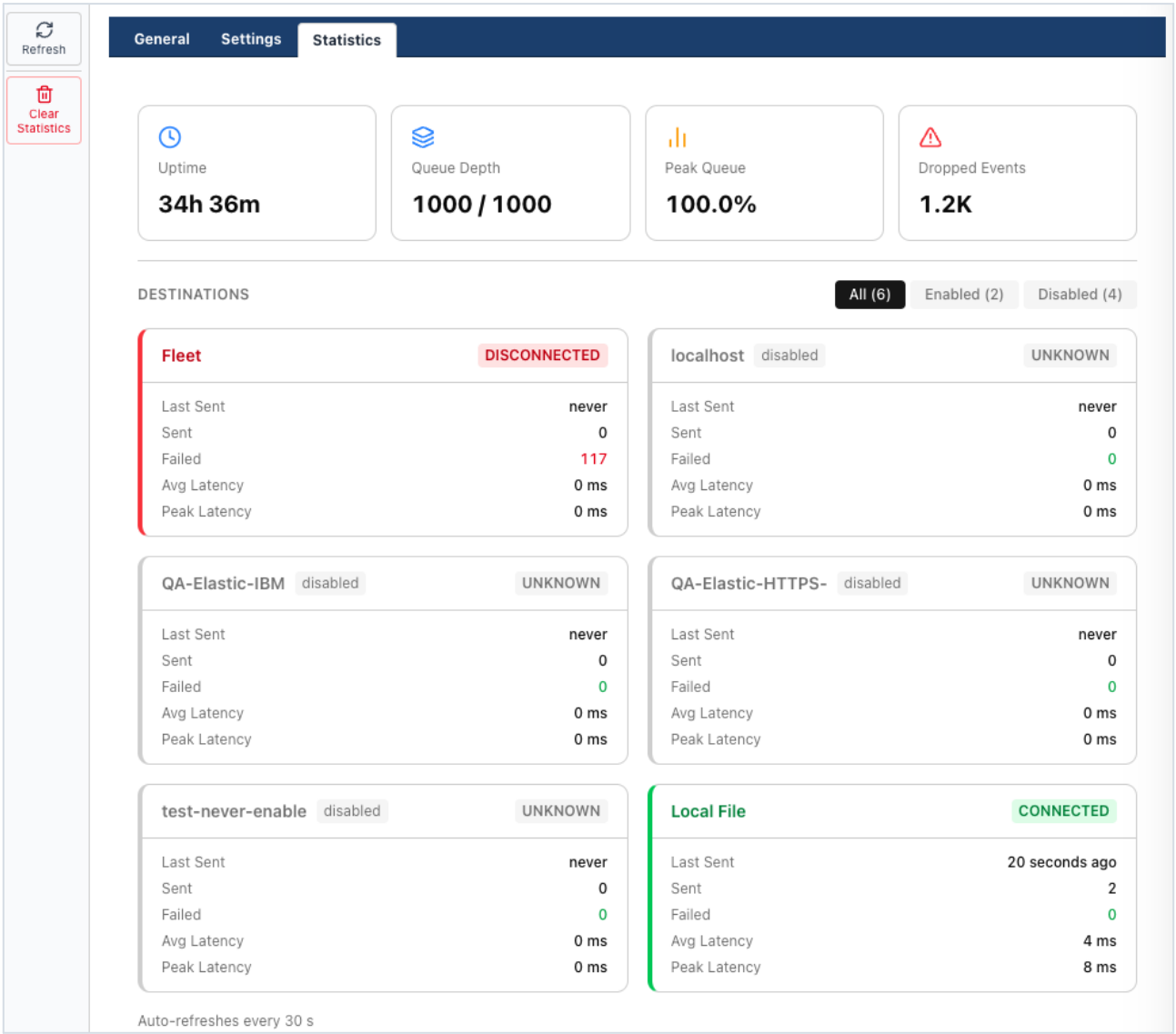
| Field | What it does | Default |
|---|---|---|
| **Send alert emails** | Master toggle for email alerts. | Off |
| **Email Recipients** | One or more email addresses to notify; add more with **Add**. | none |
| **Success Rate** | Alerts when the delivery success rate drops below this percentage. | 95% |
| **Queue Depth** | Alerts when the queue exceeds a warning threshold and a critical threshold. | 80% warn, 95% critical |
| **No Events** | Alerts if no events are sent within this many minutes. | 5 |
| **Business Hours** | Time range and time zone during which alerts are active. | 08:00 AM to 06:00 PM, America/New York (ET) |

Use **Send Test Alert** to confirm your email recipients are configured correctly before relying on the integration. Click **Save** in the action panel to apply your changes.

# Using the SIEM Plugin

## Viewing Integration Health

The **Statistics** tab shows real-time health metrics for the SIEM integration, refreshed automatically every `30` seconds or manually with **Refresh**.




Statistics tab summary cards and destination cards

| Metric | Description |
|---|---|
| **Uptime** | How long the SIEM integration has been running continuously. |
| **Queue Depth** | Current events in queue versus the maximum queue size (for example, `1000 / 1000`). |

| Metric | Description |
|---|---|
| **Peak Queue** | Highest queue utilization reached, as a percentage. |
| **Dropped Events** | Number of events dropped because the queue was full. |

If **Queue Depth** or **Peak Queue** stays near `100%` and **Dropped Events** keeps rising, consider increasing **Queue Size** or **Worker Threads** on the **Settings** tab.

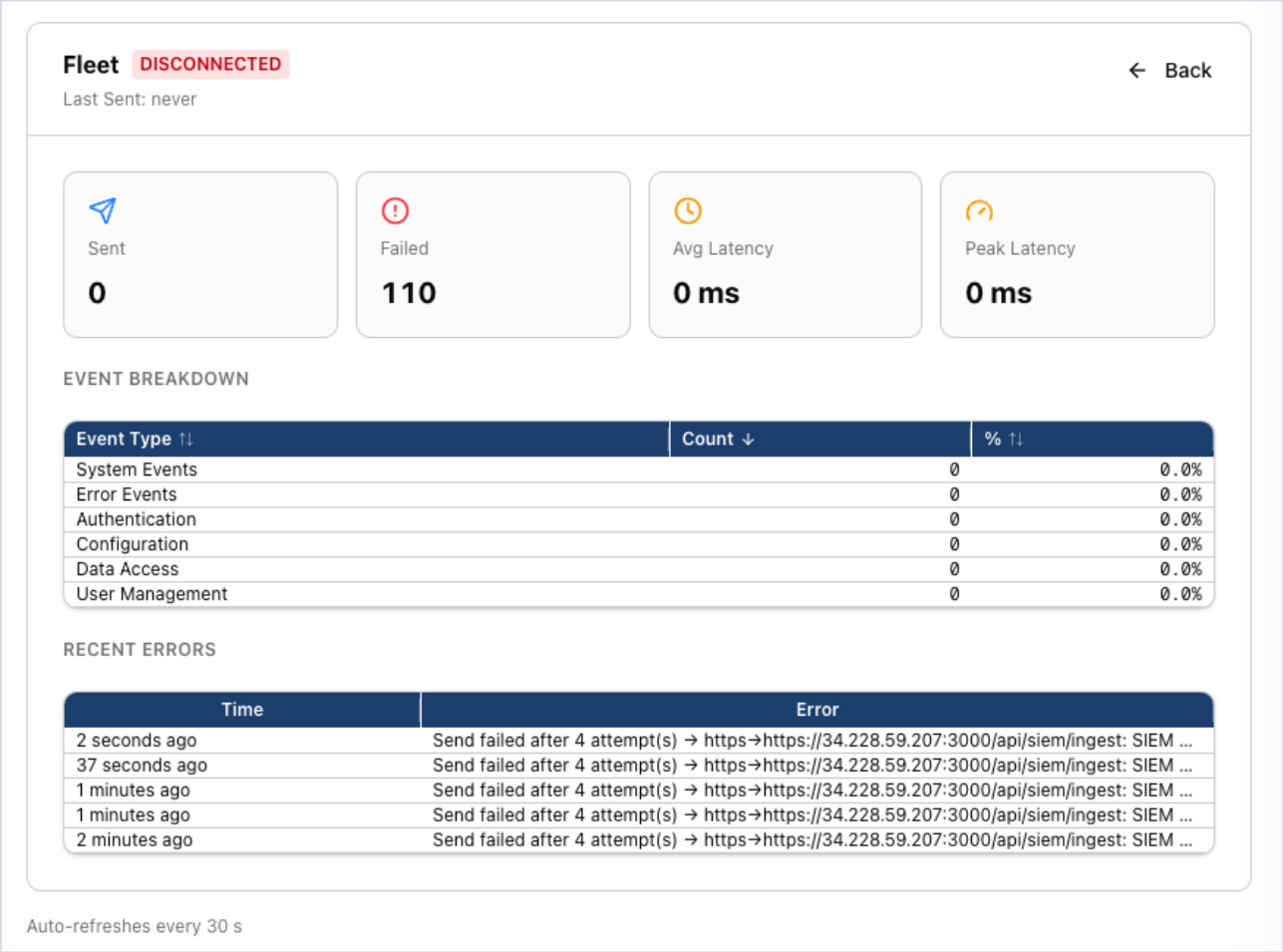
Below the summary cards, each destination appears as a card with **Last Sent**, **Sent**, **Failed**, **Avg Latency**, and **Peak Latency**, and you can filter the cards by **All**, **Enabled**, or **Disabled**.

| Badge | Meaning |
|---|---|
| **CONNECTED** (green) | The destination is enabled and successfully sending events. |
| **DISCONNECTED** (red) | The destination is enabled but currently unable to reach its target. Check the **Failed** count and verify the connection details. |
| **UNKNOWN** (gray) | The destination is disabled, so no attempt is made to connect to it. |

Use **Clear Statistics** in the action panel to reset all counters back to zero, useful after resolving an issue so you can confirm the fix by watching fresh numbers.

## Viewing Destination Details

Click any destination card to open a detailed view for that destination, with a **Back** link to return to the summary.




Destination detail view showing metrics, event breakdown, and recent errors for a disconnected destination

- **Metrics**: the same four metrics as the summary card (**Sent**, **Failed**, **Avg Latency**, **Peak Latency**), scoped to this destination only.
- **Event Breakdown**: a sortable table showing how many events of each type were sent to this destination, and what percentage of the total they represent (**System Events**, **Error Events**, **Authentication**, **Configuration**, **Data Access**, **User Management**).
- **Recent Errors**: a log of the most recent delivery failures, with **Time** (relative, for example `19 seconds ago`) and **Error** (the failure reason, including the number of attempts and the target address).

The **Recent Errors** table is the fastest place to diagnose a **DISCONNECTED** destination: it shows exactly why sends are failing (for example, connection refused, timeout, or an authentication error), without needing to check server logs.

## Editing or Deleting a Destination

1. In the **Destinations** table on the **General** tab, find the destination.
2. Click the pencil icon to open **Edit Destination**, or click the trash icon to delete it.

3. If editing, update the fields and click **Save**. If the destination was disabled, click **Save & Enable** instead to save your changes and turn it back on in one step.
4. If deleting, confirm in the dialog. Deleting a destination cannot be undone and immediately stops forwarding events to it.

## Backing Up and Restoring SIEM Configuration

1. On the **General** tab, click **Backup** in the action panel to download the current SIEM configuration.
2. To restore a previous configuration, click **Restore** in the action panel and select a backup file.

# Troubleshooting

| Symptom | Likely cause | What to do |
|---|---|---|
| No **SIEM** tab appears under **Settings**. | The SIEM Plugin extension is not installed, or it is installed but unlicensed. | Contact Innovar Healthcare support to install the extension, then check **Settings > License Manager > License Status**. |
| A destination shows **DISCONNECTED** on the **Statistics** tab. | The destination is enabled but BridgeLink cannot reach it. | Open the destination's detail view and check **Recent Errors** for the failure reason, then verify the connection details on the **General** tab. |
| **Dropped Events** keeps rising and **Queue Depth** or **Peak Queue** stays near `100%`. | The send queue cannot keep up with incoming events. | Increase **Queue Size** or **Worker Threads** on the **Settings** tab, or apply the **High Performance** preset. |
| No alert emails arrive. | **Send alert emails** is off, **Email Recipients** is empty, or the alert thresholds have not been crossed. | On the **Settings** tab, confirm **Send alert emails** is checked and recipients are listed, then use **Send Test Alert** to confirm delivery. |
| Events are missing at the SIEM platform even though the destination shows **CONNECTED**. | Event filtering is narrower than expected. | Edit the destination and review the **Send Events**, **Severity**, and **Users** filters from Step 4 of the wizard. |
| The master switch is enabled, but a specific destination never sends events. | The individual destination is disabled. | On the **General** tab, use the power icon in the **Destinations** table to enable that destination. |

# Support

Contact Innovar Healthcare support at `support@innovarhealthcare.com` for help with the SIEM Plugin. Include the following in your request:

- Your BridgeLink version
- Your SIEM Plugin version
- The affected destination's name, protocol, and format
- Relevant entries from the **Recent Errors** table on the **Statistics** tab, or from the BridgeLink Server Log

For help planning a SIEM rollout across multiple destinations, or integrating with a platform not covered by the built-in presets, Innovar Healthcare's professional services team is also available.