blacklinesafety

BLACKLINE LIVE

Technical User Manual

CONTENTS

CONTENTS

1 WHAT IS BLACKLINE LIVE?

2 ORGANIZATION STRUCTURE

2.1 Organizations....2
2.2 Groups....2
2.3 Account Users....3
2.4 Group access....3
2.5 Group roles and permissions....4
2.6 Relationships....6

3 ORGANIZATION SETUP

3.1 Registering an organization....7
3.2 Navigating Blackline Live....8
3.3 Organization details....11
3.4 Team members....12
3.5 Group setup....15
3.6 Devices and device setup....18
3.7 Contact groups....22
3.8 Configuration profiles....22
3.9 Alert profiles....26
3.10 Relationships page....28

4 ACCESSORIES

4.1 G7 Dock configuration....29
4.2 Location beacons....30

5 5. MONITORING AND REVIEW

5.1 Maps....32
5.2 Dashboard....36
5.3 Alerts....36
5.4 Bump Test and Calibration Certificates....42
5.5 Mass Notifications....42

6 BLACKLINE ANALYTICS

6.1 Tools within Blackline Analytics....45
6.2 Exporting data froM Blackline Analytics....47
6.3 Blackline Vision....47

7 SUPPORT

7.1 Learn More....47
7.2 Customer Care....47

8 GLOSSARY

1. WHAT IS BLACKLINE LIVE?

Blackline Live is your one-stop solution for configuring and managing your fleet of Blackline Safety monitoring devices. This cloud-hosted software platform can be accessed for free from any Internet-connected device, and allows you to easily customize and monitor your device fleet.

Blackline Live allows you to view and manage your organization's resources — from the devices themselves to the team that uses them. You can use this online portal to customize which features a device will use in the field, and how monitoring personnel should respond when they go into alert. In addition, Blackline Analytics — hosted within Blackline Live — automatically collects data from your device fleet and displays them in comprehensive visual reports that can help you pinpoint problem areas on the worksite or gaps in training, and displays current and trending usage time, gas compliance and much more.

What devices does Blackline Live support?

Blackline Live supports all of Blackline's safety monitoring devices. Blackline's primary device line includes:

- G7c
- G7x and G7 Bridge
- G7 EXO
- Loner Mobile

Blackline Live also supports older device lines, and allows you to monitor and configure them over the air. However, new features implemented since the release of the G7 line may not be backwards compatible to older devices — for example, any text messaging features utilizing the LCD screen and all gas detection features are not available on older devices.

Older devices that Blackline Live supports are:

- Loner M6 and M6i
- Loner 900 and Loner Bridge
- Loner SMD and Loner IS+

What accessories does Blackline Live support?

In addition to Blackline's main products, Blackline Live also allows you to configure and manage Blackline accessories, including:

- Location beacons
- G7 Dock
- Loner DUO

2. ORGANIZATION STRUCTURE

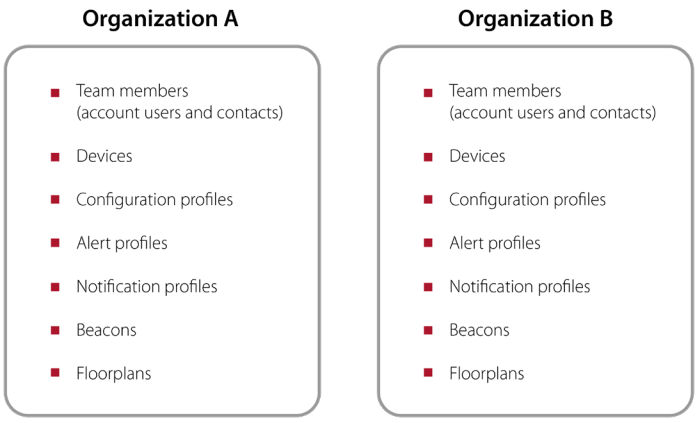
When you log into Blackline Live, you will notice that you have your own space within the portal and will not see devices or resources belonging to other Blackline customers. This space is referred to as your "organization". Organizations store all of your company's resources, including Blackline devices and accessories, team member information, devices configurations and analytics reports. Users who are part of your organization can have customizable access to these resources based on their roles and responsibilities.

Organizations exist separately by default, but can be connected through relationships, allowing you share visibility of reports and resources to users in other organizations.

This section will illustrate the architecture of Blackline Live and how organizations are structured.

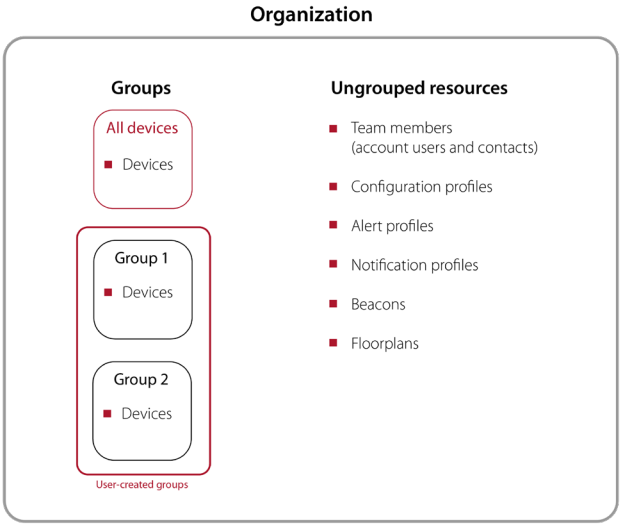
2.1 ORGANIZATIONS

An organization is an entity that represents a real-life organization or company. Organizations in Blackline Live contain devices, accessories, contact information and device data, and can be accessed by invited team members.



2.2 GROUPS

Within an organization, devices can be organized into groups. These groups can be based on whatever criteria the customer wishes. Most often, they are used to organize devices by work sites, projects or teams.



Groups are can be used as filters in reports to see trends within different parts of the organization. For example, a user could easily see whether one group is experiencing an exceptional amount of alerts, or is consistently out of gas compliance.

Additionally, groups are used to determine access and visibility within the organization. For example, if the manager of Group 1 should only see device data for their team, giving them access to that group will filter and streamline their experience in Blackline Live. They will not be able to see or manage Group 2, even though those devices are also part of the larger organization.

NOTE: Only devices are grouped — Blackline Live does not currently support grouping of team members, alert profiles or other resources. Access to "ungrouped" resources is determined with the All devices group.

The All devices group

Each organization will always have one group by default. This group — the "All devices" group — is treated differently than groups created by the users. The "All devices" group will automatically update to include all of the devices within the organization, and cannot be removed. The All devices group makes it easier to give people in your organization access to all of the organization's resources. It also plays an important role in relationships, which will be explored in the next section.

2.3 ACCOUNT USERS

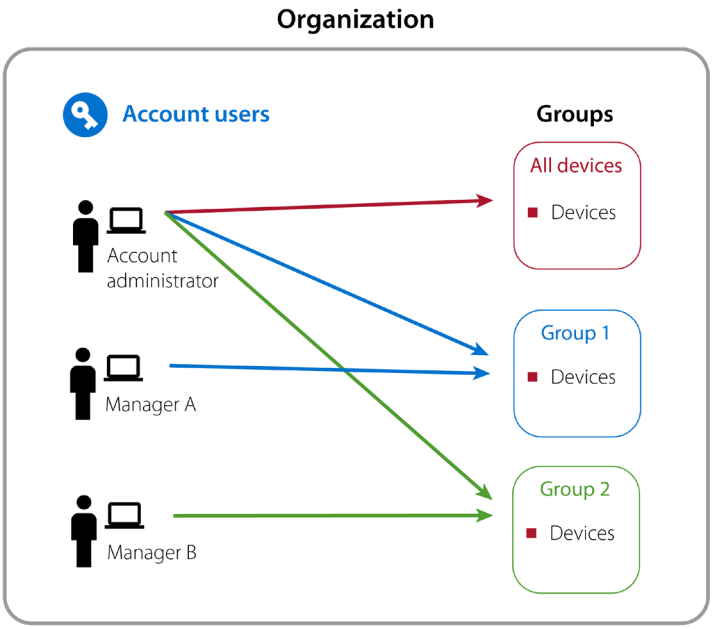
Within Blackline Live, people with log-in access to the portal are called "account users." These people can have particular roles within Blackline Live that help them complete tasks in the portal related to fleet management, contact administration, or even live alert monitoring.

Section 3.4 will provide more information about account users and other kinds of team members.

2.4 GROUP ACCESS

In order to interact with Blackline Live, account users need access to at least one group in their organization.

In the example below, an organization has three account users, all of which have access to different groups. If we assume the first account user is an administrator and should have access to all of the devices in the organization, they can be assigned to all of the groups. Meanwhile, Managers A and B are team leads and should only see devices being used by their team, so they have been given access to only one group each.



2.5 GROUP ROLES AND PERMISSIONS

Roles are a simplified bundle of permissions that are assigned to account users to determine what they are allowed to see and do. Roles are granted on a group-by-group basis. The available roles are:

Organization admin
This role includes the highest level of permissions, and should be appointed to users that are responsible for their organization's device fleet. Users with this role are able to see and edit all resources in their Blackline organization. They are also able to edit organization-wide information and settings, and are permitted to create and manage relationships with other organizations. This role can only be applied to the All devices group, since it is representative of the entire organization.

Group admin
This role should be given to users who manage a group. Depending on the criteria you are using to create your groups, this might be a site manager or a team lead. Users with this role can edit the groups they have this role in, as well as any devices within it.

Users with group admin access to the All devices group can also make any change to team members in the organization, including giving or revoking the ability to log into Blackline Live, or changing what groups or roles they have access to.

Device admin
This role should be given to users who manage devices fleets within the groups they have access to. Account users with this role can rename device, or assign them to team members in addition to being able to monitor and respond to online devices.

Contact admin*
The contact admin role is similar to the device admin role, with the exception that their access to pages in Blackline Live is limited. While they can still manage and assign devices, they cannot see the maps page, the configuration or alert profiles, accessories or Analytics, and they also cannot resolve alerts on devices.

Resolve only
The resolve only role is meant for monitoring agents. This role allows the user to see information in the organization, but the only actions they can take are those required for alert investigation and resolution. A user with the resolve only role can acknowledge alerts, and leverage the alerts management page to review emergency response protocols, assess the device's current location and status, contact device users and emergency contacts and leave notes regarding the investigation of the event.

Emergency responder*
Users with the emergency responder role have the same monitoring and alert resolution permissions as users with the resolve only role. However, they are not permitted to view all of the resources in the organization, such as team members, devices, configurations, alert profiles, and analytics. Any information from these resources that is required for alert investigation and resolution will be made available to the user through the alert management page or the maps pages.

View only
The view only role allows an account user to see all of the resources within an organization, but they are not permitted to edit or manage any of them. They are also able to view alerts, but cannot acknowledge or resolve them.

Analytics only*
Users with the analytics only role will only be able to view the Blackline Analytics page, and the reports listed there. They are not able to see the maps, alert management pages or resource pages.

*This role is only available for groups within the account user's organization. It cannot be used when using a relationship to share group access with another organization.

NOTE: Team members are not considered "grouped" resources, so only users with access to the All devices group can edit their information. A user requires either a contact admin, device admin, group admin or organization admin role in the All devices group in order to add and edit team members.

Please see the table below for a full breakdown of permissions included with each role.

Blackline Live permissions overview

Role	View	Resolve alerts	Create and manage contacts*	Reassign devices	Create and assign profiles	Create and manage groups	Create and manage account users*	Create relationships	Edit organization details
Organization admin	View all	Y	Y	Y	Y	Y	Y	Y	Y
Group admin	View all	Y	Y	Y	Y	Y	Y	N	N
Device admin	View all	Y	Y	Y	Y	N	N	N	N
Contact admin	Limited view • Devices • Team members • Quick assign	N	Y	Y	N	N	N	N	N
Resolve only	View all	Y	N	N	N	N	N	N	N
Emergency responder	Limited view • Maps (Live view & History view) • Alerts management • Alert history	Y	N	N	N	N	N	N	N
View only	View all	N	N	N	N	N	N	N	N
Analytics only	Limited view • Blackline Analytics	N	N	N	N	N	N	N	N

*In order to create and edit team members, an account user needs access to the All Devices group.

0611/R4/2020-01-30

Roles in the All devices group

Giving an account user a role on the "All devices" group means that those permissions apply to every device in the organization. This can make it easier to give someone access to the entirety of the organization's resources.

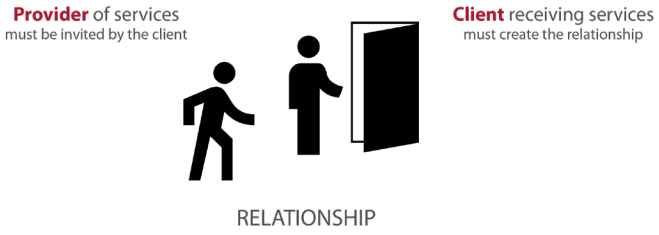
Combining roles

A single account user can have different roles in each group they have access to. For example, a manager or team lead might have a "view only" role in the All Devices group but may have a "group admin" or "device admin" role only for the group that they lead. This allows them to make changes to the group that they manage, but can still see all of the other devices in the organization.

2.1 RELATIONSHIPS

Relationships allow resources to be shared between two separate organizations for purposes such as monitoring, distribution set-up or rentals.

A relationship is a one-way connection between the two organizations, in which one organization has access to the other organization's groups. In each relationship there is a provider and a client.



The **provider** is providing a service, and is being given access to resources in the other organization. The **client** is receiving a service, and is granting access to the other organization. Only clients can initiate a relationship, since they are responsible for defining the access the provider will have.

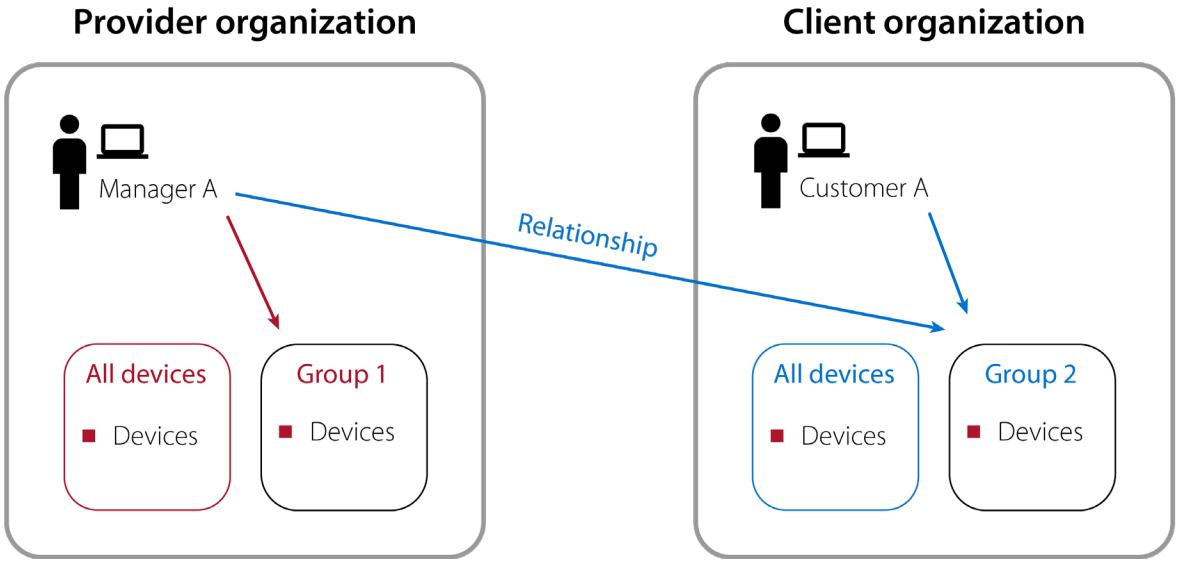
Once a relationship is activated, the organization admin who accepted the invitation will be given access to the groups that the client has chosen to share. The provider organization admin can then choose to share the access to their own team members as needed, but they can only assign the roles that the client has defined.

In the example below, a manager has access to Group 1 in their own organization, and through a relationship can also access Group 2 in a client organization.

Relationships can be considered contractual or non-contractual.

Contractual relationships lock devices into the organization once the relationship is activated — they cannot be moved to another organization by anyone other than a Blackline Safety representative. Contractual relationships only allow the "All devices group" to be shared, meaning the provider will have access to all of the devices in the client organization. Additionally, contractual relationships cannot be deactivated by either party, and must also be deactivated by a Blackline Safety representative. These relationships are more secure and recommended for safety monitoring or distribution set-up.

Non-contractual relationships are considered less secure than contractual ones, but allow more for more flexibility and customization. The client can choose to share any of their groups with the provider — not just the "All devices group". Additionally, providers can move devices in and out of client organizations as long as they have group admin access to the "All devices" group. These relationships are commonly used for rentals, so that rental distributors can easily monitor and move resources for the duration of the rental. This is also a good relationship type for larger companies that prefer to operate different branches as separate organizations.



3. ORGANIZATION SETUP

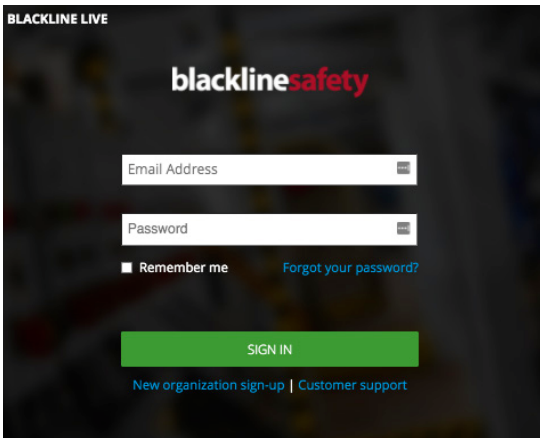
Setting up an organization requires a few important steps. This section will walk you through the different pages in Blackline Live in the order that allows the most straightforward workflow.

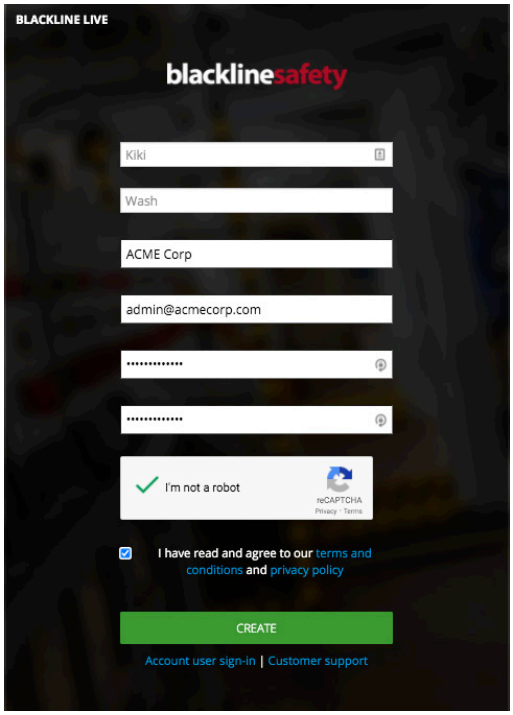
3.1 REGISTERING AN ORGANIZATION

The first step to getting into Blackline Live is to register your organization. This step should only be taken when you are first getting started with Blackline services — if your company already uses Blackline devices, then your organization will already be registered in Blackline Live. In this case, you will need to contact the existing account holder in your organization to get invited to Blackline Live.

To log in to an existing Blackline Live account or register a new organization, open up the internet browser on any Internet-connected device and navigate to live.blacklinesafety.com.

Once you land on this page, you will see the options to log in. To register a new organization, click the *New organization sign-up* button underneath the green Sign in button.





Fill in the fields and click *Create* when you are finished. Ensure you enter a valid email address that is connected to an inbox, since you will need to activate your organization through email. Also ensure your password is at least 8 characters long, includes capital and lowercase letters, a number and a special character. Review Blackline Safety's terms & conditions, and privacy policy before clicking *Create.*

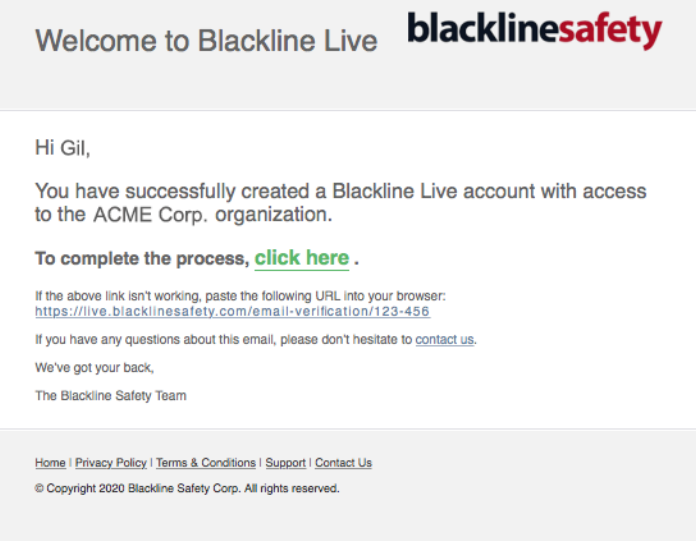
Troubleshooting tip

If you get an error that you cannot use the organization name you have entered, this is likely because your organization has already been registered in Blackline Live. Contact the Blackline Live account holder in your company or Blackline Safety's Customer Care team to get invited to the existing organization.

Activating your organization

The final step to complete before you can log into Blackline Live is to activate your account by verifying your email. Log into the email account that you used to register your organization, and look for an email from Blackline Live. Remember to check your spam or junk folder if you do not see it in your main inbox.

Open the email and click the link provided. You will be redirected back to Blackline Live, and a pop-up at the top of the screen will inform you that your email was verified. You can now use your email address and password to log in.



Welcome to Blackline Live blacklinesafety

Hi Gil,

You have successfully created a Blackline Live account with access to the ACME Corp. organization.

To complete the process, click here .

If the above link isn't working, paste the following URL into your browser:
https://live.blacklinesafety.com/email-verification/123-456

If you have any questions about this email, please don't hesitate to contact us.

We've got your back,

The Blackline Safety Team

Home | Privacy Policy | Terms & Conditions | Support | Contact Us

© Copyright 2020 Blackline Safety Corp. All rights reserved.

Troubleshooting Tip

If you get an error after clicking the link, the email may have already been verified. Try logging in with your email and password.

If you are managing multiple organizations, ensure that you are logged out of Blackline Live before clicking on the link in the email invitation. If you attempt to activate one organization while already logged into another, the activation will fail.

3.2 NAVIGATING BLACKLINE LIVE

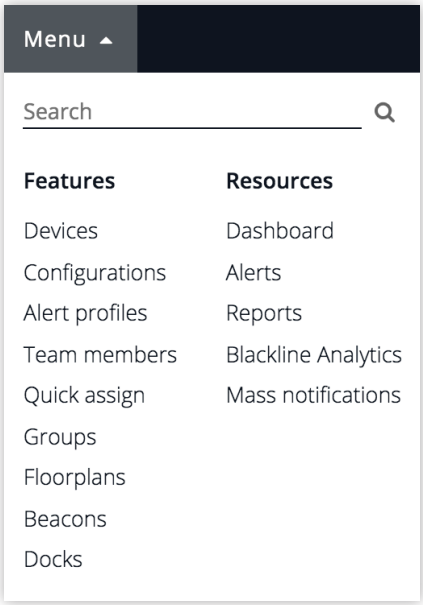
The top navigation bar allows you to access different pages or search for resources in your organization. You may also see banners in the navigation bar is there is important information that pertains to you and your organization.

Maps

The maps page is one of the most frequented pages in Blackline Live, and displays the current location of online devices in your fleet. If your role allows you to access this page, you will see it in the top navigation bar. Section 5.1 provides more information about using the maps page.

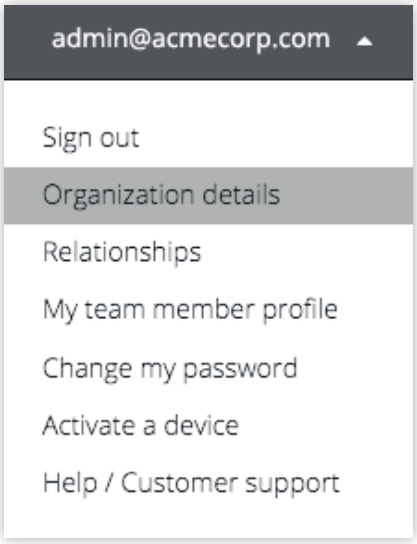
Main menu

The main menu includes the majority of the pages in Blackline Live, including Devices, Team members, Configuration and Alert profiles, Alert management and Blackline Analytics. Depending on the role you have in your organization's "All devices" group, you may see different pages in this menu than other account users in your organizations.



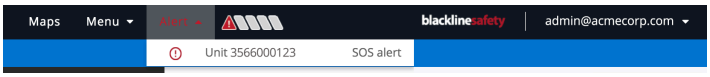
User menu

On the far right side of the navigation bar, you will see the email address that you used to log in to Blackline Live. By clicking on your email, another dropdown menu will open. The pages accessible from this "user menu" all contain information either about the organization you belong to, or abour your particular account. This menu will remain the same regardless of which roles you have been given.



Information banners

There are three kinds of banners that can appear in the navigation bar that inform you of something that affects you or your organization.



The first is the alert banner, which appears to the right of the main menu dropdown when there is an active alert on one of the devices you have access to. Clicking on the alert banner will open a new dropdown with a list of every alert that needs to be addressed. Section 5.3 will provide more information about alerts.

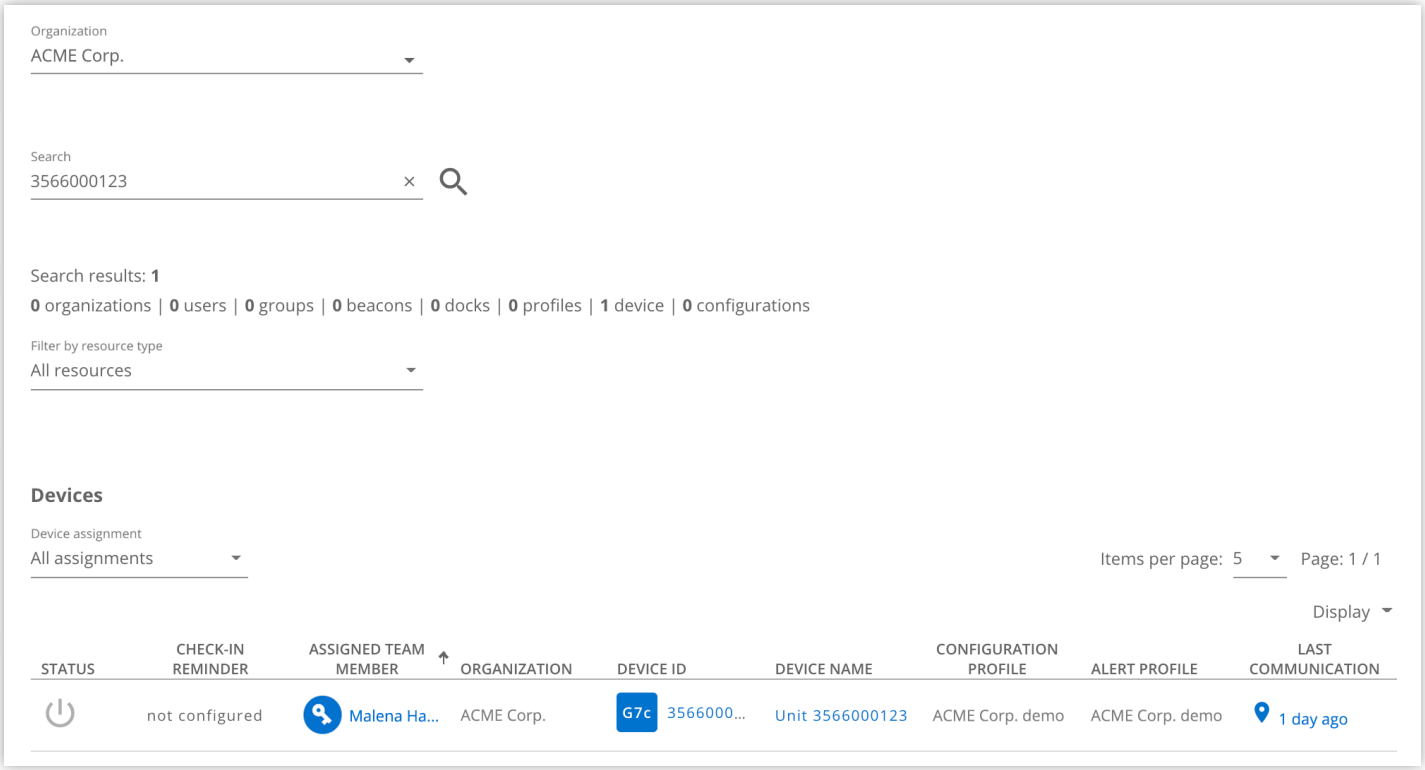
If there is an issue blocking you from hearing audio from Blackline Live, you will see a yellow banner immediately below the navigation bar. You are notified of audio issues because a lack of audio from Blackline Live can result in missed alerts. Click the message in the banner to be redirected to an audio troubleshooting article

Lastly, a blue banner immediately below the navigation bar will appear anytime there is new information Blackline Safety wants you to be informed of. This may have to do with new firmware availability, new features being added to Blackline Live, or updates on known bugs as they are being investigated and resolved.

Universal search

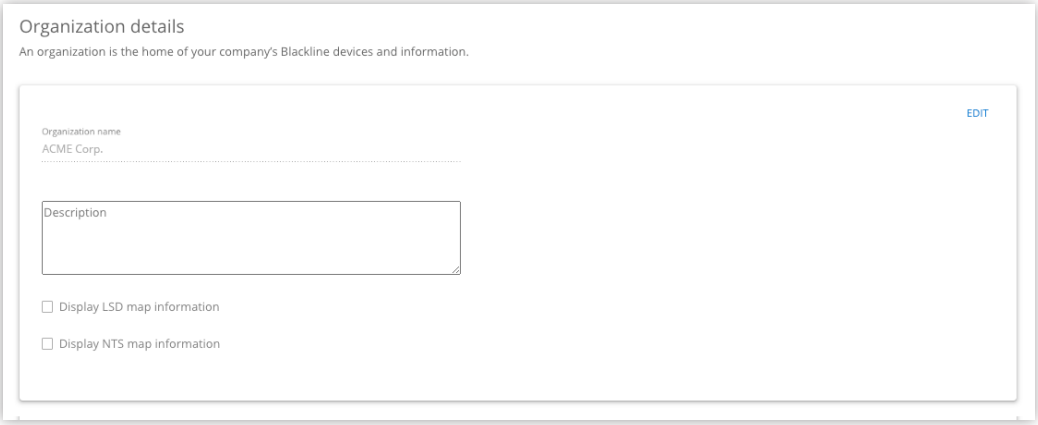
Each individual resource page (Devices, Team members, Configurations ect.) includes its own search and sort filters, the scope of these search features are limited. If you need to find a resource and are not sure how to search for it with the information you have, try the universal search.

The universal search bar can be accessed from the top of the main menu. Simply type in your search query and either click the magnifying glass icon or press the 'enter' key. You will be redirected to a search results page, which is separated in sections based on resource type. You can filter large amounts of results by resource type if you know what kind of resource you are looking for. By clicking on the name of the resource, you will be redirected to that resource's profile or details page.

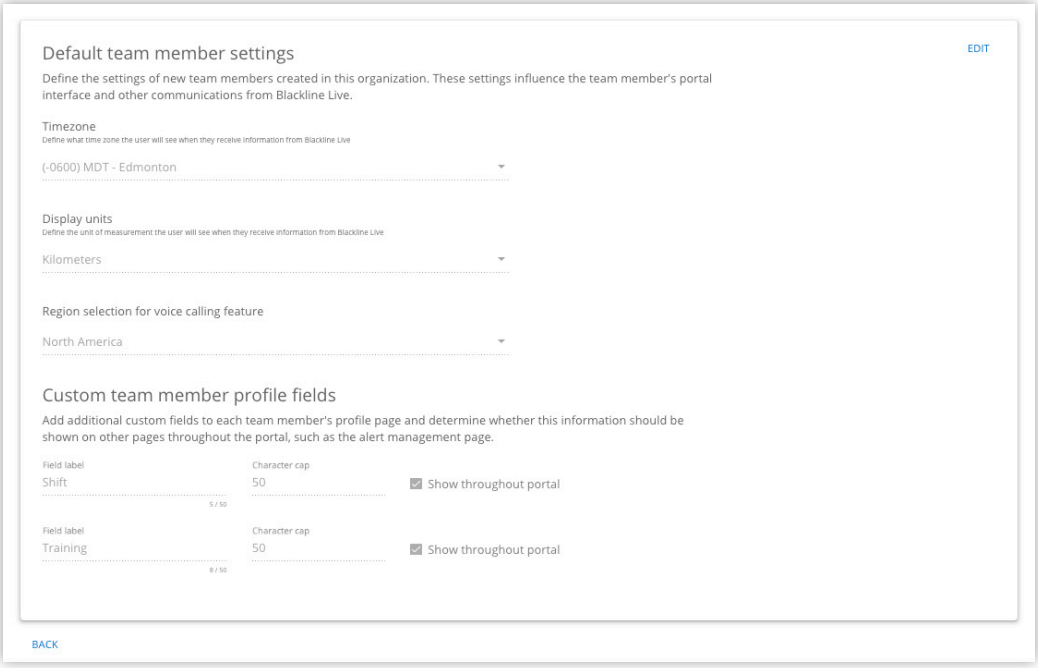


3.3 ORGANIZATION DETAILS

After logging in, the first thing you should do is define your organization details. This will define settings for your entire organization, including its name and settings such as timezone, display units and region.



In the first info card, you can customize your Organization's name and add an optional description. If your organization uses LSD or NTS map information, you can also choose to select these, and this information will be available when a device goes into alert.



In the second card you can define default team member settings, including time zone, display units and voice calling region. These settings will apply to anyone else who can log into the organization, and will define how information is displayed in the portal.

The last section of the page — the custom team member fields — allows you to add custom fields to your organization's team member profile. You can add up to 10 text fields and define a label and character cap for each. You can also choose to show this information when an alert occurs by checking the "Show throughout portal" option. If you remove a custom field, you will lose any information that has been entered into the team member profiles under this field.

3.4 TEAM MEMBERS

Team members represent people in your organization who are in contact with Blackline devices, or who are listed as emergency contacts. They should be the first resource added to your organization.

There are two kinds of team members:

Contacts represent people in your organization. They can be assigned to devices, or to alert profiles as emergency contacts. They are represented by a person icon in the portal.

Account users can also be assigned to devices or alert profiles, but additionally represent people who have log-in access to Blackline Live. They are represented by a key icon in the portal.

To see team members, navigate to the team members page in the main menu.

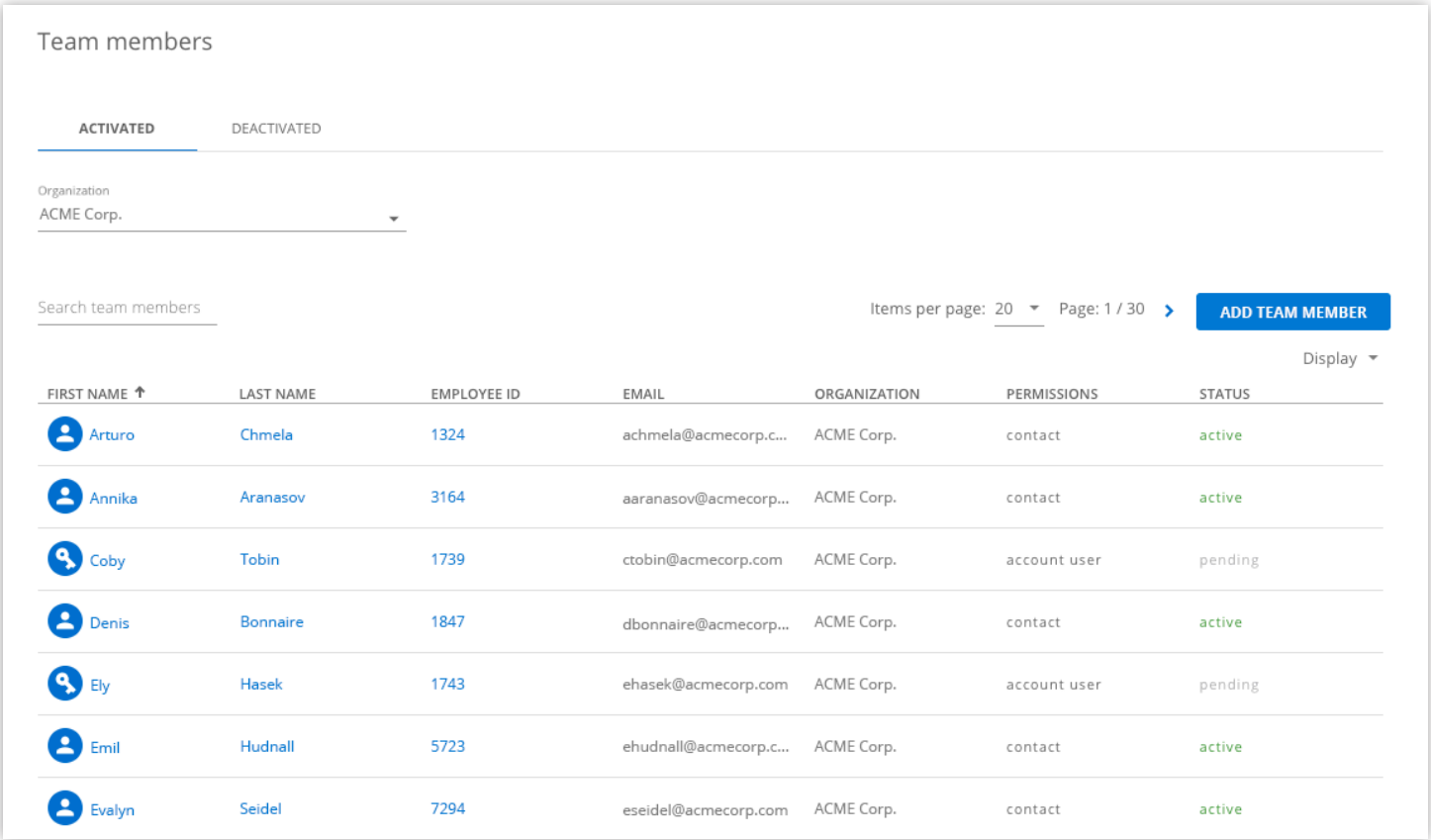
This page lists the team members registered in this organization. The icons next to their name indicate whether they are a contact or an account user. The team members table can be searched or sorted.

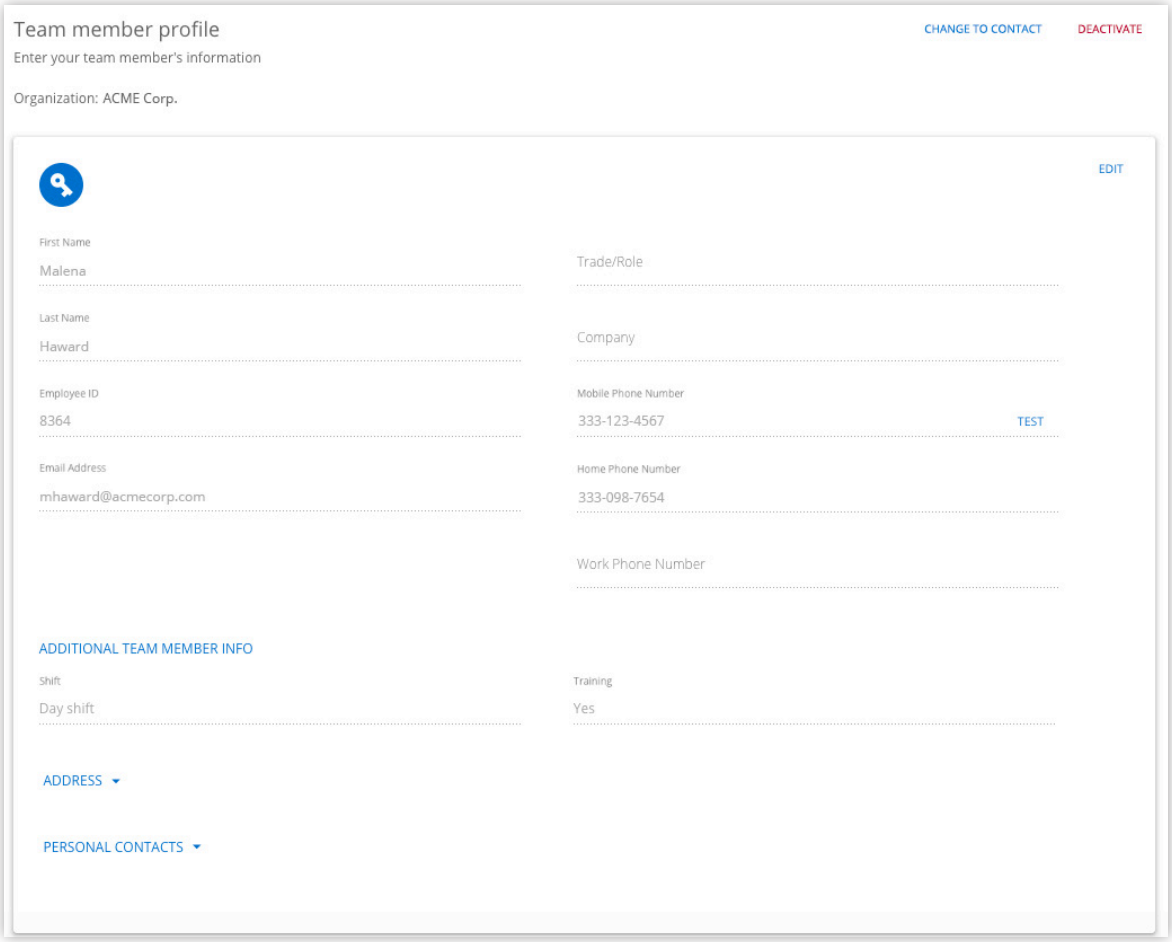
A team member's status is most valuable in regards to account users, since it indicates whether they have activated their account and have gained access to Blackline Live. A **pending** status means they have been sent an invitation to the portal, but have not accepted it through their email. An **active** status indicates that they have activated their account and logged in. Contacts will always have an active status by default.

Adding team members

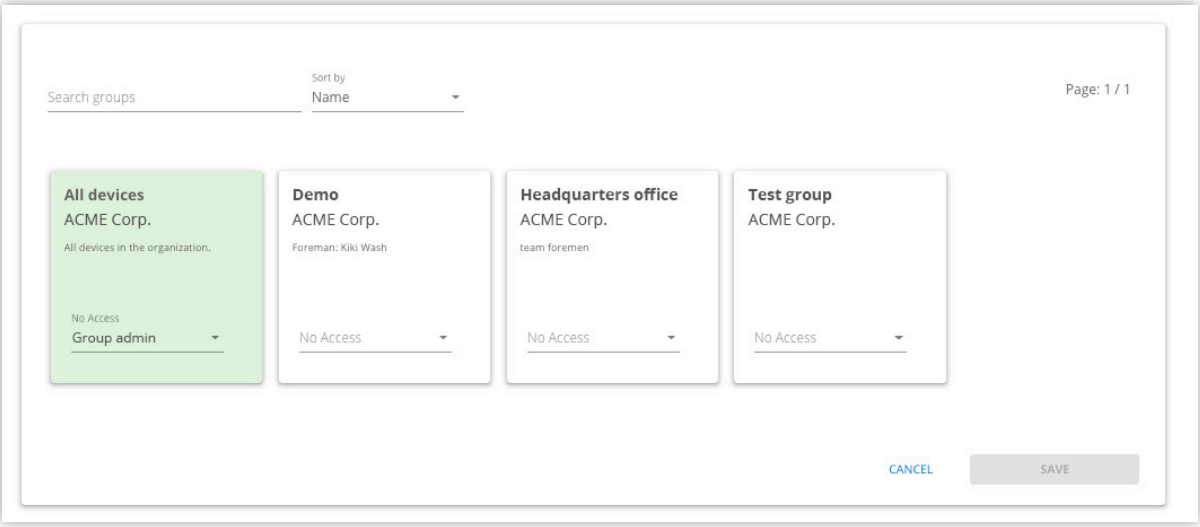
To add a new team member, click the Add team member button, and then define whether you are creating a contact or an account user.

The team member profile lists important contact information for this team member. Provide as much information as you can, since it will be displayed if this team member's device goes into alert, or will be provided to monitoring personnel if they are listed as an emergency contact.





If you are creating an account user, additional information is required. A valid email address is required in order to activate the account, and an account user must be given a role in at least one group so that they have defined visibility within Blackline Live.



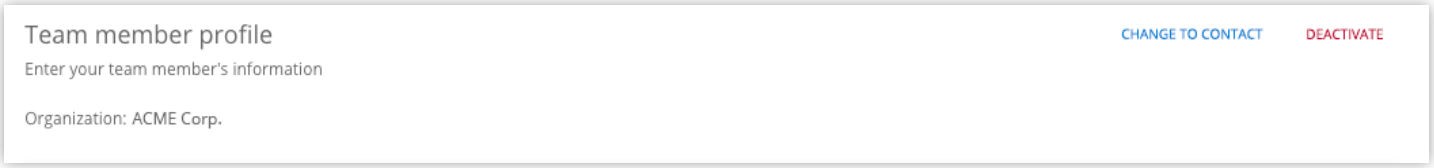
Changing team member types

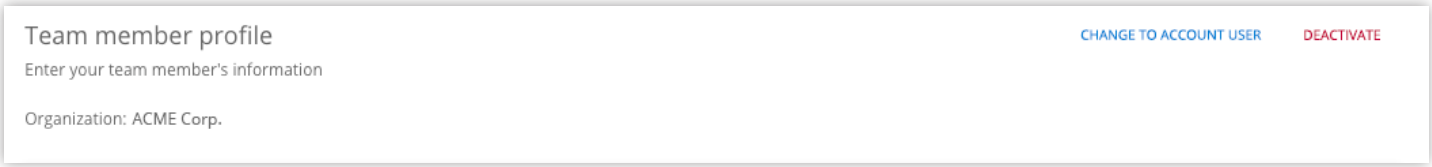
Team members can be "promoted" from contacts to accounts users and "demoted" vice versa. This allows administrators to grant and revoke access to Blackline Live as needed, without necessarily removing the team member from the organization.

This can be done through the team member profile. If you have editing permissions over team members, you will see either a *Change to contact* or *Change to account user* button at the top right of the profile page.

When changing a contact to an account user, you will be required to enter a valid email address if there is not one already available. You will also be required to assign the team member a role in at least one role so that they have defined visibility of the organization when they log in. Once they are changed to an account user, their status will be pending until they accept the invitation sent their email address.

When changing an account user to a contact, their session will be ended and they will no longer be able to log into Blackline Live and they will no longer be listed in groups. In both cases, if the user was assigned to a device, alert profiles or notification profiles as an account user, these assignments will remain intact even after they are changed to a contact.



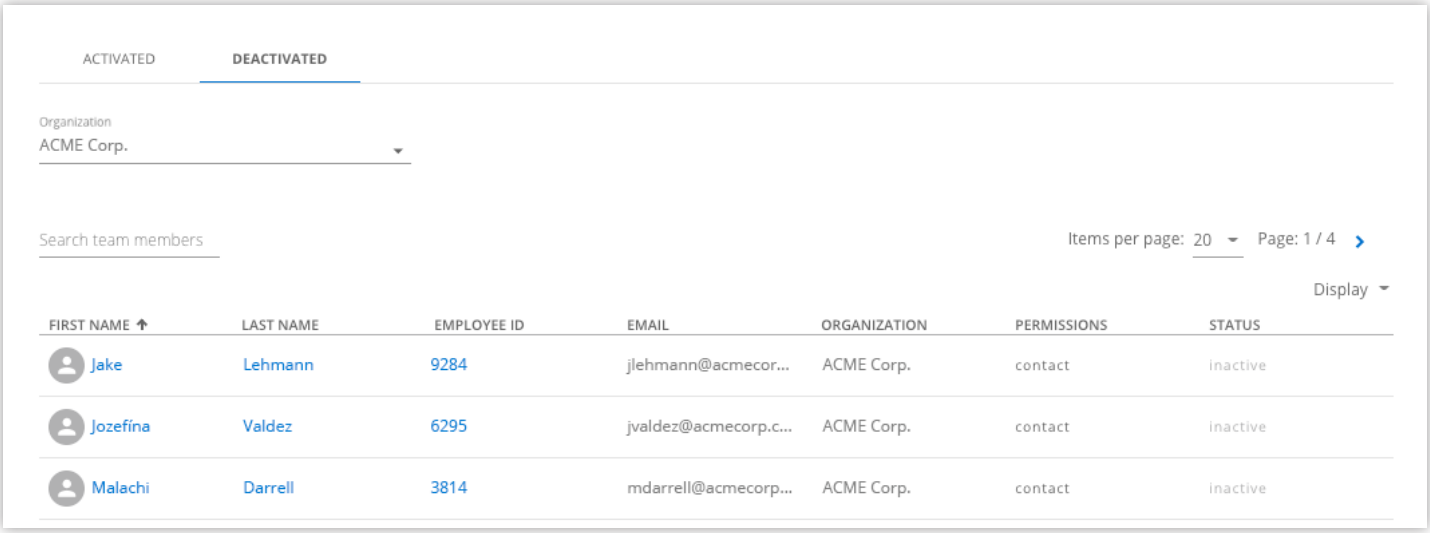


Deactivated team members

In the case that a team member is no longer part of the business, they should be deactivated in Blackline Live.

Deactivated team members can still be seen by other users in Blackline Live by clicking the Deactivated tab on the Team Members page, and will have an **inactive** status. They can no longer be assigned to devices, alert profiles, or notification profiles, and will be removed from groups and unassigned from their devices. Deactivated account users will also lose login access to Blackline Live.

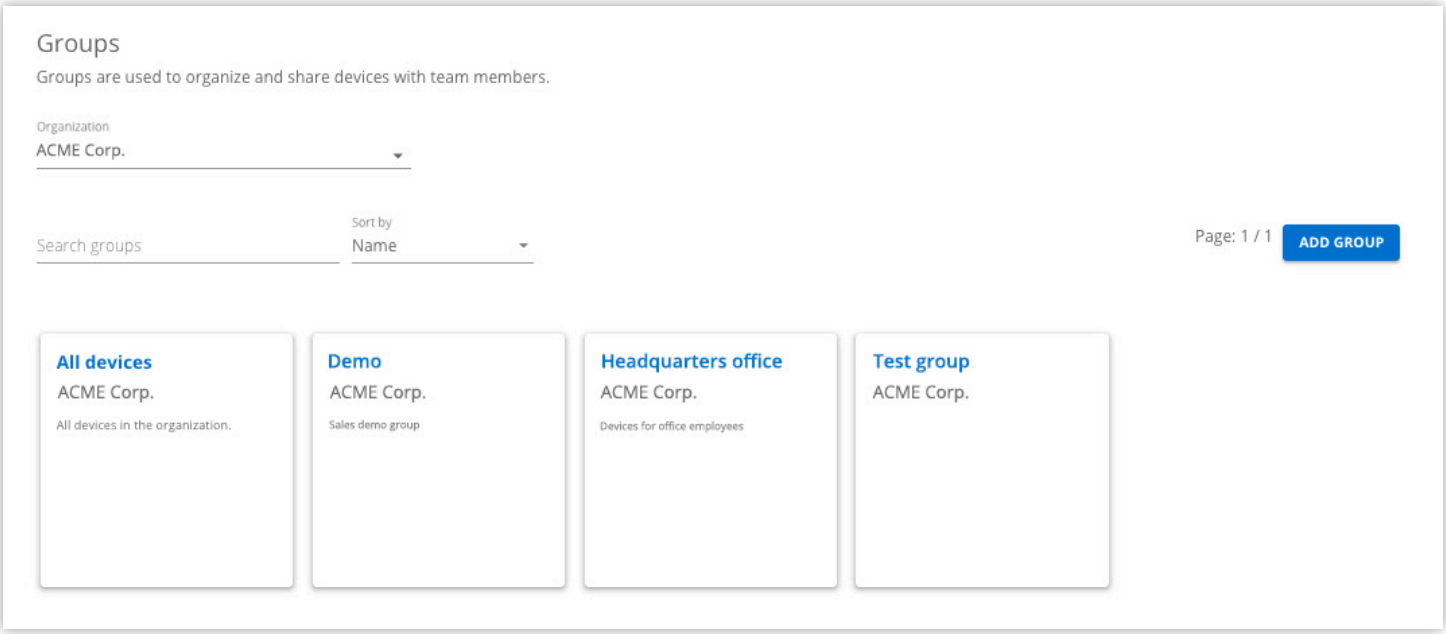
To deactivate a team member, simply navigate to their profile and click the red *Deactivate* button.Deactivated team member profiles show all their information and profile assignments at the time of their deactivations. Clicking the *Activate* button will reactivate the team member in Blackline Live, automatically putting them back into their original groups (if the groups still exist). They must be manually reassigned to a device and alert profiles.



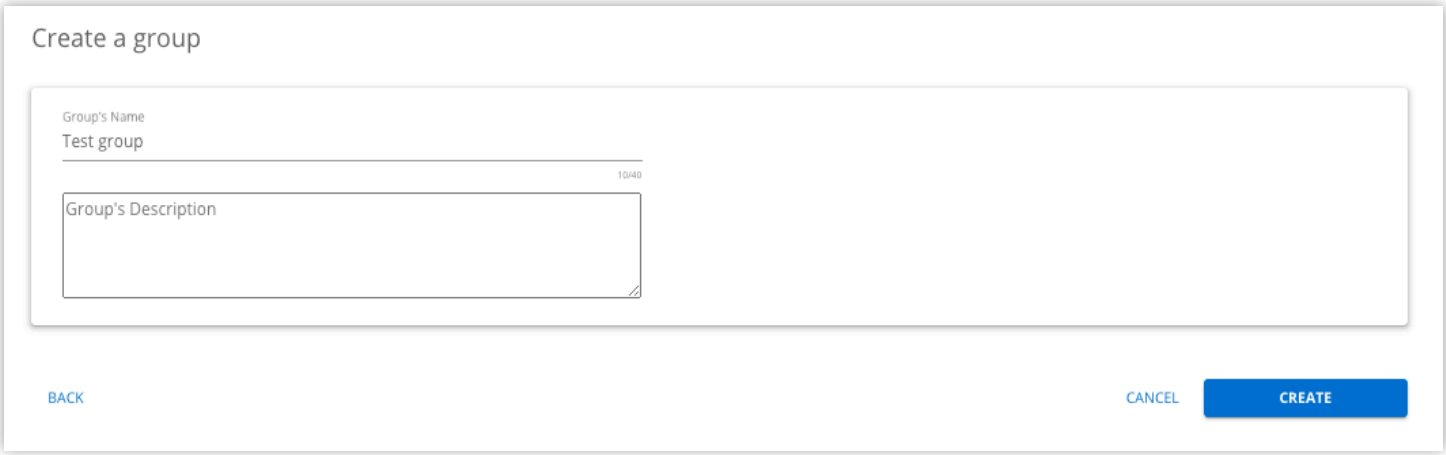
3.5 GROUP SETUP

The Groups page can be accessed through the main menu, and lists all of the groups within an organization. Each group is represented by a card on the page. The card lists the group's name and which organization it belongs to, as well as an optional description. This list can be searched and sorted by name.

To create a new group, click the blue *Add group* button on the right side of the page.

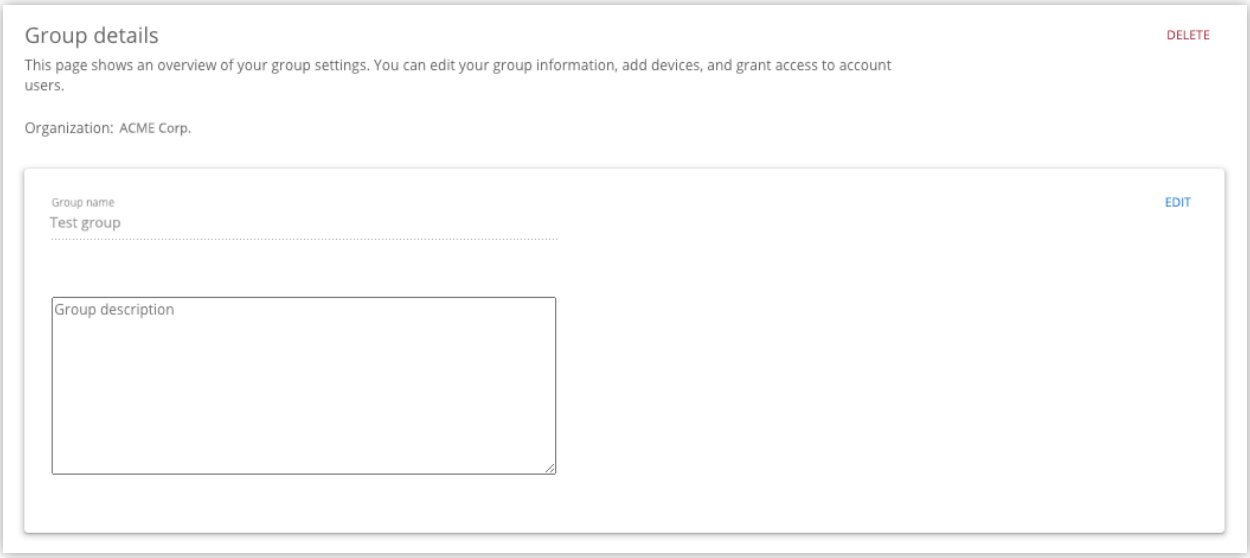


First, you will be prompted to enter a name and description for the new group. After pressing the *Create* button, the groups page will become available to edit.



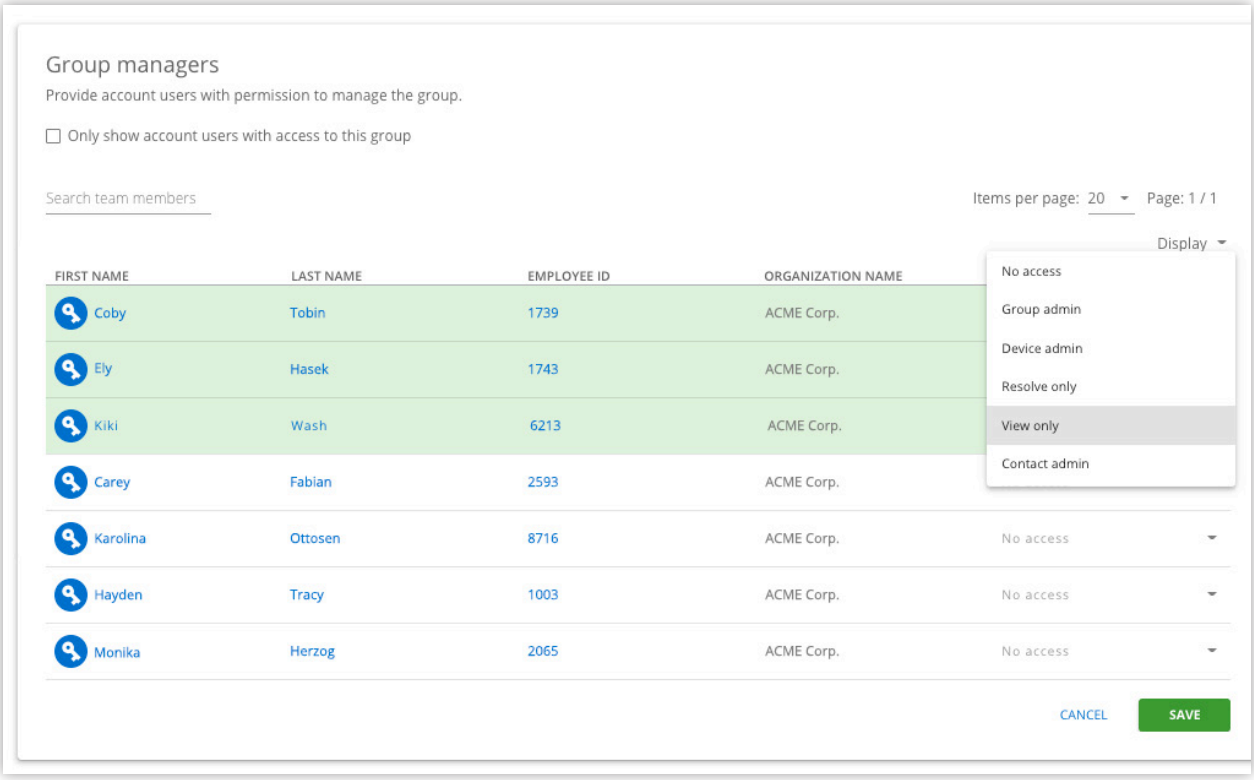
Once you are redirected to the group details page, you can proceed to customize it. The group name and description will already be populated with the information you added on the previous "Add group" page, but you can always change this information in the first card of this page.

You can also delete this group by selecting the red Delete button in the top right corner of the page. Keep in mind that deleting groups will remove them from any future reports. Groups also cannot be deleted if you have any group managers that do not have access to other groups.



Group managers

The Group managers sections lists account users that have access to this group. To add group managers, click the *Edit* button in the top right corner of the card, and select which role they should have from the dropdown. Account users selected to have access in the group will be highlighted in green. You can check the "Only show account users with access to this group" option to filter the list only to show these highlighted users.



Devices list

The Devices list defines which devices are part of the group. Simply click the edit button and check off any devices you would like to include in the group. You can search and sort devices in order to find them more easily. To remove devices from the group, click the edit button and uncheck them from the list.

All devices group

As mentioned in section 2.2, each organization has a default group called the "All devices" group. This group collects all of the devices in the organization by default and represents the organization as a whole. This group allows administrators to easily grant account users access to all of the resources in the organization. The title, description and device list of the All devices group cannot be edited, but the list of group managers can.

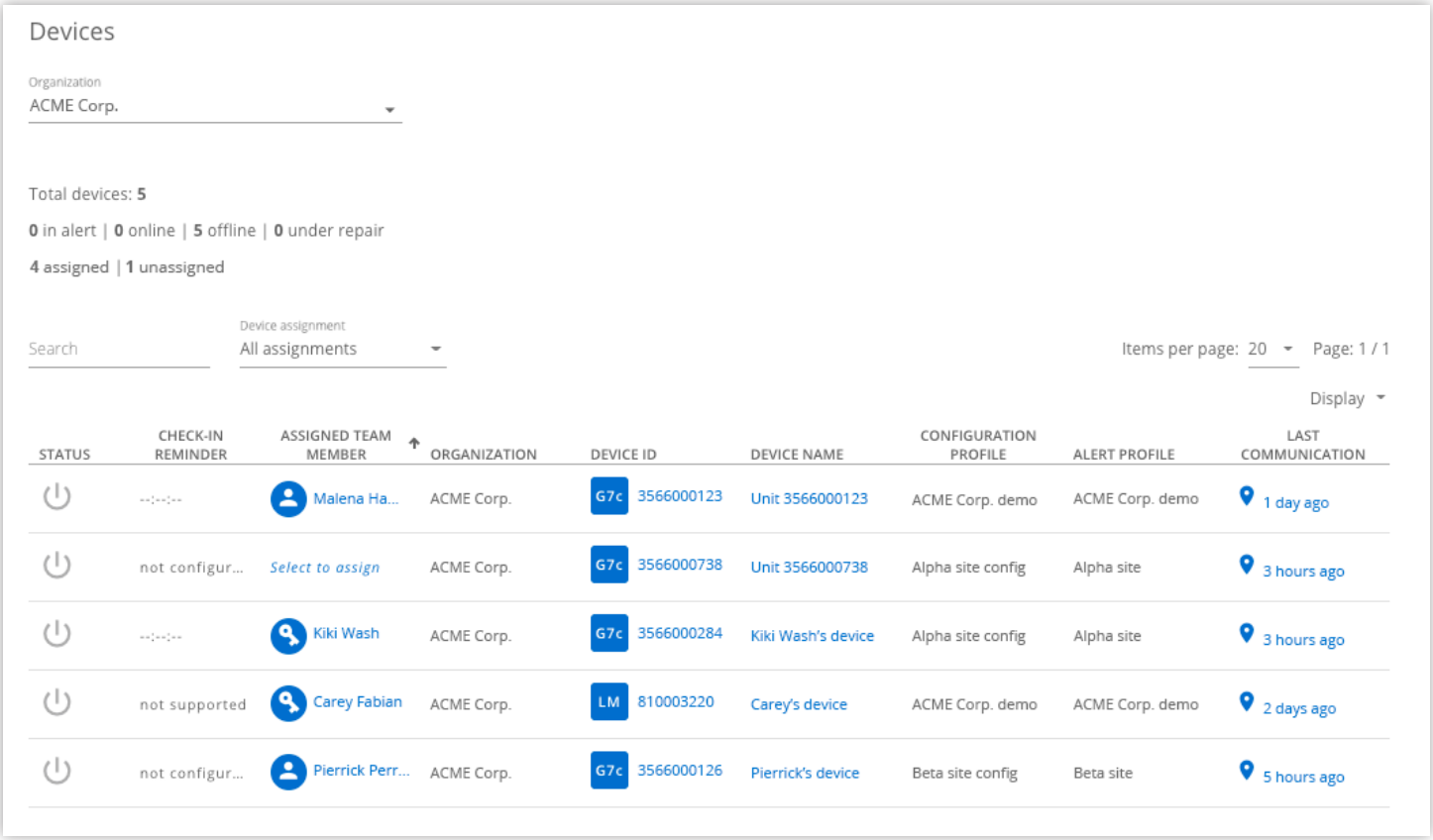
3.6 DEVICES AND DEVICE SETUP

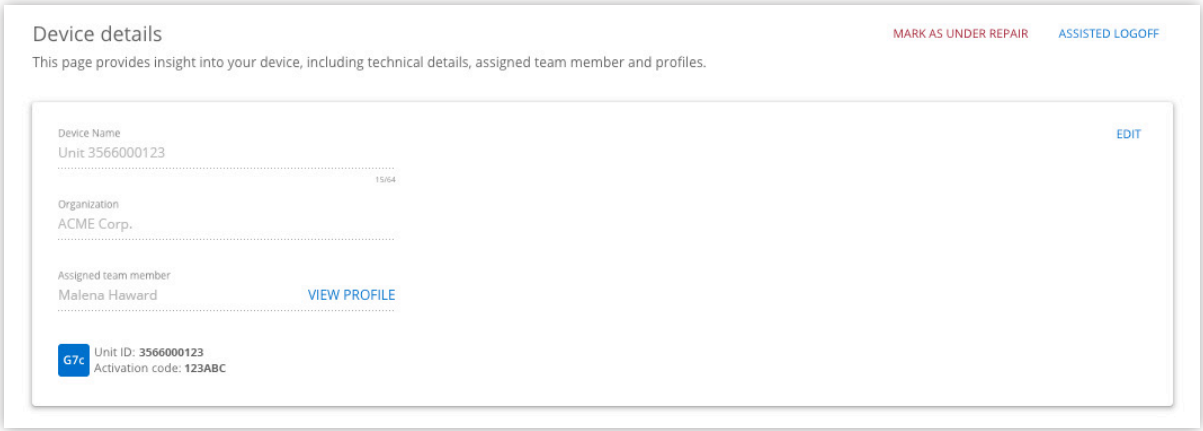
You can see the list of available devices by selecting "Devices" from the main menu. The devices page displays devices in a list with the following information:

- The device status (online, offline, in alert)
- Check-in reminder, if enabled
- Whether the device is assigned and who it's assigned it
- The organization the device belongs to
- The type of device and its ID number
- The device name
- The configuration the device is using
- The alert profile the device belongs to
- The last time the device was online

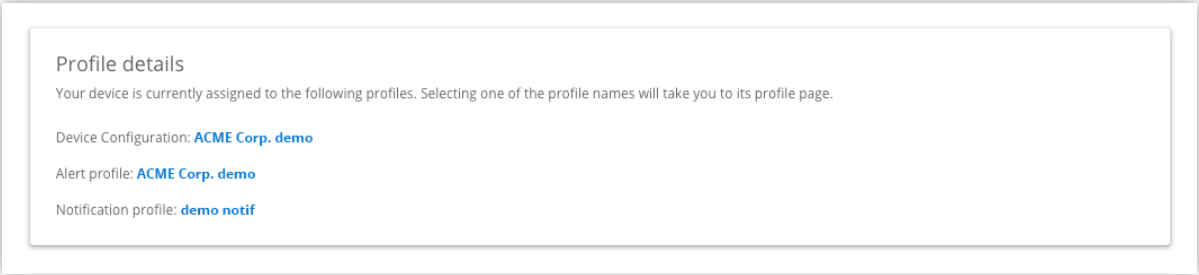
This list can be searched and sorted. To see more information about any of the devices, click on the device name or ID to open its Device details page

The device details page gives a more in-depth view of a device. The first card lists the device's name, type, ID number and activation code. In addition, it displays whether the device is currently assigned to a team member.

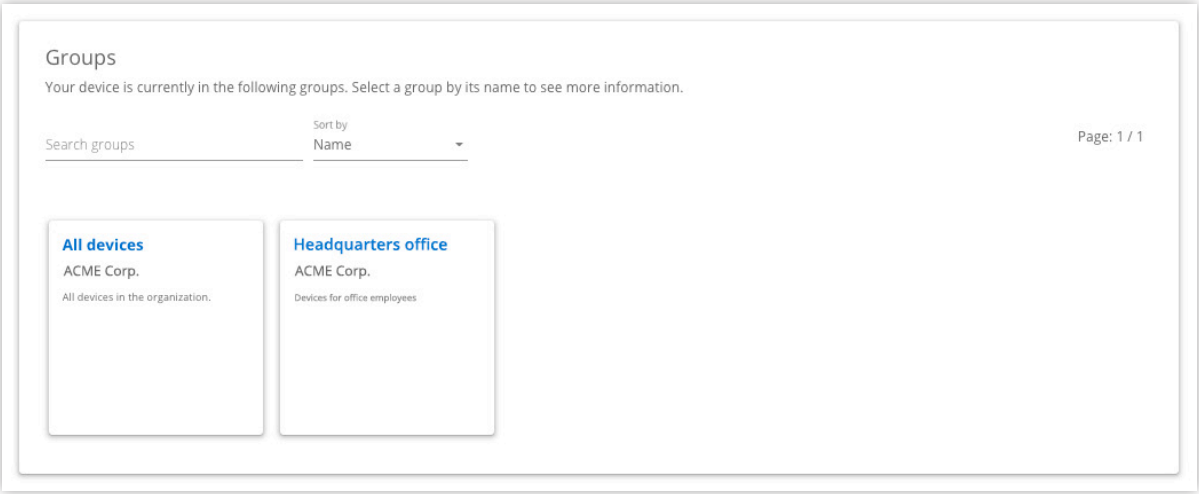




The next card on the page lists the configuration, alert and notification profiles the device is listed in, which will define how the device operates in the field, and what should happen if the device goes into alert. Clicking on the names of each profile will redirect you to the profile page, where you can see these settings in detail.



The last card on the device details page shows which groups the device is listed in. These groups are often used to indicate which site or team the device operates within. The groups section also indicates which filters this device is included in when using Blackline Analytics. Clicking on the name of each group will redirect you to the group details page, where you can see who has access to the group and what other devices are included in it.



Device user assignment

One of the key steps of setting up your organization is assigning devices to team members. When an assigned device goes into alert, monitoring personnel will instantly be aware of who was using that device, their contact information, and any other information that the organization administrator has deemed important for alert response. Knowing the identity of the person who may be in danger makes communication with emergency contacts and emergency dispatch easier and more efficient.

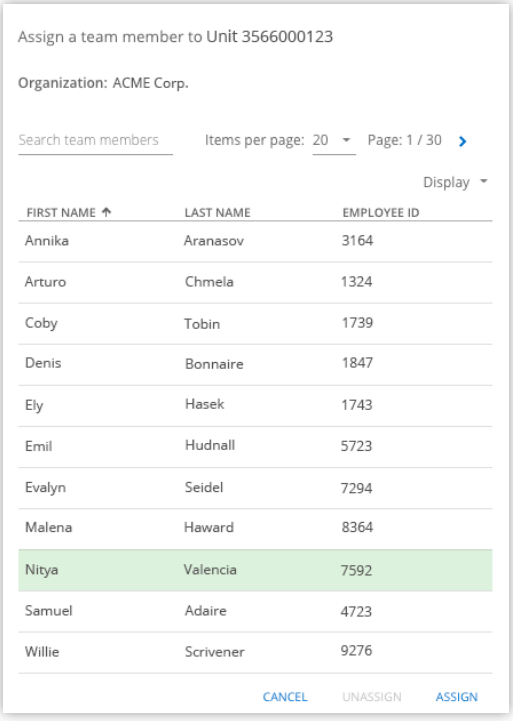
There are multiple pages in Blackline Live that allow you to assign devices, and each is useful in different situations:

- Devices page
- Device details page
- Quick assign

NOTE: A device can only be assigned to one team member at a time. If a team member already has a device, new assignments will overwrite existing ones.

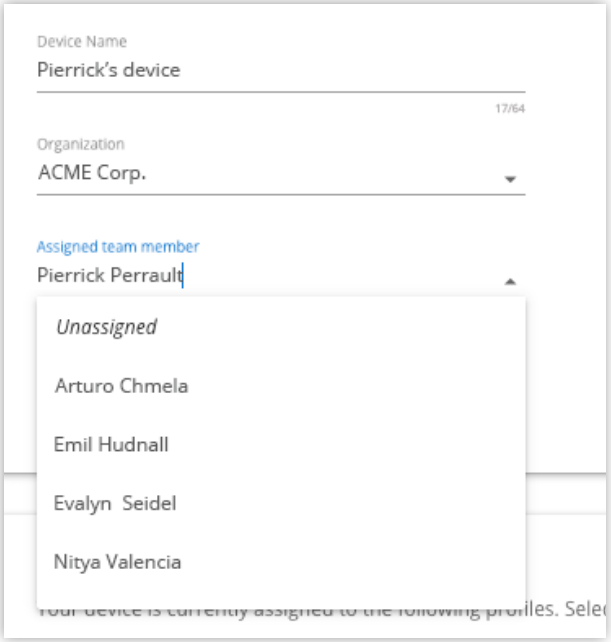
Assignment from the devices page

You can quickly and easily assign devices from the main list page. Under the "assigned team member" header, you will see if a device has been assigned to a team member. Regardless of whether it is currently assigned, clicking on the text in this column will open up a pop-up modal that allows you to quickly assign, reassign or unassign the device.



Assignment from device details

If you are already looking at a device's details page, there is no need for you to go back and find the device in the list to change its team member assignment.



Assignment from the quick assign page

The third option makes use of a specialized assignment page, which can be accessed through the main menu.

The Quick assign pages allows you to quickly and efficiently assign a large number of devices at a time with the use of a barcode scanner. In order to use the quick assign page, you will need:

- **A barcode scanner, preferably one that can scan 2D and 3D barcodes**

For even easier use, program your barcode scanner so that it performs an "enter" function after it scans. Most barcode scanners are set up with this function by default. If yours is not, check the instructions that came with your scanner for programming codes

- **Scannable identifier for each team member (eg: an ID card)**
  Before using the Quick assign page, you will have to ensure your team members are set up with a team member ID. The team member ID can be any combination of letters and numbers, as long as it corresponds to a scannable code that represents them — the most common example of this would be a company ID card.

The Quick assign page is made up of two tabs — one for assigning devices and one for unassigning devices. By default, it will load the "Assign" tab, and will highlight the "Device" field. The device field can read the device ID or the device name — the easiest way to fill this field is to scan the QR code on the back of your device. Once the device info is entered, enter the team member info. This can be either the team member ID, or the team member's first and last name.

Once both fields have been filled, click enter to submit the assignment. The page will show a pop-up that indicates whether the assignment was successful or not.

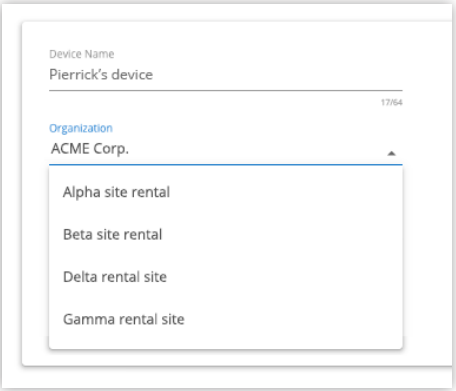
The "Unassign" tab works almost the same way, except all that is needed is the device name or ID. Once this field is submitted, the page will show a pop-up toast that indicates whether the unassignment was successful or not.

Move devices between organizations

The ability to move devices between organizations is limited to account users with specific permissions. Typically only distributors will need to move devices, either when they are setting up a new customer and transferring devices from their own organization to the customers or when they are facilitating rentals and need to move devices back and forth between their own organization and multiple rental organizations.

In order to move devices between organizations, an account user needs to have either a group or organization admin role over the All devices group of both organizations.

To move a device, navigate to the Device details page and click the Edit button in the top-right corner of the first info card. Click on the Organization dropdown field and select the new organization from the list. As with the "assigned team member" field, you can also type an organization's name into the field to narrow down the results in the dropdown.



Mark as repair, assisted logoff and send activation functions

The top of the Device details page includes a number of other features that have an impact on a specific device.

Mark as repair disables the ability to assign the device to team members. It is used by Blackline's Customer Care team to indicate devices that require RMA and should not be used in the field.

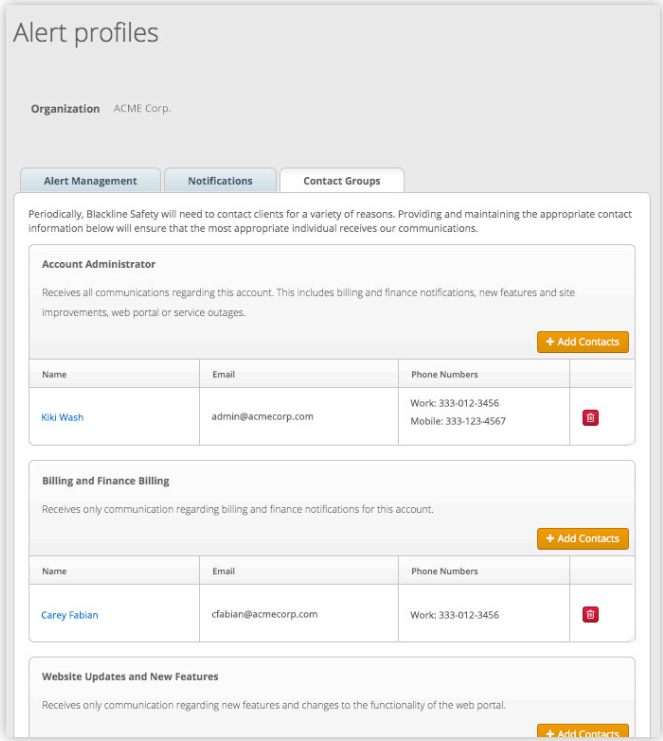
Assisted logoff forces the device to go offline on Blackline Live. It is meant to be used when the device cannot properly power down. It does not power down the physical device.

The send activation option only appears on Loner Mobile device details pages when it is assigned to a team member with a mobile phone number. Pressing this button sends an activation code to this mobile phone number so that the assigned user can register the Loner Mobile app to their phone.

3.7 CONTACT GROUPS

Contact groups define which team members should be notified of specific updates in your organization or in the Blackline Live system. Contact groups are split into four categories:

- Billing and finance billing
- Website updates and new features
- Service outage notifications
- Accound administrators



Adding team members to these groups ensures that they will be sent updates regarding one or more of these four topics. The "Account administrator" group will receive updates regarding all three of the other categories.

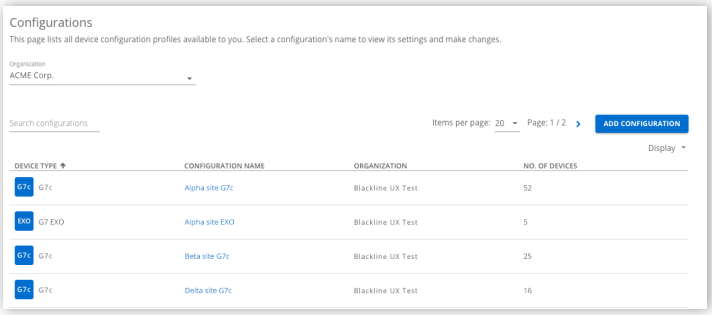
To add team members to contact groups, click the Alert profiles option in the main menu and click on the "Contact groups" tab. Once on the contract groups tab, scroll to the category you would like a team member to be notified of, and click the orange + *Add contacts* button. You can select one or more team members to add to that category.

Ensure the people you want to add to contact groups have already been added to the organization as team members.

3.8 CONFIGURATION PROFILES

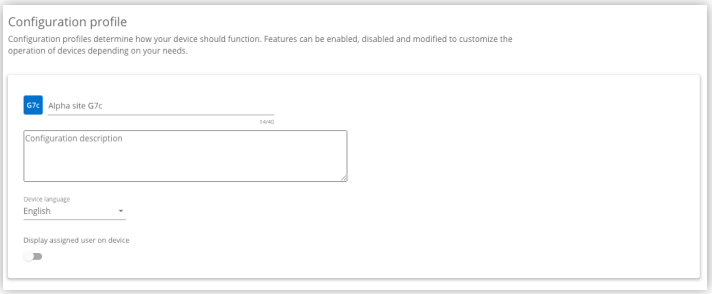
Configuration profiles define how a device will behave in the field; it indicates which features are enabled, and allows users to adjust the settings of these features. Each device type has its unique configuration profile layout that lists the features available on that device.

To edit configuration profiles, click on the "Configurations" option in the main menu. Each configuration profile will be listed in a table that can be searched and sorted.



G7 and EXO configurations

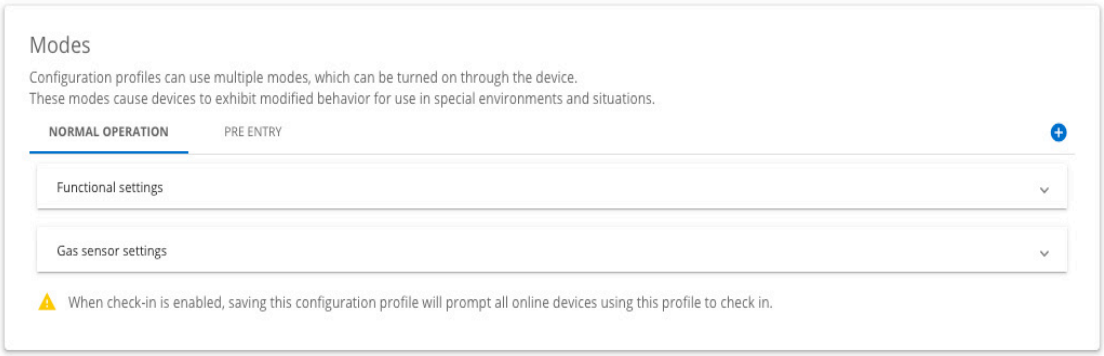
The first card of the configuration profile allows the user to enter a unique name and description for the profile, as well as dictate the default language devices should be using and indicate whether to display assigned team member names on the device screen.



The Modes or Settings card — depending on whether you are configuring for G7c, G7x or EXO — contains the majority of the device features. It is divided into two expandable sections: Functional settings and gas sensor settings. In each section, you can learn more about each feature by clicking the "i" icon next to the name of the feature.

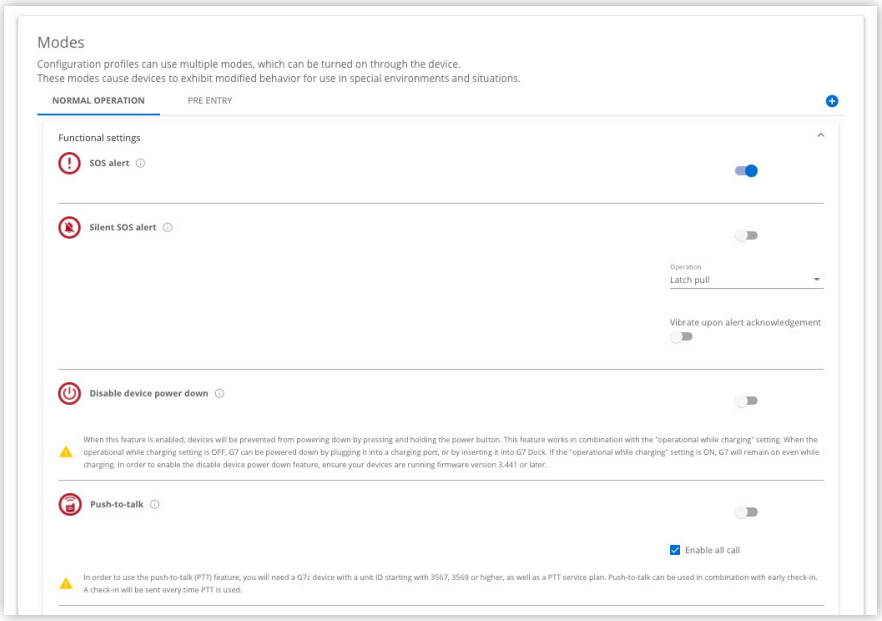
Functional settings

The functional settings section includes lone worker safety features and general device settings. Some of the primary features listed in this section include the SOS alert, push-to-talk feature and automated check-in.

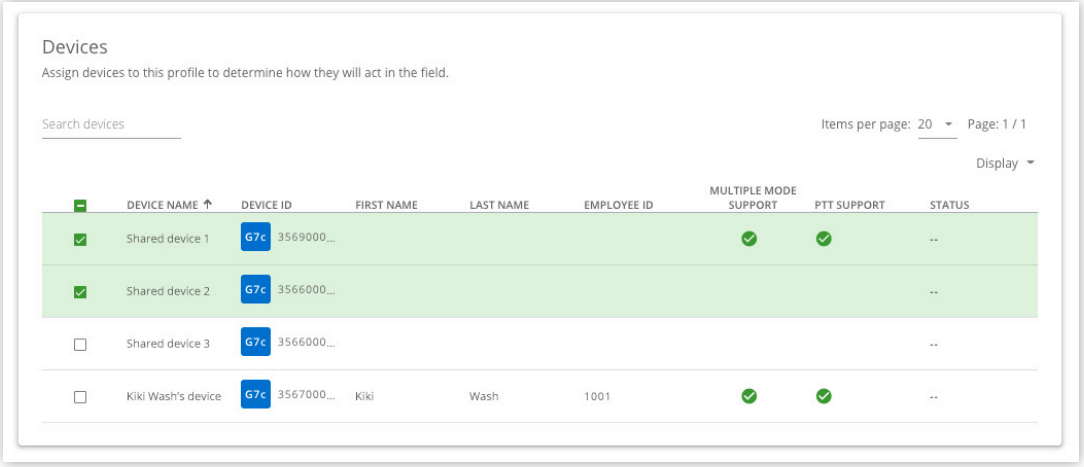


Gas sensor settings

The gas sensor settings section includes features specifically related to gas detection. This section also allows you to enable or disable certain gas sensors, and indicate alarm thresholds per sensor type. Customers who do not use Blackline Safety products for gas detection do not need to be familiar with this section.



The final section of the configuration profile is the Devices card, which indicates which devices are using these settings. The list of devices can be searched and sorted in order to find specific devices. Click on a row in order to highlight and select the device.



G7c and G7x configuration modes

G7c and G7x devices have the ability to switch between multiple configuration modes. While using these modes, G7's behaviour is slightly altered to accommodate for the environment it is being used in.

Configuration modes are most commonly used for gas detection, particularly in situations where a worker is using G7 to sample for gas while taking safety precautions to keep themselves out of harm's way. An example of this would be a user entering a confined space while wearing protective gear — like a self-contained breathing apparatus — or when they are testing a confined space with a pump before entering. In these situations, the device user may not want their device to go into alert even if it is exposed to gas, since they are protected against gas exposures and do not need monitoring personnel to dispatch emergency services.

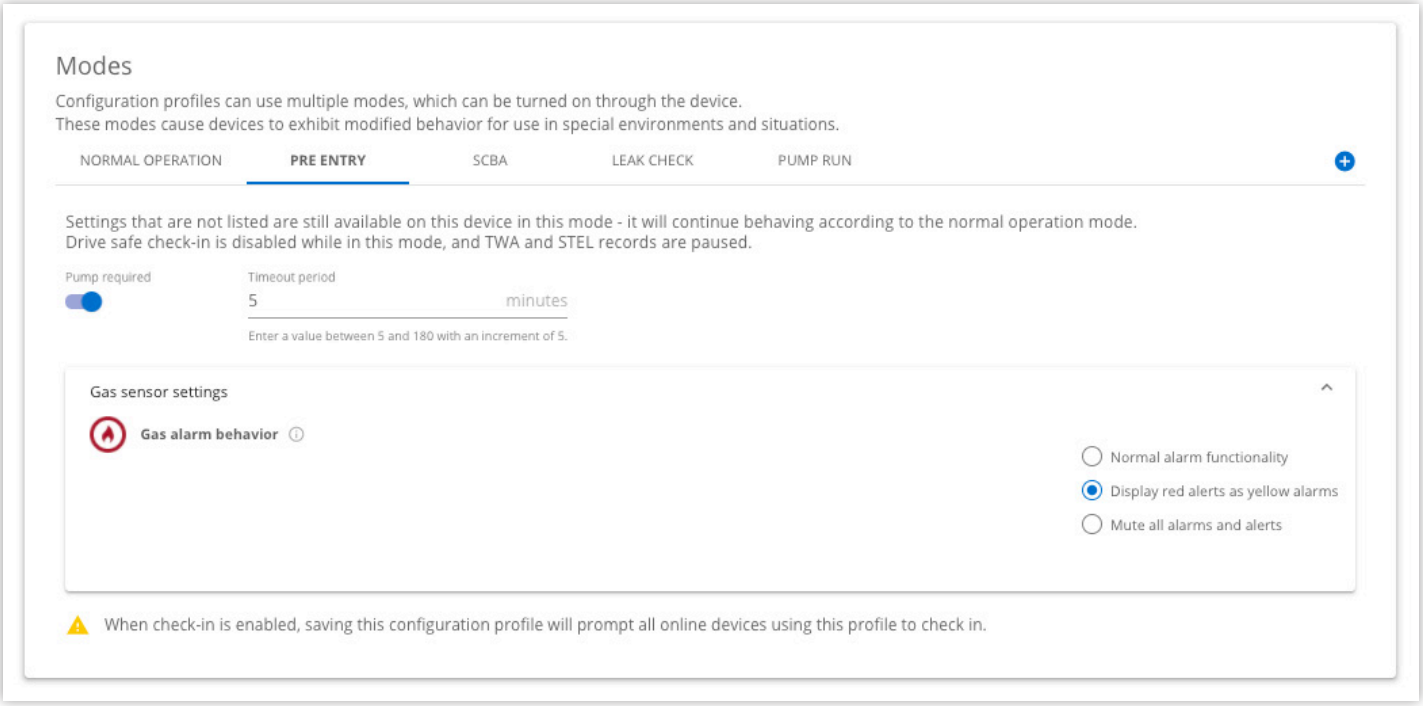
Blackline Live currently offers five configuration modes:

- Pre entry
- Pump run
- SCBA
- Leak check
- High risk

By default, every configuration profile will have Pre entry mode available, and it can be accessed from the device if it is using a pump cartridge. To manage which modes are available, navigate to the Modes card in a G7c or G7x configuration and click the '+' icon on the right side of the card. You will be able to select up to four modes at a time to include in the device configuration.

Once configuration modes are enabled, the Modes card will represent each enabled mode with a tab. Opening each tab allows you to adjust settings while using that mode — any features that are not listed will use the same settings as defined in the "Normal operations" mode.

Some modes have a mandatory mode timeout feature, which will prompt the user to confirm they are still using the mode after the countdown reaches zero. Many of the configuration modes modify alert and alarm behavior, so this timeout ensures in the case the user cannot respond that the device will exit the configuration mode and notify monitoring personnel to investigate.

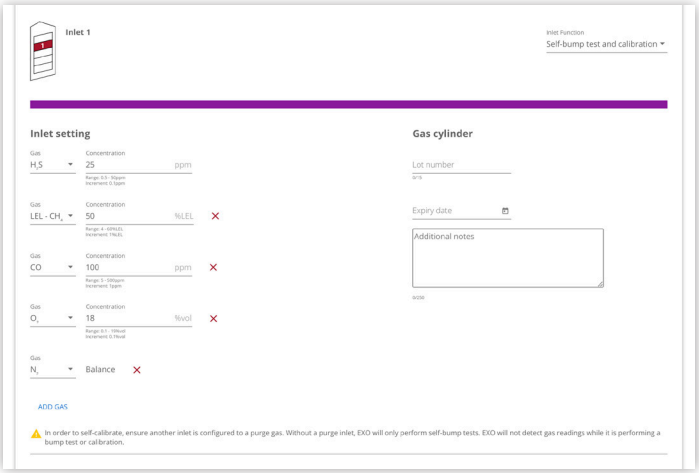


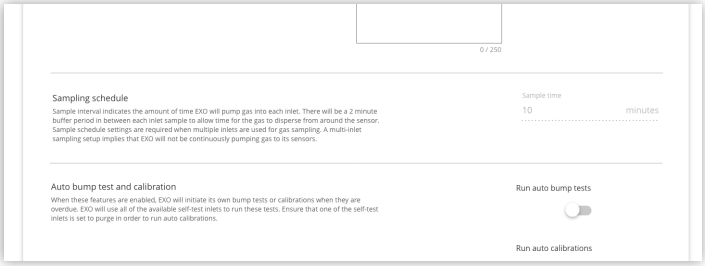
G7 pump cartridge

G7's pump cartridge works in combination with configuration modes. To turn the pump on, the user must enter a configuration mode that requires the pump. Leak check and pre entry mode have a "pump required" setting in their respective tabs in the Settings card on Blackline Live. If this setting is toggled on, a pump is required to enter the mode and the pump will start running when the mode is entered on the device. Pump run mode will always run the pump cartirdge.

EXO pump inlets

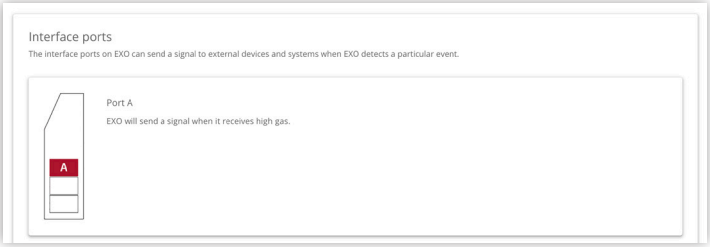
EXO's pump module has an entirely separate card to define its settings. This card allows account administrators to configure each inlet individually to define one of two functions: gas sampling, like G7's pump cartridge, or a self-test feature that allows EXO to be set up like G7 Dock in order to bump test and calibrate itself.





EXO interface ports

EXO also includes an additional section of the configuration profile to review the function of its interface ports. EXO can be set up to send a signal to an external device when it goes into a low gas event or high gas alert.



Loner mobile configurations

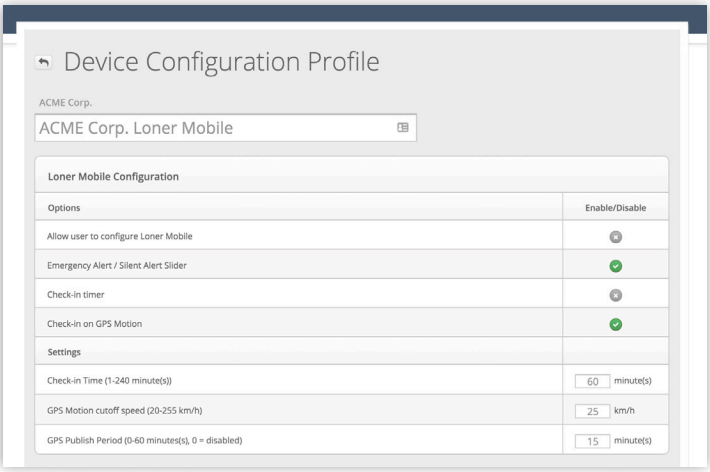
Loner mobile configurations are in a similar format to G7 configurations. The page lists out available features and allows you to toggle them on or off, or define the settings of each.

If you are using Loner DUO with you Loner Mobile app, you can also use the Loner Mobile configuration profile to configure DUO.

3.9 ALERT PROFILES

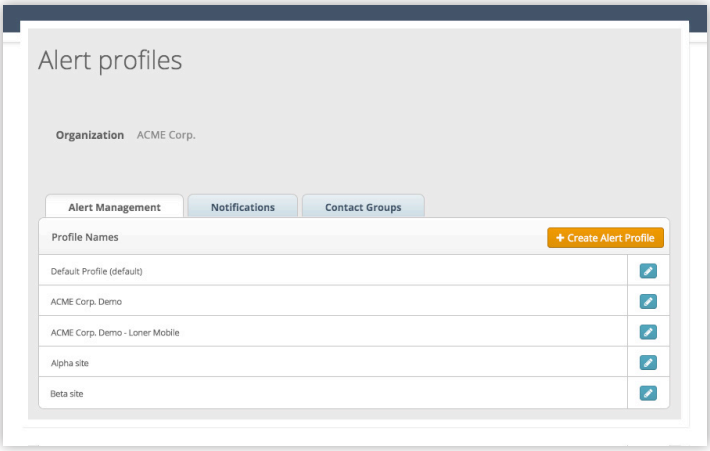
Alert profiles define how monitoring personnel respond to alerts from a group of devices. To see alert profiles, navigate to the Alert profiles option in the main menu.

Alert profiles can be applied to any kind of device type, as long as the emergency protocol and contacts are the same for all devices.

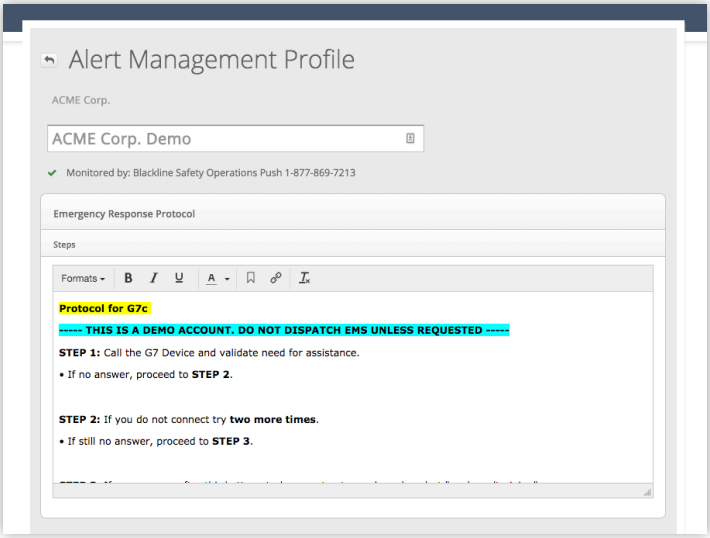


Ensure that you have registered your emergency response contacts as team members and that they have updated email and phone number information.

To get started, define a name for the profile and enter the **emergency response protocol** into the free text box. The emergency protocol will describe the steps monitoring personnel should take in the case of an emergency. If you are monitored by Blackline's Safety Operations Center (SOC), you will work with our SOC administrators to build a custom protocol that is optimal for your organization.



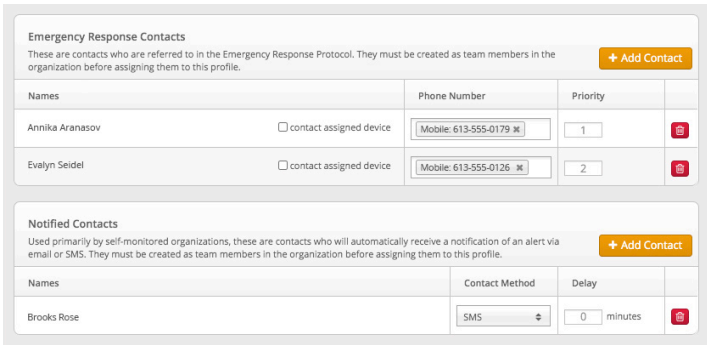
Emergency response contacts represent people who should be contacted in the case of an emergency. Their information will be made available to monitoring services when a device in the alert profile goes into alert, and they will be listed in order of priority of who to call. Ensure that any team members listed as emergency contacts have up-to-date phone numbers in their team member profiles.

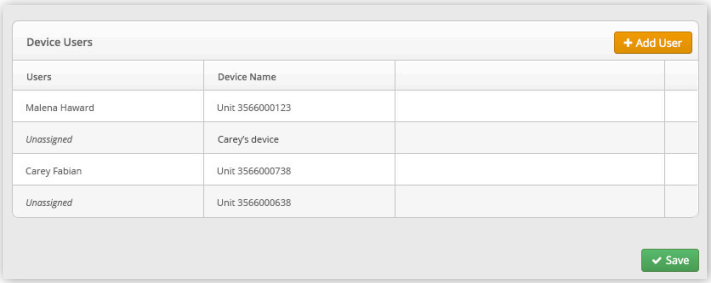


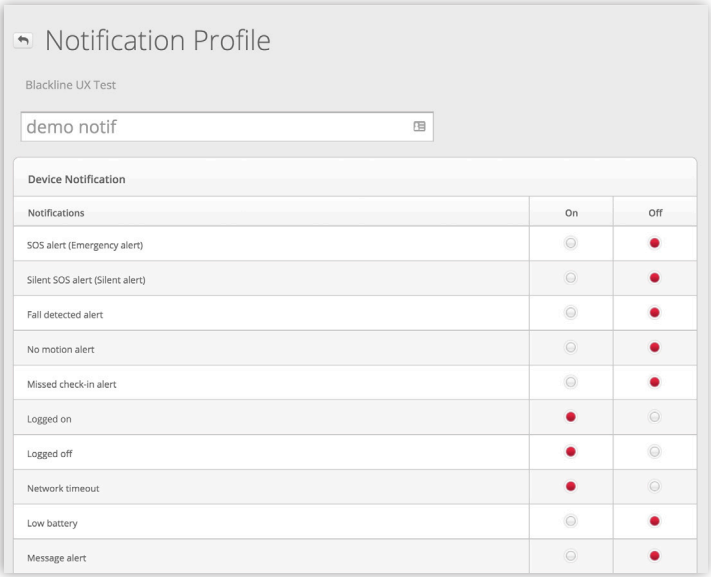
Notified contacts are people who should be notified when an alert occurs, but are not necessarily responsible for being an emergency contact. Notified contacts will be sent an email, SMS message, or both to keep them informed of the situation. Ensure that any team members listed as notified contacts have updated mobile number and email information in their team member profile.

The device alerts section lists which events on the device will result in an alert in Blackline Live. By default, lone worker and gas detection related alerts are turned on. Lower priority events such as low battery, log on and log off are turned off, but can be toggled on if they are considered a safety concern.

As with configuration profiles, you can add multiple devices to an alert profile so that they share the same emergency response protocol. If any devices require a different protocol or emergency response contacts, put them into separate alert profiles.







Edit restrictions

If your organization is monitored by Blackline's SOC, you will not be permitted to make changes to your protocol or device alerts without consulting our SOC administrators. This is to ensure that protocols are written in language and format our agents have been trained to respond to, and to avoid confusion when an alert is occurring.

Notification profiles

A notification profile is very similar in format to an alert profile. However,

this profile is only for sending out emails and SMS messages to team members, and has nothing to do with alert management in Blackline Live.

You may want to create a notification profile if you want updates sent out for non-alert events, such as low battery, log on, log off, network connection losses or hardware errors. While these events will not demand the attention of monitoring personnel, it still allows team members to be notified of the event and address the situation if needed.

As with alert profiles, notification profiles allow you to define notified contacts, device events and devices. When any of the defined devices experience an event that is toggled on in the profile, the notified contacts will receive an email or SMS.

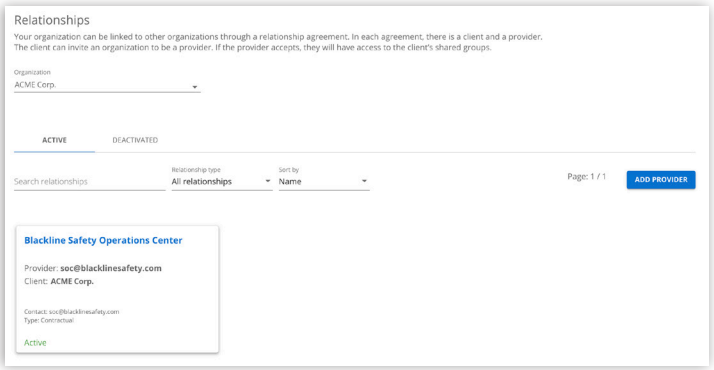
3.10 RELATIONSHIPS PAGE

The relationships page lists relationships that involve your organization. Each relationship is represented by a card that lists:

- the relationship name
- the client organization
- the provider organization
- the provider's contact email
- the relationship type
- the current status of the relationship

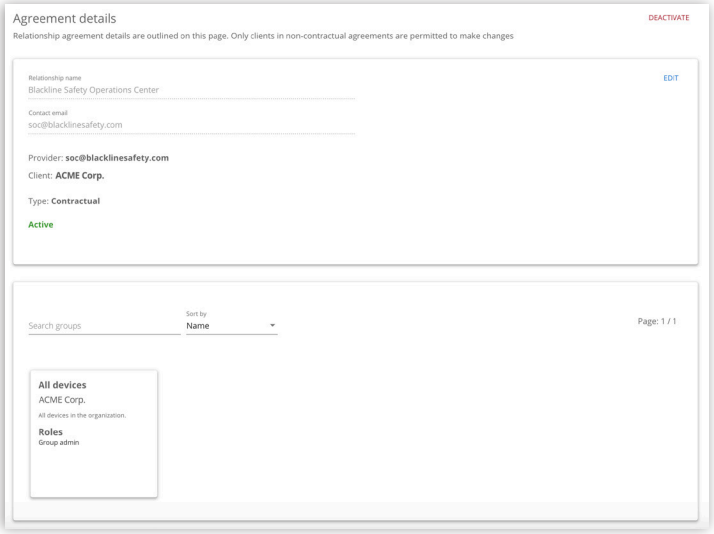
To see deactivated or cancelled relationships, click the "Deactivated" tab.

To create a new relationship, the client can navigate to this page through the user menu by clicking on their email in the navigation bar and then clicking the blue "Add provider" button.



By clicking on a relationship, you can see the details of the agreement. All of the information listed in the card version of the relationship is listed here, as well as the specific groups shared in the relationship and the roles the provider's team members are allowed to have in each group.

At the top right of the right of the page, you may see different actions you can take on the relationship depending on your permissions and on the type of relationship. For example, you may be able to deactivate non-contractual relationships, or cancel pending relationships that have not been accepted by the provider.



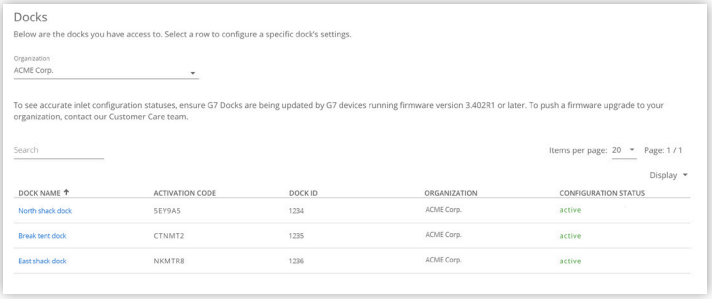
4. ACCESSORIES

In addition to Blackline Safety's safety monitoring devices, Blackline Live also supports select accessories. This ensures that any set-up required for Blackline fleets are centralized in a single software platform, and also allows you to see all different kinds of resources in your fleet.

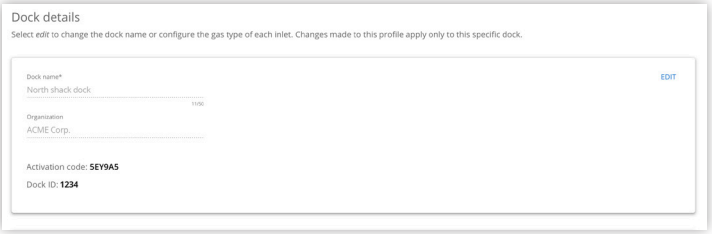
4.1 G7 DOCK CONFIGURATION

G7 Dock is a simple and easy to use solution for charging, bump testing and calibrating G7 devices. Docks are pre-set with common calibration gases when they are shipped out, but this configuration can easily be changed from the Docks page in Blackline Live.

The Dock configuration page lists all of the docks in your organization and their current configuration status. This list can be searched and sorted the same as any other resource page in Blackline Live. By clicking on G7 Dock's name, you will be redirected to the Dock's configuration page. Unlike monitoring device configurations, each Dock has its own configuration page that defines the calibration settings for that particular dock.



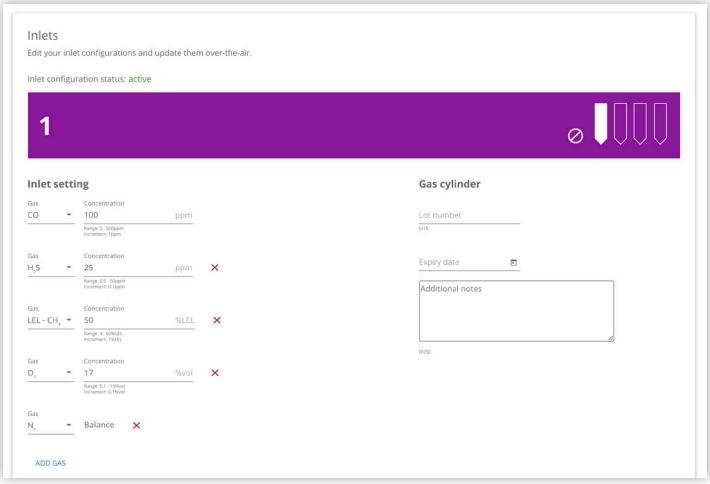
The Dock configuration page provides basic information about the Dock, such as its custom name, unit ID and activation code. The inlet settings contain the bulk of information of this page, and this is the section that defines its calibration settings.



G7 Dock includes four gas inlets and one exhaust outlet. Each of the four inlets are represented in the dock configuration page with a diagram indicating where it is located on the device.

For each inlet, select the gases that are present in the gas cylinder from the gas dropdown menus, and fill in the concentration listed on the cylinder label. You can also include the lot number of the cylinder and the expiry date of the cylinder for record-keeping purposes.

NOTE: The settings for each inlet should exactly match the information provided on the gas cylinder it will be hooked up to. Any discrepancies in settings will cause tests made from G7 Dock to fail.



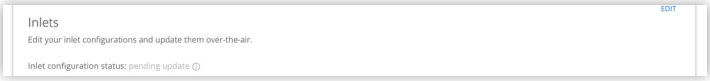
Updating G7 Dock

Once changes to the dock configuration have been made, Blackline Live will inform you that there is one more step to take before the dock is fully set up. On the configuration page, and in the Docks list page, its status will be "pending." This is because G7 Dock does not actually communicate directly with the Blackline Safety Cloud — it needs a powered on and connected G7 device inside of it to receive the new settings.

[image of g7 in dock with menu options visible]

Simply place G7 inside G7 Dock and fully close the lid until the latches click on both sides. On G7's screen, select the "Update Dock" option. Once the update is complete, G7 Dock will be able to bump test and calibrate devices based on the new settings from Blackline Live.

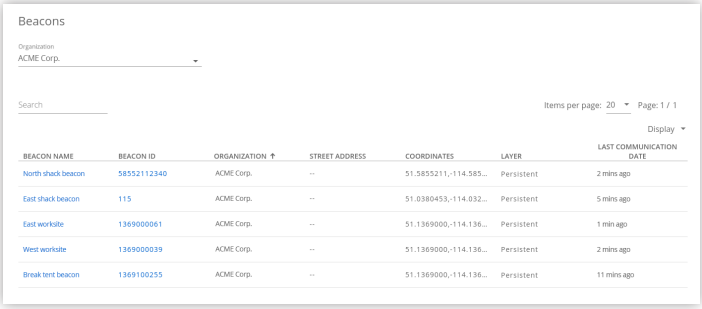
You will also see in the Dock configuration page and on the Docks list page that the Dock's status has changed to "active."

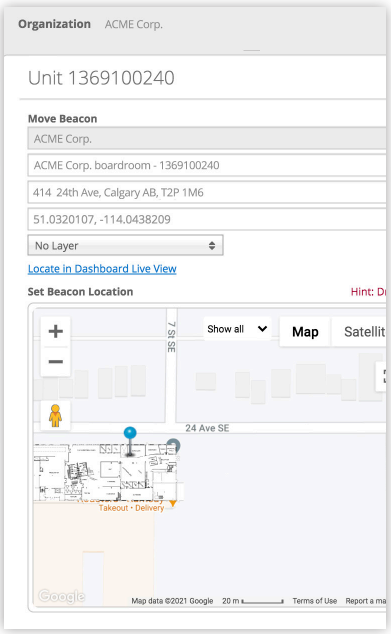


4.2 LOCATION BEACONS

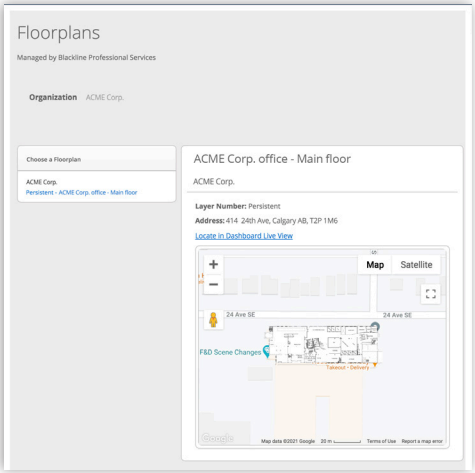
Location beacons can be set up throughout your work facility to provide more accurate locations in areas with poor GPS coverage, such as inside buildings or in areas with metal scaffolding. Location beacons represent a single GPS coordinate, and transmit this information to nearby G7 devices. When a G7 "hears" the beacon, it assumes it is in the location the beacon is transmitting. This location will be sent to Blackline Live in any communication G7 sends while it is in the vicinity of the beacon.

Beacon locations are set through Blackline Live from the Beacons page. Select the beacon you want to set, name it something recognizable — such as Control Room or North Gate — and enter a latitude/longitude coordinate in decimal format. After the coordinate is entered, you can drag the pin on the map to get an even more accurate location. Location beacons can also be placed with respect to floorplan layers to provide accurate location information in multistory buildings.





Beacons have no concept of where they actually are in space — they will only ever transmit the location they are assigned through Blackline Live. Ensure that the physical placement of the beacon matches its location in Blackline Live.



Floorplans and map overlays

Floorplans and site plans provide more context to the live maps page, and make it easier to accurately place beacons indoors. Using a combination of floorplans and location beacons allows for more efficient emergency response and dispatch, since monitoring agents can see on the map exactly where the alert is occurring.

Floorplans can be layered for multistory buildings, and users on the maps page can filter through these layers to only show devices communicating with beacons on that respective layer.

Tips for preparing floorplan files:

- Use high resolution file types (PDF, PNG, JPEG, SVG, KML or KMZ)
- Use clear and legible plans. Avoid low-resolution or scanned images
- Clearly label which file corresponds to which floor
- Use up-to-date files that are drawn to scale
- Clearly label "north"
- Provide reference of where the floorplan lays if it does not represent the entire building

Using KML/KMZ files

In addition to overlaying floorplan or site plan images on the map, Blackline Live can also display KML or KMZ files with embedded information. These files can display building or zone perimeters, or mark out important site resources like first aid kits or fire hydrants.

These files can be created through professional GIS softwares, or for free using Google's My Maps tool. Through My Maps, you can create lines, shapes or markers and place them directly on a map. Once all of the assets have been created, you can export them as an KML file, which can then be placed in Blackline Live.

Once your floorplan or site plan has been prepared, contact your sales representative or Customer Care.

Troubleshooting Tip

If you see a G7 device being displayed in a strange location, check if it is communicating with a nearby beacon that may not have an updated location.

5. MONITORING AND REVIEW

Blackline Live provides a number of tools for live monitoring as well as retroactive review and analytics:

Maps (Live view) — allows you to see the last known location of online devices, and is useful for monitoring the current status and location of your fleet

Maps (History view) — allows you to see a list of events that occurred on a selected device over a specified time range. You can click on any location or event to see where the device was, and what its status was at the time.

Dashboard — this page gives you a real-time overview of the status of your device fleet. If devices are out of gas compliance or need maintenance, they will be listed on this page with recommended resolution steps.

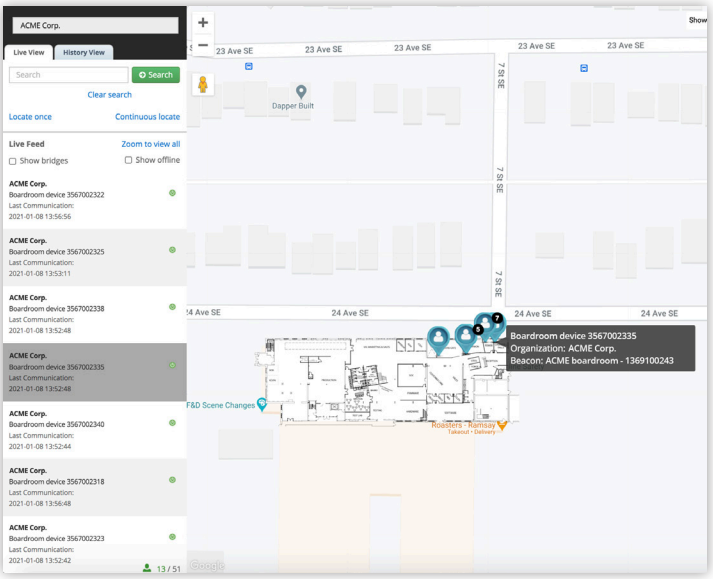
Alerts — the alerts page lists alerts that have occurred on devices you have access to. By default, this page will display alerts that occurred within the last 24 hours, but can be adjusted to show alerts within a specific date and time range.

Alert history — selecting an alert with a resolved status will direct you to the alert history. This page gives an overview of the times an alert was triggered, acknowledged and resolved, as well as the location and status at the time of the alert. This page lists out the notes that were left by the monitoring agent who managed the alerts, and allows you to download any voice calls that were made to the device.

Alert management — clicking on an alert that is currently active (with a "unacknowledged" or "acknowledged" status) will direct you to the alert management page. This page populates assigned team member info, the emergency protocol and emergency contacts assigned to that device, in addition to features that allow you to text message or voice call the end user. This page is a monitoring agent's most valuable tool for investigating and resolving active alerts.

Blackline Analytics — Blackline provides a suite of reports that allow you to review the type, amount and location of alerts occurring to identify hazardous areas or gaps in training. Analytics can also be used to track KPI's such as device usage and gas compliance to ensure your organization is meeting industry and company standards.

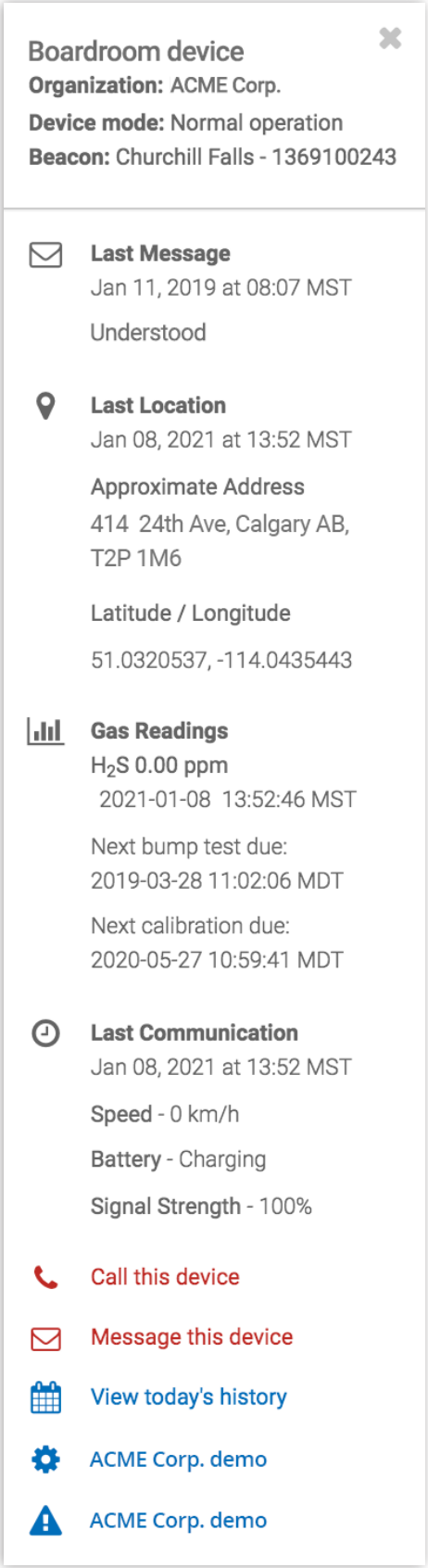
5.1 MAPS



The Maps page has two views — the live view and device history view. The live view displays the last known location and status of your device fleet. Devices are represented by maps pins with a symbol in the middle.

The colour of the map pins indicate the current state of the device. Devices in alert are also automatically shown at the top left-hand side of the page so that they are easy to identify.

Map pin locations are updated when an event occurs on the device, or according to a schedule when the device is idle. The default schedule for G7c is 5 minutes, while G7x is 30 minutes, as it is typically communicating over satellite. When the device is travelling, the map pin will indicate which direction it is travelling in.



To see more about the device's status, click on it from the left-hand sidebar or click its pin on the map to open the info panel on the right side of the screen. This panel displays the following information (if it is available):

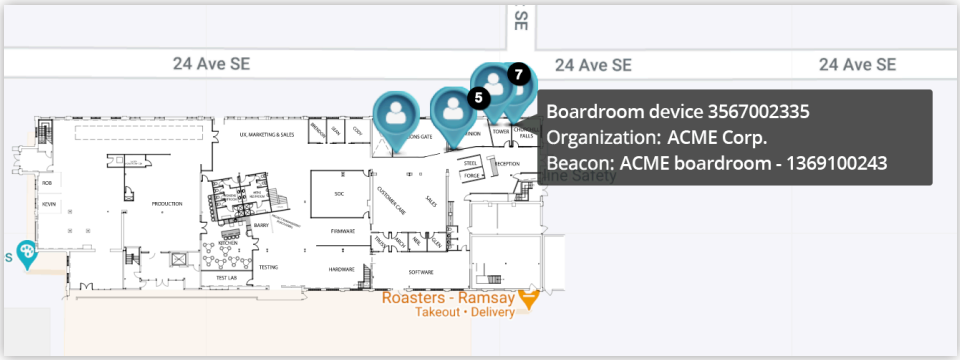
- Assigned user name or ID, or the device's name or ID
- Assigned user's mobile phone number
- Current configuration mode
- Location beacon name
- Last message sent to or from the device
- Last known location from either a beacon or GPS
- Current gas readings, and whether a pump cartridge is currently running
- Last communication to the server
- Speed
- Battery level
- Signal strength

NOTE: The device's "display name" varies depending on what information is available. If the device is assigned, the info panel will list the assigned user's name, or their ID if a name is not available. If the device is not assigned, the info panel will list it's name, or ID if a name is not available.

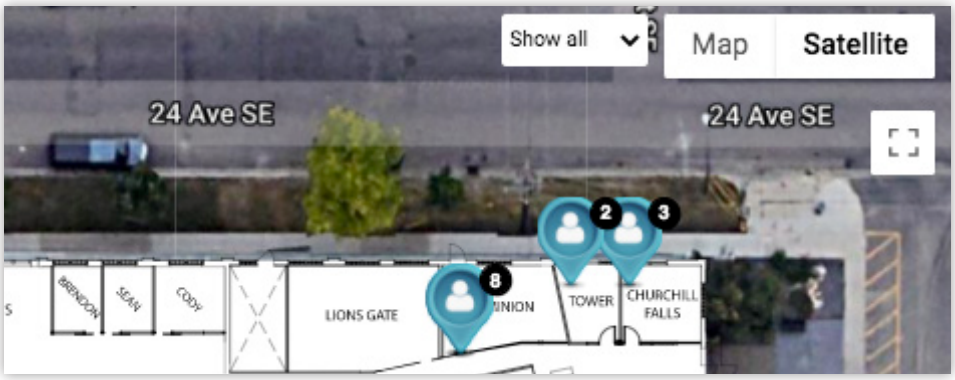
The info panel also allows you to quickly message or call the device. Taking either of these actions will require an alert to be created. Once redirected to the alert management page, you can use the message text box to send a message, or use the provided phone number to initiate a 2-way call with the device.

This panel also displays the device's current assigned configuration profile and alert profile, and clicking either of these links will direct to the respective profile page. Lastly, clicking "view today's history" provides a shortcut to the maps history view, with this device and the current day already pre-selected.

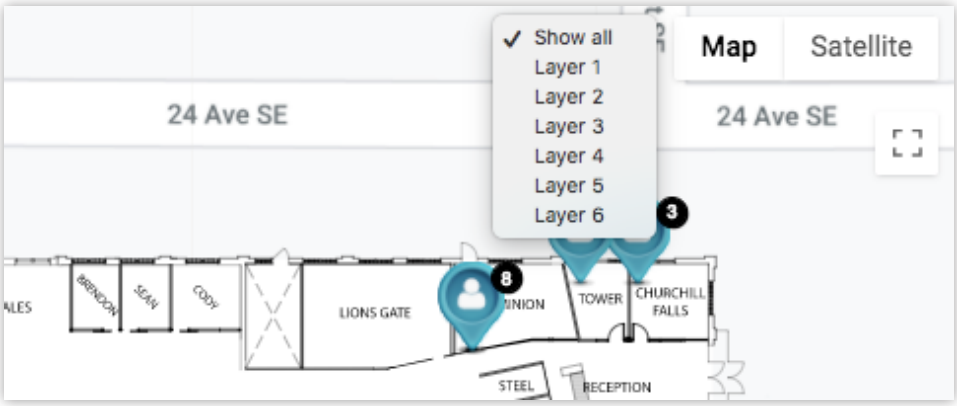
Any floorplans in your organization will be overlaid on the map so that you can clearly see where your device fleet is located, especially if your workforce operates indoors.

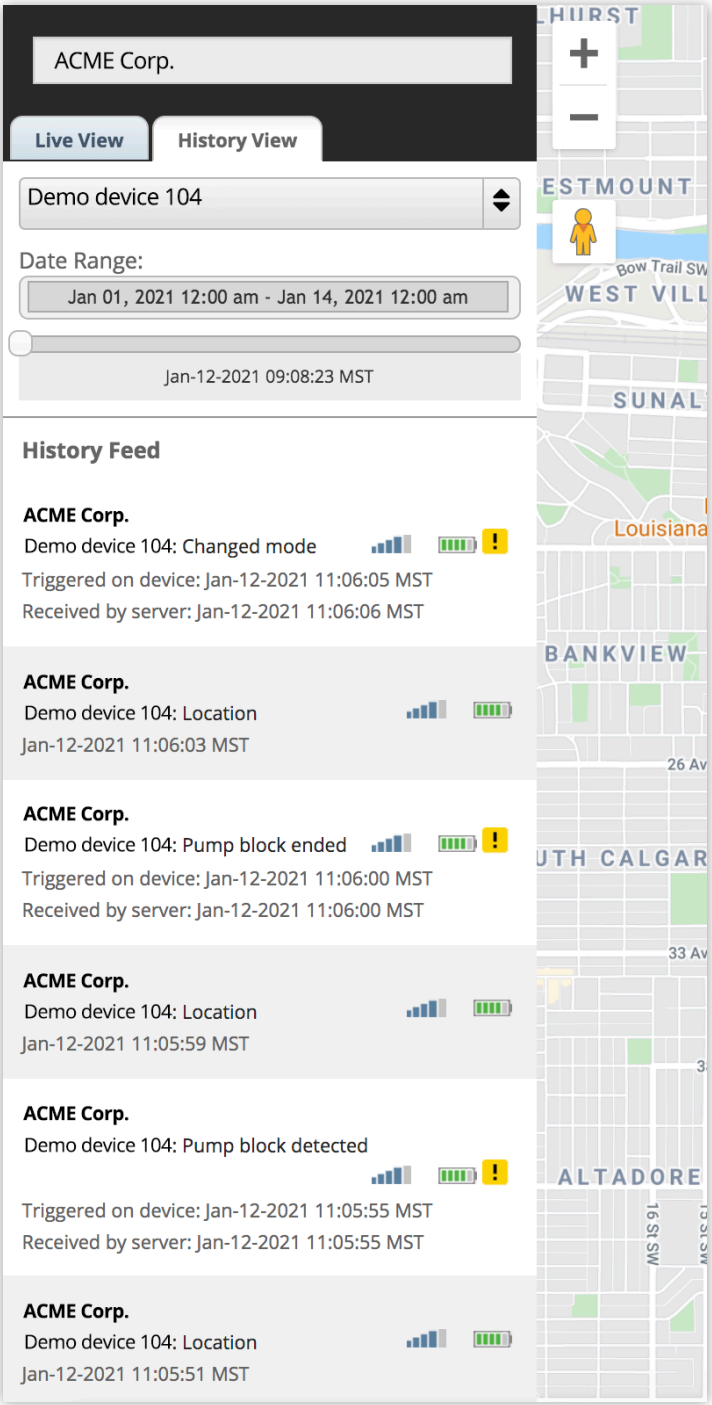


By default, Blackline Live displays a simplified map view. You can toggle the map to a satellite view if you would prefer to see your floorplans and devices overlaid on detailed satellite images. For workforces operating in remote areas, satellite imagery will provide geographical details and landmarks that are not shown in the default map view.



If your organization uses layered floorplans, you can also filter the map view to a particular layer. When filtered, only floorplans and devices communicating with beacons on this layer will be displayed.





Maps history view

In the case you need to investigate an incident, track where a device has gone over time or troubleshoot an issue with the device, you can use History View to learn more about what happened to a particular device.

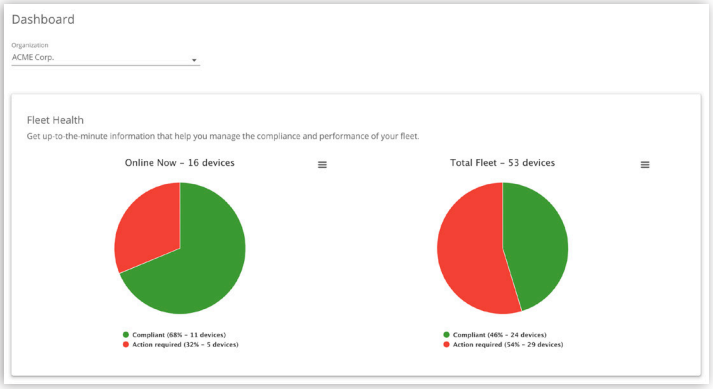
To use History View, first navigate to the Maps page and click the "History view" tab in the left-hand sidebar. Select a device from the dropdown in the left-hand sidebar and use the calendar pickers to select the time frame you would like to review. Once the data has loaded, you will see a list of messages from the device to Blackline Live that occurred during the specified time period.

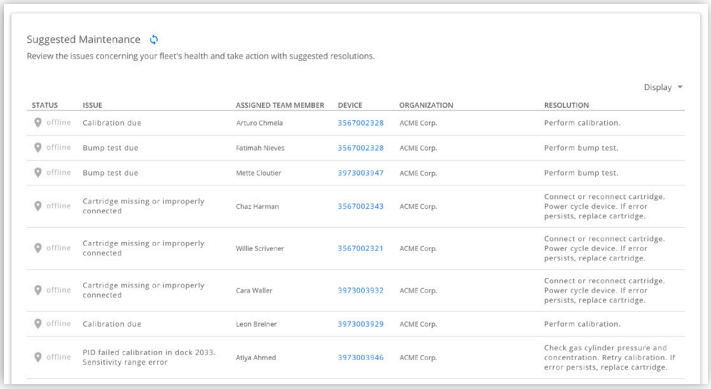
If events were not sent on a schedule, they will be marked with a yellow or red '!' icon with a description of the event that occurred. This could be a gas exposure, a compliance reminder, an alert, or a series of other events. Check-in events and message events will have their own icons to differentiate them — a check-in will have a checkmark icon, while a message will have an envelope icon. Hover over the event icon to learn more about what happened on the device. Click on the event to see where it occurred (if a location was available) and bring up the info panel to see the device's status at the time of the event.

To see where a device has been over a period of time, click and drag the slider above the event list. As you drag the slider through the specified period of time, a dot will appear on the map for each location the device was reported at. With the slider, you can get a good idea of the route a user may have travelled.

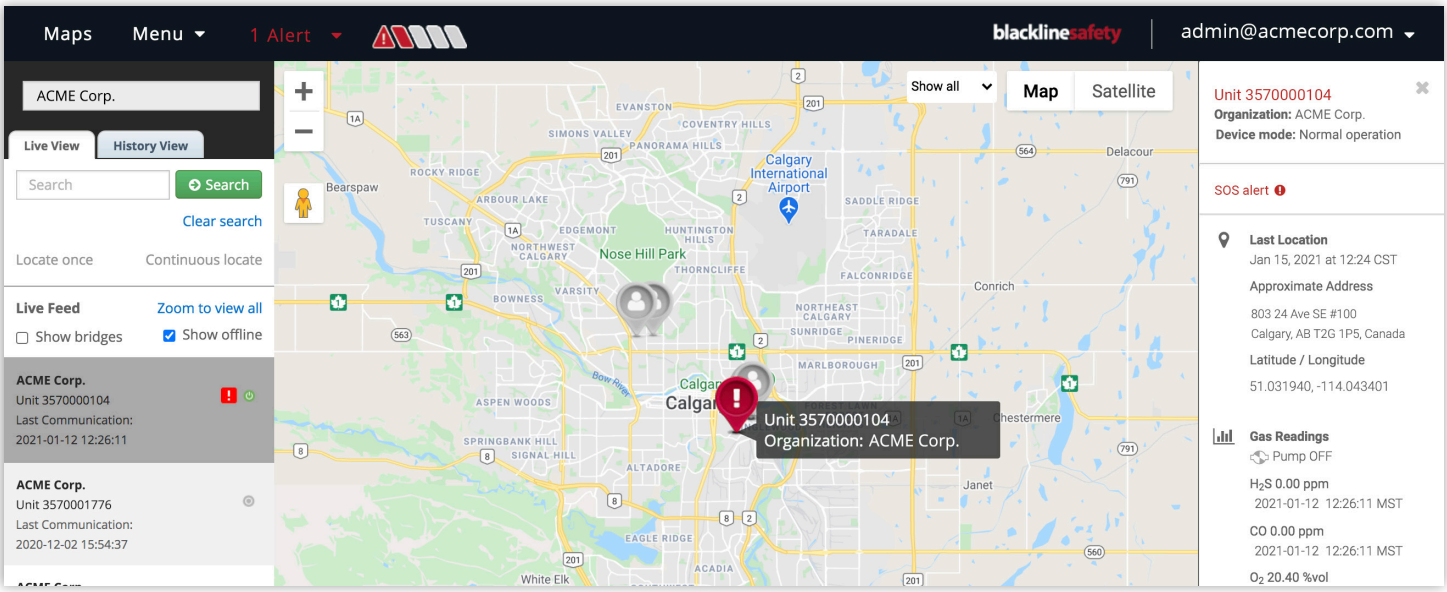
5.2 DASHBOARD

The live dashboard provides a snapshot of the compliance of your entire fleet, and can be accessed through the "Dashboard" option in the main menu. Devices that are considered "non-compliant" are listed with a description of the issue and the recommended resolution.





5.3 ALERTS



When one of your devices goes into alert, Blackline Live will inform you with a notification in the navigation bar and a loud siren sound. The device in alert will be shown with a red map pin on the maps page, and will appear at the top of the left-hand sidebar.

Troubleshooting Tip

If you see a yellow warning banner beneath the navigation bar, it means your current audio settings are blocking the alert siren sound. Click the link in the banner for troubleshooting tips for your browser and operating system.

Alerts page

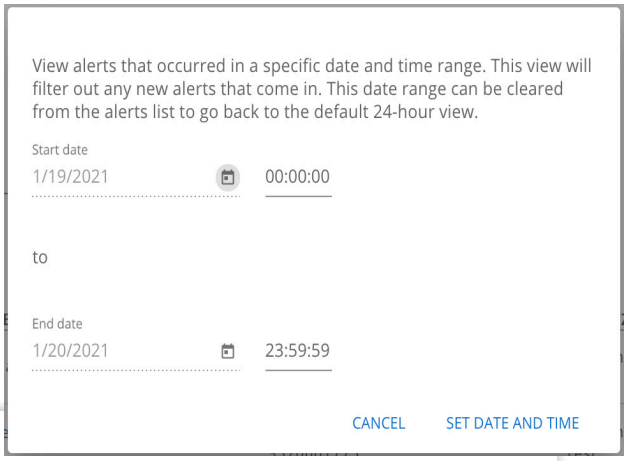
To see all current and historic alerts, navigate to the Alerts page from the main menu. This page lists all alerts and indicates the status and type of alert, when the alert occurred, the device type and ID, and to whom the device was assigned. To see more information about the alert, you can click on the timestamp or the alert type.

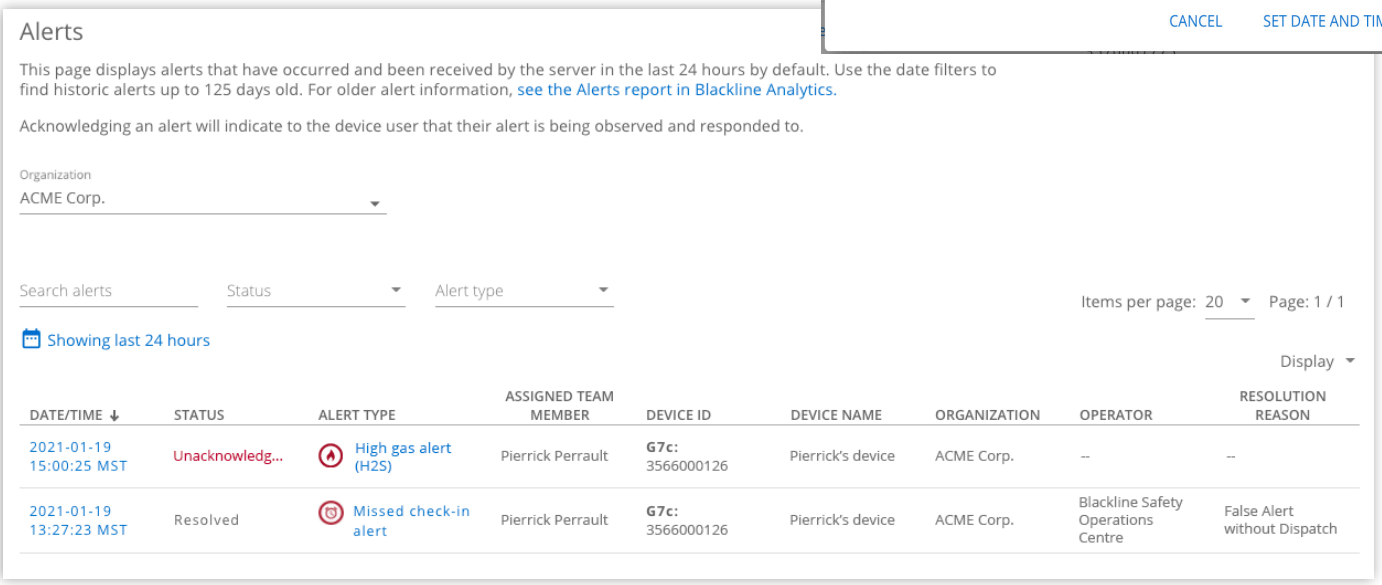
If the alert is active — with an unacknowledged or acknowledged status — clicking on it will redirect to the Alert management page. From here, you can see live information about the alert and access tools designed to help manage and resolve the alert.

If the alert is resolved, clicking on it will redirect you to the Alert history page, which displays a snapshot of the device's state when the alert occurred, as well as information regarding how and when it was resolved.

By default, this page will only display alerts that have occurred within the last 24 hours. This time filter is most useful for account users who need to see and manage alerts that are currently active. To see alerts that occurred more than 24 hours ago, click on the calendar icon to open the date selection settings.

In this pop-up, you can choose to see alerts that occurred within a specific range of time by selecting a starting date and time, as well as an ending date and time. This date range can be cleared from the alerts page to go back to viewing the last 24 hours.

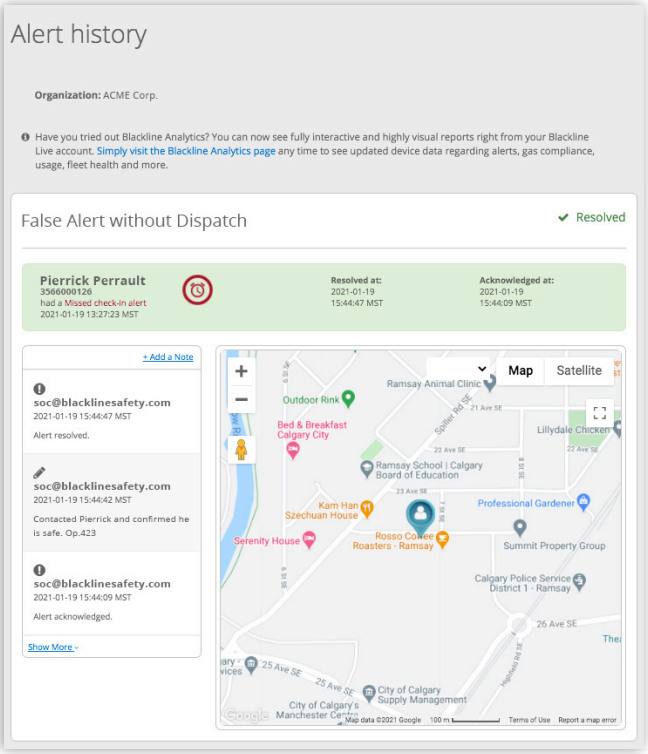




Alerts history

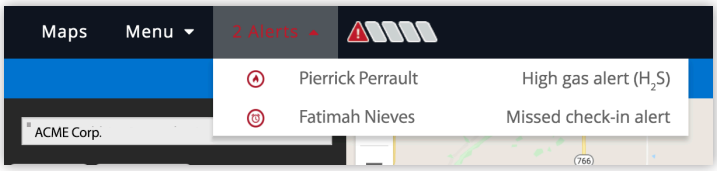
The Alert history page provides a snapshot of a device's state when it went into alert. At the top of the page, you can see what type of alert occurred, who was assigned to the device, as well as important timestamps that indicate when the alert occurred, when it was acknowledged by monitoring personnel, and when it was resolved.

The map shows where the device was located when the alert occurred, and the info panel can be opened by clicking on the map pin to see the state of the device at that time. Lastly, the notes section of the Alert management page on the left side of the map lists the steps taken by monitoring personnel to manage and resolve the alert. If any two-way calls were made between the monitoring agent and the device in alert, you can download a recording of the call from a link in the notes.



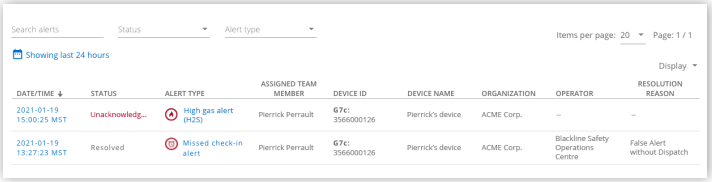
Alert management

If your organization is self-monitored, or if your organization uses Blackline Live to monitor other organizations, your account users will be responsible for managing and responding to alerts. This is done using the Alert management page, which can be accessed when there is an active alert.

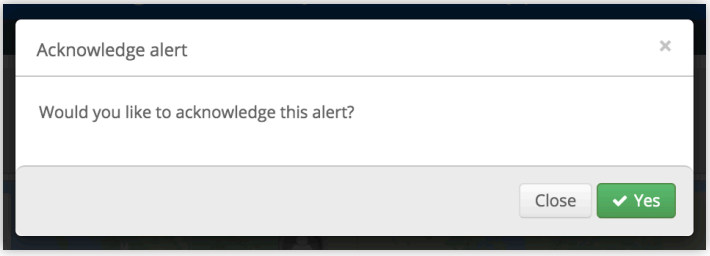


NOTE: If your organization is monitored by Blackline Safety's SOC or another monitoring service, do not attempt to manage active alerts. Giving account users the "contact admin", "view only" or "analytics only" roles will prevent them from being able to interact with alerts.

The Alerts management page can be accessed in two ways. The first is to click the animated alert banner at the top of the screen and select the alert from the alert dropdown menu. The other is to navigate to the Alerts page from the main menu and select an active alert from the list.



Once you land on the Alert acknowledgement page, you will be prompted to acknowledge the alert. Acknowledging the alert signifies that you are taking responsibility for following the alert protocol and ensuring the safety of the device user. Acknowledging the alert will also cause the blue LiveResponse light to shine on the affected device, which indicates to the device user that someone is investigating the alert and that help is on the way.

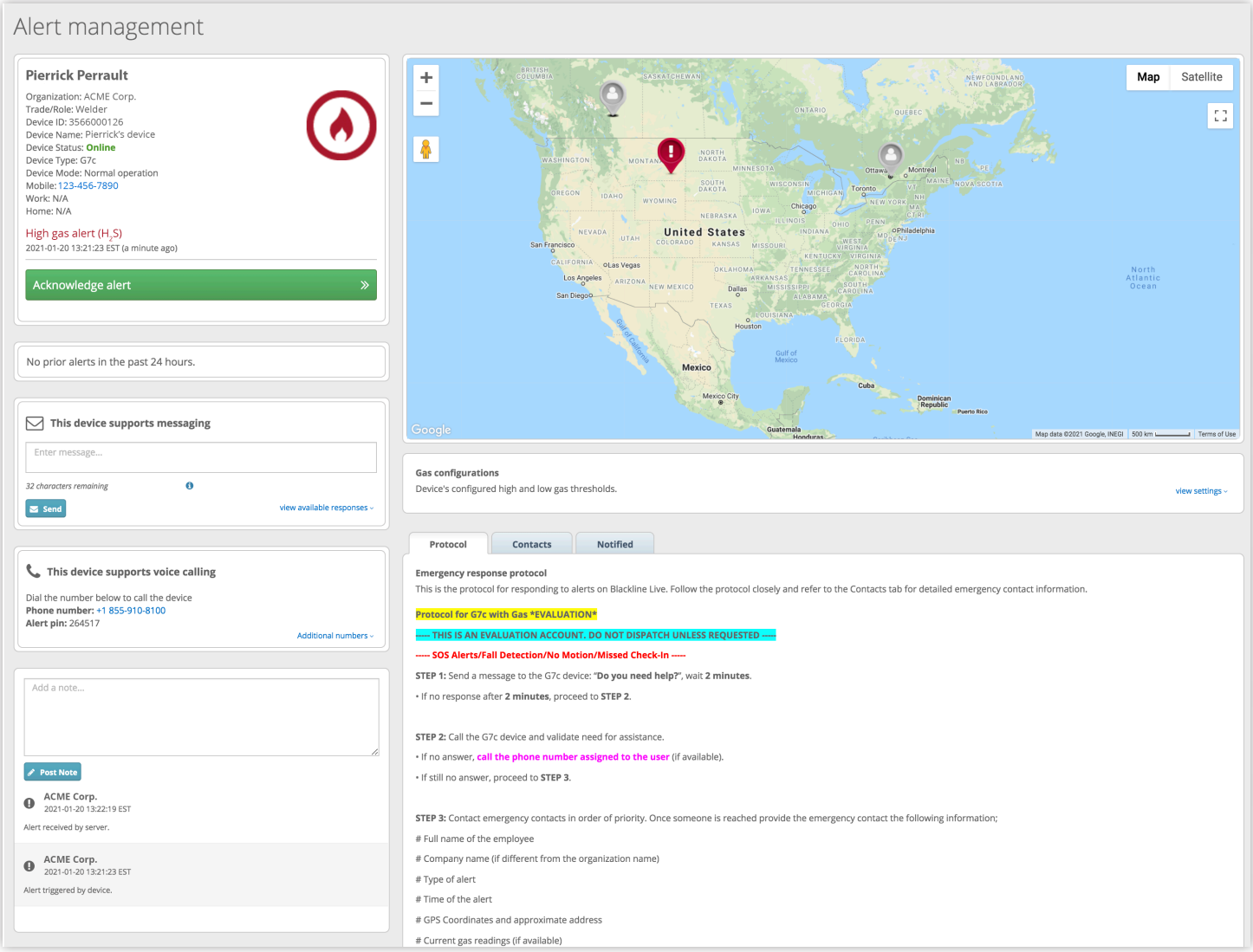


Once the alert has been acknowledged, you will be able to use the tools in the alert management page to investigate the alert, get in touch with emergency contacts and provide valuable information to dispatch services if required.

Information widget

In the top left side of the page, an information widget will list information about the device, the assigned user, and the alert itself. This information can help you identify the user to emergency contacts, or even help you contact the user directly if needed.

The information widget also contains the "resolution" option. Select this option when the user's safety has been confirmed to close the alert.A smaller widget beneath the main information widget lists any other alerts that occurred on the same device with the same user in the last 24 hours. This indicates if any other active alerts are open for this device that can also be addressed.



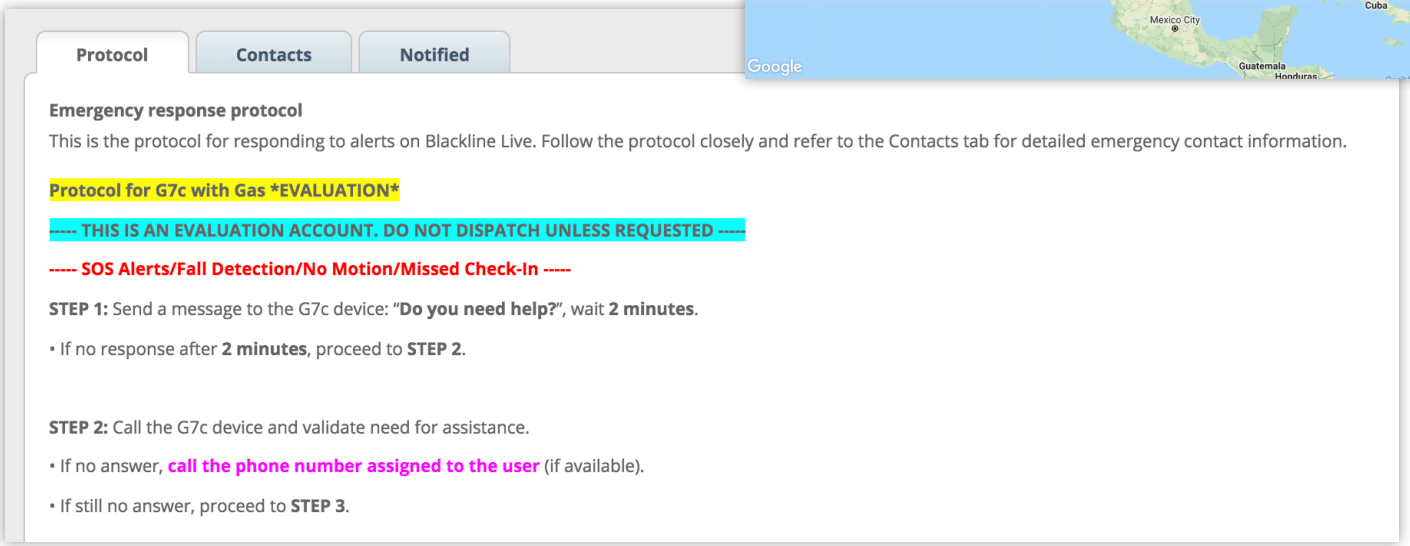
Map

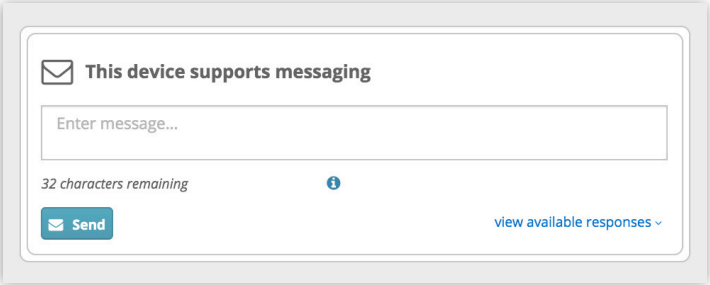
The Alert management page shows the current location of the device in alert on a live map. Click on the device pin to open the info panel and see more information about the state of the device, such as its current gas readings, the street address it was last reported at, and whether it is running a pump or configuration mode. The map can also show you nearby workers who may be able to help, or allow you to provide directions to response or dispatch teams.

Emergency response protocol

The emergency response protocol entered into the alert profile appears in a widget underneath the map, making it easy for you to reference as you piece together the alert situation and work to ensure the device user's safety. In addition to the protocol, this widget also includes a list of the emergency response contacts and their information in order of priority. A third tab lists notified contacts that were automatically informed of the alert via SMS or email.

All of the information in this widget is populated from the alert profile assigned to the device in alert. It is of utmost importance to ensure the information in alert profiles is kept updated and that device is assigned to the correct profile at all times.

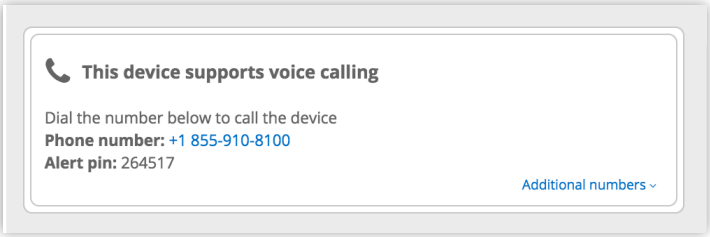




Text message

A response protocol may include a step to contact the affected device via text message. You can send a message of up to 32 characters to let the device user know help is on the way.

NOTE: This feature is not available for older devices such as SMD, IS+, M6, M6i or Loner 900 devices, as they do not have an LCD screen to support text messaging.

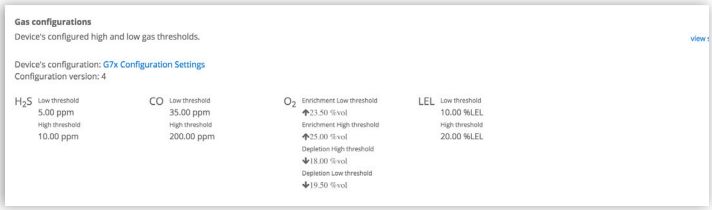


Two-way voice call

A response protocol may include a step to directly call the device. G7 devices — including EXO — can maintain a two-way voice call with a phone.

Use the information in the voice call widget to place a call to a device. If the alert on the device has not been acknowledged before you call — if it was initiated from an email or from the maps page, for instance — you will be required to acknowledge the alert before the call goes through.

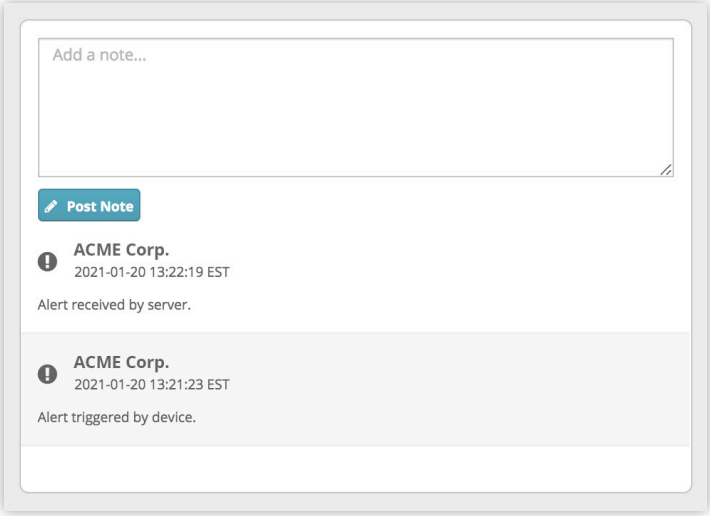
The device user is not required to do anything to accept the voice call, and the call will only end when the person on the phone hangs up.



Gas configurations

The Gas configurations widget, situated between the map and the emergency response widgets, lists the configured gas sensor thresholds the device is using based on the configuration profile it has been assigned. These measurements can be compared to the device's current gas readings to determine if the device is currently in an environment with high gas levels.

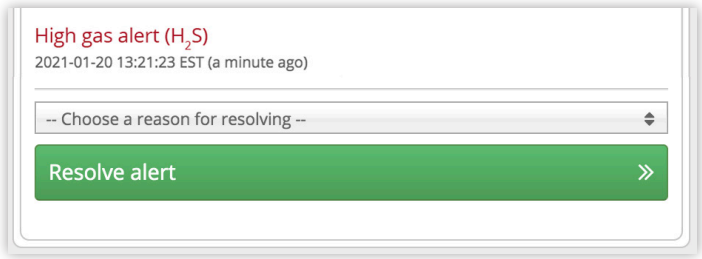
NOTE: This widget is compressed by default to make room for the emergency protocol, but can be expanded when needed.



Notes

The Notes section, located at the bottom left side of the alert management screen, provides a chronological step-by-step history of the alert and the steps taken to resolve it. It records when the alarm was triggered locally on the device, as well as when it was delivered to the portal. Any steps taken through Blackline Live — such as sending a message or placing a voice call — are recorded automatically. Notes can also be added manually to describe calls made to emergency contacts or to the device user.

NOTE: Monitoring personnel should make a habit of filling out the notes section with as much detail as possible, since they will be available in the alert history page after the alert is resolved, and can be used for investigations and retrospectives.



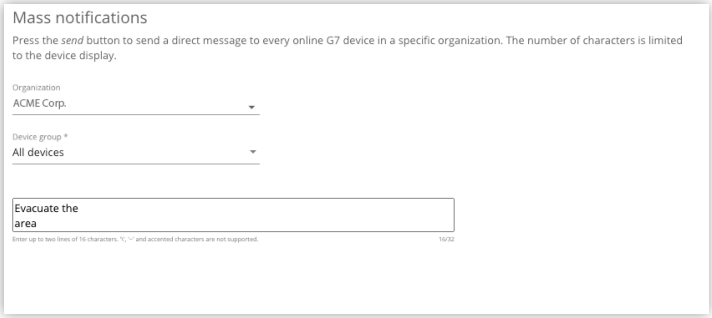
Resolution

Once the worker's safety has been confirmed, you can resolve the alert. First, select a reason for resolving from the dropdown list. Indicate whether there was a false or actual incident, and whether dispatch was sent out to the device user or not. If the alert occurred as part of testing before formal monitoring begins, it can be marked as "Pre-alert".

Once a reason has been selected, click the green "Resolve" button. The alerts will be cleared from the device, and the device will no longer be shown with an alert status throughout Blackline Live.

5.4 MASS NOTIFICATIONS

In the case of an evacuation or large-scale emergency where multiple devices need to be contacted, Blackline Live allows an account user to mass notify all of the devices in an organization or by individual device group. The mass notifications page can be accessed through the main menu under the "Resources" column.



To use the mass notifications page, first specify which organization and group should be notified. To contact all of the devices in an organization, set the group to "All devices."

Once the target devices are defined, enter a short message into the text area. Just as with the text message function in the alert management page, this message will need to be split into two lines with a maximum of 16 characters each.

Once the "send" button is clicked, the message will be sent out to all devices in the specified group.

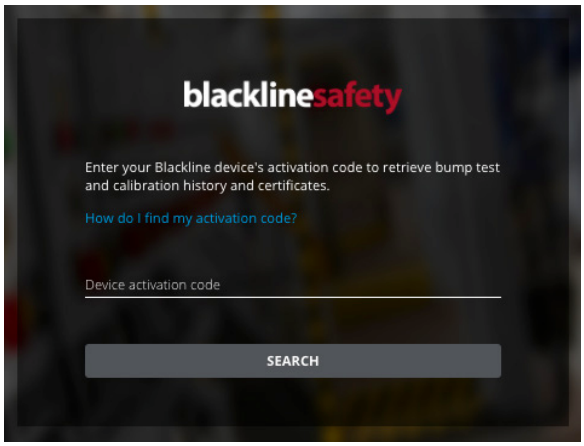
Specifications for message delivery

Blackline Safety guarantees 99% delivery of messages to all devices on cellular networks. Blackline Live will attempt to send the message three times before it times out. Devices on satellite networks or devices in areas with poor cellular reception may have issues receiving text messages — as well as other communications — from Blackline Live.

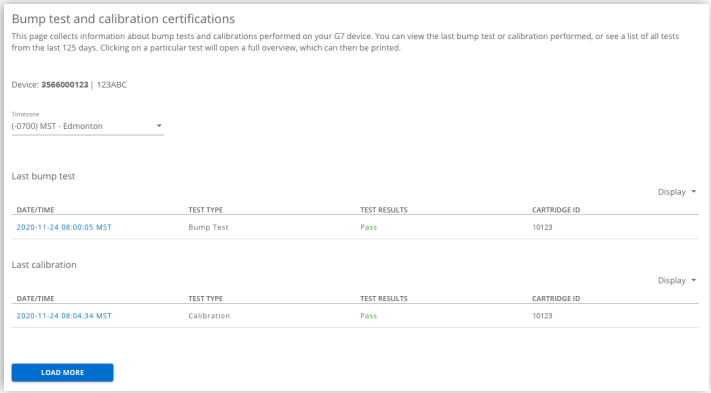
5.5 BUMP TEST AND CALIBRATION CERTIFICATES

Blackline Live can also display bump and calibration certificates for tests that have been completed on a particular device. This page is hosted separately from the rest of Blackline Live, since it can be accessed even without an account. To access this page, go to:

https://live.blacklinesafety.com/certs/



On the landing page, enter the activation code of the device you would like to look up. After submitting the code, you will immediately see when the device was last bump tested and last calibrated.

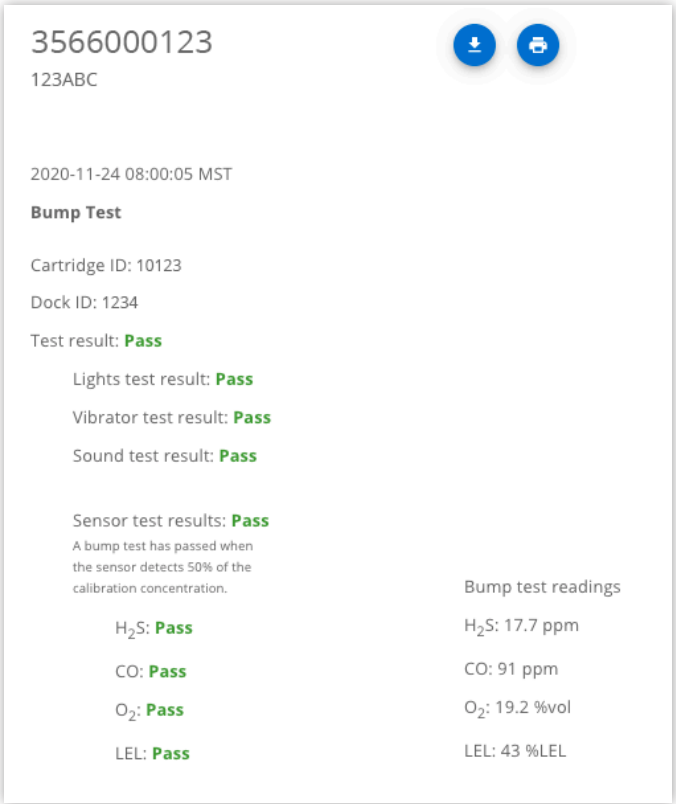


To see a longer list of test results, click the *load more* button. This displays all the tests that were performed within the last 125 days. To get information regarding older tests, contact Blackline Safety's Customer Care team to retrieve the data for you.

Click on the timestamp of the test to view a summary of the test, including the following information:

- Date and timestamp
- Cartridge ID
- Dock ID, if the test was performed in G7 Dock
- Overall test results
- Hardware test results
- Sesnor test results

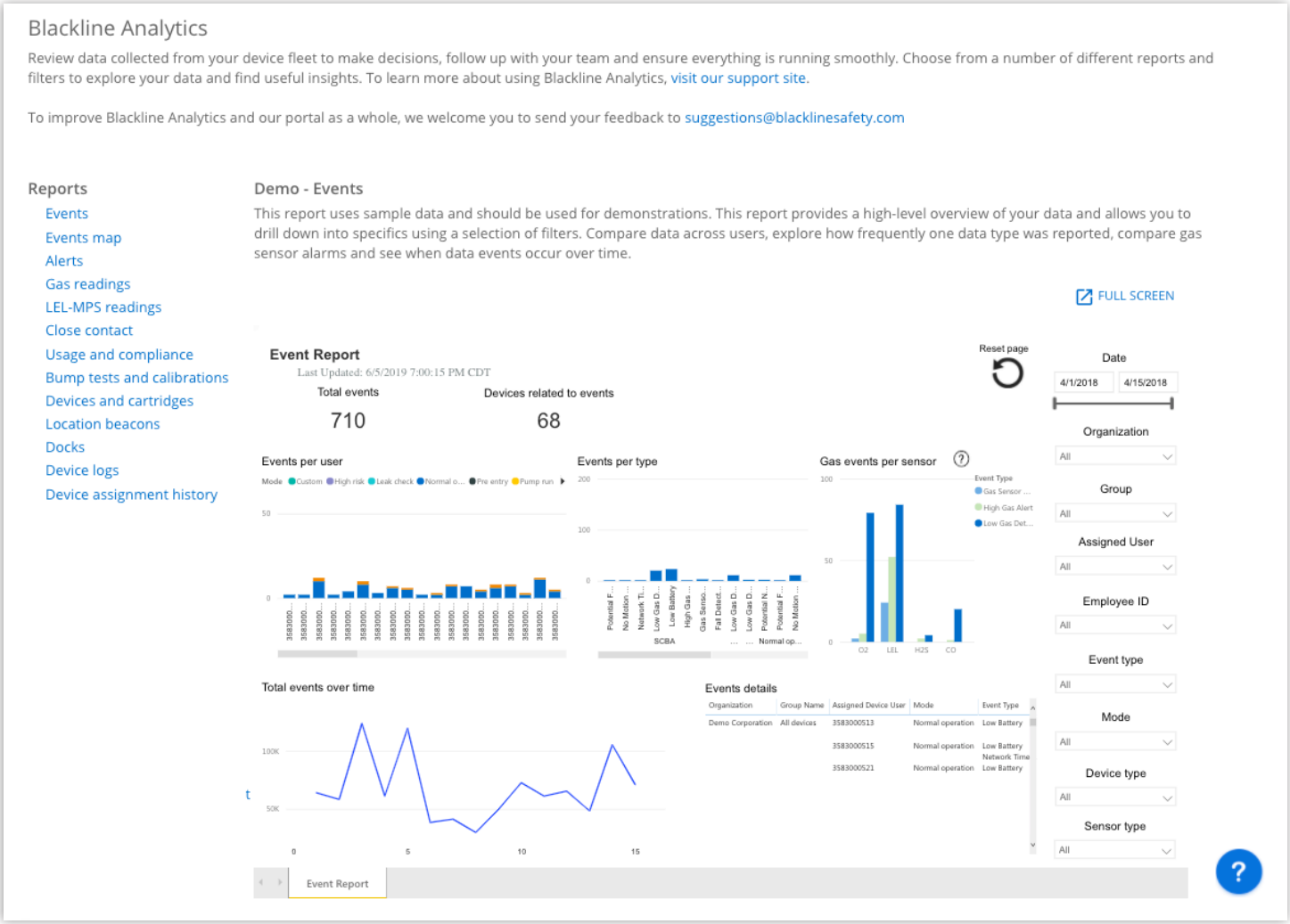
You can view the test results on any internet connected device. You can also download or print the certificate as a PDF for record-keeping purposes.



6. BLACKLINE ANALYTICS

Blackline Live includes a built in suite of analytics reports that help you better understand the data being collected from your device fleet. Blackline Analytics includes a list of reports focused on different applications of your Blackline safety devices, including event and alert counts and location, usage and compliance data, trends over time and much more.

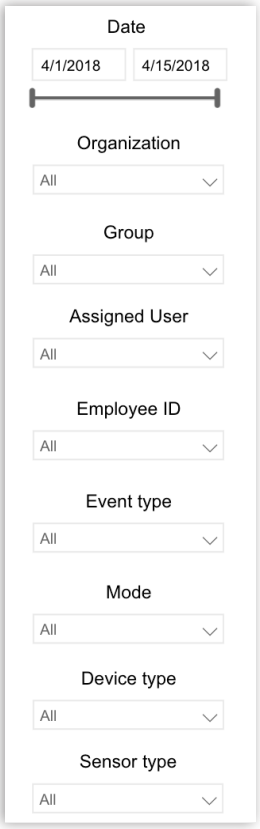
Each report that you have access to is listed along the left side of the page. Clicking one of these links will load up the corresponding report. A description of the report is available at the top of the section, with the report visible underneath. Click the full screen button to see the report in the entire browser window.



6.1 TOOLS WITHIN BLACKLINE ANALYTICS

Report filters

Each report includes a number of filters to narrow the focus of your reports. You can choose to filter by organization, group, user, device, event type, date and time, and many others. The filters appear on the far right of every report — simply open one of the dropdowns to view the available options and click on the options you want to see.

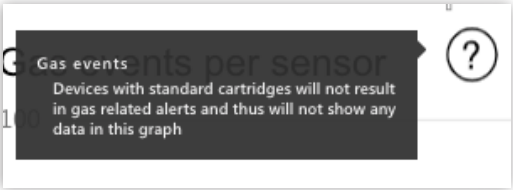


Additionally, you can focus and filter the report by clicking on a piece of data from any of the report graphs. For example, when viewing the events report, you can click on a specific user's data in the "events per user" graph, and the rest of the report will change to only show data associated with that user. You can hold down CTRL on window or Command on Mac to select multiple resources at once. Click the resources again to turn off the filter and return the report to normal.

If you would like to reset the filter and return them to the default mode, click the reset page button in the top right corner of each report.

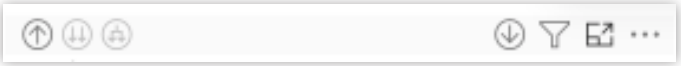
Tooltips

Hover over the question mark icon to see additional information and helpful tips about different features.



Drill up and drill down features

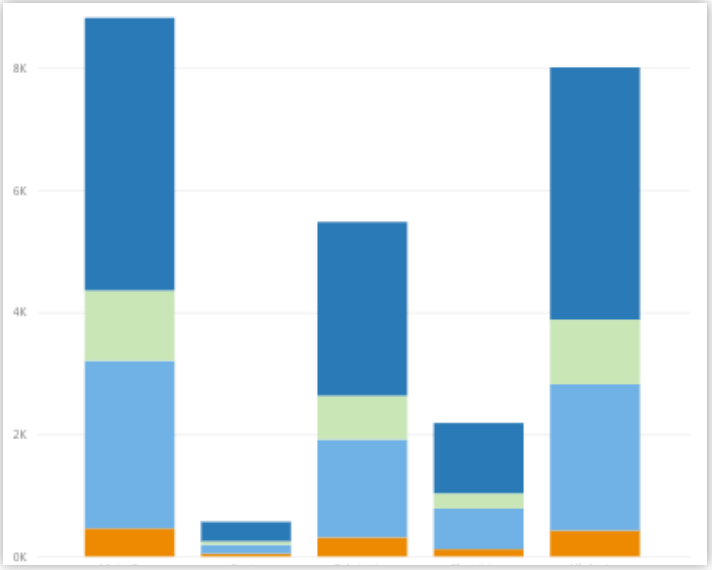
Many of the graphs feature drill up and drill down features, which allows you to see data at an organization-level, group-level or user-level. If you hover over one of the graphs in the report and see three arrow icons appear in the top-left, this indicates that the graph supports the drill up and down features.

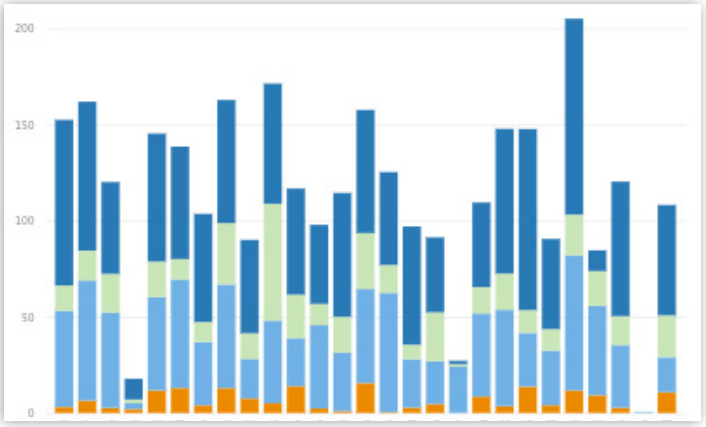


By default, these tables are drilled down to users, but pressing the icon pointing up will take your view to the group-level, and then organization-level. You can use this feature to easily compare groups of users or individuals.

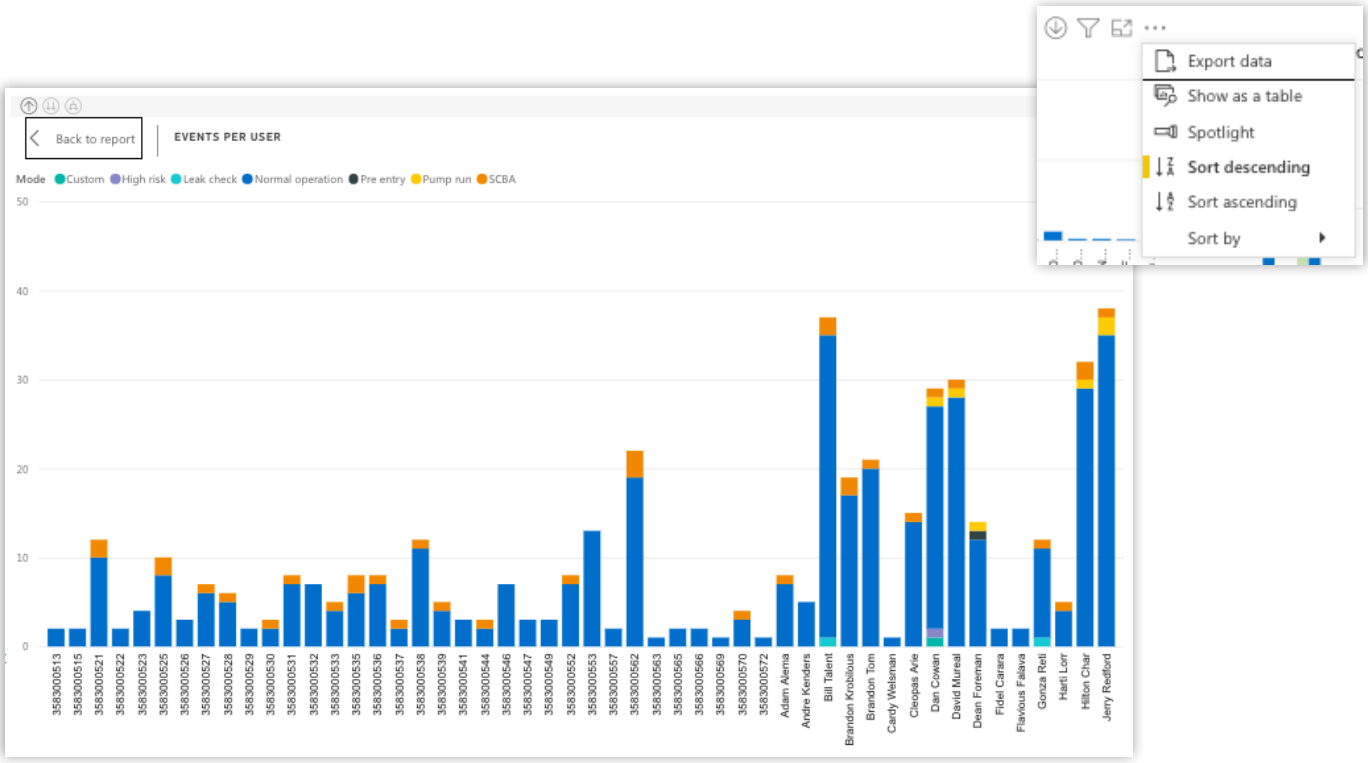
Focus mode and show data

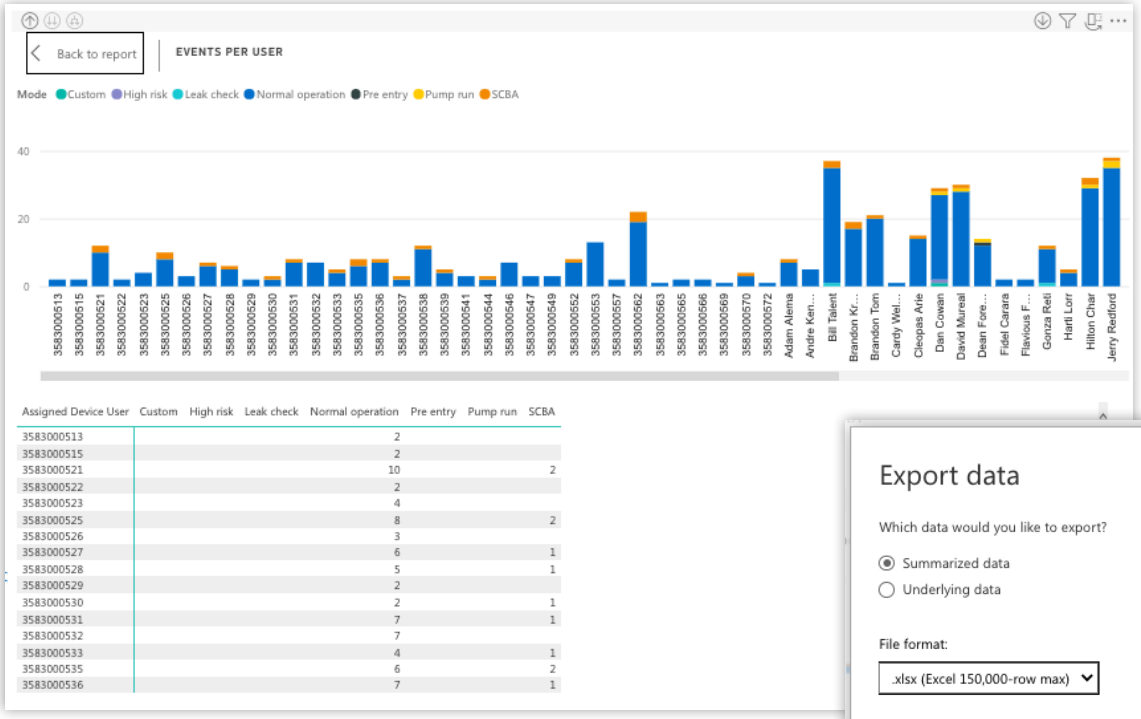
Each report graph can be viewed in "focus mode", which is an alternate screen view that shows a selected graph at a larger scale. To open focus mode, hover over a graph until you see icons appear in the top-right corner. Click the full-screen icon to the left of the three dots to open focus mode and see the graph in higher resolution and more detail.



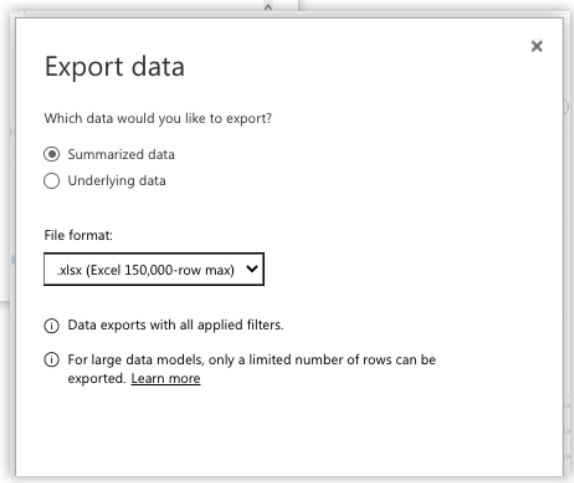


Similarly, you can view each graph alongside the tabular data it represents by clicking the three dot icon and selecting "Show as a table" from the dropdown menu. This opens a view similar to focus mode, but also displays the data that the graph is representing.





Assigned Device User	Custom	High risk	Leak check	Normal operation	Pre entry	Pump run	SCBA
3583000513				2			
3583000515				2			
3583000521				10			2
3583000522				2			
3583000523				4			
3583000525				8			2
3583000526				3			
3583000527				6			1
3583000528				5			1
3583000529				2			
3583000530				2			1
3583000531				7			1
3583000532				7			
3583000533				4			1
3583000535				6			2
3583000536				7			1



6.2 EXPORTING DATA FROM BLACKLINE ANALYTICS

Raw data can be exported from any of the individual visualizations in any of the Blackline Analytics reports. Hover over the visualization you would like to get data from until you see the different option icons appear at the top of the visual. Select the ellipses icon at the far right, and select export data from the dropdown list.

You can choose to export the data as an .xlsx file for Microsoft Excel, or as a .csv file.

NOTE: Any filters applied to the report when you choose to export will be reflected in the exported data. For example, if you were to filter down to one device and then export, you would only get data from that particular device. Once the data has finished exporting, it will be saved to your computer and can be repurposed for a different reporting format.

NOTE: When exporting data from large data tables, selecting every available organization and device may cause Blackline Analytics to time out due to the large number of rows being exported. It is recommended that you apply filters before exporting data to avoid the risk of timing out.

6.3 BLACKLINE VISION

If Blackline Analytics piques your interest in using data to learn more about your organization and your worker's behaviour, Blackline Vision offers even more personalized services in the way of data integration and visualization. Blackline Vision focuses on services that enhance time and cost efficiency, as well as precautionary safety measures.

To learn more about Blackline Vision or book a consultation, visit blacklinesafety.com/vision.

7. SUPPORT

7.1 LEARN MORE

Visit Support.BlacklineSafety.com to find more support and training materials for EXO.

7.2 CUSTOMER CARE

For technical support, please contact our Customer Care team.

North America (24 hours)
Toll Free: 1-877-869-7212 | support@blacklinesafety.com

United Kingdom (8am-5pm GMT)
+44 1787 222684 | eusupport@blacklinesafety.com

International (24 hours)
+1-403-451-0327 | support@blacklinesafety.com

8. GLOSSARY

Organzation

...

Groups

...

All devices group

Account

Account user

Contact

Contact group

Team member

Relationship

Provider

Client

Organization admin

Group admin

Device admin

Resolve only

View only

Analytics only

Contact admin

Emergency responder

Blackline Analytics

Resources

Alert

Safety Operations Center (SOC)

Info panel

Main menu

User menu

blacklinesafety

www.BlacklineSafety.com

0761/V1/2021-01-29