

blacklinesafety

Blackline Live

Technical User Manual

Contents

1	OVERVIEW	6
1.1	SUPPORTED DEVICES	6
1.2	SUPPORTED ACCESSORIES	6
2	NAVIGATING BLACKLINE LIVE	7
2.1	SIGNING IN TO BLACKLINE LIVE	9
3	BLACKLINE LIVE STRUCTURE	10
3.1	ORGANIZATIONS	10
3.2	TEAM MEMBERS	10
3.2.1	Team Member Status	11
3.3	GROUPS	12
3.3.1	The All Devices group	12
3.3.2	Group Membership	13
3.3.3	Group Roles and Permissions	13
3.3.4	Sharing Roles with Providers	17
3.4	RELATIONSHIPS	18
3.4.1	Contractual and Non-contractual Relationships	19
3.4.2	Relationship Status	19
4	MANAGING ORGANIZATIONS	20
4.1	REGISTERING AN ORGANIZATION	20
4.2	ACTIVATING AN ORGANIZATION	22
4.3	EDITING ORGANIZATION DETAILS	22
5	MANAGING TEAM MEMBERS	24
5.1	ADDING TEAM MEMBERS	25
5.2	EDITING TEAM MEMBER DETAILS	25
5.3	CHANGING TEAM MEMBER TYPES	27
5.3.1	Promoting a Contact to an Account user	27
5.3.2	Demoting an Account User to a Contact	28
5.4	DEACTIVATING TEAM MEMBERS	28
5.5	REACTIVATING TEAM MEMBERS	29

6	MANAGING GROUPS	30
6.1	ADDING A NEW GROUP	30
6.2	EDITING GROUP DETAILS.....	31
6.3	DELETING A GROUP	33
7	MANAGING DEVICES	34
7.1	VIEWING DEVICE INFORMATION	35
7.2	EDITING DEVICE DETAILS	35
7.3	ASSIGNING A DEVICE TO A TEAM MEMBER.....	37
7.3.1	Assigning a Device from the Device Page	38
7.3.2	Assigning a Device from the Device Details Page	38
7.3.3	Assigning a Device using the Quick Assign Page.....	39
7.4	UNASSIGNING A DEVICE FROM A TEAM MEMBER.....	40
7.4.1	Unassigning a Device using the Device page	40
7.4.2	Unassigning a Device using the Device Details Page	40
7.4.3	Unassigning a Device using the Quick Assign Page	40
7.5	UPDATING A DEVICE CONFIGURATION PROFILE	41
7.6	CHANGING THE ALERT PROFILE FOR A DEVICE	41
7.7	CHANGING THE NOTIFICATION PROFILE FOR A DEVICE	41
7.8	MOVING DEVICES BETWEEN ORGANIZATIONS.....	42
7.9	MARKING A DEVICE AS UNDER REPAIR.....	42
7.10	MARKING A DEVICE AS OPERATIONAL.....	43
7.11	LOGGING A DEVICE OUT OF BLACKLINE LIVE.....	43
7.12	SENDING AN ACTIVATION CODE FOR LONER MOBILE DEVICES	44
8	MANAGING CONTACT GROUPS	44
8.1	ADDING TEAM MEMBERS TO CONTACT GROUPS	45
9	MANAGING CONFIGURATION PROFILES	46
9.1	VIEWING CONFIGURATION PROFILES.....	46
9.2	CREATING A NEW CONFIGURATION PROFILE	46
9.3	EDITING CONFIGURATION PROFILE DETAILS.....	47
9.4	EDITING CONFIGURATION PROFILE MODE SETTINGS (G7 ONLY).....	52
10	MANAGING ALERT MANAGEMENT PROFILES.....	54

10.1	VIEWING ALERT MANAGEMENT PROFILES	55
10.2	CREATING A NEW ALERT MANAGEMENT PROFILE.....	55
10.3	EDITING ALERT MANAGEMENT PROFILE DETAILS	55
11	MANAGING NOTIFICATION PROFILES	58
11.1	VIEWING NOTIFICATION PROFILES.....	59
11.2	CREATING A NEW NOTIFICATION PROFILE.....	59
11.3	EDITING NOTIFICATION PROFILE DETAILS.....	59
12	MANAGING RELATIONSHIPS.....	61
12.1	VIEWING ACTIVE RELATIONSHIPS.....	61
12.2	VIEWING DEACTIVATED RELATIONSHIPS.....	62
12.3	CREATING A RELATIONSHIP	62
12.4	EDITING RELATIONSHIP DETAILS	63
12.5	DEACTIVATING A RELATIONSHIP AGREEMENT.....	64
13	MANAGING DOCK.....	64
13.1	VIEWING DOCKS	65
13.2	EDITING DOCK CONFIGURATION DETAILS.....	65
14	MANAGING LOCATION BEACONS	68
14.1	VIEWING LOCATION BEACONS.....	68
14.2	PLACING LOCATION BEACONS.....	69
15	MANAGING FLOORPLANS AND MAP OVERLAYS.....	70
15.1	FLOORPLANS	70
15.2	MAP OVERLAYS	70
15.3	VIEWING FLOORPLANS AND MAP OVERLAYS	71
16	MAPS	72
16.1	MAPS (LIVE VIEW).....	73
16.1.1	Locating Devices.....	74
16.1.2	Accessing the Device Info Panel.....	76
16.1.3	Messaging a G7 Device	78
16.1.4	Calling a G7 Device	78
16.1.5	Accessing a Device's Configuration Profile	79
16.1.6	Accessing a G7 Device's Alert Profile.....	79

16.1.7	Accessing a Device's history.....	79
16.1.8	Finding a G6 Device.....	80
16.1.9	Displaying Floorplans	81
16.1.10	Displaying Satellite Imagery	82
16.2	MAPS (HISTORICAL VIEW).....	83
16.2.1	Accessing Device Information in the Map History View.....	84
16.2.2	Navigating Device Events in the Map History View	84
17	FLEET HEALTH DASHBOARD.....	85
18	COMPLIANCE CERTIFICATES	87
18.1	VIEWING BUMP TEST AND CALIBRATION CERTIFICATES	87
19	G7 AND EXO DEVICE ALERTS	89
19.1	VIEWING DEVICE ALERTS.....	90
19.2	VIEWING ALERT DETAILS	91
19.3	ACKNOWLEDGING ACTIVE ALERTS	92
19.4	MANAGING ALERTS	93
19.5	VIEWING ALERTLINK MESSAGES.....	97
19.6	CLEARING ALERTLINK MESSAGES	98
19.7	VIEWING ALERT HISTORY	99
20	G6 DEVICE NOTIFICATIONS.....	99
21	MASS NOTIFICATIONS	102
21.1	SENDING MASS NOTIFICATIONS	102
22	BLACKLINE ANALYTICS	103
23	SUPPORT	106
23.1	LEARN MORE.....	106
23.2	TECHNICAL SUPPORT	106

1 OVERVIEW

Blackline Live is cloud-hosted software that allows you to easily configure and monitor your device fleet. Blackline Live allows you to:

- View and manage your organization's resources in the domain (U.S., EUR, or UAE) of your choice.
- Configure which features a device will use in the field.
- Configure how monitoring personnel should respond when they receive an alert.
- Access your device data.



1.1 SUPPORTED DEVICES

Blackline Live supports Blackline's safety monitoring devices, including:

- G7c
- G7x and G7 Bridge
- G7 EXO
- G6
- Loner Mobile
- EXO 8

Blackline Live also provides support for Blackline's legacy devices and allows you to monitor and configure them over the air. New features may not be backwards compatible to legacy devices (e.g., text messaging features using the LCD screen and gas-detection features are not available on legacy devices).

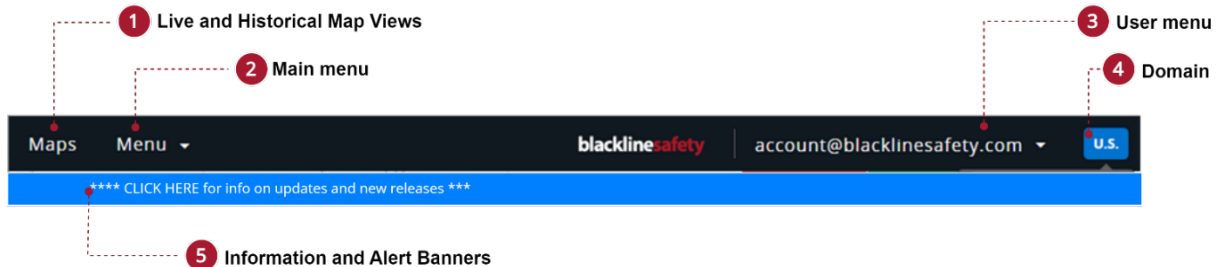
1.2 SUPPORTED ACCESSORIES

Blackline Live allows you to configure and manage Blackline accessories, including:

- Location beacons
- G7 Dock
- G6 Dock
- Loner DUO

2 NAVIGATING BLACKLINE LIVE

Use the navigation bar to access Blackline Live functionality for your organization. The navigation bar is composed of the following components:



Maps (Live view and Historical views)


- 1 The Maps pages display the current and historical location and status of online devices in your fleet. For more information about using the Maps page, see section 16.
NOTE: Access to the Maps pages depends on your Blackline Live permissions. For more information on Blackline Live group membership, roles, and permissions, see sections 3.2 and 3.3.

Main menu

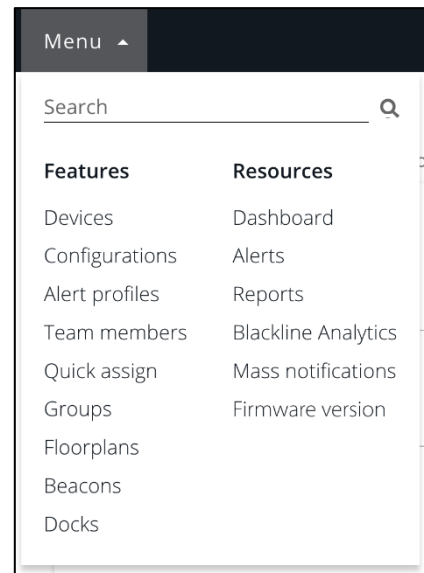
The Main menu provides access to Blackline Live's administrative features and resources.

NOTE: Access to features and resources depends on your permissions. For more information on Blackline Live group membership, roles, and permissions, see section 3.3.3.

Universal search

- 2 You can access the universal search bar from the top of the Main menu. Type in your search query, then select . Open items related to your search results by selecting the item from the search results.

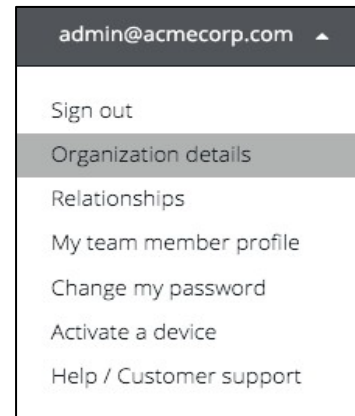
NOTE: Each feature (Devices, Team members, Configurations, etc.) includes its own search and sort filters.



3

User menu

Provides access to information about your organization or account.



Domain

A badge in the navigation bar indicates which domain you are using to access Blackline Live.

4

If you use the European Blackline Live domain (<https://eu.live.blacklinesafety.com/>) and Cloud services, your data is processed and stored entirely within Europe.

If you use the U.S. Blackline Live domain (<https://live.blacklinesafety.com/>) and Cloud services, your data is processed and stored entirely within the United States.

If you use the UAE Blackline Live domain (<https://uae.live.blacklinesafety.com/>) and Cloud services, your data is processed and stored entirely within the United Arab Emirates.

Banners

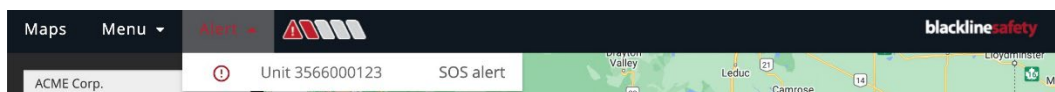
The navigation bar can display three kinds of banners to inform you of something that affects you or your organization.

5

Alert banner

Alert banners display when there is one or more active alerts on G7 or EXO devices in your organization.

Select the alert dropdown to display a list of every alert that must be addressed. For more information about managing alerts, see section 10.



Audio warning banner

If there is an issue blocking you from hearing audio from Blackline Live, a yellow banner immediately displays below the navigation bar.

You are notified of audio issues because a lack of audio from Blackline Live can result in missed alerts. Select the banner message to open troubleshooting information related to the warning.

Information banner

A blue banner (U.S. domain), gray banner (EUR domain), or green banner (UAE domain) immediately displays below the navigation bar to inform you of important information from Blackline Safety.

NOTE: The information banner only displays if they are major release notices or critical notifications.



2.1 SIGNING IN TO BLACKLINE LIVE

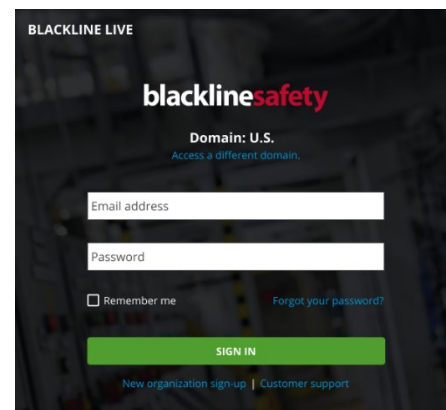
You must be an active Account user within an active organization to sign into Blackline Live. For more information on registering and activating your organization, see section 4.

To sign into Blackline Live:

1. Navigate to live.blacklinesafety.com (U.S. domain), eu.live.blacklinesafety.com (European domain), or uae.live.blacklinesafety.com (UAE domain), depending on which domain your organization is registered in.

For more information on Blackline Live domains, see section 2.

2. Enter the **Email Address** and **Password** for the organization you want to sign in to.
3. Select **SIGN IN**.

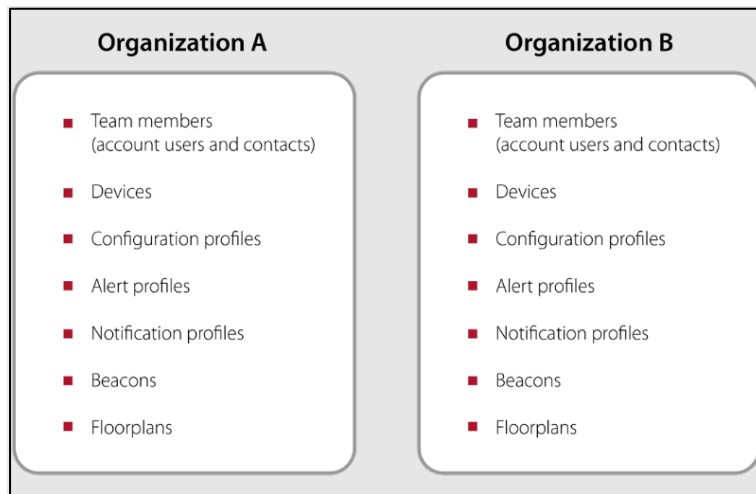


NOTE: Once you are signed in to Blackline live, select **Change my Password** from the User menu to change your password.

3 BLACKLINE LIVE STRUCTURE

3.1 ORGANIZATIONS

Blackline Live organizations contain information about your device fleets, accessories, team members, contact details, and device configurations and data. Organizations are composed of team members. A team member's access to an organization's resources is based on their roles and responsibilities.



By default, individual organizations exist separately, but can be connected through relationships, allowing you to share reports and resources with users in other organizations. For more information on relationships, see section 3.4.

For more information on administering organizations, see section 4.

3.2 TEAM MEMBERS

Team members represent people who are part of your organization, or who act as emergency contacts for your organization. There are two kinds of team members:



Contacts can be assigned to devices or to alert profiles as emergency contacts. They do not have sign-in access to Blackline Live.



Account users can be assigned to devices or alert profiles and have sign-in access to Blackline Live.

Account users can use their log-in access for tasks like fleet management, contact administration, or live-alert monitoring. Their ability to perform tasks in Blackline Live depends on their assigned roles.

3.2.1 TEAM MEMBER STATUS

A team member's status indicates whether they have activated their account and have access to Blackline Live.

Pending

A pending status means an email invitation from Blackline Live was sent has not yet been accepted.

Active

An active status indicates that the account is activate and the user is logged in. Contacts have an **active** status by default.

Deactivated

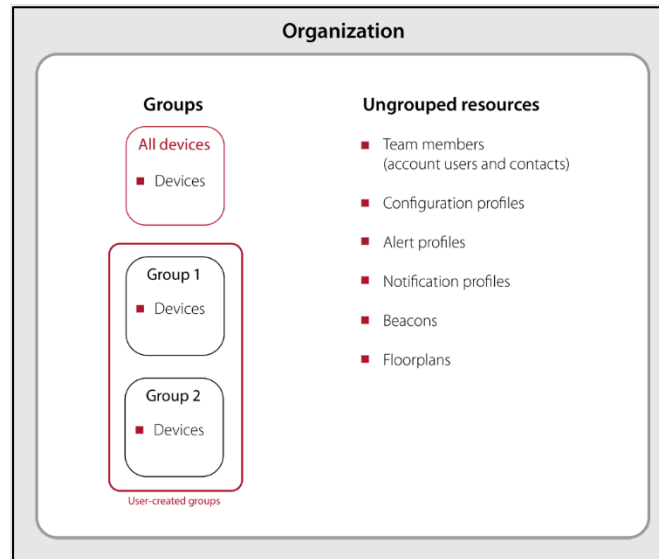
A deactivated status means that a team member is no longer active in an organization.

A team member that is deactivated can no longer be assigned to devices, alert profiles, or notification profiles, and is no longer part of any groups. Any devices that they were assigned to them become unassigned. Additionally, deactivated Account users lose log-in access to Blackline Live. Deactivated team members can be reactivated and manually re-assigned to their devices and alert profiles.

For more information about setting up team members (Account users and Contacts), see section 5.

3.3 GROUPS

Groups are collections of devices in your organization that are managed by specified Account users. Groups are arranged based on logical criteria. Most often, they are used to organize devices by work sites, projects, or teams.



You can use groups as filters in Blackline Analytics reports to see trends within different parts of the organization. For example, you can filter groups to see whether one group is experiencing an exceptional number of alerts or is consistently out of gas compliance.

Groups are also used to determine access capability within an organization. For example, if the manager of Group one only sees device data for their team, giving them access to that group filters and streamlines their experience in Blackline Live. They cannot see or manage Group two, even though those devices are also part of the larger organization.

NOTE: Only devices can be 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.

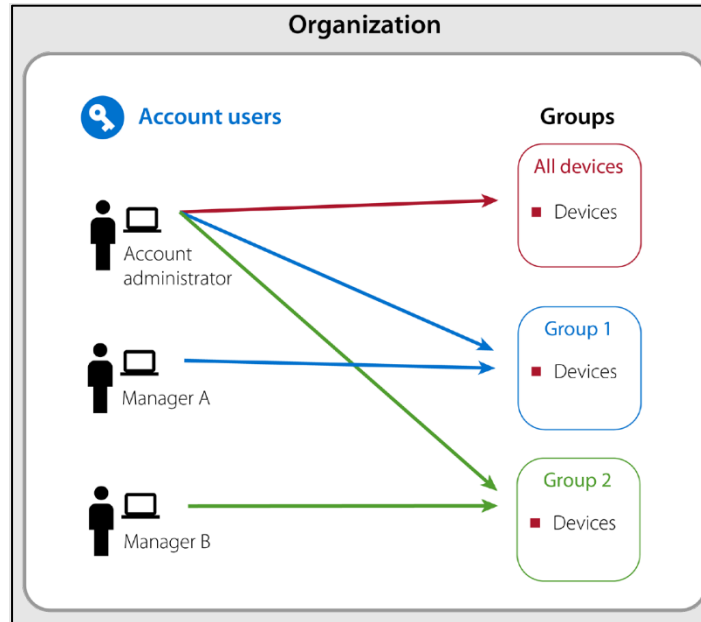
3.3.1 THE ALL DEVICES GROUP

The All devices group is the default group in every organization that automatically contains all devices. It collects devices as they are activated or moved into the organization. It cannot be deleted, and devices cannot be removed from it unless they are moved to a different organization altogether.

The All devices group plays a large part in relationships and sharing it with another organization allows them to see the resources in your organization. For more information, see section 3.4.

3.3.2 GROUP MEMBERSHIP

To interact with Blackline Live, Account users must belong to at least one group in their organization. In the following example, an organization has three Account users, each has access to different groups.



3.3.3 GROUP ROLES AND PERMISSIONS

Roles define the permissions that are assigned to Account users and determine what they can see and do. Roles are granted on a group-by-group basis.

A single Account user can have a different role in each group they have access to. An Account user's role in the All devices group acts as their most basic role throughout the entire organization. For example, if an Account user has a resolve-only role in the All devices group, they can see the organization's devices and resolve alerts on every device. They can also be given higher-access roles in other groups, where they might be able to manage or edit specific devices.

The available Blackline Live roles are:

Organization admin	<p>This role includes the highest level of permissions and should be appointed to users that are responsible for the organization's device fleet.</p> <p>Users with this role can see and edit all resources in their Blackline organization. They can edit organization-wide information and settings and can create and manage relationships with other organizations. Users with this role can also view analytics for all devices in their organization.</p> <p>This role can only be applied to the All devices group, since it represents the entire organization.</p>
Organization assistant	<p>This role supports the Organization admin role.</p> <p>A user with this role can manage devices, team members, profiles, groups, and organization details, but cannot request or manage relationships with other organizations. They can also view analytics for devices in the groups they have access to.</p> <p>This role does not have access to maps unless resolving an alert.</p>
Group admin	<p>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.</p> <p>Users with this role can edit the groups they have this role in, as well as any devices within it. They can also view analytics for the groups they have access to.</p> <p>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 Blackline Live access, or changing what groups or roles they have access to.</p>
Fleet admin	<p>This role is meant to give permissions for management of the devices only within the user's fleet.</p> <p>A user with this role can assign devices, manage mass notifications, and resolve alerts. In the groups they have this role in, users can also view analytics for devices.</p> <p>This role does not have access to maps unless resolving an alert.</p>
Device admin	<p>This role should be given to users who manage device fleets within the groups they have access to.</p> <p>Account users with this role can rename devices or assign them to team members and are able to monitor and respond to online devices. They can also view analytics for devices in the groups they have access to.</p>

Contact admin*

This role is meant for users that assign devices to workers. Users with this role can access the devices, team members, and quick assign pages to make device assignments. The Contact admin role is like 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 cannot resolve alerts on devices.

**Contact admin
(No repair)**

This role is meant for users that assign devices to workers. Users assigned to this role have the same permissions as the Contact admin role but cannot mark devices as under repair.

Resolve only

This role is meant for monitoring agents. Users can see information in the organization but can only investigate and resolve alerts.

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 response
admin**

This role is meant for a monitoring administrator. Users can respond to alerts but in a more limited way than the Resolve only role.

A user with this role can only access alert management pages and the Mass notifications page.

This role does not have access to maps unless resolving an alert.

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 the resources in the organization, such as team members, devices, configurations, alert profiles, and analytics. Any information that is required for alert investigation and resolution is made available to the user through the Alert management page or the Maps page.

Compliance

This role is meant to monitor the compliance of their device fleet. A user with this role only has access to the Compliance dashboard page and the Mass notifications page.

View only

The View only role allows an Account user to see the resources within an organization, but they cannot edit or manage any of them. They can also view alerts but cannot acknowledge or resolve them.

Analytics only*

Users with the Analytics only role can only view the Blackline Analytics page and the reports listed there. They cannot 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 creating a relationship to share group access with another organization.

NOTE: Team members are not considered to be grouped resources. An Account user requires either a Contact admin, Device admin, Group admin, or Organization admin role in the All devices group to add and edit team members.

Refer to the following table to see the permissions included with each role.

Role	Page access	Resolve alerts	Mass notifications	Create and manage contacts*	Reassign devices*	Create and assign profiles	Create and manage groups	Create and manage account users*	Create relationships	Edit organization details	Access Blackline Analytics
Organization admin	View all	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Organization assistant	Limited view <ul style="list-style-type: none"> No maps No quick assign No beacons/floorplans No relationships 	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Group admin	View all	Y	Y	Y	Y	Y	Y	Y	N	N	Y
Device admin	View all	Y	N	Y	Y	Y	N	N	N	N	Y
Fleet admin	Limited view <ul style="list-style-type: none"> Devices Team members Alerts management Alert history Docks Dashboard Blackline Analytics 	Y	N	N	Y	N	N	N	N	N	Y
Contact admin	Limited view <ul style="list-style-type: none"> Devices Team members Quick assign 	N	N	Y	Y	N	N	N	N	N	N
Contact admin (No repair)	Limited view <ul style="list-style-type: none"> Devices Team members Quick assign <p>Cannot use the "Mark as under repair" feature</p>	N	N	Y	Y	N	N	N	N	N	N
Resolve only	View all	Y	N	N	N	N	N	N	N	N	Y
Emergency response admin	Limited view <ul style="list-style-type: none"> Alerts management Alert history Mass notifications 	Y	Y								N
Emergency responder	Limited view <ul style="list-style-type: none"> Maps (Live view & History view) Alerts management Alert history 	Y	N	N	N	N	N	N	N	N	N
Quick Assign only	Limited view <ul style="list-style-type: none"> Quick assign 	N	N	Y	Y	N	N	N	N	N	N
Compliance	Limited view <ul style="list-style-type: none"> Dashboard Mass notifications 	N	Y	N	N	N	N	N	N	N	N
View only	View all	N	N	N	N	N	N	N	N	N	Y
Analytics only	Limited view <ul style="list-style-type: none"> Blackline Analytics 	N	N	N	N	N	N	N	N	N	Y

* To create and edit team members or assign devices to team members, an account user needs access to the All devices group.

3.3.4 SHARING ROLES WITH PROVIDERS

Provider organizations can monitor your devices or manage your fleet on your behalf. For example, if you would like Blackline Safety or a third-party company to respond to alerts on your devices, they would be considered as a provider organization.

The following roles can be shared to a provider organization:

- Group admin
- Device admin
- Resolve only
- View only

These roles noted have access to the Maps page and to team members (if access is provided to the All devices group).

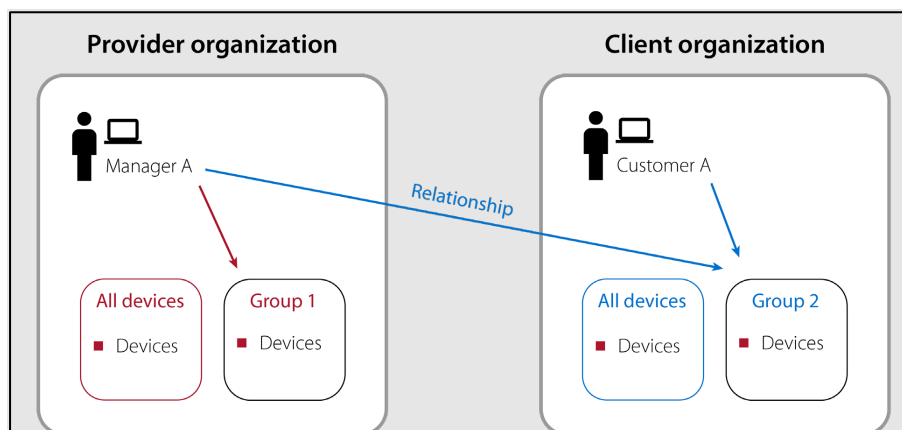
3.4 RELATIONSHIPS

Relationships allow resources to be shared between two separate organizations for reasons that include monitoring, distribution setup, or rentals.

A relationship is a one-way connection between the two organizations, where one organization has access to the other organization's groups. Relationships are based on the sharing of groups and always involve two parties: the client and the provider. Only clients can initiate a relationship and are responsible for defining the provider's access. For example, monitoring service providers in a relationship with your organization can observe the safety statuses of your devices and resolve alerts as they occur. Another example would be resellers using relationships to help set up accounts and walk customers through the onboarding process.

As soon as a relationship is activated, the provider organization administrator can choose to share access to their own Account users as needed but can only assign the roles that the client has defined.

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



For more information, see section 12.

3.4.1 CONTRACTUAL AND NON-CONTRACTUAL RELATIONSHIPS

Relationships can be considered contractual or non-contractual.

Contractual

A relationship that locks devices into the organization as soon as the relationship is activated — devices 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 has access to the devices in the client organization.

Additionally, contractual relationships cannot be deactivated by either party and must be deactivated by a Blackline Safety representative. These relationships are more secure and recommended for safety monitoring or distribution setup.

Non-contractual

A relationship that is considered less secure than contractual ones but allows for more flexibility and customization. The client can choose to share any of their groups with the provider — not just the All devices group.

Providers can move devices in and out of client organizations if 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.

3.4.2 RELATIONSHIP STATUS

The relationship status indicates whether a relationship agreement is in effect.

Pending

The client has invited the provider to a relationship agreement, but the provider has not yet agreed or has declined the invitation.

Active

The provider has accepted the client's invitation and the agreement is in effect.

Deactivated

The relationship has been deactivated and is no longer in effect.

4 MANAGING ORGANIZATIONS

To start using Blackline Live you must register and then activate your organization.

4.1 REGISTERING AN ORGANIZATION

Registering your organization is only required when you are first getting started with Blackline Live. If your company already uses Blackline devices, your organization is already registered in Blackline Live. In this case, you need to contact the Organizational administrator for your organization to get invited to Blackline Live.

To register your organization:

1. Navigate to live.blacklinesafety.com (U.S. domain), eu.live.blacklinesafety.com (European domain), or uae.live.blacklinesafety.com (UAE domain), depending on whether you want your organization hosted in the U.S., in Europe, or in the UAE. The Blackline Live Sign-in page opens.

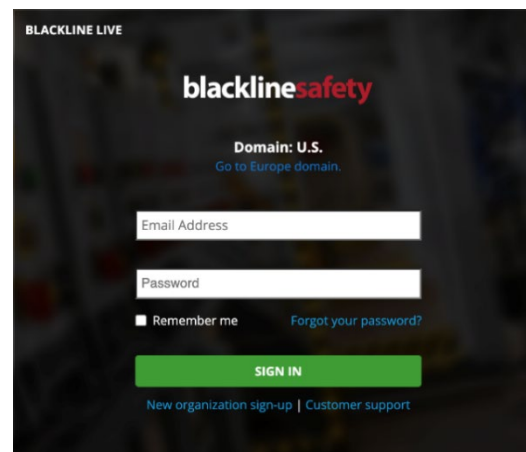
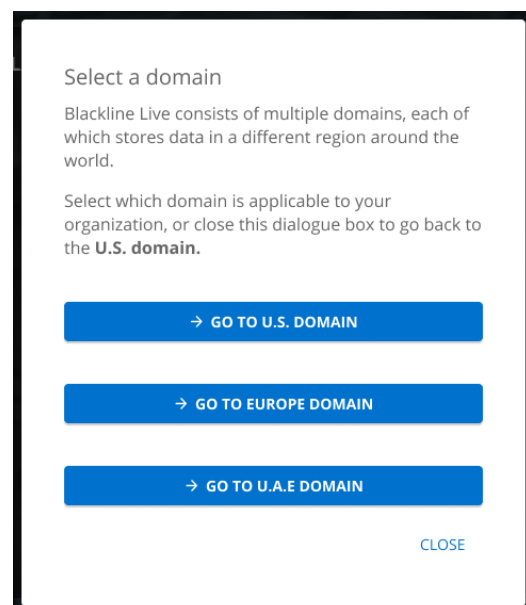
For more information on Blackline Live domains, see section 2.

2. Verify that you have selected the correct domain. To navigate to a different domain, select **Log into a different domain**. The Select a domain modal opens.

NOTE: When your organization is registered, you cannot change the domain.

3. Select the correct domain.
4. Select **New organization sign-up**.

The Blackline Live New Organization Sign In page opens.

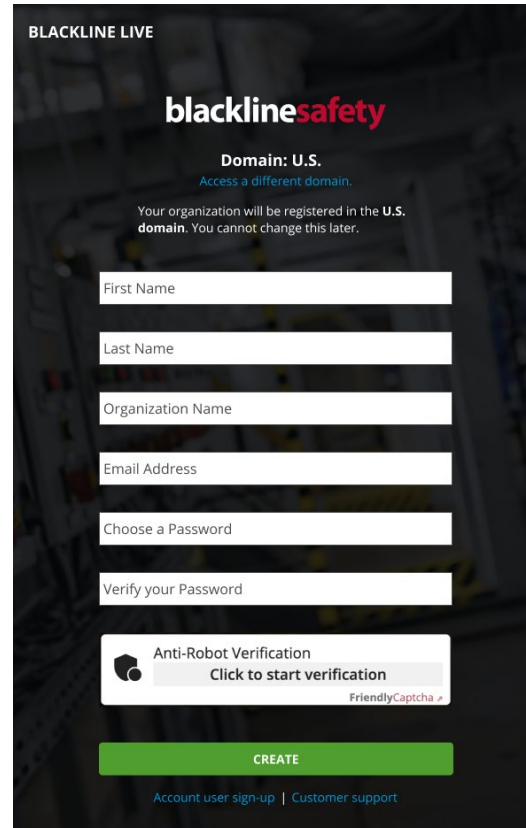
The image shows the Blackline Live sign-in page. At the top, it says "BLACKLINE LIVE" and "blacklinesafety". Below that, it indicates the current domain is "U.S." with a link to "Go to Europe domain". There are input fields for "Email Address" and "Password". Below these are checkboxes for "Remember me" and a link for "Forgot your password?". A green "SIGN IN" button is present. At the bottom, there are links for "New organization sign-up" and "Customer support".The image shows a "Select a domain" modal. It explains that Blackline Live has multiple domains for different regions. It asks the user to select the applicable domain for their organization or to close the dialog to return to the U.S. domain. There are three blue buttons: "→ GO TO U.S. DOMAIN", "→ GO TO EUROPE DOMAIN", and "→ GO TO U.A.E DOMAIN". A "CLOSE" link is at the bottom right.

5. In the fields provided, enter your name, your organization's name, administrative email, and password.

NOTE: Enter a valid email address, as you need to activate your organization through email.

Your Password should be at least eight characters long, include capital and lowercase letters, a number, and a special character.

6. Complete the security Captcha requirements by selecting **I am human**.
7. Select **CREATE**.



The screenshot shows the 'BLACKLINE LIVE' registration page. At the top, the 'blacklinesafety' logo is displayed. Below it, the text 'Domain: U.S.' is shown with a link 'Access a different domain.' A note states: 'Your organization will be registered in the U.S. domain. You cannot change this later.' The form contains several input fields: 'First Name', 'Last Name', 'Organization Name', 'Email Address', 'Choose a Password', and 'Verify your Password'. Below these fields is an 'Anti-Robot Verification' section with a 'Click to start verification' button and a 'FriendlyCaptcha' logo. At the bottom of the form is a large green 'CREATE' button. At the very bottom of the page, there are links for 'Account user sign-up' and 'Customer support'.

TROUBLESHOOTING TIP: If you get an error that you cannot use the organization name you have entered, your organization may already be registered in Blackline Live. Contact the Blackline Live account holder in your company or Blackline Safety's [Technical Support](#) team to get invited to the existing organization.

4.2 ACTIVATING AN ORGANIZATION

You must activate your organization's account before your organization can begin using Blackline Live.

To activate your organization:

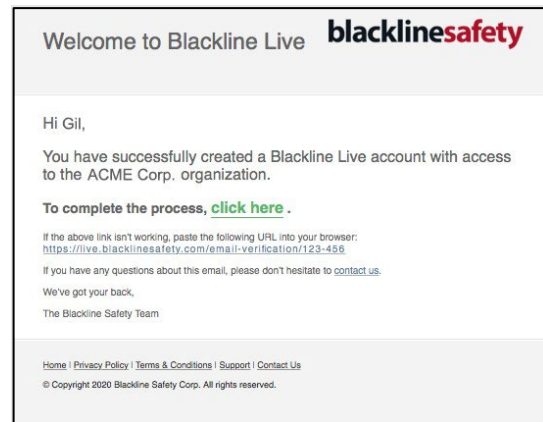
1. Sign in to the email account that you used to register your organization, then look for an email from Blackline Live.

Remember to check your spam or junk folder if you do not see it in your main inbox.

2. Open the email, then select **click here**.

You are redirected to Blackline Live. A pop-up at the top of the screen informs you that your email was verified.

3. Once verified, you can use your email address and password to sign in.



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

4.3 EDITING ORGANIZATION DETAILS

The Organization details page defines settings for your entire organization. The Organization details page is composed of two sections, organization description and default team member settings.

NOTE: To open any section for updating, select **EDIT**. To save your updates and stop editing, select **SAVE**. To cancel your updates without saving your changes at any time, select **CANCEL**.

NOTE: Only users assigned to the correct administrative role (Organization admin) can edit organization details.

To edit organization details:

1. In the User menu, select **Organization details**.
2. Edit any of the following information:

Organization details — Define organization details including organization name, description, and what map units to use when devices go into an alert state.

NOTE: Select the map units that are relevant to your region, choosing legal subdivision (LSD) or national topographic survey (NTS), if appropriate. If you select neither, the devices use latitude and longitude coordinates.

A screenshot of a web form titled "Organization details". The form has a light gray background and a thin black border. At the top, there is a label "Organization name" followed by a text input field containing "ACME Corp.". Below this is a horizontal dashed line. Under the line is a large text area labeled "Description". At the bottom of the form, there are two checkboxes: "Display LSD map information" and "Display NTS map information", both of which are currently unchecked.

Default Team Member Settings — Define the default team member settings for new team members added to your organization. Configurable fields are:

Timezone	Define what timezone to display on the device when information is received from Blackline Live.
Display units	Define the units of measure the device displays when they receive information from Blackline Live (kilometers or miles).
Voice calling region	Define the general geographic region to select for voice calling purposes (e.g., North America, United Kingdom).
Custom profile field	Define additional custom fields to add to the Team member profile page and select whether the information should be shown on pages throughout Blackline Live (e.g., on the Alert management page).

Default team member settings

Define the settings of new team members created in this organization. These settings influence the team member's portal interface and other communications from Blackline Live.

Timezone
Define what time zone the user will see when they receive information from Blackline Live

(-0600) MDT - Edmonton

Display units
Define the unit of measurement the user will see when they receive information from Blackline Live

Kilometers

Region selection for voice calling feature

North America

Custom team member profile fields

Add additional custom fields to each team member's profile page and determine whether this information should be shown on other pages throughout the portal, such as the alert management page.

Field label	Character cap	
Shift	50	<input checked="" type="checkbox"/> Show throughout portal

5 / 50

5 MANAGING TEAM MEMBERS

The Team members page lists the team members registered in an organization. Team members represent the employees, supervisors, managers, and emergency response contacts in the organization.

You can search and sort the team members list. The icon next to each name indicates whether team members are Contacts or Account users. For more information, see section 3.2.

Team members

ACTIVATED

DEACTIVATED

Organization

ACME Corp.

Search team members

Items per page: 20

Page: 1 / 30

ADD TEAM MEMBER

Display

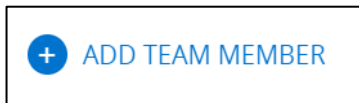
FIRST NAME	LAST NAME	EMPLOYEE ID	EMAIL	ORGANIZATION	PERMISSIONS	STATUS
<div><div></div><div>Arturo</div></div>	Chmela	1324	achmela@acmecorp.c...	ACME Corp.	contact	active
<div><div></div><div>Annika</div></div>	Aranasov	3164	aaranasov@acmecorp...	ACME Corp.	contact	active

5.1 ADDING TEAM MEMBERS

NOTE: Only Account users assigned to the correct administrative role can add team members. If you have a device admin role in the All devices group, you can only create Contacts. If you have a group admin or org admin role, you can create both Contacts and Account users.

To add a team member:

1. From the Main menu, select **Team members**.
2. Select **ADD TEAM MEMBER**.



3. Select the type of team member (**Contact** or **Account user**) you want to add.
For more information on team member types, see section 3.2.
4. Select **NEXT**.
The Team member details page opens, displaying the Team member's contact profile, Account settings, and assigned groups.
5. Enter the team member details. For more information, see section 5.2.
6. Select **ADD TEAM MEMBER**.

5.2 EDITING TEAM MEMBER DETAILS

The Team member details page lists important contact information. It also shows the account settings and assigned groups for Account users. The Team member page is composed of three sections Team member profile, account settings, and group settings.

NOTE: To update a section, select **EDIT**. To save your updates and stop editing, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

NOTE: Account users can view or modify their own information by selecting **My Team Member Profile** from the User menu.

To edit team member details:

1. From the Main menu, select **Team members**.
2. To open the Team member details page for a team member, select their **FIRST NAME**, **LAST NAME**, or **EMPLOYEE ID** from the team member list.

3. Edit any of the following:

Team member profile — Define contact information for an individual. Add as much information as possible. The data entered here displays if this team member's device goes into alert and is provided to monitoring personnel if this team member is listed as an emergency contact.

NOTE: Confirm that phone numbers are entered using a valid 10- or 14-digit phone number format.

First Name Malena	Trade/Role
Last Name Haward	Company
Employee ID 8364	Mobile Phone Number 333-123-4567 TEST
Email Address mhaward@acmecorp.com	Home Phone Number 333-098-7654
	Work Phone Number

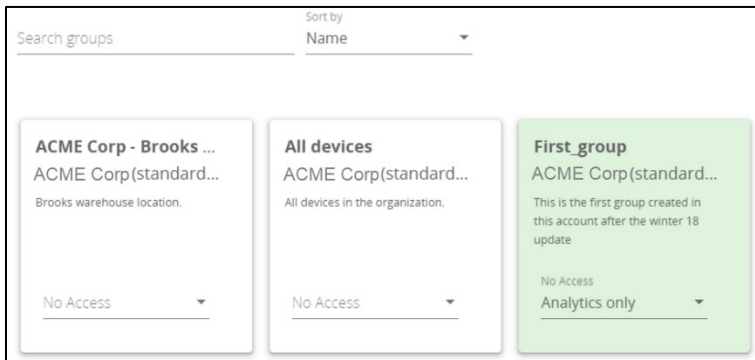
Account settings (Account users only) — Define the team member's Blackline Live settings, including language and alarm volume where:

- **Language** — Defines what language is used to display Blackline Live content. Blackline Live supports content translation into 33 languages.
- **Alarm volume** — Defines the volume in Blackline Live when a device goes into alert.

Language English
Alarm volume Adjust the volume of the portal's alert banner when a device has gone into alert.

Groups (Account users only) — If you are configuring an Account user, assign team members to a role in one or more groups in Blackline Live. For more information on available roles, see section 3.3.3.

NOTE: The groups the team member is assigned to are automatically highlighted.



5.3 CHANGING TEAM MEMBER TYPES

Team members can be promoted from contacts to Account users and demoted from Account users to Contacts. Assigning a type allows administrators to grant and revoke access to Blackline Live as needed, without needing to remove and re-add a team member within an organization.

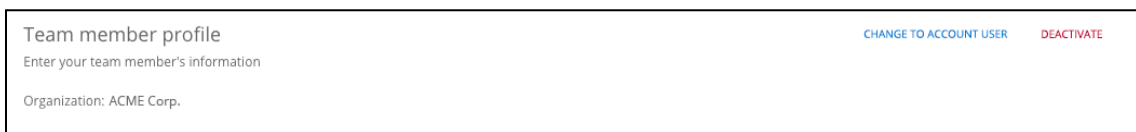
NOTE: Only Account users assigned to the correct administrative role can update the team member type.

5.3.1 PROMOTING A CONTACT TO AN ACCOUNT USER

Account users are team members with assigned roles in Blackline Live that help them complete tasks in Blackline Live related to fleet management, contact administration, and live-alert monitoring.

To promote a Contact to an Account user:

1. On the Team member details page, select **CHANGE TO ACCOUNT USER**.



2. In the confirmation dialog box that opens, select **MAKE ACCOUNT USER**.
3. Update the team member details. For more information, see section 5.2.
4. When changing a Contact to an Account user, you must enter a valid email address in the new Account user's profile, if there is not one already available.

NOTE: As soon as a team member is changed to an Account user, their status is pending until they accept the invitation sent in their email address.

5.3.2 DEMOTING AN ACCOUNT USER TO A CONTACT

Contacts are team members that can be assigned to devices, or to alert profiles as emergency Contacts, but do not have sign-in access to Blackline Live.

As soon as an Account user is demoted to a Contact, the team member's session ends, they can no longer sign in to Blackline Live and are no longer listed in groups.

NOTE: If the team member was assigned to device alert profiles or notification profiles as an Account user, these assignments remain intact after they are changed to a Contact.

To demote an Account user to a Contact:

1. In the Team member details page, select **CHANGE TO CONTACT**.



The screenshot shows a 'Team member profile' form. At the top, it says 'Enter your team member's information'. Below that, it says 'Organization: ACME Corp.'. In the top right corner, there are two buttons: 'CHANGE TO CONTACT' (in blue) and 'DEACTIVATE' (in red).

2. A confirmation dialog box opens. Select **MAKE CONTACT**.
3. Update the team member details. For more information, see section 5.2.


5.4 DEACTIVATING TEAM MEMBERS

If a team member is no longer part of an organization, they should be deactivated in Blackline Live. Deactivated team members are not deleted but have an **inactive** status in Blackline Live.

Deactivated team members cannot be assigned to devices, alert profiles, or notification profiles, and are removed from groups and unassigned from their devices. Deactivated Account users cannot sign in to Blackline Live. Deactivated team members can be reactivated and manually reassigned to their devices and alert profiles.

To deactivate a team member:

1. On the Team members page, open the team member profile to be deactivated, then select **DEACTIVATE**.



The screenshot shows the same 'Team member profile' form as before. In the top right corner, the 'CHANGE TO CONTACT' button is now disabled (greyed out), and the 'DEACTIVATE' button is highlighted in red.

2. A confirmation dialog box opens. Select **DEACTIVATE**.

The team member's profile is automatically made inactive in Blackline Live.

To view deactivated team members:

1. On the Team members page, select the **DEACTIVATED** tab. The deactivated Team member page opens.

ACTIVATED		DEACTIVATED				
Organization ACME Corp.						
Search team members						Items per page: 20 Page: 1 / 4
FIRST NAME	LAST NAME	EMPLOYEE ID	EMAIL	ORGANIZATION	PERMISSIONS	STATUS
Jake	Lehmann	9284	jlehmann@acmecor...	ACME Corp.	contact	inactive
Jozefina	Valdez	6295	jvaldez@acmecorp.c...	ACME Corp.	contact	inactive
Malachi	Darrell	3814	mdarrell@acmecorp...	ACME Corp.	contact	inactive

2. Deactivated team member profiles display the information and profile assignments associated with the profile at the time of their deactivation.
3. To open the Team member details page for a deactivated team member, select **FIRST NAME**, **LAST NAME**, or **EMPLOYEE ID**.

5.5 REACTIVATING TEAM MEMBERS

Reactivating the team member profile automatically puts them back into their original groups (if the groups still exist). The team member must be manually re-assigned to a device and alert profiles.

To reactivate a team member:

1. From the Team member page, select the **DEACTIVATED** tab, open the team member details page, then select **Activate**.

Deactivated team member profile

Enter your team member's information

ACTIVATE

The team member's profile is automatically made active in Blackline Live.

6 MANAGING GROUPS

The Groups page lists 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. You can search and sort the group list by name. For more information on group structure, roles, and permissions, see section 3.3.2.

The screenshot shows the 'Groups' management interface. At the top, it says 'Groups' and 'Groups are used to organize and share devices with team members.' Below this is a dropdown menu for 'Organization' set to 'ACME Corp.'. There is a search bar labeled 'Search groups' and a 'Sort by' dropdown set to 'Name'. On the right, it says 'Page: 1 / 1' and has a blue 'ADD GROUP' button. Below these are four group cards: 'All devices' (description: 'All devices in the organization.'), 'Demo' (description: 'Sales demo group'), 'Headquarters office' (description: 'Devices for office employees'), and 'Test group' (no description).

NOTE: Each organization has a default group called the All devices group. This group collects the devices in the organization and represents the whole organization. The All devices group enables administrators to easily grant Account users access to resources in an organization.

You cannot edit the title, description, and device list of the All devices. You can edit the group managers of the All devices group.

6.1 ADDING A NEW GROUP

To add a new group:

1. From the Main menu, select **Groups**.
2. Select **ADD GROUP**.
3. Type the **Group name** and if applicable, a description for the new group.

The screenshot shows the 'Create a group' form. It has a title 'Create a group'. Below the title is a text input field for 'Group's Name' with the value 'Test group' and a character count '10/40'. Below that is a text area for 'Group's Description'. At the bottom left is a blue 'BACK' button, and at the bottom right are a blue 'CANCEL' button and a blue 'CREATE' button.

4. Select **CREATE**. The Group details page opens, displaying information related to the Group description, assigned managers, and assigned devices.

For information on editing group details, see section 6.2.

6.2 EDITING GROUP DETAILS

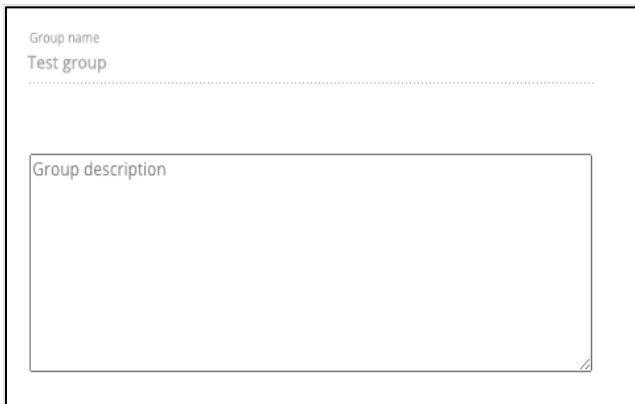
Update the group description, manage team member permissions for the group, and assign devices to the group by editing the Group details page.

NOTE: To update a section, select **EDIT**. To save your updates and stop editing, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To edit Group details:

1. From the Main menu, select **Groups**.
2. To open the Group details page, select the group name you are interested in viewing.
3. Edit any of the following:

Group description — Manage the Group name and optional Description for the group.



The screenshot shows a form with two main sections. The top section is labeled 'Group name' and contains the text 'Test group' followed by a dotted line indicating it is editable. The bottom section is labeled 'Group description' and contains a large, empty rectangular box for text input.

Group managers — Manage how team members (Account users) access the group:

- Add a team member as a group manager by selecting a **ROLE**.
- Update an existing group manager's permission by navigating to the team member of interest, then selecting a **ROLE**.
- Filter the team member list to show only those Account users that already have access by selecting **Only show Account users with access to this group**.
- Open a Team member's details page for editing by selecting the **FIRST NAME**, **LAST NAME**, or **EMPLOYEE ID** from the team member list.

NOTE: Account users that have access to the group are highlighted in green. For detailed information on the available group roles, see section 3.3.3.

☐ Only show account users with access to this group

Search team members

Items per page: 20 Page: 1 / 1

FIRST NAME	LAST NAME	EMPLOYEE ID	ORGANIZATION NAME	
Coby	Tobin	1739	ACME Corp.	<div>Display</div> <ul style="list-style-type: none"> No access Group admin Device admin Resolve only View only Contact admin
Ely	Hasek	1743	ACME Corp.	
Kiki	Wash	6213	ACME Corp.	
Carey	Fabian	2593	ACME Corp.	
Karolina	Ottosen	8716	ACME Corp.	
				No access

Group devices — Manage the devices assigned to a group:

G7, EXO, AND LONER G6

Search ☐ Only show devices assigned to this profile

Devices selected: 5

	DEVICE NAME	DEVICE ID	FIRST NAME	LAST NAME	EMPLOYEE ID
<input type="checkbox"/>	Unit 3567000101	G7c: 3567000101	Anita	Kunkel	2848WD
<input checked="" type="checkbox"/>	Unit 3567000104	G7c: 3567000104	Cheryl	Smith	Y6DUYV
<input type="checkbox"/>	Unit 3567000110	G7c: 3567000110	Gerhard	Brent	HR9JR3
<input type="checkbox"/>	Unit 3567000111	G7c: 3567000111	Jake	Lehmann	TN3E56
<input type="checkbox"/>	Unit 3567000123	G7c: 3567000123	Leon	Breiner	PGR238
<input type="checkbox"/>	Unit 3580000125	G7 EXO: 3580000125			
<input checked="" type="checkbox"/>	Unit 3580000163	G7 EXO: 3580000163	Miguel	Vemulakonda	BT3T2E
<input type="checkbox"/>	Unit 3581000234	EXO 8: 3581000234	Poncio	Macias	093LK3
<input type="checkbox"/>	Unit 3581000236	EXO 8: 3581000236	Shireen	Bousaid	YT230U
<input type="checkbox"/>	Unit 3582000113	EXO 8: 3582000113			

Items per page: 10 1 - 10 of 16

- Add devices to the group by selecting new devices you want to include in the group.
- **NOTE:** You can search and sort the device list by name.
- Remove devices from the group by unselecting the devices to exclude from the group.
- Filter the device list to only those team members that already have access by selecting Only show devices assigned to this group.
- Filter the device list by device type by selecting the G7, EXO, AND LONER, or G6 tab.

- Open a device's Device details page for editing by selecting the **DEVICE NAME** or **DEVICE ID** from the device list.

NOTE: Devices already assigned to the group are highlighted in green.

6.3 DELETING A GROUP

Groups cannot be recovered if they are deleted. Assigned devices are automatically removed from the group, and team members and providers no longer have access to this group.

NOTE: Removing a group does not remove the assigned devices from an organization.

Deleting groups removes them from any future reports. Groups cannot be deleted if the group contains group managers that do not have access to other groups.

To delete a group:

1. From the Group details page, select **DELETE**.



2. A confirmation dialog box opens. Select **DELETE**.

7 MANAGING DEVICES

The Devices page provides an overview of your device fleet. The page is useful for monitoring the status of your devices. For example, you can review how many devices are assigned to an organization, whether they are online, in alert, how they are configured, and the last time they connected and uploaded data to Blackline Live.

Devices

Organization
ACME Corp.

Total devices: 16
0 in alert | 11 online | 5 offline | 2 under repair
8 assigned | 8 unassigned

G7, EXO, AND LONER G6

Search: _____ Device assignment: All assignments

STATUS	CHECK-IN REMINDER	ASSIGNED TEAM MEMBER	ORGANIZATION	DEVICE ID	DEVICE NAME	CONFIGURATION PROFILE	ALERT PROFILE	LAST COMMUNICATION
	00:20:12	Anita Kunkel	ACME Corp.	G7c: 3567000101	Unit 3567000101	ACME G7c	ACME G7c	5 minutes ago
	00:34:56	Gerhard Brent	ACME Corp.	G7c: 3567000110	Unit 3567000110	ACME G7c	ACME G7c	2 minutes ago
	not configured	Jake Lehmann	ACME Corp.	G7c: 3567000111	Unit 3567000111	ACME G7c	ACME G7c	3 minutes ago
	not supported	Poncio Macías	ACME Corp.	EXO 8: 3581000234	Unit 3581000234	ACME EXO	ACME EXO	23 minutes ago
	not supported	Select to assign	ACME Corp.	EXO 8: 3582000113	Unit 3582000113	ACME EXO	ACME EXO	12 minutes ago

Items per page: 5 1 - 5 of 16

You can search and sort the device list. Filter the device list by device type by selecting the **G7, EXO, AND LONER**, or **G6** tab. The device list displays the following information:

- **Status** — the device's status (e.g., connected, disconnected, in alert, or under repair)
- **Check-in reminder (G7 only)** — indicates whether the device has a configured check-in reminder and how much time is left until the device's next check-in
- **Assigned team member** — if assigned, the device's assigned team member
- **Organization** — the device's assigned organization
- **Device ID** — the device model and identifier
- **Device name** — the device name
- **Configuration profile** — the device's assigned configuration profile
- **Alert profile (G7 and EXO only)** — the device's assigned alert profile
- **Last communication** — the last time the devices connected and uploaded data to Blackline Live

7.1 VIEWING DEVICE INFORMATION

Use the device list to access information about the assigned team member, device location, or details about the device.

STATUS	CHECK-IN REMINDER	ASSIGNED TEAM MEMBER	ORGANIZATION	DEVICE ID	DEVICE NAME	CONFIGURATION PROFILE	ALERT PROFILE	LAST COMMUNICATION
	not supported	 Cherilyn Weiss	ACME Corp.	G6: 35660000056	Unit 35660000056	ACME G6	ACME G6	 4 minutes ago
	not supported	 Alejandro Oliva	ACME Corp.	G6: 35660000072	Unit 35660000072	ACME G6	ACME G6	 8 minutes ago

To view device information:

1. From the Main menu, select **Devices**.
2. In the device list:
 - Select **ASSIGNED TEAM MEMBER** to view the details about a device's assigned team member. For more information about configuring team members, see section 5.
 - Select **DEVICE ID** or **DEVICE NAME** to view and edit a device's details. The Device details page opens. For information on how to edit information related to a device, see section 7.2.
 - Select **LAST COMMUNICATION** to view the current geographic location for a device in the Blackline Live map view. The Blackline Live map view opens, displaying the current location and status of the device. For more information on viewing device information using the map, see section 16.1.

7.2 EDITING DEVICE DETAILS

The Device details page helps you manage technical information related to a device. The page is composed of three sections: device description, device profiles, and assigned groups.

NOTE: To update section, select **EDIT**. To save your updates and stop editing, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To edit device details:

1. From the Device details page, edit any of the following:

Device description — review the device's name, type, ID number, activation code, assigned organization, and assigned team member.

Device Name
Unit 3588100023
15/64

Organization
ACME Corp.

Assigned team member
Unassigned

EXO 8
Unit ID: **3588100023**
Activation code: **5BWCMP**

For more information about assigning an organization to a device, see section 7.8.

For more information about assigning devices to team members, see section 7.3.

Profile details — profiles define how the device operates in the field. Manage the device's assigned configuration profile, alert profile (G7 devices only), and notification profile.

Device Configuration: **ACME Corp. demo**
Alert profile: **ACME Corp. demo**
Notification profile: **demo notif**

For more information on editing a device's assigned configuration profile, see section 7.5.

For more information on editing a G7 device's assigned alert profile, see section 7.6.

For more information on editing a device's assigned notification profile, see section 7.7.

Groups — manage the groups the device is assigned to.

Search groups
Sort by
Name

All devices
ACME Corp.
All devices in the organization.

Headquarters office
ACME Corp.
Devices for office employees

Groups indicate which site or team the device operates within. Groups also indicate which filters the device is included in when using Blackline Analytics. For more information on groups, see section 6.

Gas cylinder info (EXO only) — if automatic bump tests and calibrations are enabled, use the Gas cylinder info section to record the lot number, expiry date, and other information about the gas cylinder that is connected to EXO.

NOTE: You must have a subscription to enable automatic bump tests and calibrations. For more information, contact your Customer Relationship Manager (CRM).

7.3 ASSIGNING A DEVICE TO A TEAM MEMBER

There are multiple pages in Blackline Live where you can assign devices:

- Devices page
- Device details page
- Quick assign (G7 only)

NOTE: You can only assign a device to one team member at a time. If a team member already has a device, the new assignments overwrite existing ones.

Assigning a team member to a device does not cause Blackline Live to immediately connect and update the device. The device assignment is updated the next time the device connects and synchronizes with Blackline Live.

7.3.1 ASSIGNING A DEVICE FROM THE DEVICE PAGE

To assign a device to a team member from the Devices page:

1. In the devices list, navigate to the device to be assigned.
2. In the **ASSIGNED TEAM MEMBER** field, select **Select to assign**. The Assign team member dialog box opens.
3. Select a team member.
4. Select **ASSIGN**. The Devices page displays the new assignment.

Assign a team member to Unit 3566000123

Organization: ACME Corp.

Search team members Items per page: 20 Page: 1 / 30 Display ▾

FIRST NAME ↑	LAST NAME	EMPLOYEE ID
Annika	Aranasov	3164
Arturo	Chmela	1324
Coby	Tobin	1739
Denis	Bonnaire	1847
Ely	Hasek	1743
Emil	Hudnall	5723
Evalyn	Seidel	7294
Malena	Haward	8364
Nitya	Valencia	7592
Samuel	Adaire	4723
Willie	Scrivener	9276

CANCEL UNASSIGN ASSIGN

7.3.2 ASSIGNING A DEVICE FROM THE DEVICE DETAILS PAGE

NOTE: To update a section, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To assign a device to a team member from the Device details page:

1. In the Device description card, select a name from the Assigned team member dropdown.
- The devices description card displays the new assignment.

Device Name
Pierrick's device

Organization
ACME Corp.

Assigned team member
Pierrick Perrault

Unassigned

Arturo Chmela

Emil Hudnall

Evalyn Seidel

Nitya Valencia

Your device is currently assigned to the following profiles. Sele

7.3.3 ASSIGNING A DEVICE USING THE QUICK ASSIGN PAGE

The Quick assign page allows you to assign many devices at a time with the use of a barcode scanner.

To use the Quick assign page, you 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. Check the instructions that came with your scanner for programming codes.

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

To assign a device to a team member from the Quick assign page:

1. From the Main menu, select **Quick assign**.
2. In the Device field, type the *Device ID* or *Name*.

The 10-digit device ID is available on the back of the device. Alternatively, the ID is available in the device's Advanced Info menu under **Device Info**.

3. In the **Employee ID** field, type the employee ID to assign to the device.
4. To submit the assignment, press the **Enter** key.

7.4 UNASSIGNING A DEVICE FROM A TEAM MEMBER

7.4.1 UNASSIGNING A DEVICE USING THE DEVICE PAGE

To unassign a device from the Device page:

1. In the devices list, navigate to the device to be unassigned.
2. In the **ASSIGNED TEAM MEMBER** field, select the existing team member's name. The Assign device dialog box opens.
3. Select **UNASSIGN**. The Devices page displays the device's new status.

Assign a team member to Unit 3566000123

Organization: ACME Corp.

Search team members Items per page: 20 Page: 1 / 30 Display ▾

FIRST NAME ↑	LAST NAME	EMPLOYEE ID
Annika	Aranasov	3164
Arturo	Chmela	1324
Coby	Tobin	1739
Denis	Bonnaire	1847
Ely	Hasek	1743
Emil	Hudnall	5723
Evalyn	Seidel	7294
Malena	Haward	8364
Nitya	Valencia	7592
Samuel	Adaire	4723
Willie	Scrivener	9276

CANCEL UNASSIGN ASSIGN

7.4.2 UNASSIGNING A DEVICE USING THE DEVICE DETAILS PAGE

To open a section for updating, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To unassign a device from the Device details page:

1. In the Device description card, select **UNASSIGN** in the Assigned team member dropdown. The devices description card displays the unassigned status of the device.

7.4.3 UNASSIGNING A DEVICE USING THE QUICK ASSIGN PAGE

To unassign a device from a team member from the Quick assign page:

1. From the Main menu, select **Quick assign**.
2. Select the **UNASSIGN** tab.
3. In the Device field, type the *Device ID* or *name*.
4. To submit the update, press the **Enter** key.

7.5 UPDATING A DEVICE CONFIGURATION PROFILE

NOTE: To update a section, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To update a device configuration profile:


1. From the Device details page, select the device's assigned **Device configuration**.
2. Remove the device from the configuration profile by unselecting the checkbox for the device in the list.
3. Assign the device to a different configuration profile from the appropriate Configuration profile details page.

For detailed information on updating a device's configuration profile, see section 9.3.

7.6 CHANGING THE ALERT PROFILE FOR A DEVICE

NOTE: G6 does not support alert profiles.

To change the assigned alert profile for a device:


1. From the Device details page, select the device's assigned **Alert profile**. The Alert profile details page opens.
2. Remove the device from the alert profile by selecting  for the device in the list.
3. Assign the device to a different alert profile from the appropriate Alert management profile details page.

For detailed information on updating an alert management profile assigned device, see section 10.3.

7.7 CHANGING THE NOTIFICATION PROFILE FOR A DEVICE

To update a section, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To change the notification profile for a device:

1. From the Device details page, select the device's assigned **Notification profile**. The Notification profile details page opens.
2. Remove the device from the notification profile by selecting  for the device in the list.

3. Assign the device to a different notification profile from the new profile's Notification profile details page.

For detailed information on how to assign a device to a notification profile, see section 11.3.

7.8 MOVING DEVICES BETWEEN ORGANIZATIONS

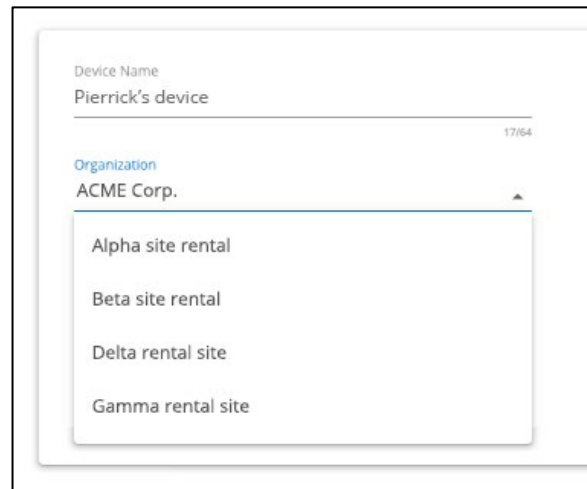
To move devices between organizations, an Account user must have a group or organization admin role for the All devices group of both organizations.

In general, distributors 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.

To update a section, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To move devices between organizations:

1. From the Device details page, select a new **Organization**.



The screenshot shows a form for editing device details. The 'Device Name' field contains 'Pierrick's device'. Below it, the 'Organization' field is set to 'ACME Corp.'. A dropdown menu is open, showing a list of other organizations: 'Alpha site rental', 'Beta site rental', 'Delta rental site', and 'Gamma rental site'.

7.9 MARKING A DEVICE AS UNDER REPAIR

Devices marked as under repair cannot be assigned to team members, require return merchandise authorization (RMA), and should not be used in the field.

To mark a device as under repair:

1. From the Device details page, select **MARK AS UNDER REPAIR**.

Device details

MARK AS UNDER REPAIR ASSISTED LOGOFF

This page provides insight into your device, including technical details, assigned team member and profiles.

Device Name

Unit 3567001219

EDIT

15/64

2. To confirm your selection, select **MARK AS UNDER REPAIR** in the confirmation dialog box.

The Devices page displays the device status as under repair. If the device was assigned to a team member, it is automatically unassigned.

7.10 MARKING A DEVICE AS OPERATIONAL

Repaired devices marked as under repair can be marked as operational and assigned to team members.

To mark a device as operational:

1. From the Device details page, select **MARK AS OPERATIONAL**.

The Devices page displays the device's new status as operational.

7.11 LOGGING A DEVICE OUT OF BLACKLINE LIVE

Assisted logoff forces the device to go offline on Blackline Live. Monitoring personnel use it during troubleshooting when the device cannot properly power down. It does not power down the physical device.

NOTE: G6 does not support assisted logoff.

To log a device out of Blackline Live:

1. From the Device details page, select **ASSISTED LOGOFF**.

The Devices page displays the devices new status as under repair. You cannot assign a device to a team member while it is marked as under repair.

7.12 SENDING AN ACTIVATION CODE FOR LONER MOBILE DEVICES

The Send activation option only appears on Loner Mobile device details page when it is assigned to a team member with a mobile phone number.

To send an activation code to a Loner Mobile device:

1. From the Device details page, select **SEND ACTIVATION CODE**.

An activation code is sent to the mobile phone number so that the assigned user can register the Loner Mobile app to their phone.

8 MANAGING 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	Receives only communication regarding billing and finance notifications for this account.
Website updates and new features	Receives only communication regarding new features and changes to the functionality of the web portal.
Service outage notifications	Receives information if Blackline, or any services that Blackline Live depends on (e.g., cellular providers or web services providers), are interrupted resulting in a temporary loss of service.
Account administrators	Receives all communications regarding this account. This includes billing and finance notifications, new features and site improvements, web portal or service interruptions.

8.1 ADDING TEAM MEMBERS TO CONTACT GROUPS

Adding team members to contact groups ensures that they are sent relevant updates.

To add team members to contact groups:

1. From the Main menu, select **Alert profiles**. The Alert profile page opens.
2. Select the **Contact Groups** tab.
3. For the contact group of interest, select **Add Contacts**.
The Choose a Contact dialog box opens.

Alert profiles

Organization: ACME Corp.

Contact Groups

Periodically, Blackline Safety will need to contact clients for a variety of reasons. Providing and maintaining the appropriate contact information below will ensure that the most appropriate individual receives our communications.

Account Administrator
Receives all communications regarding this account. This includes billing and finance notifications, new features and site improvements, web portal or service outages.

[+ Add Contacts](#)

Name	Email	Phone Numbers
Kiki Wash	admin@acmecorp.com	Work: 333-012-3456 Mobile: 333-123-4567

Billing and Finance Billing
Receives only communication regarding billing and finance notifications for this account.

[+ Add Contacts](#)

Name	Email	Phone Numbers
Carey Fabian	cfabian@acmecorp.com	Work: 333-012-3456

Website Updates and New Features
Receives only communication regarding new features and changes to the functionality of the web portal.

[+ Add Contacts](#)

4. Select one or more team member names.
Team members that are already a member of the group are highlighted in the list.
Team members flagged with a do not have an email address included in their profile.

Device details MARK AS UNDER REPAIR ASSISTED LOGOFF

This page provides insight into your device, including technical details, assigned team member and profiles.

Device Name

Unit 3567001219

[EDIT](#)

9 MANAGING CONFIGURATION PROFILES

Configuration profiles define how a device behaves in the field, manage which features are enabled, and allow users to adjust the settings related to these features. You can change device configurations over-the-air (OTA), without having to power cycle the device. You can search and sort the configuration profiles list.

G7, EXO, AND LONER

G6

ADD CONFIGURATION

Search configurations

Columns

CONFIGURATION TYPE	CONFIGURATION NAME	ORGANIZATION	NO. OF DEVICES
G7c	ACME G7c	ACME Corp.	9
EXO	ACME EXO	ACME Corp.	5

9.1 VIEWING CONFIGURATION PROFILES

Use the configuration profile list to access information about the type of device, assigned organization, and devices.

To view configuration profiles information:

1. From the Main menu, select **Configurations**.
2. To view a profile, select the **CONFIGURATION NAME** for the item. The Configuration profile details page opens.

For information on how to edit information related to a configuration profile, see section 9.3.

9.2 CREATING A NEW CONFIGURATION PROFILE

To create a new configuration profile:

1. From the Configurations profile page, select **ADD CONFIGURATION**. The device type dialog box opens.
2. Select the configuration type to apply the profile to. You cannot change the type of device associated with a configuration profile after it is selected.

Select configuration type

Select the type of device this new configuration will be for.

☐ G6
☒ EXO

☐ G7c
☐ G7x

☐ Loner 900
☐ Bridge

☐ Loner IS
☐ Loner M6

☐ Loner M6i
☐ Loner Mobile

☐ Loner SMD

CANCEL
NEXT

3. Select **NEXT**. The Configuration profile details page opens.

For information on how to update information related to a configuration profile, see section 9.3.

4. To save the new profile settings, select **SAVE**.

9.3 EDITING CONFIGURATION PROFILE DETAILS

You can update a configuration profile by editing the Configuration profile details page. The details available for editing depend on the device type:

Configuration Profile	G6	G7c / G7x	G7EXO/EXO8
Description	✓	✓	✓
Operating mode		✓	
Functional settings	✓	✓	✓
Sensor settings	✓	✓	✓
Pump module			✓
Interface ports			✓
Assigned devices	✓	✓	✓
Last profile change	✓		
AlertLink messaging			✓

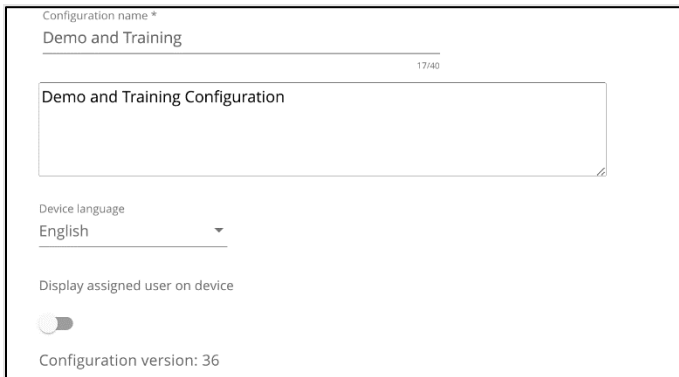
To update a section, select **EDIT**. To save your updates and stop editing, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

Because configuration profile updates impact device behavior in the field, you must confirm edits to configuration profiles.

To edit configuration profile details:

1. From the Configuration profile details page, edit any of the following:

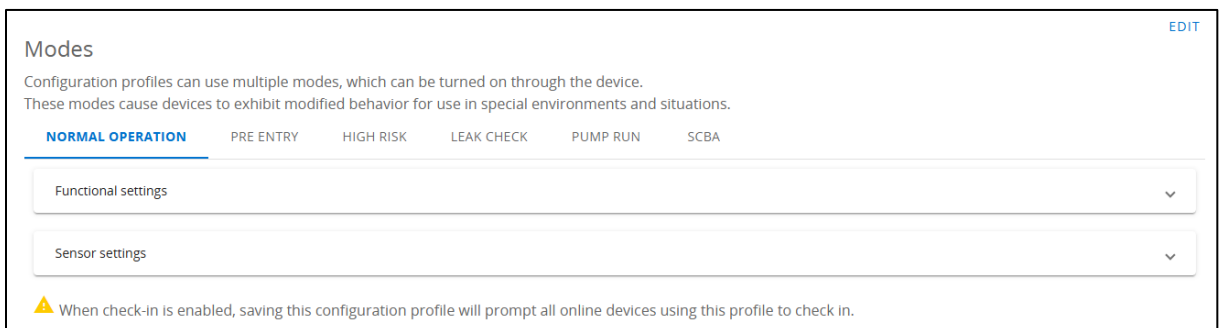
Configuration profile description — manage the configuration profile name, device language, and assigned team member display settings.



The screenshot shows a configuration profile details form. At the top, there is a field for 'Configuration name' with the value 'Demo and Training' and a character count '17/40'. Below this is a large text area for the profile description, containing 'Demo and Training Configuration'. Further down is a 'Device language' dropdown menu currently set to 'English'. Below that is a toggle switch for 'Display assigned user on device', which is currently turned off. At the bottom, it shows 'Configuration version: 36'.

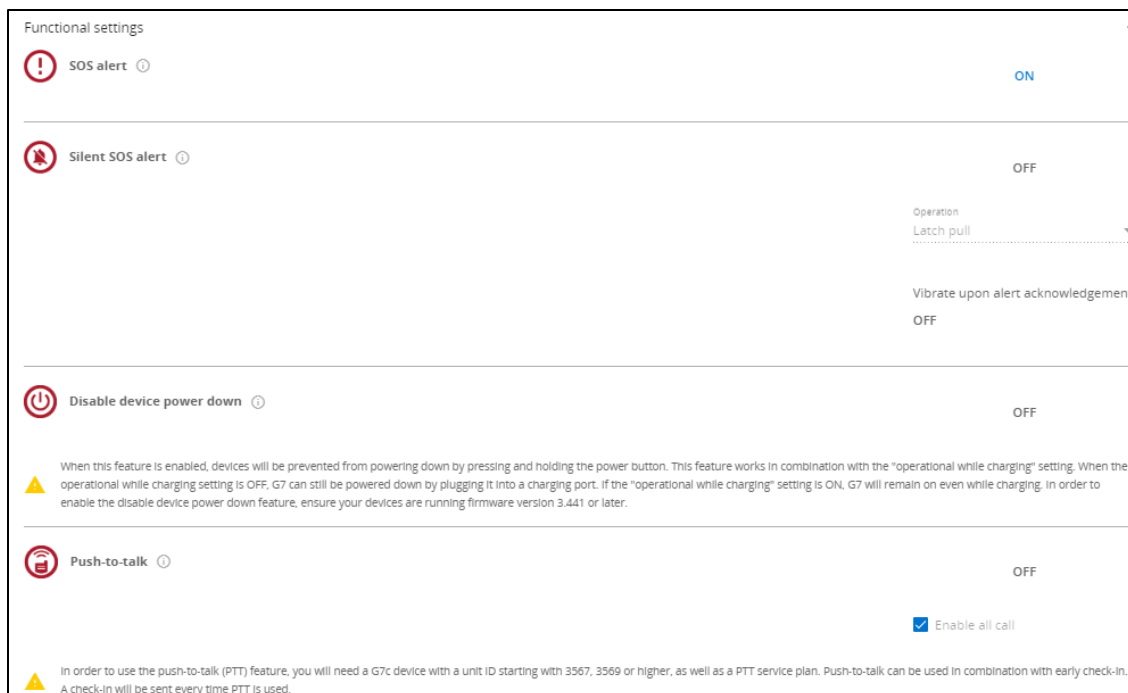
Operating modes (G7) — configure the functional and sensor settings according to operating mode (normal operation, pre entry, high risk, leak check, pump run, and SCBA). Modes cause devices to exhibit modified behavior depending on the environment or situation.

For detailed information on modes and settings, see section 9.4.



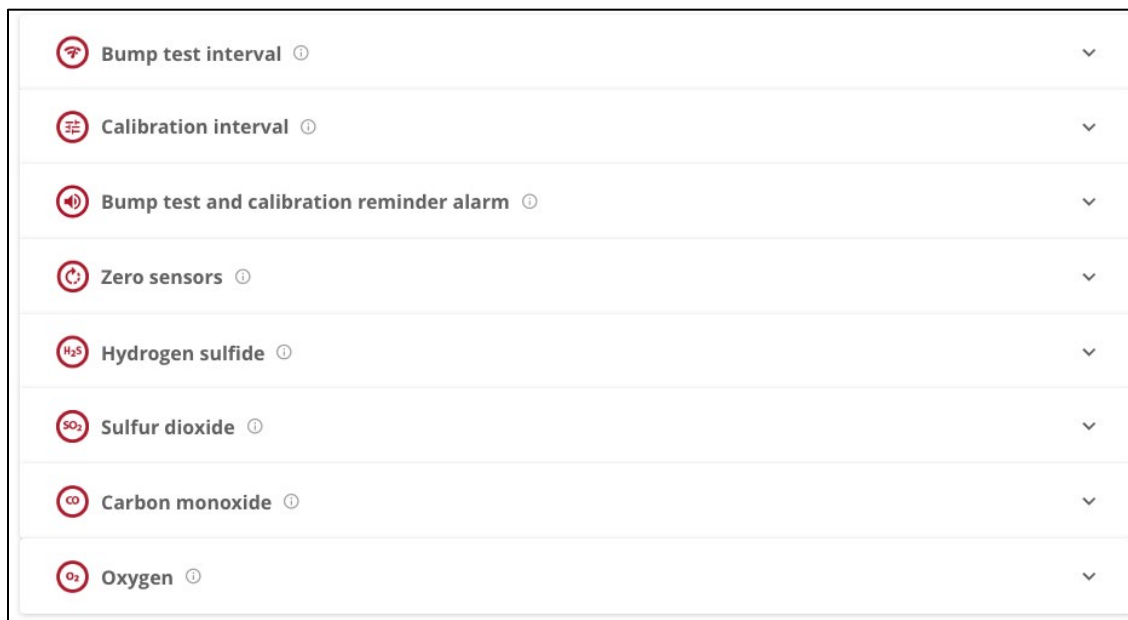
The screenshot shows the 'Modes' configuration page. At the top right is an 'EDIT' link. Below the title 'Modes' is a descriptive paragraph: 'Configuration profiles can use multiple modes, which can be turned on through the device. These modes cause devices to exhibit modified behavior for use in special environments and situations.' Below this is a row of tabs: 'NORMAL OPERATION' (selected), 'PRE ENTRY', 'HIGH RISK', 'LEAK CHECK', 'PUMP RUN', and 'SCBA'. Under the 'NORMAL OPERATION' tab, there are two expandable sections: 'Functional settings' and 'Sensor settings', each with a downward arrow. At the bottom, there is a warning icon and text: 'When check-in is enabled, saving this configuration profile will prompt all online devices using this profile to check in.'

Functional settings — manage general device settings. Depending on the device type and operating mode, functional settings allow you to configure the behavior of certain device features (e.g., SOS Alert, device power down, low-battery threshold, or fall detection threshold).



Sensor settings—manage settings specifically related to gas and gamma detection. Depending on the device type, sensor settings let you enable or disable certain gas sensors, indicate alarm thresholds per sensor type, and specify bump testing and calibration intervals.

NOTE: The gamma sensor is factory calibrated. Calibration interval settings are not available.



Pump module (EXO) — configure EXO's pump module. For each inlet, set the Inlet function as gas sampling, self-bump test and calibration, or disabled.

NOTE: The pump module settings do not apply to the EXO Diffusion module.

You must configure inlets in order, with disabled inlets listed after self-bump test and calibration inlets, purge inlets, and gas sampling inlets.

For inlets configured for gas sampling, toggle the Default to ON upon startup setting to ON or OFF for each inlet. If multiple inlets are used for gas sampling, enter the Sampling schedule (minutes). The interval entered indicates the amount of time EXO pumps gas over the sensors from each inlet. There is a two-minute buffer period in between each sample where air is pumped over the sensor to purge the gas from the first inlet before replacing it with gas from the next inlet.

A multi-inlet sampling setup implies that EXO does not continuously monitor any single environment.

If enabled, you can configure the EXO Pump module to complete automatic bump tests and calibrations. EXO initiates its own bump tests and calibrations when they are overdue.

You must have a service plan to enable automatic bump tests and calibrations. For more information, contact your Customer Relationship Manager (CRM).

You must configure EXO's pump inlets 1 and 2 to complete automatic bump tests and calibrations. Confirm that one of the inlets configured to self-bump test and calibration functionality is set to purge and is connected to an Ultra Zero Grade Air gas cylinder to run automatic calibrations. If you do not configure an inlet to purge, EXO only performs automatic bump tests.

Inlet 1

Inlet Function
Self-bump test and calibration ▼

Inlet setting

Gas	Concentration		
H ₂ S	25	ppm	
Range: 0.5 - 50ppm Increment: 0.1ppm			
Gas	Concentration		
LEL - CH ₄	50	%LEL	✗
Range: 4 - 60%LEL Increment: 1%LEL			
Gas	Concentration		
CO	100	ppm	✗
Range: 5 - 500ppm Increment: 1ppm			
Gas	Concentration		
O ₂	18	%vol	✗
Range: 0.1 - 10%vol Increment: 0.1%vol			
Gas			
N ₂	Balance		✗

Gas cylinder

Lot number

015

Expiry date

Additional notes

0150

[ADD GAS](#)

⚠ In order to self-calibrate, ensure another inlet is configured to a purge gas. Without a purge inlet, EXO will only perform self-bump tests. EXO will not detect gas readings while it is performing a bump test or calibration.

Sampling schedule

Sample interval indicates the amount of time EXO will pump gas into each inlet. There will be a 2 minute buffer period in between each inlet sample to allow time for the gas to disperse from around the sensor. Sample schedule settings are required when multiple inlets are used for gas sampling. A multi-inlet sampling setup implies that EXO will not be continuously pumping gas to its sensors.

Sample time

10 minutes

Auto bump test and calibration

When these features are enabled, EXO will initiate its own bump tests or calibrations when they are overdue. EXO will use all of the available self-test inlets to run these tests. Ensure that one of the self-test inlets is set to purge in order to run auto calibrations.

Run auto bump tests

Run auto calibrations

Interface Ports (EXO) — configure EXO's interface ports to determine how EXO communicates a signal to an external device (e.g., a horn or light). Use the settings to indicate which event type activates each interface port and define how EXO supplies power to external devices when an event occurs.

The interface ports can be activated by a high-gas event, a low-gas event, a text message, or an AlertLink message. You can also configure EXO to apply or remove power from an external device for the duration of an event.

Port A

EXO will activate the port when the following events occur:

- ☒ High gas
- ☐ Low gas
- ☐ Text message
- ☒ AlertLink message

Assigned Devices — assign devices to the configuration profile by selecting a device from the list. The assigned devices are automatically highlighted.

Search devices

Columns ▾

<input checked="" type="checkbox"/>	DEVICE NAME ↑	DEVICE ID	FIRST NAME	LAST NAME	EMPLOYEE ID	PTT SUPPORT	STATUS
<input checked="" type="checkbox"/>	Unit 3588000012	EXO: 3588000012					pending ⓘ
<input checked="" type="checkbox"/>	Unit 3588000024	EXO: 3588000024					pending ⓘ
<input checked="" type="checkbox"/>	Unit 3588000103	EXO: 3588000103					active

Items per page: 20 ▾ Page: 1 / 1

Last profile change (G6) — display the last time the profile was changed and the name and organization of the person who last edited the profile.

Last change	February 2, 2022 11:37 AM MST
Changed by	Taelynn Graham ACME Corp

AlertLink messaging (EXO) — configure AlertLink message notification behaviour on EXO devices when a message is received by the device. Use the setting to determine if AlertLink messages persist for a maximum of 90 minutes until they are manually acknowledged on the device, or if the message automatically clears after a pre-set timeout period between 5 and 90 minutes (15 minutes is the default).

AlertLink messaging ⓘ

AlertLink message behavior

AlertLink messages time out ▾

Timeout

15 minutes

Enter a value between 5 and 90 minutes with an interval of 5.

9.4 EDITING CONFIGURATION PROFILE MODE SETTINGS (G7 ONLY)

Use configuration profile mode settings to manage the G7 response for specific operating environments. The settings available depend on the device type and mode.

Modes cause devices to exhibit modified behavior depending on the environment or situation. The modes available for configuration depend on the type of device. Blackline Live currently offers the following configuration modes for each device type:


Mode	G7c	G7x
Normal operations	✓	✓
Pre entry	✓	✓
Pump run	✓	✓
High risk	✓	✓
Leak check	✓	✓
SCBA	✓	✓

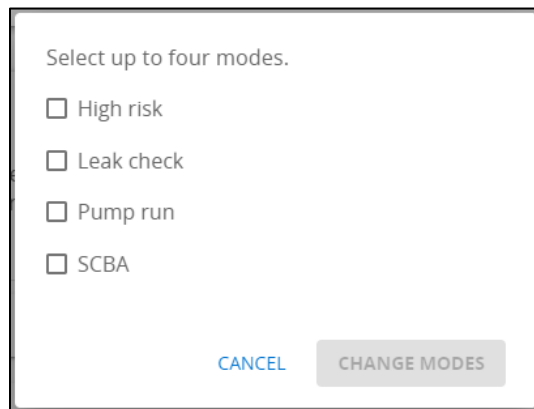
By default, every configuration profile has Pre entry mode available, which can be accessed from the device if it is using a pump cartridge.

Some modes (Pre entry, Leak check, SCBA) have a mandatory mode time-out feature, which prompts the user to confirm they are still using the mode after the countdown reaches zero. Because many of the configuration modes modify alert and alarm behavior, this time out ensures that if the user cannot respond, the device exits the configuration mode and notifies monitoring personnel to investigate.

The settings configured for normal operating mode also apply to the other operating modes.

To edit configuration profile operating mode settings:

1. In the Configuration profile modes card:
 - Add additional operating modes to configure by selecting . The change modes dialog box opens.
 - Select the additional modes to configure.
 - Select **CHANGE MODES** to add the additional mode tabs to the Configuration profile mode card.



2. For each active mode, configure the gas sensor and functional settings. For detailed information about the settings available, refer to [Configuration Modes](#).
3. To save the updated profile, select **SAVE**.

G7 Pump Cartridge Configuration



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 modes have a **Pump required** setting in their respective tabs in the Mode settings card on Blackline Live. If this setting is toggled on, a pump must enter the mode and the pump starts running when the mode is entered on the device.

NOTE: Pump run mode always runs the pump cartridge.

Loner Mobile Configurations

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

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

10 MANAGING ALERT MANAGEMENT PROFILES


Alert management profiles define how monitoring personnel respond to alerts from a group of devices. You can apply alert profiles to any kind of device type if the emergency protocol contacts are the same for the devices.

If your organization is monitored by Blackline's Safety Operations Center (SOC), you cannot make changes to your protocol or device alerts without consulting a Blackline SOC administrator. This ensures that protocols are written in a language and format our agents have been trained to respond to, and to avoid confusion during an alert.

G6 does not support alert management profiles. Alerts from G6 devices are not displayed in the Alerts page, do not trigger the alert banner/animation in Blackline Live, and do not have any alert histories or alert management pages associated with them.

10.1 VIEWING ALERT MANAGEMENT PROFILES

To view alert management profiles:

1. From the Main menu, select **Alert profiles**.
2. Select the **Alert Management** tab to view a list of the existing Alert management profiles.
3. Select  to view the details of an existing profile. The Alert management profile details page opens.

For information on how to edit an Alert Management profile, see section 10.3.

10.2 CREATING A NEW ALERT MANAGEMENT PROFILE

To create an alert management profile:

1. From the Alert management profiles page, select **Create Alert Profile**. The Alert Management profile details page opens.

For information on how to edit information related to an Alert Management profile, see section 10.3.

10.3 EDITING ALERT MANAGEMENT PROFILE DETAILS

Update an alert management profile by editing cards on the Alert management details page. The page is composed of multiple sections, including emergency response protocol, emergency response contacts, notified contacts, device alerts, device users, and AlertLink.

To edit alert management profile details:

1. From the Alert management profile details page, edit any of the following:
Emergency Response Protocol — review the standard steps monitoring personnel take in the case of an emergency.

Organizations monitored by Blackline's Safety Operations Center (SOC) work with Blackline Safety SOC administrators to review and build a protocol. Do not modify emergency response protocols without consulting with SOC administrators.

Alert Management Profile

Phil Benson (standard access) - BLN

Calgary

Emergency Response Protocol

Steps

Formats
B
I
U
A
Link
Text

Protocol for G7c with Gas
For SOS Alerts, No Motion, Fall Detection, Missed Check-ins:
Step 1: Call the G7 Device and validate need for assistance, note the gas readings and the user's GPS location & time and add it to your notes, if there is no response, attempt to contact the device users phone number and validate need for assistance, if still no answer, please proceed to step 2.
Step 2: Send a message to the G7 device: Are you ok? And wait 2 minutes for response, if no answer, proceed to step 3.
Step 3: Contact company emergency contacts in order of priority. Once someone is reached from the emergency contact list please provide the emergency contact the following information;
Full name of the employee
Type of Alarm

Emergency Response Contacts — manage the emergency response contacts who should be contacted in case of an emergency. Their information is made available to monitoring services when a device in the alert profile goes into alert and is 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. Always enter phone numbers using a 10- or 14-digit phone number format.

Emergency Response Contacts

These are contacts who are referred to in the Emergency Response Protocol. They must be created as team members in the organization before assigning them to this profile.

Add Contact

Names	Phone Number	Priority	
Nathan Boucher <input type="checkbox"/> contact assigned device	Mobile: 555-253-8576	2	
Sarah Carpenter <input type="checkbox"/> contact assigned device	Mobile: 555-345-7685	3	

Notified Contacts — manage who should be notified when an alert occurs but are not necessarily responsible for being an emergency contact. Notified contacts are sent an email, SMS message, or both, either immediately, or after a specified delay.

Ensure that any team members listed as notified contacts have an updated mobile number and email information in their team member profile. Always enter phone numbers using a 10- or 14-digit phone number format.

Notified Contacts
 Used primarily by self-monitored organizations, these are contacts who will automatically receive a notification of an alert via email or SMS. They must be created as team members in the organization before assigning them to this profile.

+ Add Contact

Names	Contact Method	Delay	
Nathan Boucher	Email	0 minutes	

Device Alerts — manage what events on the device 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.

Device Alerts
 When an alert in this list is toggled **ON** it will be shared remotely — in addition to a local alarm, an alert will also be displayed in Blackline Live, a proximity message will be shared and a notification will be sent to notified contacts in this profile. When an alert is toggled **OFF** the device will still alarm locally, but the alert will not be communicated remotely.

Alert Type	On	Off
SOS triggered (Emergency alert)	<input checked="" type="radio"/>	<input type="radio"/>
Silent SOS triggered (Silent emergency alert)	<input checked="" type="radio"/>	<input type="radio"/>
Fail detected	<input checked="" type="radio"/>	<input type="radio"/>
No motion detected	<input checked="" type="radio"/>	<input type="radio"/>
Missed check-in detected	<input checked="" type="radio"/>	<input type="radio"/>
Tumble detected (EXO only)	<input type="radio"/>	<input checked="" type="radio"/>
Pump blocked (EXO only)	<input type="radio"/>	<input checked="" type="radio"/>
Logged on	<input type="radio"/>	<input checked="" type="radio"/>
Logged off	<input type="radio"/>	<input checked="" type="radio"/>
Network timeout	<input type="radio"/>	<input checked="" type="radio"/>
Low battery	<input type="radio"/>	<input checked="" type="radio"/>
Over limit detected	<input type="radio"/>	
High threshold detected	<input type="radio"/>	
STEL detected	<input type="radio"/>	
TWA detected	<input type="radio"/>	

Device Users — add multiple device users to an alert profile so that they share the same emergency response protocol.

If any devices require a different protocol or emergency response contacts, assign them to separate alert profiles

Device Users

+ Add User

Users	Device Name	
Unassigned	Unit 3566000638	
Angie Hunt	Unit 3567001219	

AlertLink — manage whether G7c, G7x, and EXO devices in alert prompt Blackline Live to send AlertLink messages to nearby G7c and EXO devices within the same

organization. Only devices whose last known location is within the specified proximity radius of the source device at the time of the initial alert receive AlertLink messages.

NOTE: AlertLink is only available for self-monitored or Blackline-monitored organizations. G7x devices can trigger AlertLink messages but are unable to receive them.

The Message radius can be configured within a range of 10 m (50 ft) to 5,000 m (16,000 ft). The message includes the alert type, the assigned user of the origin device, the origin device type, and other device information.

NOTE: You can exclude EXO devices from receiving AlertLink messages.

AlertLink messages

When this feature is enabled, G7c, G7x, and EXO devices in alert will prompt Blackline Live to send an automated message to G7c or EXO devices nearby belonging to the same organization. Only devices whose last known location is within the specified radius of the initial alert will receive AlertLink messages. EXO devices can optionally be excluded from receiving AlertLink messages. G7x can trigger AlertLink messages, but cannot receive them.

AlertLink messages will only be sent when the following alerts are enabled and triggered: SOS alert, no-motion alert, fall detection alert, high gas alert, and gas sensor over limit alert.

AlertLink messages on EXO can be configured to persist or time out through the EXO configuration profile. Additionally, if you would like EXO's interface ports to be activated by AlertLink messages, this can be set up in the EXO configuration profile.

Message content	Message radius	On	Off
Device type Alert type Assigned user Device information	<div>100 meters</div> <div>Enter a value between 10 and 5000 m with an interval of 10.</div>	<input type="radio"/>	<input checked="" type="radio"/>

Include EXO in AlertLink messages

☒ Transmit AlertLink messages from devices in this profile to EXO

11 MANAGING NOTIFICATION PROFILES


Notification profiles are used to send out emails and SMS messages to team members. Although notification profiles are similar in format to alert management profiles, they are separate from the alert management process in Blackline Live.

Create notification profiles to send updates for non-alert events, such as low battery, log on, log off, network connection losses, or hardware errors. While these events do not demand the attention of monitoring personnel, it allows team members to be notified of the event and address the situation if needed.

As with alert profiles, notification profiles let you define notified contacts, device events, and devices. When a defined device experiences an event that is toggled on in the profile, the notified contacts receive an email or SMS.

11.1 VIEWING NOTIFICATION PROFILES

To view notification profiles:

1. From the Main menu, select **Alert profiles**. The Alert profiles page opens.
2. Select the **Notifications** tab to view the Notification profile page.
3. Select  to view the details of an existing profile. The Notification profile details page opens.

11.2 CREATING A NEW NOTIFICATION PROFILE

To create a new notification profile:

1. From the Notification profiles page, select **Create Notification Profile**. The Notification profile details page opens.

11.3 EDITING NOTIFICATION PROFILE DETAILS

Update a notification profile by editing cards on the Notification profile details page. The page is composed of multiple sections, including device notification, notified contacts, and device users.

To edit notification profile details:

1. From the Notification profile details page, edit any of the following:


Device notification — manage what events on the device result in a notification in Blackline Live by toggling each event type on or off.

For G6 devices, Blackline Safety recommends only turning on notifications for high gas, STEL, and gas sensor over limit alerts.

Device Notification

NOTE: For G6 devices, Blackline Safety recommends only turning on notifications for SOS, high threshold, STEL, TWA, and over limit detected events.

Notifications	On	Off
SOS triggered (Emergency alert)	<input checked="" type="radio"/>	<input type="radio"/>
Silent SOS triggered (Silent emergency alert)	<input checked="" type="radio"/>	<input type="radio"/>
Fall detected	<input checked="" type="radio"/>	<input type="radio"/>
No motion detected	<input checked="" type="radio"/>	<input type="radio"/>
Missed check-in detected	<input checked="" type="radio"/>	<input type="radio"/>
Tumble detected (EXO only)	<input checked="" type="radio"/>	<input type="radio"/>
Pump blocked (EXO only)	<input type="radio"/>	<input checked="" type="radio"/>
Pump block resolved (EXO only)	<input type="radio"/>	<input checked="" type="radio"/>
Logged on	<input checked="" type="radio"/>	<input type="radio"/>
Logged off	<input checked="" type="radio"/>	<input type="radio"/>
Network timeout	<input checked="" type="radio"/>	<input type="radio"/>

Notified contacts — manage who should be notified when an alert occurs. Notified contacts are sent an email, SMS message, or both. Remove existing contacts by selecting .

Notified Contacts

+ Add Contact

Names	Contact Method	
Nathan Boucher	SMS	
Doris Knight	All	


Ensure that team members listed as notified contacts have an updated mobile number and email information in their team member profile.


Device users — add multiple device users to a notification profile so that they share the same notification protocol.

Device Users

+ Add User

G7, EXO, and LonerG6

Users	Device Name	
Amber Dunleavy	Amber's device	
Unassigned	Unit 4000001023	
Unassigned	Unit 4000001024	

Select **Add User** to add device users to the notification profile. Remove existing device users by selecting .

Choose Devices

G7, EXO, and Loner
G6

[Show all](#)
[Select all](#)

User	Device Name	Firmware
Kiki Wash	Loner Mobile iOS	
Leon Breiner	Unit 3567001219	
Unassigned	Unit 3567002340	
Unassigned	Unit 3567002342	

12 MANAGING RELATIONSHIPS

Relationships link your organization to other organizations through a relationship agreement. In each agreement, there is a client (you) and a provider. You can invite an organization to be a provider. If the provider accepts, they have access to your shared groups.

For more information on relationship structures, see section 3.4.

12.1 VIEWING ACTIVE RELATIONSHIPS

The Relationships page lists relationships that involve your organization.

Relationships

Your organization can be linked to other organizations through a relationship agreement. In each agreement, there is a client and a provider. The client can invite an organization to be a provider. If the provider accepts, they will have access to the client's shared groups.

Organization
ACME Corp.

ACTIVE
DEACTIVATED

Search relationships
Relationship type
All relationships
Sort by
Name

Page: 1 / 1

Blackline Safety Operations Center

Provider: soc@blacklinesafety.com
Client: ACME Corp.
Contact: soc@blacklinesafety.com
Type: Contractual
Active

To view active relationships:

1. From the user menu, select **Relationships**. The Relationships page opens, displaying the relationships registered in this organization.
2. To view the details of an active agreement, select the associated Relationship card.

For information on how to edit the agreement details, see section 12.4.

12.2 VIEWING DEACTIVATED RELATIONSHIPS

To view deactivated relationships:

1. From the Relationships page, select the **DEATIVATED** tab. The Relationships page displays a list of inactive relationships.
2. To view the details of an inactive agreement, select the associated Relationship card.

12.3 CREATING A RELATIONSHIP

Only client organizations can initiate a relationship, since they are responsible for defining the provider's access. To give another organization access to your resources, you can invite them to be your provider.

Add provider

A provider is the organization you choose to service your Blackline Live account. As the client, you can control the amount of access they have by editing their group permissions, and can terminate the partnership at any time.

Relationship name

Distributor relationship

Create a relationship name to describe the service your provider will have with your organization (eg. Monitor, Distributor, Contractor). 24 / 50

Contact email

distributor@gmail.com

Relationship type

A non contractual relationship allows you to customize your provider's access to shared groups. Choosing not to assign your provider to your All Devices group will limit user and customer admin roles to resolve only.

A contractual relationship gives the provider either resolve only or customer admin access to your organization's All Devices group. Contracts cannot be changed by either party once agreed upon, and require Blackline's Customer Care team to edit or deactivate the agreement.

☒ Non-contractual
☐ Contractual - Resolve only
☐ Contractual - Group admin

Search groups

Sort by: Name

Page: 1 / 2

All Devices

Org A

All devices in your organization

Roles

No access

Group 1

Org A

Group 1 description

Roles

Group admin

Group 2

Org A

Group 2 description

Roles

No access

Group 3

Org A

Group 3 description

Roles

Device admin

Group 4

Org A

Group 4 description

Roles

Group admin

BACK

CANCEL

SEND

To create a relationship:

1. From the Relationships page, select **Add Provider**. The Agreement details page opens.
2. Update the agreement details.

You must provide a unique relationship name and the email of the Organization admin that is facilitating your shared resources.

3. Select the relationship type (Non-contractual, Contractual-Resolve only, or Contractual-Group admin).

A non-contractual relationship lets you customize your provider's access to shared groups. Choosing not to assign your provider to your All Devices group limits user and customer admin roles to resolve-only.

A contractual relationship gives the provider either resolve only or customer admin access to your organization's All devices group. Contractual relationships cannot be changed by either party after they are agreed on and require Blackline's [Technical Support](#) team to edit or deactivate the agreement.

For more information on relationship types, see section 3.4.

4. If you are creating a non-contractual relationship, select group roles for your provider.

NOTE: If you are creating a contractual relationship, your provider automatically has access to your organization's All devices group.

5. To send the relationship request to your provider, select **SEND**.

The Relationship agreement details page opens. The new agreement appears on the Relationships page with a pending status. Once the provider accepts the agreement, this status changes to active.

12.4 EDITING RELATIONSHIP DETAILS

The Relationship agreement details page lists the details of a relationship involving your organization. The page is composed of two sections, including relationship agreement details and shared groups.

The ability to update relationship details depends on your permissions and the relationship type. For example, depending on your role, you may be able to deactivate non-contractual relationships, or cancel pending relationships that are not yet accepted by the provider. Contractual relationships cannot be changed by the client or provider. Contact the Blackline Safety [Technical Support](#) to make changes or deactivate the relationship.

To edit a card, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To edit relationship details:

1. From the Relationship agreement details page, edit any of the following:

Relationship agreement card — view or edit the current details of the relationship including name, provider email, client, type, and status.



The screenshot shows a card with the following information:

- Relationship name: Blackline Safety Operations Center
- Contact email: soc@blacklinesafety.com
- Provider: soc@blacklinesafety.com
- Client: ACME Corp.
- Type: Contractual
- Status: Active (indicated by a green dot)

Shared groups card — manage the groups that the client is currently sharing with the provider.

12.5 DEACTIVATING A RELATIONSHIP AGREEMENT

To deactivate a relationship agreement:

1. From the user menu, select **Relationships**.
2. Select the relationship card of the agreement to be deactivated. The Agreement details page opens.
3. Select **DEACTIVATE**.

13 MANAGING DOCK

Dock is Blackline Safety's solution to gas sensor calibrating, bump testing and charging portable gas monitoring devices.

G7 Dock supports both G7c and G7x devices with single-gas, multi-gas diffusion or multi-gas pumped cartridges. For detailed information on G7 Dock, refer to the [G7 Dock Technical User Manual](#).

G6 Dock supports G6 devices. For detailed information on G6 Dock, refer to the [G6 Dock Technical User Manual](#).

The Docks page lists the G6 and G7 docks in your organization and their current configuration status. You can search and sort the list.

Docks

This page lists all of the docks you have access to. To update a dock's settings, click on the dock in the list below and edit its profile.

To see accurate inlet configuration settings, ensure G7 Docks are being updated by G7 devices running firmware version 3.402R1 or higher. To push a firmware upgrade to your organization, contact our Customer Care team.

Organization

ACME Corp.

G7, EXO, and Loner

G6

Search

Columns

DOCK NAME ↑	ACTIVATION CODE	DOCK ID	ORGANIZATION	CONFIGURATION STATUS
Office Demo Dock	6T27H1	13613	ACME Corp.	active
Warehouse H2S	RVW682	13698	ACME Corp.	active
Warehouse SO2	U8P52E	13651	ACME Corp.	active

13.1 VIEWING DOCKS

1. From the Main menu, select **Docks**. The Docks page opens.
2. Filter the list by dock type by selecting the **G7, EXO, and Loner**, or **G6** tab.
3. To open the Dock details page for a dock, select the **DOCK NAME** in the dock list.

13.2 EDITING DOCK CONFIGURATION DETAILS

Update dock details by editing the Dock configuration details page. The Dock configuration details page is composed of two sections, including the dock description and inlet settings.

To edit a card, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

To update dock configuration details:

1. From the Main menu, select **Docks**. The Docks page opens.
2. From the Docks page, select the dock you are interested in viewing. The Dock configuration details page opens.
3. **For G7 Dock:** From the Dock configuration details page, edit any of the following:
Dock description — view and manage basic information about the dock, including its name, assigned organization, ID, and activation code.

Dock name*

North shack dock

11/50

Organization

ACME Corp.

Activation code: **5EY9A5**

Dock ID: **1234**

Inlet settings and gas cylinder information — manage the dock’s inlet calibration gas settings (gas, gas concentration), inlet configuration status (pending update, active, failed), and gas cylinder information (lot number, expiry date, and notes).

G7 Dock has 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.

NOTE: Docks are pre-configured with common calibration gases when they are shipped out. You can update this configuration from the Inlet settings card.

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

Updated docks display on the Docks page with a Configuration status of pending update. To propagate the updated configuration settings to a dock, connect a device with the dock to be updated, then select **Update Dock** from the device menu.

Once the update is complete, the updated dock displays on the Docks page with a Configuration status of active and the dock can bump test and calibrate devices based on the new settings from Blackline Live. For more information, refer to the [G7 Dock Technical User Manual](#).

Inlets

Edit your inlet configurations and update them over-the-air.

Inlet configuration status: pending update ⓘ

1

⊘

▾

▾

▾

▾

Inlet setting

Gas	Concentration	
H ₂ S ▾	25	ppm
Gas	Concentration	
CO ▾	100	ppm
Gas	Concentration	
LEL - CH ₄ ▾	50	%LEL
Gas	Concentration	
O ₂ ▾	18	%vol

Gas cylinder

Lot number

015

Expiry date ⓘ

Additional notes

0/250

4. For **G6 Dock**: From the Dock configuration details page, view and edit any of the following:

Profile information — view and manage basic information about the dock, including its name, assigned organization, ID, and activation code.

The screenshot shows the 'Dock details' configuration page. At the top, it says 'Select *edit* to change the dock name or configure the gas type of each inlet. Changes made to this profile apply only to this specific dock.' Below this is a form with the following fields: 'Dock name' with the value 'Warehouse H2S' and a character count '13/50'; 'Organization' with the value 'ACME Corp.'; 'G7 Dock' (likely a typo for G6); 'Activation code' with the value '253KCW'; and 'Unit ID' with the value '13660'.

Inlet settings and gas cylinder information — manage the dock's inlet calibration gas settings (gas, gas concentration) and gas cylinder information (lot number, expiry date, and notes).

The settings for the gas inlet should exactly match the information provided on the gas cylinder it will be hooked up to. Discrepancies in settings cause tests from G6 Dock to fail.

Implement updates to G6 Dock configuration settings by connecting a G6 to the dock and updating the dock. After you have updated your inlet settings and updated G6 Dock, check your G6 Dock inlet settings to ensure that the update was successful. For more information, refer to the [G6 Dock Technical User Manual](#).

The screenshot shows the 'Inlet' configuration page. It starts with the heading 'Inlet' and the instruction 'Edit your inlet configurations and update them over-the-air.' Below this, it says 'Inlet configuration status: pending update' with a circular arrow icon. A yellow progress bar is shown. The page is divided into two main sections: 'Inlet setting' and 'Gas cylinder'. In the 'Inlet setting' section, 'Gas' is set to 'H₂S' and 'Concentration' is set to '25 ppm'. In the 'Gas cylinder' section, 'Lot number' is '4894038403493' and 'Expiry date' is '11 / 03 / 2021'. There is a 'Cylinder notes' text area and 'CANCEL' and 'SAVE' buttons at the bottom right.

Last profile change — view details about the last time the profile was updated, including when it was updated and who updated it.

Last profile change

Last profile change February 2, 2022
11:37 AM MST

Changed by Taelynn Graham
ACME Corp

14 MANAGING LOCATION BEACONS

You can set up location beacons 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 and EXO devices. When a G7 or EXO connects with the beacon, it assumes it is in the location the beacon is transmitting. This location is sent to Blackline Live in any communication G7 or EXO sends while it is in the vicinity of the beacon.



The Beacons page lists the location beacons in your organization, their locations, and last communication date.

Beacons						
Organization ACME Corp.						
Search Items per page: 20 Page: 1 / 1						
BEACON NAME	BEACON ID	ORGANIZATION ↑	STREET ADDRESS	COORDINATES	LAYER	LAST COMMUNICATION DATE
North shack beacon	58552112340	ACME Corp.	--	51.5855211,-114.585...	Persistent	2 mins ago
East shack beacon	115	ACME Corp.	--	51.0380453,-114.032...	Persistent	5 mins ago
East worksite	1369000061	ACME Corp.	--	51.1369000,-114.136...	Persistent	1 min ago
West worksite	1369000059	ACME Corp.	--	51.1369000,-114.136...	Persistent	2 mins ago
Break tent beacon	1369100255	ACME Corp.	--	51.1369000,-114.136...	Persistent	11 mins ago

14.1 VIEWING LOCATION BEACONS

To view the beacons configured for your organization:

1. From the Main menu, select **Beacons**. The Beacons page opens.

2. To open the Location beacon details page for a dock, select the **BEACON NAME** or **BEACON ID** in the beacon list.

14.2 PLACING LOCATION BEACONS

Placing beacons in the correct location in Blackline Live can decrease the response time to team members in need of assistance.

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

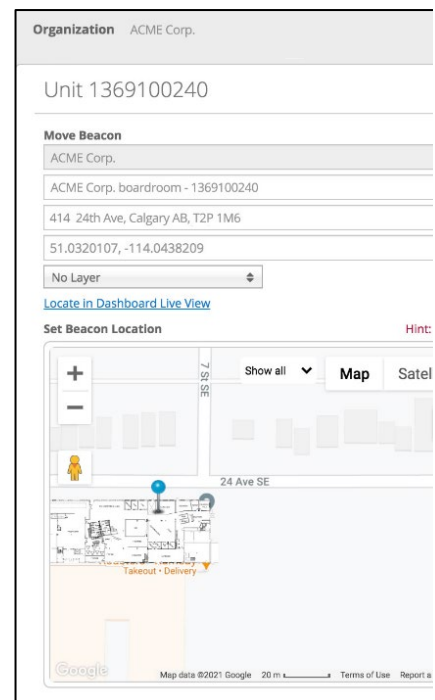
To place a location beacon:

1. From the Beacons page, select the location beacon you wish to update to Blackline Live. The Beacon configuration details page opens.
2. Update the beacon name. Enter a recognizable name (e.g., Control Room or North Gate).
3. Enter the street address for the beacon.
4. Set an initial location of the beacon by entering a set of latitude and longitude coordinates in decimal format. The location beacon map pin automatically updates to the coordinates entered.
5. **If you are using floorplans:** Select the layer that corresponds with the floorplan the beacon is on.

NOTE: Placing location beacons with respect to floorplan layers can provide accurate location information in multi-story buildings.

If you are not using floorplans, select **No Layer**.

6. After you enter map coordinates, you can drag the pin on the map to get an even more accurate location:
7. Select the blue beacon pin.
8. Drag the pin to where it is positioned in your building.
9. Select **Save**.



15 MANAGING FLOORPLANS AND MAP OVERLAYS

You can display floorplan or site-plan images, as well as Google Earth KML or KMZ files (including embedded information) on your Blackline Live map. Floorplans and map overlays, in combination with location beacons, help monitoring agents see precisely where an alert is occurring and reduce response time for emergency responders.

15.1 FLOORPLANS

Floorplan images show detailed views of a building layout, including rooms, hallways, and doors on the map.

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

For information on adding or updating information related to floorplans or map overlays for your organization, contact your sales representative or Blackline Safety [Technical Support](#).

Make sure that the floorplan files you provide to Blackline Live for implementation:

- 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.

15.2 MAP OVERLAYS

You can display Google Earth KML or KMZ files with embedded information in Blackline Live. These files can display building or zone perimeters or mark out important site resources like first-aid kits or fire hydrants.

Google Earth files can be created through professional GIS software, or for free using Google’s My Maps tool. You can create lines, shapes, or markers and place them directly on a map. Once the assets are created, you can export them as a KML file for implementation on the map.

For information on adding or updating information related to a map overlay for your organization, contact your sales representative or Blackline Safety [Technical Support](#).

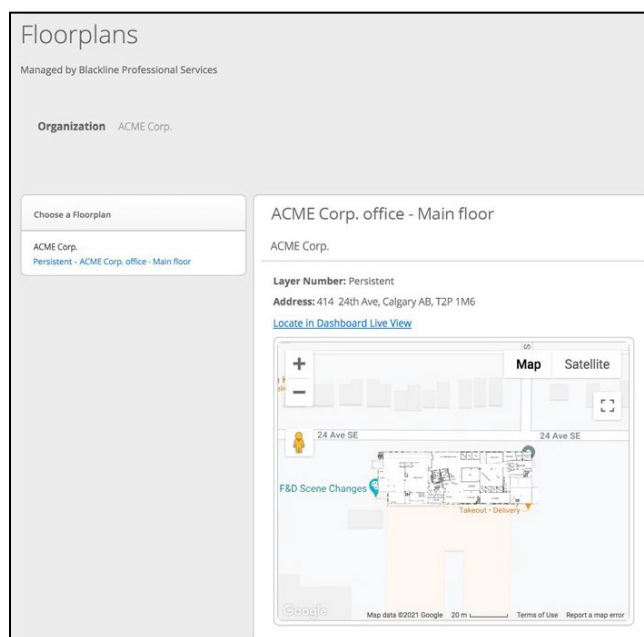
15.3 VIEWING FLOORPLANS AND MAP OVERLAYS

The Floorplans page lists the floorplan name, site address, and the map layer it is placed on. You can search and sort the list.

Floorplans			
Organization ACME Corp.			
Search		Items per page: 20	Page: 1 / 1
		Display	
FLOORPLAN NAME	ORGANIZATION	LAYER	STREET ADDRESS
ACME Corp. office	ACME Corp.	Persistent	ACME Corp. office
Alpha site plan	ACME Corp.	Persistent	Alpha site
Alpha Facility Main floor	ACME Corp.	1	123 Alpha Str.
Alpha Facility 2nd floor	ACME Corp.	2	123 Alpha Str.
Beta site plan	ACME Corp.	Persistent	803 24 Ave SE #100, Calgary, AB T2G...
Blackline Office	ACME Corp.	Persistent	Beta site

To view available floorplans:

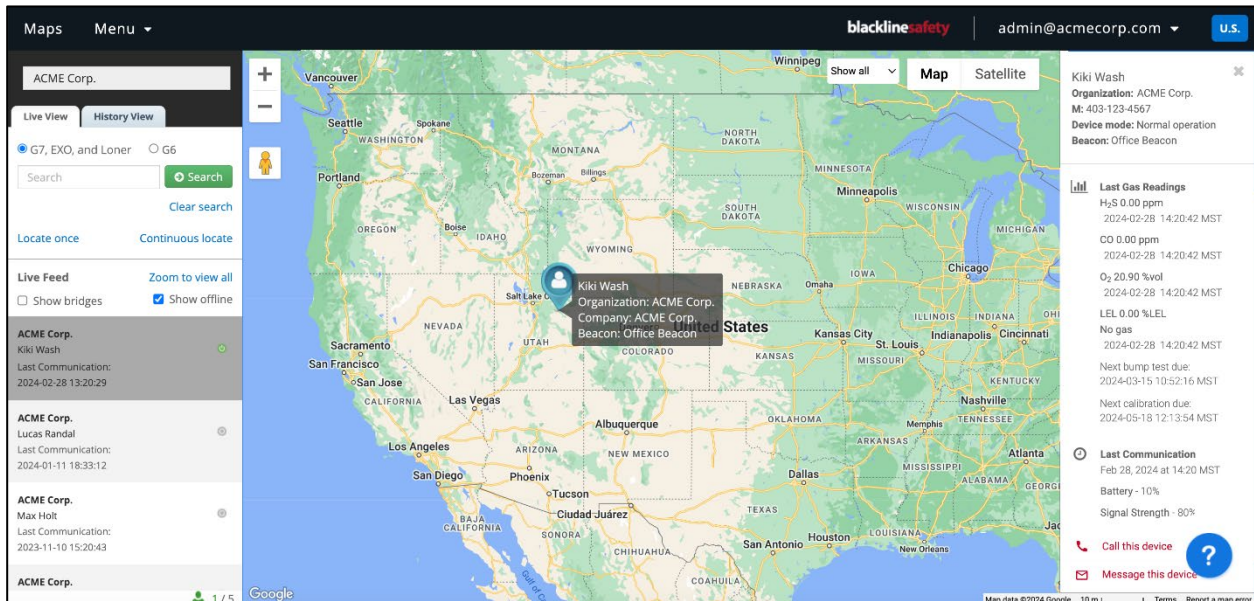
1. From the Main menu, select **Floorplans**. The Floorplan page opens.
2. To open the Floorplan details page, select the **FLOORPLAN NAME** in the list. The Floorplan details page opens.



- To view the floorplan on the Blackline Live map view, select **Locate** in Dashboard Live View.

16 MAPS

Blackline Live provides tools for live monitoring, as well as retroactive review and reporting.



Maps (Live view)

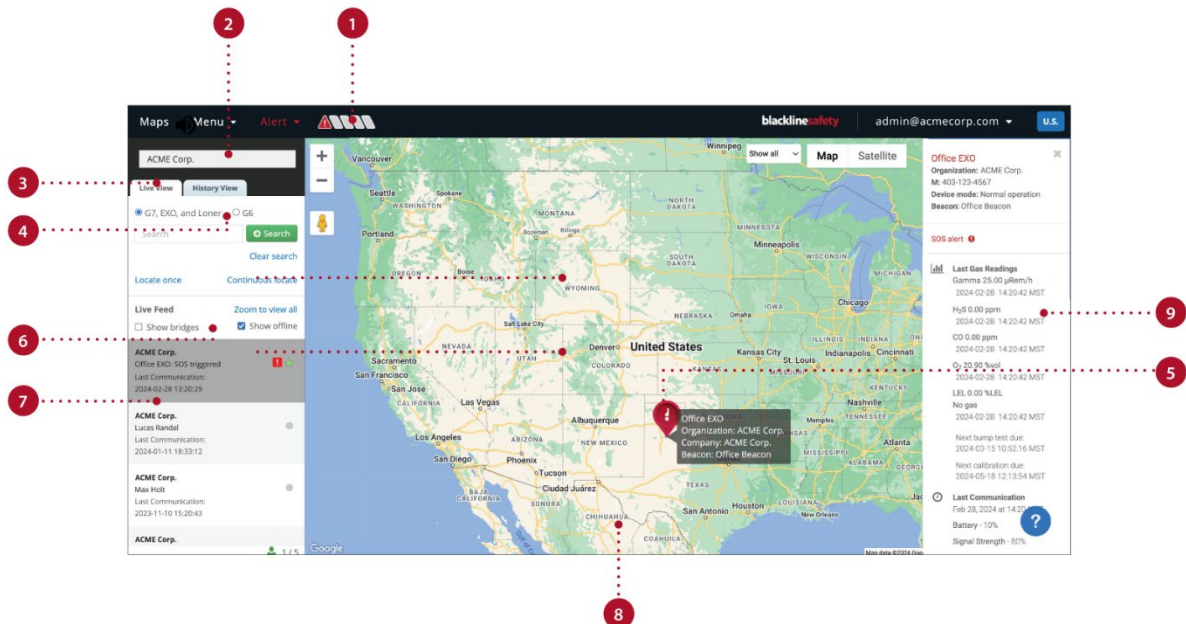
The Maps Live view displays the last known location of online devices and is useful for monitoring the current status and location of your fleet.

Maps (History view)


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

16.1 MAPS (LIVE VIEW)

Use the Maps page (Live view) to view the current locations, statuses, and details about your device fleet, including both online and offline devices.



The Maps page (Live view) includes the following features:

- 1 The alert banner indicates any devices that may be in alert. This banner is visible on every page.
- 2 The Live View menu panel enables you to search, filter, and select the devices displayed on the Live map view.
- 3 Display either the Live map view or Historical map view.
- 4 Display either G7, EXO, and Loner devices, or G6 devices on the Live map view.
- 5 Map pins show the location and status of a device on the map.


Different device types are represented on maps as pins with a symbol in the middle.



The color of the map pins indicates the current state of the device. Devices in alert automatically display 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 five minutes, while G7x is 30 minutes, as it is typically communicating over satellite. When the device is travelling, the map pin indicates which direction it is travelling in.

6

Display disconnected devices on the Live map view.

NOTE: G6 devices display as disconnected by default.

7

The Live View tab displays the most active devices at the top of the device list.

8

The Maps Live view displays the last known location of online devices and is useful for monitoring the status and location of your organization's devices. You can navigate, minimize, and enlarge the map display as needed.

9

The Info panel displays detailed information about the selected device.

16.1.1 LOCATING DEVICES

By default, the Live map view displays G7, EXO, and Loner, or G6 devices in your organization. You can search and filter the device list to locate specific devices on the map.

Live View

History View

☒ G7, EXO, and Loner
 ☐ G6

➔ Search

[Clear search](#)

[Locate once](#)
[Continuous locate](#)

To locate a single device:

1. In the Live map view menu panel, type a search term into the **Search** field. The device list displays units matching the search criteria.
2. To highlight the map pin showing the last recorded location of the device, and open the Info panel for a device, select it from the device list in the left panel.
3. **For G7 devices only:** Select **Locate once** to receive a single update on the device's location or select **Continuous locate** to receive updates every five seconds for 10 minutes.

To locate a group of devices:

1. To filter based on device type in the Live map view menu panel, select either **G7, EXO, and Loner**, or **G6**.
2. To display only disconnected devices, select **Show offline**.
3. To display G7 Bridges, select **Show bridges**.

16.1.2 ACCESSING THE DEVICE INFO PANEL

To access device information using Live Map View:

1. In the Live map view menu panel, select a device from the list to highlight it on the map and open the device Info panel.

For G7: The panel displays the following device information (as available):

- Assigned username or ID, or the device's name or ID
- **NOTE:** The device's display name varies depending on what information is available. If the device is assigned, the info panel lists the assigned user's name, or their ID if a name is not available. If the device is not assigned, the info panel lists its name, or ID if a name is not available.
- Assigned organization
- Company
- Location Beacon
- Team member's mobile phone number
- Last message sent to or from the device
- Last known location (timestamp, address, geographic coordinates)
- Current gas readings, and whether a pump cartridge is currently running
- Last communication to Blackline Live (timestamp, speed, battery level, signal strength)

In addition, the panel:

- Lets you message (✉) or call (☎) the device.

NOTE: An alert must be created to take either of these actions. 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 two-way call with the device.

Boardroom device

Organization: ACME Corp.

Device mode: Normal operation

Beacon: Churchill Falls - 1369100243

✕

✉ Last Message

Jan 11, 2019 at 08:07 MST

Understood

📍 Last Location

Jan 08, 2021 at 13:52 MST

Approximate Address

414 24th Ave, Calgary AB, T2P 1M6

Latitude / Longitude

51.0320537, -114.0435443

📊 Gas Readings

H₂S 0.00 ppm

2021-01-08 13:52:46 MST

Next bump test due:

2019-03-28 11:02:06 MDT

Next calibration due:

2020-05-27 10:59:41 MDT

🕒 Last Communication

Jan 08, 2021 at 13:52 MST

Speed - 0 km/h

Battery - Charging

Signal Strength - 100%




☎ Call this device

✉ Message this device

📅 View today's history

⚙ ACME Corp. demo

⚠ ACME Corp. demo

- Displays the device's alert profile () and assigned configuration profile (). Selecting either of these links opens the respective profile page.
- Lets you view a device's daily history (). Selecting the link directs you to the device in the map history view.

For **G6**: The panel displays the following device information (as available):


- Assigned username or ID, or the device's name or ID


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

- Organization
- Assigned user's mobile phone number
- Gas readings (timestamp, next bump test due date, next calibration due date)
- Last communication to Blackline Live (timestamp, battery level, signal strength)

In addition, the panel:

- Lets you activate **Find my G6**.

Lets you view a device's daily history (). Selecting the link directs you to the device in the map history view.

- Displays the device's assigned configuration profile (). Selecting the configuration profiles opens the Configuration profile page.

Kiki Wash

Organization: ACME Corp.
M: 403-123-4567

Gas readings

H2S 0.00 ppm
2022-05-06 15:38:44 MDT

CO 0.00 ppm
2022-05-06 15:38:44 MDT

O2 20.90 %vol
2022-05-06 15:38:44 MDT

LEL 0.00 %LEL
No gas
2022-05-06 15:38:44 MDT

Next bump test due:
2022-05-06 15:29:34 MDT

Next calibration due:
2022-05-06 15:29:34 MDT

Last Communication

May 06, 2022 at 15:38 MDT

Battery - 60%

Signal Strength - 80%

Find my G6

View today's history

Configuration profile

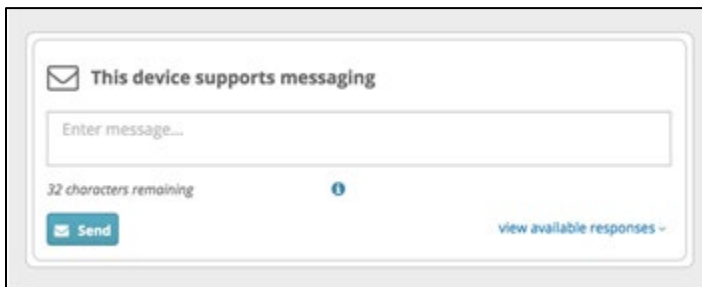
16.1.3 MESSAGING A G7 DEVICE

You can send a message to a specific device.

NOTE: If you message a device, an alert is automatically created.

To message a device:

1. Open the device's Info panel, then select **Message this device**.
An alert is automatically created and the Alert management page for the device opens.
2. Enter a message, then select **Send**.

A screenshot of a web interface for messaging a device. At the top, there is a header with an envelope icon and the text "This device supports messaging". Below this is a text input field with the placeholder "Enter message...". Under the input field, it says "32 characters remaining" and there is a small blue information icon. At the bottom left is a blue button with a white envelope icon and the text "Send". At the bottom right is a link that says "view available responses" with a downward arrow.

To optimize your message, view the responses a device has by selecting **view available responses**.

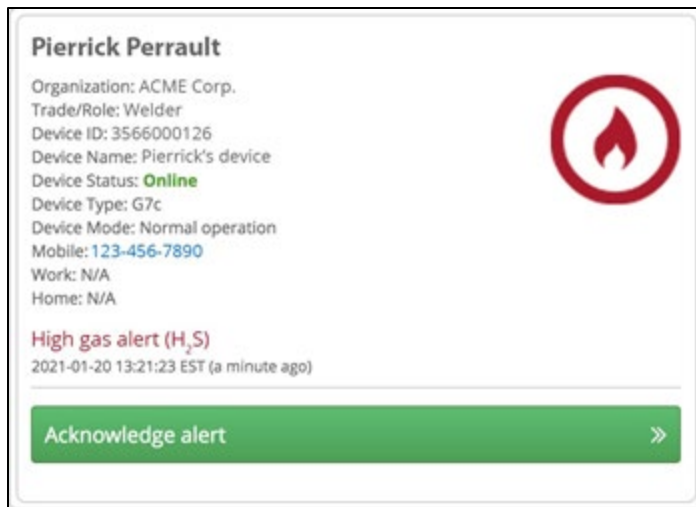
16.1.4 CALLING A G7 DEVICE

You can initiate a two-way call with a device.

NOTE: If you call a device, an alert is automatically created.

To call a device:

1. Open the device's Info panel, then select **Call this device**.
An alert is automatically created and the Alert management page for the device opens.
2. Initiate a two-way call using the phone number assigned to the device.



16.1.5 ACCESSING A DEVICE'S CONFIGURATION PROFILE

To access a device's configuration profile:

1. Open the device's Info panel, then select the device's configuration profile.



The Configuration profile detail page opens, displaying the device's details. For more information on the configuration profiles, see section 9.1.

16.1.6 ACCESSING A G7 DEVICE'S ALERT PROFILE

To access a device's alert profile from the Map:

1. Open the device's Info panel and select the device's alert profile.



The Alert management profile page opens, displaying the device's details. For more information on the alert profiles, see section 10.1.

16.1.7 ACCESSING A DEVICE'S HISTORY

To access a device's history:

1. Open the device's Info panel, then select **View today's history**.



The Map (Historical View) opens, displaying the device's historical information for the previous 24 hours. For more information, see section 16.2.1.

16.1.8 FINDING A G6 DEVICE

Use Find my G6 to locate missing G6 devices. Devices with this feature toggled on communicate their locations to Blackline Live every 30 minutes for 2.5 hours.

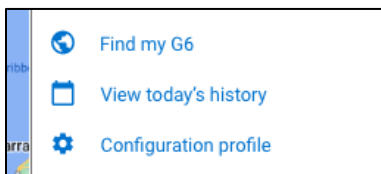
NOTE: Increasing the frequency that G6 connects to Blackline Live reduces a device's battery life.

To turn on Find my G6:

1. In the Live map view, locate then select the missing G6 device.

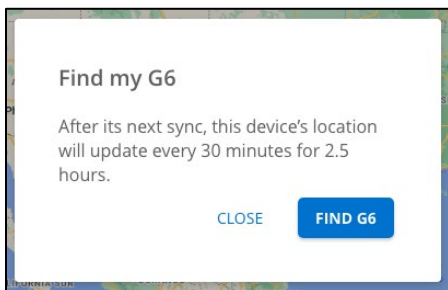
Search for specific G6 devices. The device's info panel opens, displaying the last known details for the device. The device location pin indicates the device's location the last time it connected to Blackline Live.

2. In the selected device's Info panel, select **Find my G6**.



The Find my G6 dialog box opens, informing you that the device connects to Blackline Live every 30 minutes while find my G6 is turned on.

3. To confirm your selection, select **Find G6** in the Find my G6 dialog box.

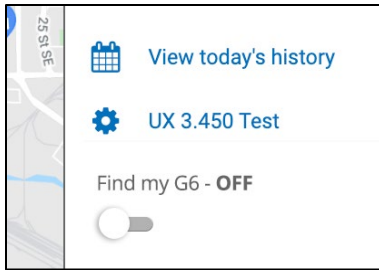


To turn off Find my G6:

1. In the Live map view, locate then select the G6 device.

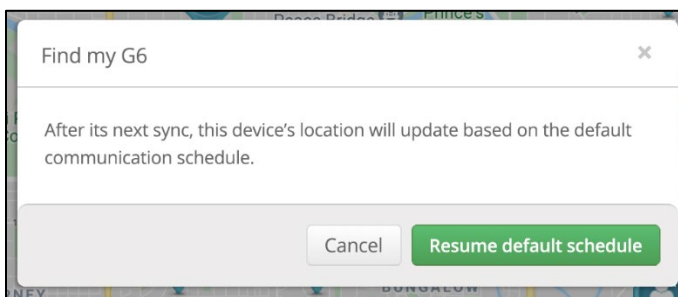
The device's Info panel opens, displaying the last known details for the device. The device location pin indicates the device's location the last time it connected to Blackline Live.

2. In the selected device's Info panel, toggle off **Find my G6**.



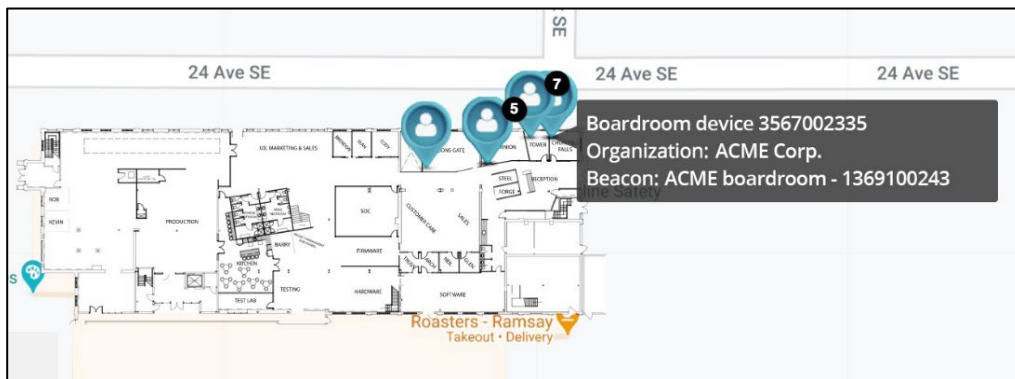
The Find my G6 dialog box opens, informing you that the device will resume its default communication schedule with Blackline Live.

- To confirm your selection, select **Resume default schedule** in the Find my G6 dialog box.

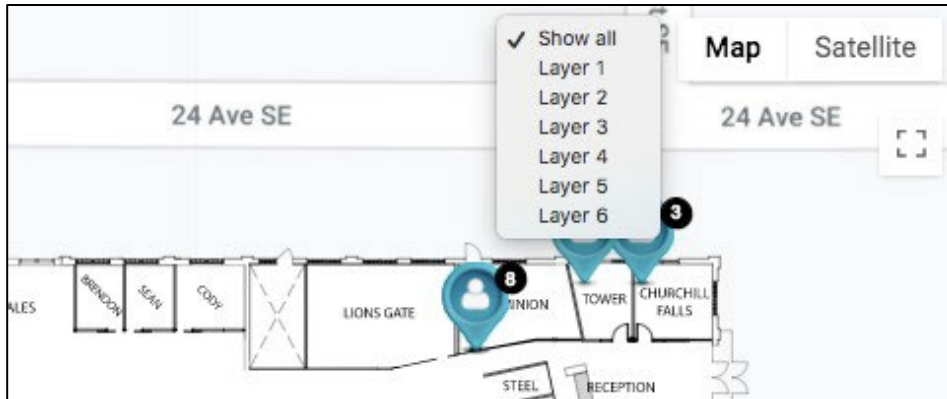


16.1.9 DISPLAYING FLOORPLANS

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



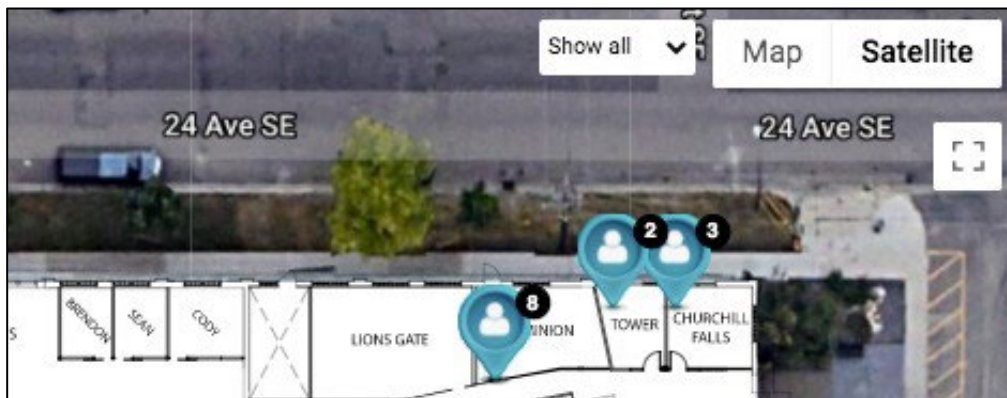
If your organization uses layered floorplans, you can also filter the map view to a particular layer. When filtered, only floorplans and devices communicating with beacons on this layer are displayed.



NOTE: If you see a device displayed in a strange location on the floorplan, check if it is communicating with a nearby beacon that may not have an updated location.

16.1.10 DISPLAYING SATELLITE IMAGERY

By default, Blackline Live displays a simplified map view. You can toggle the map to a satellite view to see your floorplans and devices overlaid on detailed satellite images. For workforces operating in remote areas, satellite imagery provides geographical details and landmarks that may not be displayed in the simplified map view.



To display satellite imagery:

1. On the Map view, select **Satellite**.

16.2 MAPS (HISTORICAL VIEW)

If 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. The page also provides several tools for viewing historical data and analytics information:

The screenshot shows the Blackline Safety Maps (Historical View) interface. The main map displays the United States with a location pin for 'Kiki Wash' in the Midwest. A date range selector is open, showing February 2024. A sidebar on the right displays device details and gas readings.

Device Details:

- Organization: ACME Corp.
- M: 403-123-4567
- Device mode: Normal operation
- Beacon: Office Beacon

Last Gas Readings:

Gas Type	Reading	Time
H ₂ S	0.00 ppm	2024-02-28 14:20:42 MST
CO	0.00 ppm	2024-02-28 14:20:42 MST
O ₂	20.90 %vol	2024-02-28 14:20:42 MST
LEL	0.00 %LEL	2024-02-28 14:20:42 MST

Last Communication:

- Feb 28, 2024 at 14:20 MST
- Battery - 10%
- Signal Strength - 80%

Map Data: ©2024 Google, INEGI 200 km

16.2.1 ACCESSING DEVICE INFORMATION IN THE MAP HISTORY VIEW

To access device information in the Map history view:



1. From the Maps page, select the **History View** tab.
2. Select a device in the Map.
3. To set a time interval to review for the selected device, select **Date Range**.

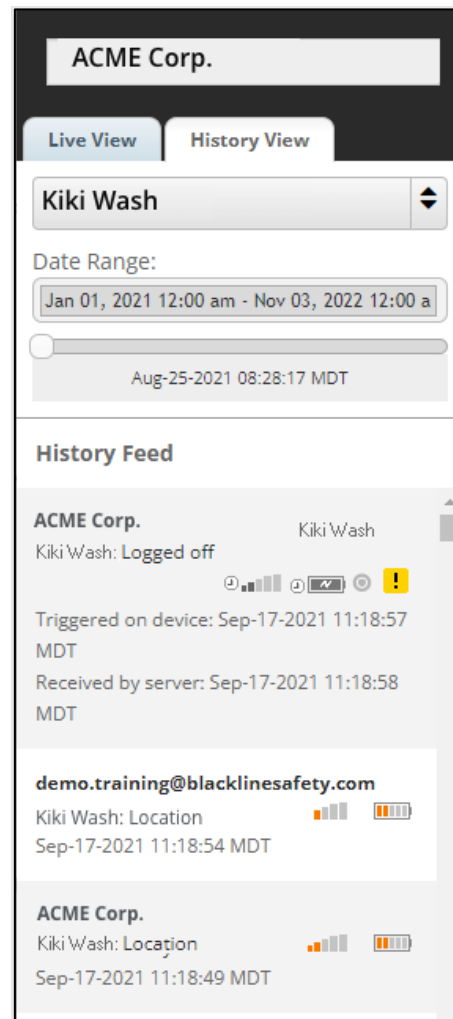
Once the data has loaded, a list of device messages to Blackline Live that occurred during the specified time interval displays.

If enabled, the list includes AlertLink messages and indicates whether the message was sent to or cleared on the device.

Notifications are marked with a  or .

Examples of notifications include gas exposures, compliance reminders, or alerts.

For G7 devices, check-in events and message events have their own icons to differentiate them — a check-in has an  icon, while a message has an .



16.2.2 NAVIGATING DEVICE EVENTS IN THE MAP HISTORY VIEW

To navigate device events in the Map history view:

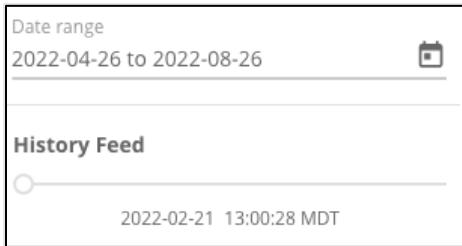
1. Rest your cursor over the event icon to view the device event summary.

NOTE: For EXO devices, if you have automatic bump tests and calibrations enabled and a bump test or calibration is completed on the device, the device summary indicates if it was initiated automatically by EXO or if it was performed manually by a device user.

2. Select the event to see where it occurred on the map (if a location is available).

Selecting the event also opens the device's Info panel, displaying detailed information about the device at the time of the event.

3. Select the **History Feed** to view the device location for the specified time interval.



As you drag the slider through the specified time interval, a marker displays on the map for each logged location of the device.

17 FLEET HEALTH DASHBOARD

The live dashboard provides a snapshot of the compliance of your entire fleet. Devices that are non-compliant are listed with a description of the issue and the recommended resolution.

The Compliance Dashboard page is composed of two sections, including fleet health and suggested maintenance.

To view the Fleet health dashboard:

1. From the Main menu, select **Dashboard**.
2. On the Fleet health dashboard, review any of the following information:
Fleet Health — the Fleet health card displays an overview of the compliance and performance of your device fleet. You can print the information displayed or download it as a JPEG, SVG, or PDF.




Suggested Maintenance — the suggested maintenance card displays a list of devices that require maintenance and the maintenance they require (e.g., bump test, calibration, firmware update, hardware repair). The list displays the current Status, Issue, Assigned team member, Device ID, Organization, and Resolution.

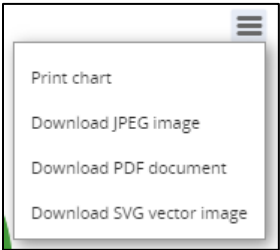
Suggested Maintenance

Review the issues concerning your fleet's health and take action with suggested resolutions.

STATUS	ISSUE	ASSIGNED TEAM MEMBER	DEVICE	ORGANIZATION	RESOLUTION
offline	Calibration due	Arturo Chmela	3567002328	ACME Corp.	Perform calibration.
offline	Bump test due	Fatimah Nieves	3567002328	ACME Corp.	Perform bump test.
offline	Bump test due	Mette Cloutier	3973003947	ACME Corp.	Perform bump test.
offline	Cartridge missing or improperly connected	Chaz Harman	3567002343	ACME Corp.	Connect or reconnect cartridge. Power cycle device. If error persists, replace cartridge.
offline	Cartridge missing or improperly connected	Willie Scrivener	3567002321	ACME Corp.	Connect or reconnect cartridge. Power cycle device. If error persists, replace cartridge.
offline	Cartridge missing or improperly connected	Cara Waller	3973003932	ACME Corp.	Connect or reconnect cartridge. Power cycle device. If error persists, replace cartridge.
offline	Calibration due	Leon Breiner	3973003929	ACME Corp.	Perform calibration.
offline	PID failed calibration in dock 2033. Sensitivity range error	Atiya Ahmed	3973003946	ACME Corp.	Check gas cylinder pressure and concentration. Retry calibration. If error persists, replace cartridge.

To download fleet health information from the Fleet health dashboard:

- From the Fleet health dashboard page, in the Fleet health section, select .
- Select the desired download format from the shortcut menu.



To access device details from the dashboard:

1. From the Compliance Dashboard page, in the Suggested maintenance section, select the device of interest.

The Device details page opens. For more information on configuring devices using the Device details page, see section 7.

18 COMPLIANCE CERTIFICATES

Blackline Live displays bump test and calibration certificates for tests that have been completed on a particular device.

The certification page shows a device's most recent bump test and calibration results. It lets you view up to 125 days (U.S.) or 7 days (Europe) of device history.

NOTE: The Certification page is hosted independently from Blackline Live. You can access the page without being an account user.

18.1 VIEWING BUMP TEST AND CALIBRATION CERTIFICATES

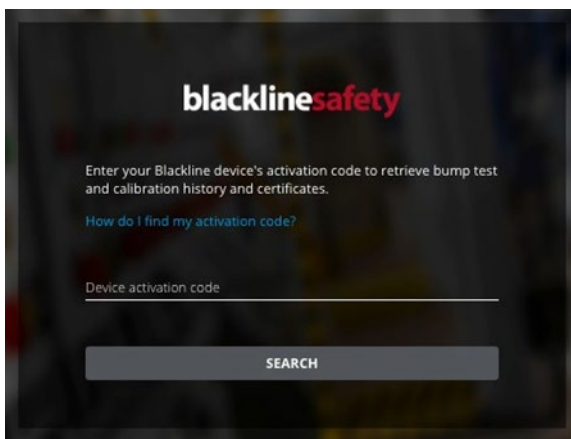
To view bump test and calibration certificates:

1. Depending on the Blackline Live domain you are accessing, navigate to one of the following pages:

North America (NA): <https://live.blacklinesafety.com/certs/>

Europe (EUR): <https://eu.live.blacklinesafety.com/certs/>

United Arab Emirates (UAE): <https://uae.live.blacklinesafety.com/>



2. On the sign-in page, enter the activation code of the device. The activation code can be found on the label located on the back or side of your device.

The Bump test and calibration certifications page opens, displaying when the device was last bump tested and calibrated.

Bump test and calibration certifications

This page collects information about bump tests and calibrations performed on your G7 device. You can view the last bump test or calibration performed, or see a list of all tests from the last 125 days. Clicking on a particular test will open a full overview, which can then be printed.

Device: **3566000123** | 123ABC

Timezone
(-0700) MST - Edmonton

Last bump test

DATE/TIME	TEST TYPE	TEST RESULTS	CARTRIDGE ID
2020-11-24 08:00:05 MST	Bump Test	Pass	10123

Last calibration

DATE/TIME	TEST TYPE	TEST RESULTS	CARTRIDGE ID
2020-11-24 08:04:34 MST	Calibration	Pass	10123

LOAD MORE

To view more test results, select **LOAD MORE**. The tests that were performed within the last 125 days (U.S.) or seven days (Europe) display.

NOTE: To view older tests, contact Blackline Safety [Technical Support](#).

Test archive

Showing test results from the last 125 days. Contact Blackline for tests that took place over 125 days ago.

Search Date Test type All test types Items per page: 20 Page: 1 / 1

DATE/TIME	TEST TYPE	TEST RESULTS	CARTRIDGE ID
2020-11-24 08:04:34 MST	Calibration	Pass	10123
2020-11-24 08:00:05 MST	Bump Test	Pass	10123
2020-10-08 10:26:10 MDT	Bump Test	Pass	10123

- To view a summary of a specific test, select the timestamp **DATE/TIME** of the test.

The summary displays the following information:

- Device ID
- Device activation code
- Date and timestamp
- Cartridge ID (G7 only)
- Type of test (bump test or calibration)
- Dock ID (if applicable)
- Overall test result
- Hardware test results
- Sensor test results (including readings)

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.

G7 Certificate:

3566000123
123ABC

2020-11-24 08:00:05 MST
Bump Test
Cartridge ID: 10123
Dock ID: 1234
Test result: **Pass**
Lights test result: **Pass**
Vibrator test result: **Pass**
Sound test result: **Pass**
Sensor test results: **Pass**
A bump test has passed when the sensor detects 50% of the calibration concentration.
Bump test readings
H₂S: **Pass**
CO: **Pass**
O₂: **Pass**
LEL: **Pass**
H₂S: 17.7 ppm
CO: 91 ppm
O₂: 19.2 %vol
LEL: 43 %LEL

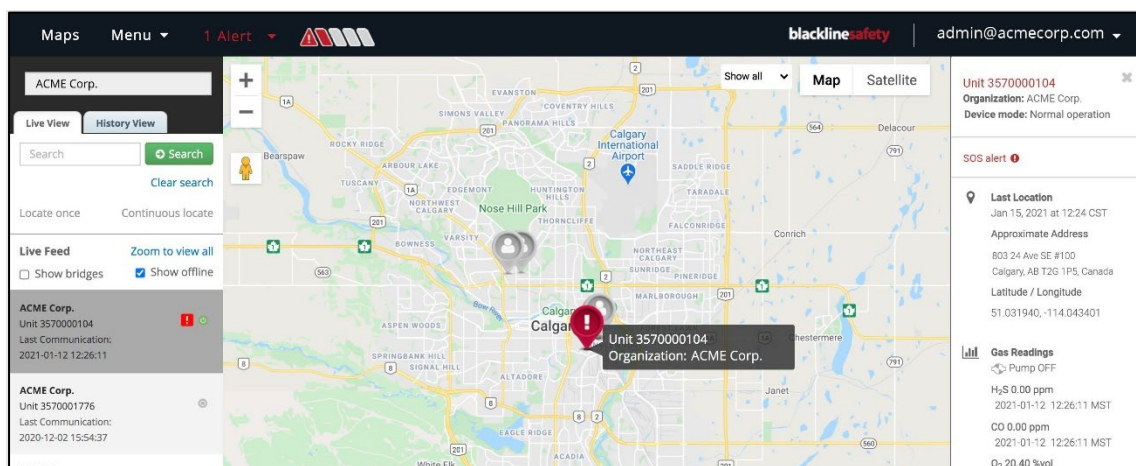
G6 Certificate:

3570001775
Q4TJ7K

2021-05-25 15:29:34 MDT
Bump Test
Dock ID: 1432
Test result: **Pass**
Lights test result: **Pass**
Vibrator test result: **Pass**
Sound test result: **Pass**
Sensor test results: **Pass**
A bump test has passed when the sensor detects 50% of the calibration concentration.
H₂S: **Pass**

19 G7 AND EXO DEVICE ALERTS

When a G7 or EXO device goes into alert, Blackline Live informs you with a notification in the navigation bar and a loud siren sound. The device in alert displays with a red map pin on the Maps page and at the top of the left-hand sidebar. You can use the Alerts page to view device alerts and AlertLink messages.



A yellow warning banner beneath the navigation bar means your current audio settings are blocking the alert siren sound. Select the link in the banner for troubleshooting tips for your browser and operating system.

NOTE: Alerts from G6 devices are not displayed in the Alerts page, do not trigger the Alert banner in Blackline Live, and do not have any alert histories or alert management pages associated with them. For more information on G6 notifications, see section 20.

19.1 VIEWING DEVICE ALERTS

On the Alerts page, the Alerts tab lists all alerts and indicates the status and type of alert, when the alert occurred, the device type and ID, and the device's assigned user.

DATE/TIME ↓	STATUS	ALERT TYPE	ASSIGNED TEAM MEMBER	DEVICE ID	DEVICE NAME	ORGANIZATION	OPERATOR	RESOLUTION REASON
2021-01-19 15:00:25 MST	Unacknowledged	High threshold detected (H ₂ S)	Pierrick Perrault	67c: 3566000126	Pierrick's device	ACME Corp.	--	--
2021-01-19 13:27:23 MST	Resolved	Missed check-in detected	Pierrick Perrault	67c: 3566000126	Pierrick's device	ACME Corp.	Blackline Safety Operations Centre	False Alert without Dispatch

To view recent device alerts:

1. From the Main menu, select **Alerts**. The Alerts page opens.

By default, the Alerts page displays alerts that occurred within the last 24 hours. This time filter is useful for Account users who need to see and manage alerts that are currently active.

To view device alerts for a specified date and time interval:

1. From the Alerts page, select **Showing last 24 hours**.

View alerts that occurred in a specific date and time range. This view will filter out any new alerts that come in. This date range can be cleared from the alerts list to go back to the default 24-hour view.

Start date
2/19/2022 00:00:00

to

End date
6/24/2022 23:59:59

CANCEL SET DATE AND TIME

2. In the date and time dialog, select a **Start date and time** and **End date and time**.
3. Select **SET DATE AND TIME** to view alerts for the specified interval in the Alerts page.

To clear the specified time interval, select **Clear date range**.

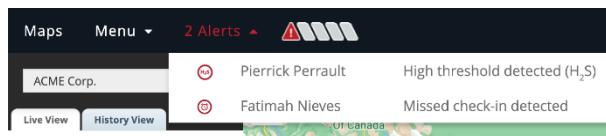
19.2 VIEWING ALERT DETAILS

To view alert details:

1. Do one of the following:
 - From the Alerts page, select the **Date/Time** or the **Alert type** from the list of alerts:

DATE/TIME	STATUS	ALERT TYPE	ASSIGNED TEAM MEMBER	DEVICE ID	DEVICE NAME	ORGANIZATION	OPERATOR	RESOLUTION REASON
2021-01-19 15:00:25 MST	Unacknowledged	High threshold detected (H ₂ S)	Pierrick Perrault	67c1 3566000126	Pierrick's device	ACME Corp.	---	---
2021-01-19 13:27:23 MST	Resolved	Missed check-in detected	Pierrick Perrault	67c1 3566000126	Pierrick's device	ACME Corp.	Blackline Safety Operations Centre	False Alert without Dispatch

- Select the animated Alert banner at the top of the Blackline Live window and select the alert from the dropdown list.



2. If the alert is **active** (with an unacknowledged or acknowledged status), the Alert management page opens. The Alert management page displays live information about the alert and enables you to access tools designed to help manage and resolve the alert.

Alert management

Pierrick Perrault

Employee ID: 1245
Company: ACME Corp.
Organization: ACME Corp.
TradeRole: Technician
Device ID: 3566000126
Device Name: Unit 3566000126
Device Status: Online
Device Type: G/L
Device Model: Normal operation
Mobile: 123-456-7890
Work: N/A
Home: N/A

High threshold detected (LIL)

2025-01-28 13:12:13 MST to minute ago

Choose a reason for resolving...

Resolve alert

No prior alerts in the past 24 hours.

This device supports messaging

Enter message...

22 characters remaining

Send

view available responses

Add a note...

Post Note

ACME Corp.
2025-01-28 13:12:19 MST
Alert received by server.

ACME Corp.
2025-01-28 13:12:50 MST
Alert triggered on device.

Store Note

Map

Satellite

United States

Mexico

Guatemala

Nicaragua

Costa Rica

Panama

Venezuela

Sensor configurations

Devices configured high and low sensor thresholds.

view settings

Protocol

Contacts

Notified

Emergency response protocol

This is the protocol for responding to alerts on Blackline Live. Follow the protocol closely and refer to the Contacts tab for detailed emergency contact information.

Protocol for G/L with Gas "EVALUATION"

*** THIS IS AN EVALUATION ACCOUNT. DO NOT DISPATCH UNLESS REQUESTED ***

SOS Alert/fall detection/No motion/Missed Check-in

STEP 1: Send a message to the G/L device. "Do you need help?", wait 2 minutes.

If no response after 2 minutes, proceed to STEP 2.

STEP 2: Call the G/L device

If no answer, call the phone number assigned to the user.

If still no answer, proceed to STEP 3.

STEP 3: Contact emergency contacts in order of priority. Once someone is reached, provide emergency contact the following information:

Full name of the employee.

3. If the alert is **Resolved**, the Alert history page opens, which displays a snapshot of the device's state when the alert occurred, and information regarding how and when it was resolved. For more information, see section 19.7.

19.3 ACKNOWLEDGING ACTIVE ALERTS

The Alert management page is used to manage and respond to active alerts.

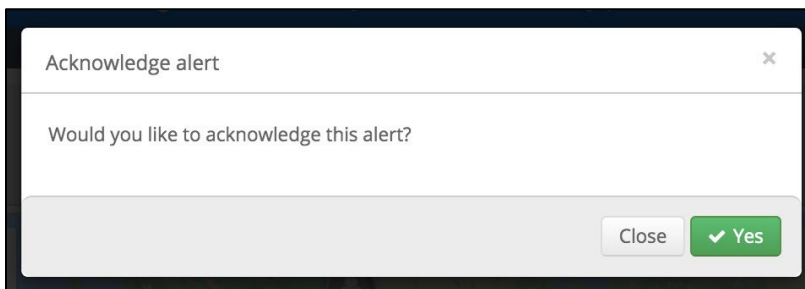
If your organization is self-monitored, or if your organization uses Blackline Live to monitor other organizations, your Account users are responsible for managing and responding to alerts.

If your organization is monitored by Blackline Safety's SOC or another monitoring service, do not try to manage active alerts. Giving Account users the **Contact admin**, **View only**, or **Analytics only** roles prevents them from interacting with alerts. For more information, see section 3.3.3.

To acknowledge an active Alert:

When you view an active, unacknowledged alert, you are prompted to acknowledge the alert.

1. In the Acknowledge alert dialog box, select **Yes**. The Alert management page opens.

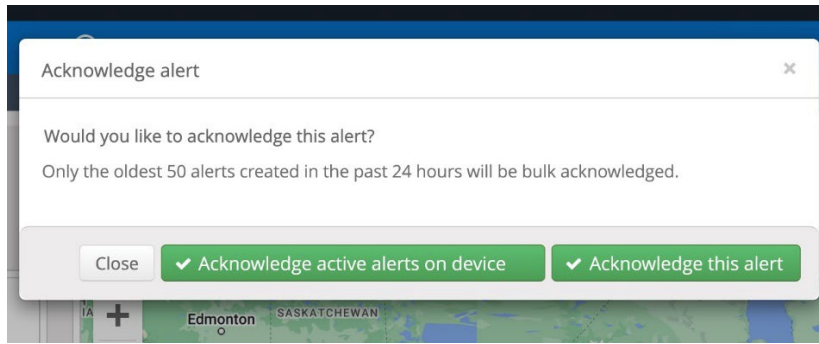


Acknowledging the alert signifies that you are taking responsibility for following the alert protocol and ensuring the safety of the device user. Acknowledging the alert causes the blue LiveResponse light to activate on the affected device and indicates to the device user that someone is investigating the alert, and that help is on the way.

During an event, multiple alerts may be activated by the same device within a short period of time. Your Account users can acknowledge multiple associated alerts at the same time. To learn more about managing associated alerts, see [Resolving Alerts](#).

To acknowledge associated alerts:

1. In the Acknowledge alert dialog box, select **Acknowledge all active alerts on device**. The Alert management page opens.



19.4 MANAGING ALERTS

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.

Alert management

Pierrick Perrault

Employee ID: 1245
Company: ACME Corp.
Organization: ACME Corp.
Trade/Role: Technician
Device ID: 3566001234
Device Name: Unit 3566001234
Device Status: **Online**
Device Type: G7c
Device Mode: Normal operation
Mobile: 123-456-7890
Work: N/A
Home: N/A

High threshold detected (LEL)
2025-01-28 13:12:13 MST (a minute ago)

— Choose a reason for resolving —

Resolve alert

No prior alerts in the past 24 hours.

This device supports messaging

Enter message...

32 characters remaining

Send

[view available responses](#)

Add a note...

Post Note

ACME Corp.
2025-01-28 13:12:59 MST
Alert received by server.

ACME Corp.
2025-01-28 13:12:50 MST
Alert triggered on device.

[Show More](#)

Sensor configurations
Device's configured high and low sensor thresholds.

[view settings](#)

Protocol **Contacts** **Notified**

Emergency response protocol
This is the protocol for responding to alerts on Blackline Live. Follow the protocol closely and refer to the Contacts tab for detailed emergency contact information.

Protocol for G7c with Gas *EVALUATION*

****** THIS IS AN EVALUATION ACCOUNT. DO NOT DISPATCH UNLESS REQUESTED******

— SOS Alert/fail detection/No motion/Missed Check-in —

STEP 1: Send a message to the G7c device. **"Do you need help?"**, wait **2 minutes**.

- If non response after **2 minutes**, proceed to **STEP 2**.

STEP 2: Call the G7c device

- If no answer, **call the phone number assigned to the user**.
- If still no answer, proceed to **STEP 3**.

STEP 3: Contact emergency contacts in order of priority. Once someone is reached, provide emergency contact the following information:

- Full name of the employee.

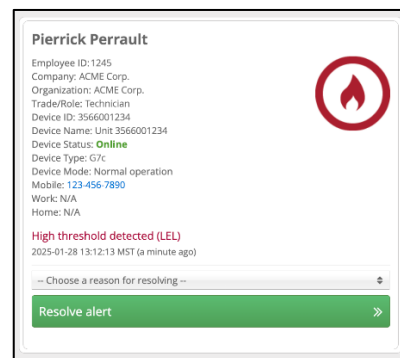
The Alert management page is composed of the following sections:

Description:

Lists information about the device, the assigned user, and the alert, including any other alerts that occurred on the same device with the same user in the last 24 hours.

Select **Acknowledge alert** to investigate the alert.

NOTE: During a gamma event, the gamma icon displays in the description section.

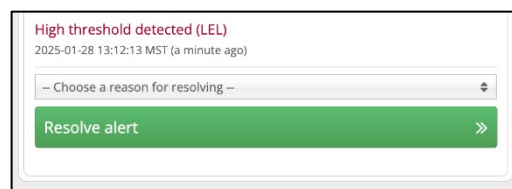


Resolution:

Select **Resolve alert** to close an active alert once the device user's safety is confirmed.

Prior to resolving the alert, select a reason 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 resolved, the alert is cleared from the device and the device is no longer shown with an alert status in Blackline Live.

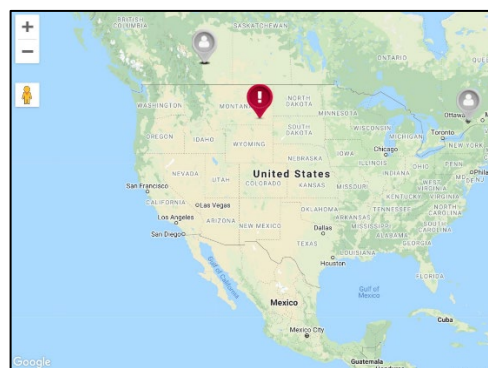


Map:

Shows the current location of the device in alert on a live map.

Select the device pin to open the map 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.

Use the map to identify nearby workers who may be able to help or to provide directions to response or dispatch teams.



Emergency response protocol:

View the emergency response protocol, emergency response contacts, and notified contacts for the device. Use the procedure outlined in the protocol to respond to the alert.

The information provided is assigned to the device's configuration profile. Make sure the information in alert profiles is kept up to date and that devices are assigned to the correct profiles. In addition, Blackline monitored device protocols must not be modified. For more information, contact Blackline Safety [Technical Support](#).

The screenshot shows a web interface with tabs for Protocol, Contacts, Notified, and AlertLink Messages. The 'Protocol' tab is active, displaying the 'Emergency response protocol' for a G7c device with Gas. It includes a warning: 'THIS IS AN EVALUATION ACCOUNT. DO NOT DISPATCH UNLESS REQUESTED'. The protocol steps are: STEP 1: Send a message to the G7c device: "Do you need help?", wait 2 minutes. If no response after 2 minutes, proceed to STEP 2. STEP 2: Call the G7c device and validate need for assistance. If no answer, call the phone number assigned to the user (if available). If still no answer, proceed to STEP 3.

AlertLink Messages:

If AlertLink is enabled, view the list of devices that received AlertLink messages when the alert was activated.

The screenshot shows the 'AlertLink Messages' tab. It displays a table of devices notified of the alert. The table has columns: DEVICE ID, DEVICE NAME, USER, DEVICE TYPE, SENT ALERTLINK MESSAGE AT, RECEIVED ALERTLINK MESSAGE AT, DISTANCE FROM ALERT, and LOCATION. Two devices are listed: one with ID 35700001234 (Maintenance, Bill Talent, G7c) and one with ID 39730005487 (Supervisor, Renford Trey, G7c). Both received messages at 10:38:52 MDT on 2023-07-09. The distance from the alert is 5 m for the first device and 279 m for the second. The location is 51.0319938, -114.0435084 for both.

DEVICE ID	DEVICE NAME	USER	DEVICE TYPE	SENT ALERTLINK MESSAGE AT	RECEIVED ALERTLINK MESSAGE AT	DISTANCE FROM ALERT	LOCATION
35700001234	Maintenance	Bill Talent	G7c	2023-07-09 10:34:17 MDT	2023-07-09 10:34:19 MDT	5 m	51.0319938 -114.0435084
39730005487	Supervisor	Renford Trey	G7c	2023-07-09 10:34:17 MDT	2023-07-09 10:38:52 MDT	279 m	51.0319938 -114.0435084

Messages:

If the response protocol includes a step to contact the affected device via text message, send a message of up to 32 characters to the device user.

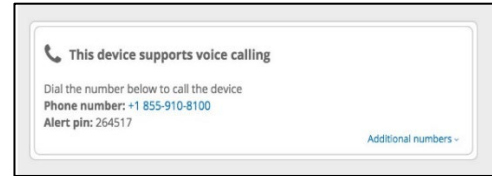
The screenshot shows a messaging interface for a device. It has a header 'This device supports messaging' with an envelope icon. Below is a text input field with the placeholder 'Enter message...'. A status bar indicates '32 characters remaining'. There is a 'Send' button with an envelope icon and a 'view available responses' link.

Two-way voice call:

If the response protocol includes a step to directly call the device (G7 or EXO devices), use the information noted to place a two-way voice call to the device using a phone.

If the alert on the device is unacknowledged before you call (for example, if it was initiated from an email or from the Maps page) you must acknowledge the alert before the call will connect.

The device user does not have to do anything to accept the voice call. The call only ends when the person on the phone hangs up.



Gas configurations:

Lists the configured gas-sensor thresholds for the device. 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.

To view the configured gas sensor thresholds, select **view settings**.

Gas configurations			
Device's configured high and low gas thresholds.			
Device's configuration: EXO SEM config			
Configuration version: 6			
H₂S Low threshold 5.00 ppm High threshold 10.00 ppm	CO Low threshold 50.00 ppm High threshold 200.00 ppm	O₂ Enrichment Low threshold ↑23.50 %vol Enrichment High threshold ↑25.00 %vol Depletion High threshold ↓18.00 %vol Depletion Low threshold ↓19.50 %vol	LEL Low threshold 10.00 %LEL High threshold 20.00 %LEL
SO₂ Low threshold 2.00 ppm High threshold 5.00 ppm	NH₃ Low threshold 25.00 ppm High threshold 50.00 ppm	HCN Low threshold 4.70 ppm High threshold 10.00 ppm	H₂ Low threshold 4000 ppm High threshold 8000 ppm

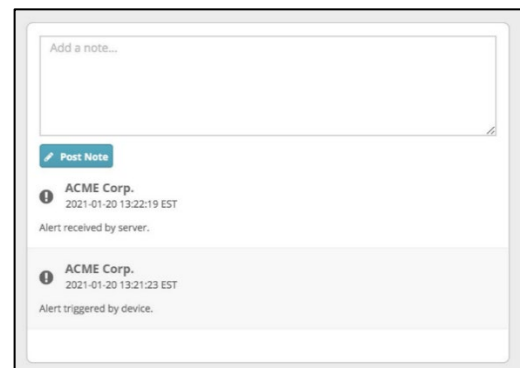
Notes:

List of the chronological steps taken to resolve the alert.

It records when the event was triggered locally on the device, as well as when it was delivered to the portal. Any steps taken through Blackline Live (e.g., sending a message or placing a voice call) are recorded automatically.

Add manual notes, by entering information, then selecting **Post Note**.

Monitoring personnel should fill out the Notes section with as much detail as possible, since they are available in the Alert history page after the alert is resolved and can be used for investigations and retrospectives.



19.5 VIEWING ALERTLINK MESSAGES

On the Alerts page, the AlertLink Messages tab displays a list of all devices with active AlertLink messages. The list displays the device name and ID, the device's assigned user, the time of the last AlertLink message, the source alert type and timestamp, the source alert device ID, and the source alert device's assigned user. For more information about AlertLink, see section 10.3.

ALERTS

ALERTLINK MESSAGES

If your organization uses the AlertLink feature, devices that have an active AlertLink message will be listed below. You can remotely clear these messages by selecting devices from the table and selecting the *clear all AlertLink messages* button. You can also retrieve a full list of messages by clicking the *download all* button.

Filter

Device Types

Show all

DOWNLOAD ALL

CLEAR ALL ALERTLINK MESSAGES

Columns

<div><div></div></div>	DEVICE ID	DEVICE NAME	ASSIGNED USER	TIME OF LAST ALERTLINK MESSAGE	ORGANIZATION	SOURCE ALERT DEVICE ID	SOURCE ALERT DEVICE NAME	SOURCE ALERT ASSIGNED USER	SOURCE ALERT TYPE / TIMESTAMP
<div><div></div></div>	EXO: 3588100005	Unit 3588100005	Leon Breiner	2024-09-10 09:47:19 MDT	ACME Corp.	EXO: 3588100009	Unit 3588100009	Unassigned	Fall detected 2024-09-10 09:47:20 MDT
<div><div></div></div>	EXO: 3588100011	Unit 3588100011	Unassigned	2024-09-10 09:47:19 MDT	ACME Corp.	EXO: 3588100009	Unit 3588100009	Unassigned	Fall detected 2024-09-10 09:47:20 MDT

19.6 CLEARING ALERTLINK MESSAGES

Use the Alerts page to remotely clear active AlertLink messages on specific G7c and EXO devices.

To clear AlertLink messages:

- 1. On the Alerts page, select **AlertLink Messages**.
- 2. Select the checkboxes beside the desired devices in the list. The Clear all AlertLink messages button displays above the list.

Filter	Device Types Show all								DOWNLOAD ALL
								CLEAR ALL ALERTLINK MESSAGES	Columns
	DEVICE ID	DEVICE NAME	ASSIGNED USER	TIME OF LAST ALERTLINK MESSAGE	ORGANIZATION	SOURCE ALERT DEVICE ID	SOURCE ALERT DEVICE NAME	SOURCE ALERT ASSIGNED USER	SOURCE ALERT TYPE / TIMESTAMP
	EXO: 3588100005	Unit 3588100005	Leon Breiner	2024-09-10 09:47:19 MDT	ACME Corp.	EXO: 3588100009	Unit 3588100009	Unassigned	Fall detected 2024-09-10 09:47:20 MDT

- 3. Select **Clear all AlertLink messages**. A pop-up modal appears.

This feature will remotely clear all active AlertLink messages on **3 devices**.

CANCELCLEAR ALL ALERTLINK MESSAGES

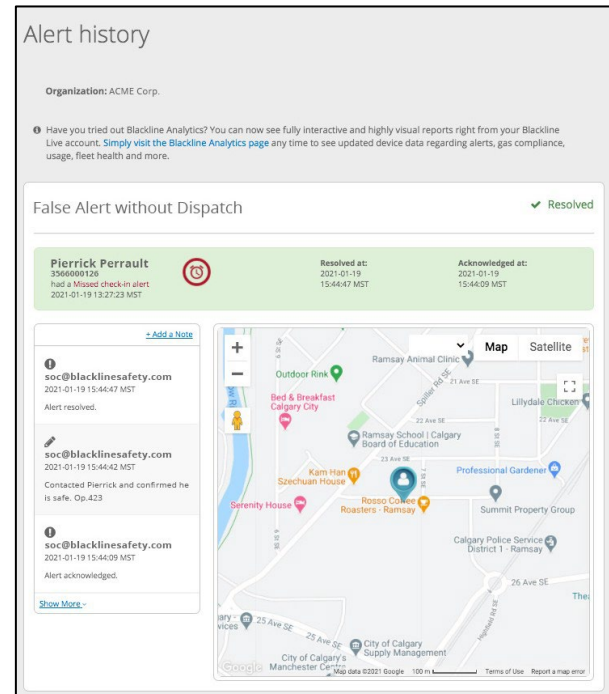
- 4. Select **Clear all AlertLink messages** to confirm. The AlertLink message is automatically cleared and the AlertLink notification on the selected devices ends.

19.7 VIEWING ALERT 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. You can open the Info panel by selecting the map pin to see the state of the device at that time. 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.

When enabled, the AlertLink Messages section displays below the map to list devices that were notified at the time of the alert.



20 G6 DEVICE NOTIFICATIONS

Blackline Live automatically generates and sends out emails or SMS messages when G6 devices experience a high-gas event, Short Term Exposure Limit (STEL) gas event, or gas sensor Over Limit (OL) event. In addition, notifications are sent when the event is resolved.

For more information on setting up notification profiles for G6, see section 11.

NOTE: Notifications from G6 devices are not displayed in the Alerts page, do not trigger the alert banner in Blackline Live, and do not have any alert histories or alert management pages associated with them.

The high-urgency notification email includes the following information (as available):

- Assigned username (at time of the event)
- Event type (including gas type if applicable)
- Employee ID
- Device ID
- Device name
- Organization
- Site address
- Map (geographic coordinates)
- Hardware failures
- Gas errors
- Date/time of the event triggered by device
- Date/time of the event received by server
- User information (contact numbers [mobile, work, home], trade/role, company, custom team member fields)

Bob Smith
High threshold detected (H₂S)

Employee Id: 10124
Device ID: 3570001774
Device Name: Unit 3570001774
Organization: ACME Corp.

Last Known Location (2024-05-21 14:29:10 MDT)
Location is 4 seconds old.

The map displays a residential area with a large body of water, Glenmore Reservoir, in the center. A red pin marks the location of the event on the eastern shore of the reservoir. Surrounding areas include North Glenmore Park to the north, South Glenmore Park to the south, and Bayview to the east. A street labeled '90 Ave SW' is visible. The map is credited to Google and dated 2025.

Latitude & Longitude
[51.0319622, -114.0435553](#)

Triggered by Device
2024-05-21 14:29:13 MDT

Received by Server
2024-05-21 14:29:13 MDT

User Information
Employee Id: 10124
Device ID: 3570001774
Device Name: Unit 3570001774

The high-urgency event resolution email includes the following information (as available):

- Assigned username (at time of the event)
- Employee ID (at the time of the event)
- Device ID
- Device name
- Organization
- Event type (gas type if applicable)
- Date/time event triggered by device
- Date/time event received by server
- Date/time event resolved on device
- Site address
- User information contact numbers [mobile, work, home], trade/role, company, custom team member fields)

Bob Smith
Employee Id: 10124
Device ID: 3570001774
Device Name: Unit 3570001774
Organization: Blackline UX Test

High threshold detected (H₂S) has been resolved as a System Test.

Alert Type
High threshold detected (H₂S)

Triggered by Device
2024-05-21 14:27:59 MDT

Received by Server
2024-05-21 14:28:02 MDT

Acknowledged
2024-05-21 14:30:25 MDT

Resolved
2024-05-21 15:29:48 MDT

Resolution Reason
System Test

Notes

kwash@acmecorp.com
2024-05-21 15:29:48 MDT
Alert resolved.

kwash@acmecorp.com
2024-05-21 14:30:25 MDT
Alert acknowledged.

ACME Corp.
2024-05-21 14:28:02 MDT
Alert received by server.

ACME Corp.
2024-05-21 14:27:59 MDT
Alert triggered by device.

User Information
Employee Id: 10124
Device ID: 3570001774
Device Name: Unit 3570001774

The high-urgency event SMS message includes the following information (as available):

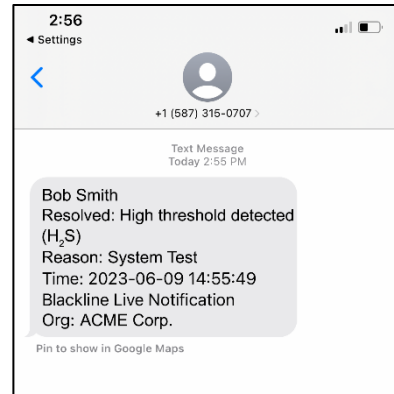
- Assigned username (at time of the event)
- Event type (gas type if applicable)
- Date/time event triggered by device
- Geographic coordinates
- Sender information (Blackline Live Notification)
- Organization

2:56
Settings
+1 (587) 315-0707
Text Message
Today 2:55 PM

Bob Smith
Alert: High threshold detected (H₂S)
Time: 2023-06-09 14:55:49
Lat/Long: <https://maps.google.com/maps?q=51.1450693,-114.1495676>
Blackline Live Notification
Org: ACME Corp.
Pin to show in Google Maps

The high-urgency event resolution SMS message includes the following information (as available):

- Assigned username (at time of the event)
- Event type (gas type if applicable)
- Date/time event resolved by device
- Sender information (Blackline Live Notification)
- Organization



21 MASS NOTIFICATIONS

In the case of an evacuation or large-scale emergency where multiple devices need to be contacted, Blackline Live helps an Account user mass notify all devices in an organization or by individual device group.

NOTE: G6 does not support mass notifications.

Mass notifications

Select the *send* button to send a direct message to every online G7 and EXO devices in a specific organization. The number of characters is limited to the device display.

Organization

ACME Corp.

Device group*

All devices

Message

Evacuate the area

Enter up to two lines of 16 characters. '\', '-' and accented characters are not supported. 16/32

SEND

21.1 SENDING MASS NOTIFICATIONS

Blackline Safety guarantees 99% delivery of messages to devices on cellular networks. Blackline Live tries 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.

To send a mass notification:

1. From the Main menu, select **Mass notifications**. The Mass notifications page opens.
2. Select the **Device group** to contact. For example, to contact all the devices in an organization, set the Device group to **All devices**.
3. Enter a short message into the text area.

NOTE: The message must be split into two lines with a maximum of 16 characters on each line.

4. Select **SEND**. The message is sent to the devices in the specified group.

22 BLACKLINE ANALYTICS

Blackline Live includes a built-in suite of analytics reports that help you 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, and trends over time.

To view the Blackline Analytics Essential reports:

1. From the Main menu, select **Blackline Analytics**. The analytics report page opens.
2. Select a link to display the corresponding report.

The following Blackline Analytics Essential reports are available with the basic analytics service that comes with the purchase of one or more of Blackline's connected devices.

Report	G7c/G7x	G6	G7EXO/EXO8	Beacon
Overview This dashboard is the Analytics landing page. It provides a collection of metrics from the other reports and shows trends across key safety metrics: usage, compliance, and alerts for the last four months.	✓	✓	✓	
Usage and Compliance Display the total usage of your fleet's devices during a chosen period of time, as well as the percentage of compliance within that time frame. Use this report to determine which users are staying compliant and track overall compliance trends over time.	✓	✓	✓	

Report	G7c/G7x	G6	G7EXO/EXO8	Beacon
Bump Tests and Calibrations Review your fleet's bump test and calibration history. You can select a date range to see the number of devices tested, tests performed, tests performed with a G7 Dock, and the overall success rate. You can also use the data in this report in combination with the Usage and Compliance report to determine whether compliance trends coincide with bump test and calibration frequency and success.	✓	✓	✓	
Worker Safety Analytics Review worker safety trends, including alerts by device, alerts by day of the week, alerts over a worker's shifts, the impact of longer shifts on alerts, and alert types by month compared against planned operations and maintenance events. These trends can assist you in narrowing down possible root causes of alerts, which can help determine corrective measures to improve worker safety and reduce alerts. NOTE: The Worker Safety Analytics report was retired on October 31, 2024. Data from the Worker Safety Analytics report is included in the updated Alerts report.	✓		✓	
Gas Exposures (formerly the Gas Readings report) View a combined chart of gas-sensor readings alongside an interactive map. This can help you understand the profile for a worker's gas exposure risk	✓	✓		
EXO Analytics Review area monitoring gas readings by sensor and device. This data can help you to identify trends worth investigating and to create area monitoring logs.			✓	
LEL-MPS Readings View LEL readings for LEL-MPS sensors over a selected date range, separated by the classification of gases detected. The readings in this report are shown alongside an interactive map. This can help you identify where exposures are occurring, when they are highest, and understand the profile of a worker's gas-exposure risk.	✓		✓	
Events View a high-level overview of your data that allows you to drill down into specifics using a selection of filters. Compare data across users, explore how frequently certain event types are reported, compare gas-sensor alerts, and see when events occur over time.	✓	✓	✓	

Report	G7c/G7x	G6	G7EX0/EX08	Beacon
Events map Explore the locations of your data events to help determine if there are issues that may require further investigation. For example, if multiple events of the same type occur in the same location, you may want to investigate the cause.	✓	✓	✓	
Alerts View the full breakdown of alerts across your device fleet. This includes which device users are triggering the most alerts, when and where alerts are being triggered, and which types of alerts are most common. If your organization is using Blackline's monitoring services, you can also see how long it takes for alerts to be resolved and resolution trends, including the most common resolutions. NOTE: The Alerts report has been updated and includes the data originally found in the Worker Safety Analytics report, which will be retired on October 31, 2024.	✓		✓	
Devices and Cartridges View an overview of the status of your devices, including their firmware and cartridges. You can use these logs to stay on top of firmware updates and ensure your devices and device cartridges are being used and maintained regularly.	✓	✓	✓	
Device Assignment History Track changes made to devices to aid in troubleshooting and device management. Device changes can include team member reassignments, device name changes, and instances where devices are moved between organizations.	✓	✓	✓	
Device Logs Review data from device alerts from the past seven days.	✓	✓	✓	
Docks View information on the locations and usage of docks. Use the map to see where a dock was last used and view each dock's bump test and calibration results to track performance and ensure regular maintenance.	✓	✓		
Location Beacons Reivew the status and effectiveness of your Location Beacons. You can use this report to monitor battery levels and ensure locations are being delivered frequently and consistently.				✓

In addition to the listed Essential reports, there are three Essential emailed reports, including:

- Usage report. This report provides usage details for G7 devices only. It does not include compliance details.
- Alerts/Worker Safety analytics reports (populated for customers on self-monitored or Blackline-monitored plans)
- High Gas Exposures report

Emailed Analytics Essential reports are available on a weekly or a monthly cadence. To request an emailed report, please contact your Blackline Safety Customer Service Manager (CSM).

For more information, please see [Blackline Analytics](#).

23 SUPPORT

23.1 LEARN MORE

Visit support.blacklinesafety.com to find support and training materials for Blackline Live.

23.2 TECHNICAL SUPPORT

Contact our Technical Support team for assistance.

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