

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 37
 - 7.3.2 Assigning a Device from the Device Details Page..... 38
 - 7.3.3 Assigning a Device using the Quick Assign Page 38
 - 7.4 UNASSIGNING A DEVICE FROM A TEAM MEMBER..... 39
 - 7.4.1 Unassigning a Device using the Device page 39
 - 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..... 40
 - 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..... 41
 - 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 43
- 8 MANAGING CONTACT GROUPS 44**
 - 8.1 ADDING TEAM MEMBERS TO CONTACT GROUPS..... 45
- 9 MANAGING CONFIGURATION PROFILES..... 45**
 - 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 AND G7 EXO ONLY)..... 52
- 10 MANAGING ALERT MANAGEMENT PROFILES 53**
 - 10.1 VIEWING ALERT MANAGEMENT PROFILES..... 54
 - 10.2 CREATING A NEW ALERT MANAGEMENT PROFILE..... 54

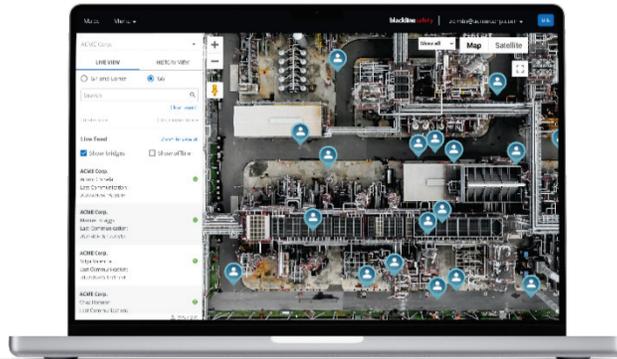
10.3	EDITING ALERT MANAGEMENT PROFILE DETAILS.....	54
11	MANAGING NOTIFICATION PROFILES	57
11.1	VIEWING NOTIFICATION PROFILES	57
11.2	CREATING A NEW NOTIFICATION PROFILE	58
11.3	EDITING NOTIFICATION PROFILE DETAILS	58
12	MANAGING RELATIONSHIPS	60
12.1	VIEWING ACTIVE RELATIONSHIPS.....	61
12.2	VIEWING DEACTIVATED RELATIONSHIPS.....	61
12.3	CREATING A RELATIONSHIP	61
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.....	73
16.1	MAPS (LIVE VIEW).....	74
16.1.1	Locating Devices.....	76
16.1.2	Accessing the Device Info Panel	77
16.1.3	Messaging a G7 Device	78
16.1.4	Calling a G7 Device.....	79
16.1.5	Accessing a Device's Configuration Profile	80
16.1.6	Accessing a G7 Device's Alert Profile	80
16.1.7	Accessing a Device's history.....	80
16.1.8	Finding a G6 Device	81
16.1.9	Displaying Floorplans	83

- 16.1.10 Displaying Satellite Imagery.....83
- 16.2 MAPS (HISTORICAL VIEW).....84
 - 16.2.1 Accessing Device Information in the Map History View.....85
 - 16.2.2 Navigating Device Events in the Map History View.....85
- 17 FLEET HEALTH DASHBOARD 86
- 18 COMPLIANCE CERTIFICATES..... 88
 - 18.1 VIEWING BUMP TEST AND CALIBRATION CERTIFICATES88
- 19 G7 DEVICE ALERTS..... 90
 - 19.1 VIEWING DEVICE ALERTS.....91
 - 19.2 VIEWING ALERT DETAILS92
 - 19.3 ACKNOWLEDGING ACTIVE ALERTS93
 - 19.4 MANAGING ALERTS.....95
 - 19.5 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..... 105
 - 23.1 LEARN MORE 105
 - 23.2 TECHNICAL SUPPORT..... 105

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. or EUR) 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 all of Blackline's safety monitoring devices, including:

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

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., any text messaging features utilizing the LCD screen and all gas detection features are not available on legacy devices).

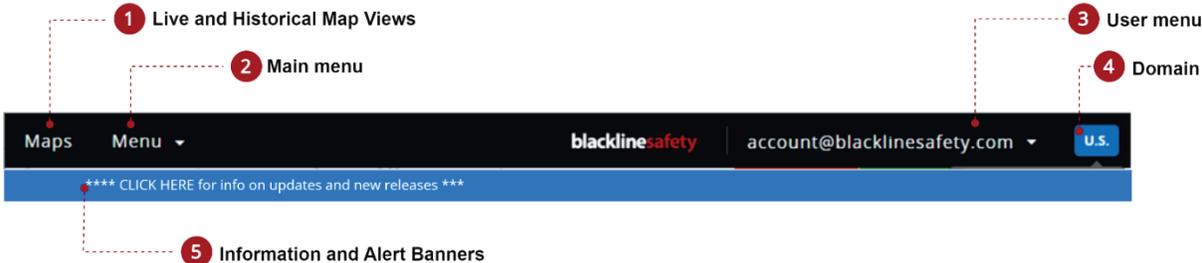
1.2 SUPPORTED ACCESSORIES

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)

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, refer to [Maps](#).

1

NOTE: Access to the Maps pages depends on your Blackline Live permissions. For more information on Blackline Live group membership, roles, and permissions, refer to [Team Members](#) and [Groups](#).

Main menu

Provides access to Blackline Live’s administrative features and resources.

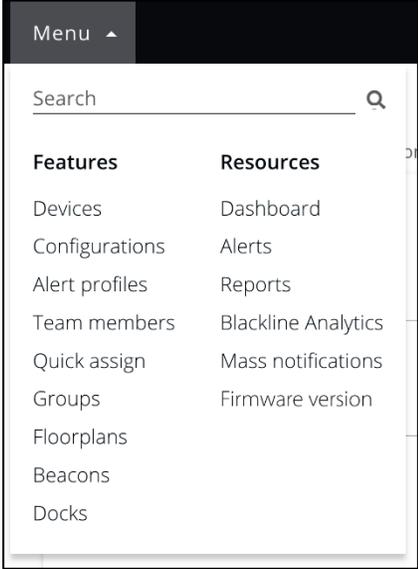
NOTE: Access to features and resources depends on your permissions. For more information on Blackline Live group membership, roles, and permissions, refer to [Group Roles and Permissions](#).

2

Universal search

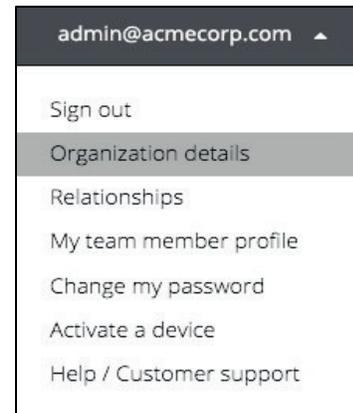
The universal search bar can be accessed from the top of the Main menu. Type in your search query and select . Open items related to your search results by selecting the item from the search results.

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



User menu

- 3 Provides access to information either about the organization you belong to, or about your 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 will be processed and stored entirely within Europe.

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

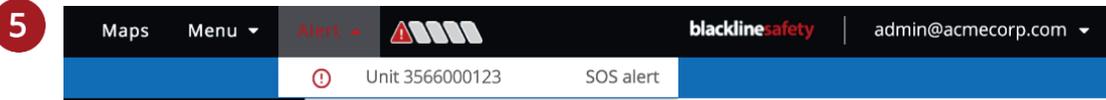
Banners

Three kinds of banners can appear in the navigation bar informing you of something that affects you or your organization.

Alert banner

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

Selecting the alert dropdown will open a list of every alert that needs to be addressed. For more information about managing alerts, refer to [Managing Alert Management Profiles](#).



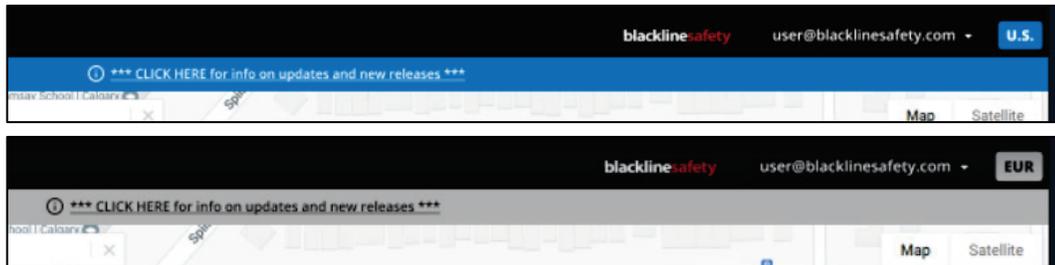
Audio warning banner

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

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

Information banner

A blue (U.S. domain) or Gray (EUR domain) banner immediately below the navigation bar appears if there is new information Blackline Safety wants you to be informed of, including new firmware availability, new features being added to Blackline Live, or updates on known bugs as they are being investigated and resolved.



2.1 SIGNING IN TO BLACKLINE LIVE

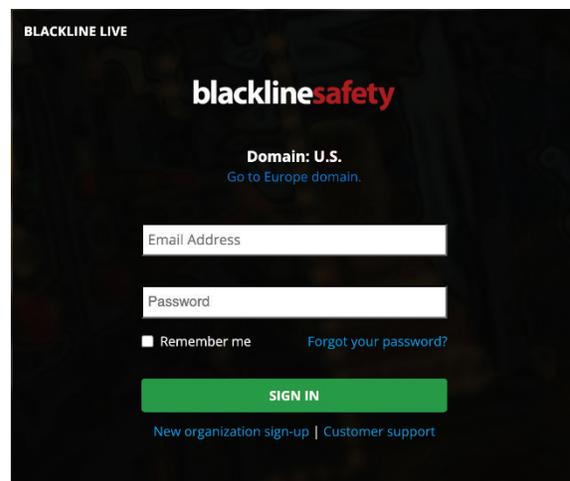
You must be an active Account user within an active organization to sign into Blackline Live. For more information on registering and activating your organization, refer to [Managing Organizations](#).

To sign-in to Blackline Live:

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

For more information on Blackline Live domains, refer to [Navigating Blackline Live](#).

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

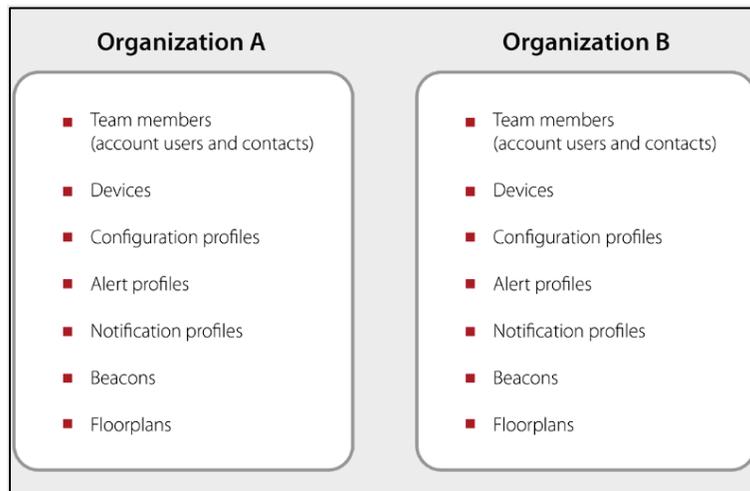


NOTE: Once you are signed into Blackline live, change your password by selecting **Change my Password** from the User menu.

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. The ability of each team member to access 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 share reports and resources with users in other organizations. For more information on relationships, refer to [Relationships](#).

For more information on administering organizations, refer to [Managing Organizations](#).

3.2 TEAM MEMBERS

Team members represent people who are part of your organization, or who act as emergency contacts to 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 they have been sent an invitation to Blackline Live but have not accepted their email invitation.

Active An active status indicates that they have activated their account and logged in. Contacts will always have an **active** status by default.

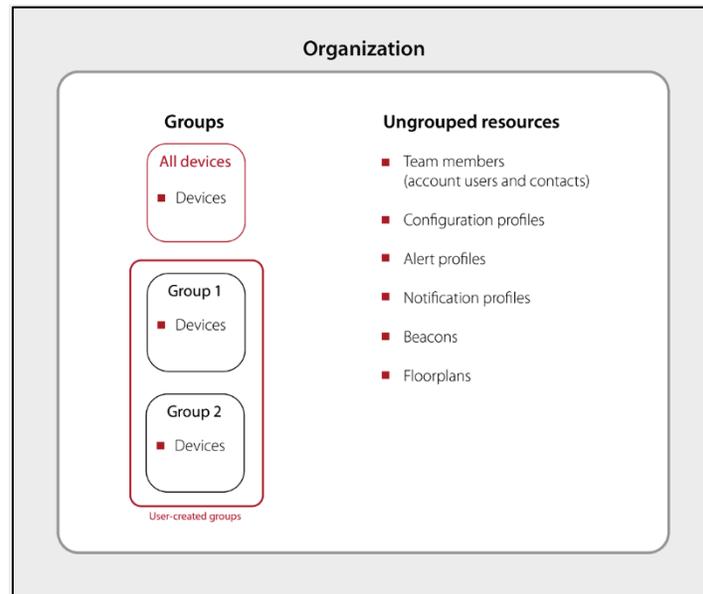
A deactivated status means that a team member is no longer active in an organization.

Deactivated A team member that is deactivated can no longer be assigned to devices, alert profiles, or notification profiles, and will no longer be in any groups. Any devices that they were assigned to them will be become unassigned. Additionally, deactivated Account users will 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), refer to [Managing Team Members](#).

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.



Groups can be used as filters in Blackline Analytics reports to see trends within different parts of the organization. For example, groups can be filtered 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 and visibility within an organization. For example, if the manager of Group one should only see device data for their team, giving them access to that group will filter and streamline their experience in Blackline Live. They will not be able to see or manage Group two, even though those devices are also part of the larger organization.

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

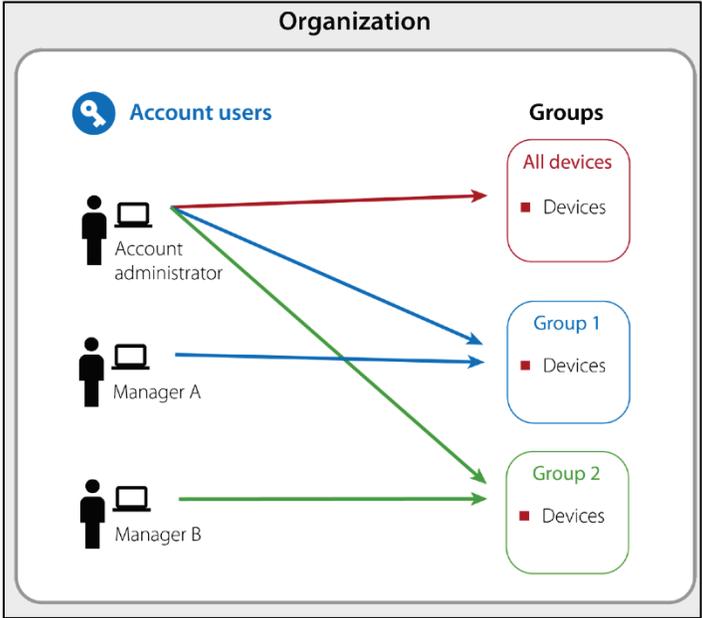
3.3.1 THE ALL DEVICES GROUP

The All devices group is the default group in every organization that automatically contains all devices. It collects all 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 all the resources in your organization. For more information, refer to [Relationships](#).

3.3.2 GROUP MEMBERSHIP

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



3.3.3 GROUP ROLES AND PERMISSIONS

Roles define the permissions that are assigned to Account users and determine what they are allowed to 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 all 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

This role includes the highest level of permissions and should be appointed to users that are responsible for their organization's device fleet.

Users with this role can see and edit all resources in their Blackline organization. They can edit organization-wide information and settings and are permitted to create and manage relationships with other organizations.

This role can only be applied to the All devices group, since it is representative of the entire organization.

Organization assistant

This role supports the Organization admin role.

A user with this role can manage devices, team members, profiles, groups, and organization details, but cannot request or manage relationships with other organizations.

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

Group admin

This role should be given to users who manage a group. Depending on the criteria you are using to create your groups, this might be a site manager or a team lead.

Users with this role can edit the groups they have this role in, as well as any devices within it.

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

Fleet admin

This role is meant to have limited abilities to manage their own fleet.

A user with this role can assign devices, manage mass notifications, and resolve alerts.

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

Device admin

This role should be given to users who manage devices fleets within the groups they have access to.

Account users with this role can rename devices or assign them to team members and are able to monitor and respond to online devices.

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 also 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. It allows the user to see information in the organization, but the only actions they can take are those required for alert investigation and resolution.

A user with the Resolve only role can acknowledge alerts and leverage the Alerts Management page to review emergency response protocols, assess the device's current location and status, contact device users and emergency contacts, and leave notes regarding the investigation of the event.

**Emergency response
admin**

This role is meant for a monitoring administrator. It allows a user to respond to alerts but is more limited 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 will have access to the Compliance dashboard page and the Mass notifications page.

View only

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

Analytics only*

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

*This role is only available for groups within the Account user's organization. It cannot be used when 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
Organization admin	View all	Y	Y	Y	Y	Y	Y	Y	Y	Y
Organization assistant	Limited view • No maps • No quick assign • No beacons/floorplans • No relationships	Y	Y	Y	Y	Y	Y	Y	N	Y
Group admin	View all	Y	Y	Y	Y	Y	Y	Y	N	N
Device admin	View all	Y	Y	Y	Y	Y	N	N	N	N
Fleet admin	Limited view • Devices • Team members • Alerts management • Alert history • Docks • Dashboard • Mass notifications	Y	Y	N	Y	N	N	N	N	N
Contact admin	Limited view • Devices • Team members • Quick assign	N	N	Y	Y	N	N	N	N	N
Contact admin (No repair)	Limited view • Devices • Team members • Quick assign Cannot use the "Mark as under repair" feature	N	N	Y	Y	N	N	N	N	N
Resolve only	View all	Y	N	N	N	N	N	N	N	N
Emergency response admin	Limited view • Alerts management • Alert history • Mass notifications	Y	Y							
Emergency responder	Limited view • Maps (Live view & History view) • Alerts management • Alert history	Y	N	N	N	N	N	N	N	N
Compliance	Limited view • Dashboard • Mass notifications	N	Y	N	N	N	N	N	N	N
View only	View all	N	N	N	N	N	N	N	N	N
Analytics only	Limited view • Blackline Analytics	N	N	N	N	N	N	N	N	N

*To create and edit 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

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

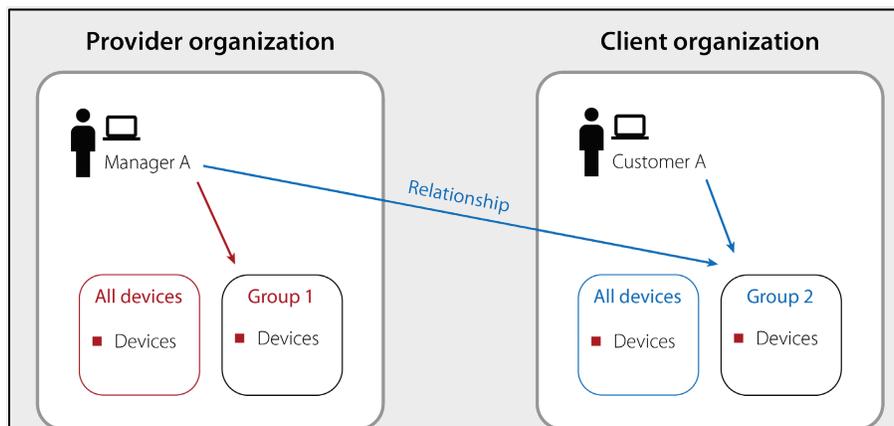
3.4 RELATIONSHIPS

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 they are responsible for defining the access the provider will have. 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 they can only assign the roles that the client has defined.

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



For more information, refer to [Managing Relationships](#).

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 — they cannot be moved to another organization by anyone other than a Blackline Safety representative. Contractual relationships only allow the All devices group to be shared, meaning the provider will have access to all 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 set-up.

Non-contractual

A relationship this is considered less secure than contractual ones but allow more for more flexibility and customization. The client can choose to share any of their groups with the provider — not just the All devices group. 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, then your organization will already be registered in Blackline Live. In this case, you will 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) or eu.live.blacklinesafety.com (European domain), depending whether you want your organization hosted in the U.S. or in Europe. The Blackline Live Sign in page opens.

For more information on Blackline Live domains, refer to [Navigating Blackline Live](#).

2. Select **New organization sign-up**.

The Blackline Live New Organization Sign In page opens.

BLACKLINE LIVE

blacklinesafety

Domain: U.S.
[Go to Europe domain.](#)

Email Address

Password

Remember me [Forgot your password?](#)

SIGN IN

[New organization sign-up](#) | [Customer support](#)

BLACKLINE LIVE

blacklinesafety

Domain: Europe
[Go to U.S. domain.](#)

Email Address

Password

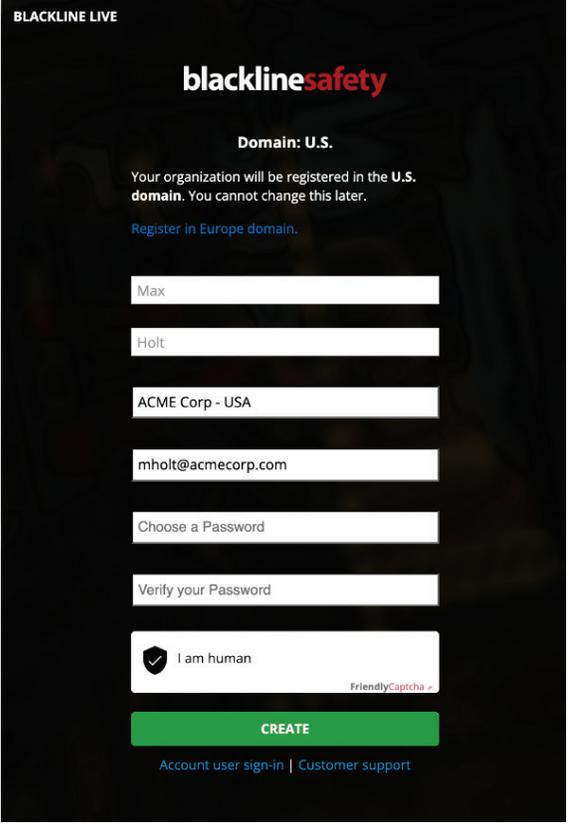
Remember me [Forgot your password?](#)

SIGN IN

[New organization sign-up](#) | [Customer support](#)

blacklinesafety

3. Verify that you have selected the correct domain.
NOTE: When your organization has been registered, you cannot change the domain.
4. In the fields provided, enter your name, your organization's name, administrative email, and password.
IMPORTANT: Enter a valid email address, as you will need to activate your organization through email.
Your Password should be at least 8 characters long, include capital and lowercase letters, a number, and a special character.
5. Complete the security Captcha requirements by selecting I am human.
6. Select **CREATE**.



The screenshot shows the Blackline Live registration interface. At the top left, it says "BLACKLINE LIVE". The logo "blacklinesafety" is centered at the top. Below the logo, it indicates "Domain: U.S." and states "Your organization will be registered in the U.S. domain. You cannot change this later." There is a link to "Register in Europe domain." The form contains several input fields: "Max" (name), "Holt" (organization name), "ACME Corp - USA" (organization name), "mholt@acmecorp.com" (email), "Choose a Password", and "Verify your Password". Below these is a "FriendlyCaptcha" widget with a checkmark and the text "I am human". A green "CREATE" button is at the bottom, with links for "Account user sign-in" and "Customer support" below it.

TROUBLESHOOTING TIP: If you get an error that you cannot use the organization name you have entered, your organization may have already been 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

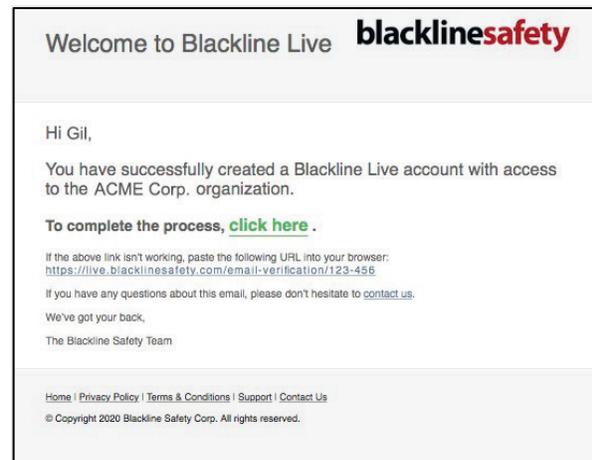
You must activate your organization's account before your organization can begin using Blackline Live.

To activate your organization:

1. Sign into the email account that you used to register your organization and look for an email from Blackline Live.

Remember to check your spam or junk folder if you do not see it in your main inbox.
2. Open the email and select **click here**.

You will be redirected back to Blackline Live, and a pop-up at the top of the screen will inform you that your email was verified.
3. As soon as verified, you can use your email address and password to sign in.



TROUBLESHOOTING TIPS: 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 on the link in the email invitation. If you attempt 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**.

IMPORTANT: 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 device will use latitude and longitude coordinates.



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

- Default time zone** Define what time zone to display on the device when information is received from Blackline Live.
- Display units** Define the units of measure the device will display when they receive information from Blackline Live (kilometers, miles).
- Voice calling region** Define the general geographic region to select when for voice calling (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	<input type="checkbox"/> Show throughout portal
Shift	50	

5 / 50

5 MANAGING TEAM MEMBERS

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

The team member list can be searched and sorted by name. The icon next to each name indicates whether team members are Contacts or Account users. For more information, refer to [Team Members](#).

Team members

ACTIVATED DEACTIVATED

Organization
ACME Corp.

Search team members

Items per page: 20 Page: 1 / 30 [ADD TEAM MEMBER](#)

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

Display ▾

5.1 ADDING TEAM MEMBERS

NOTE: Only Account users assigned to the correct administrative role can add new 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 new 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, refer to [Team Members](#).
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, refer to [Editing Team Member Details](#).
6. Select **ADD TEAM MEMBER**.

5.2 EDITING TEAM MEMBER DETAILS

The Team member details page lists important contact information, and for Account users, account settings and assigned groups. The Team member page is composed of three sections, Team member profile, account settings, and group 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, select **CANCEL**.

IMPORTANT: Account users can view or modify their own information by selecting **My Team Member Profile** in 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** in the team member list.
3. Edit any of the following:

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

IMPORTANT: Always ensure 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

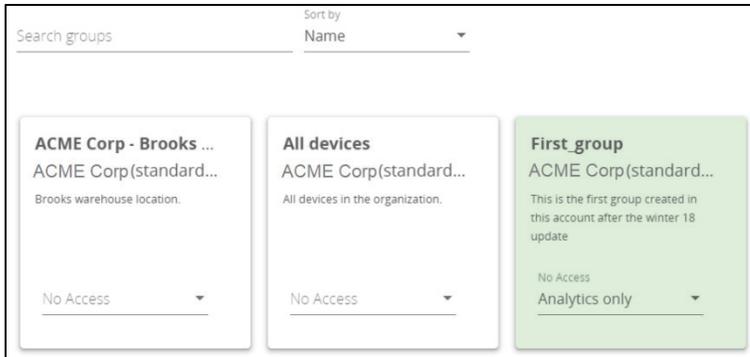
Account settings (Account users only) — Define the team member's Blackline Live settings, including language and alarm volume where:

- **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, refer to [Group Roles and Permissions](#).

NOTE: The groups the team member has been 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.

IMPORTANT: 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, or even live alert monitoring.

To promote a Contact to an Account user:

From the Team member details page:

1. 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, refer to Editing Team Member Details.

IMPORTANT: When changing a Contact to an Account user, you will be required to 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 will be pending until they accept the invitation sent their email address.

5.3.2 DEMOTING AN ACCOUNT USER TO A CONTACT

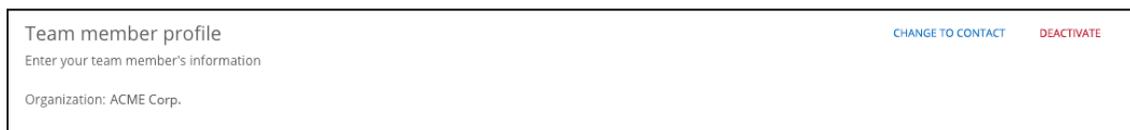
Contacts are team members that can be assigned to devices, or to alert profiles as emergency Contacts, but do not have sign-in access to Blackline Live.

As soon as an Account user is demoted to a Contact, the team member's session will be ended, they will no longer be able to sign into Blackline Live, and they will no longer be listed in groups.

IMPORTANT: If the team member was assigned to device alert profiles or notification profiles as an Account user, these assignments will 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 with the text 'Enter your team member's information' and 'Organization: ACME Corp.'. In the top right corner, there are two buttons: 'CHANGE TO CONTACT' (highlighted in blue) and 'DEACTIVATE' (in red).

2. In the confirmation dialog box that opens, select **MAKE CONTACT**.
3. Update the team member details. For more information, refer to [Editing Team Member Details](#).

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 will not be deleted but will have an **inactive** status in Blackline Live.

Deactivated team members cannot be assigned to devices, alert profiles, or notification profiles, and will be removed from groups and unassigned from their devices. Deactivated Account users will not be able to sign into Blackline Live. Deactivated team members can be reactivated and manually re-assigned 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, and select **DEACTIVATE**.

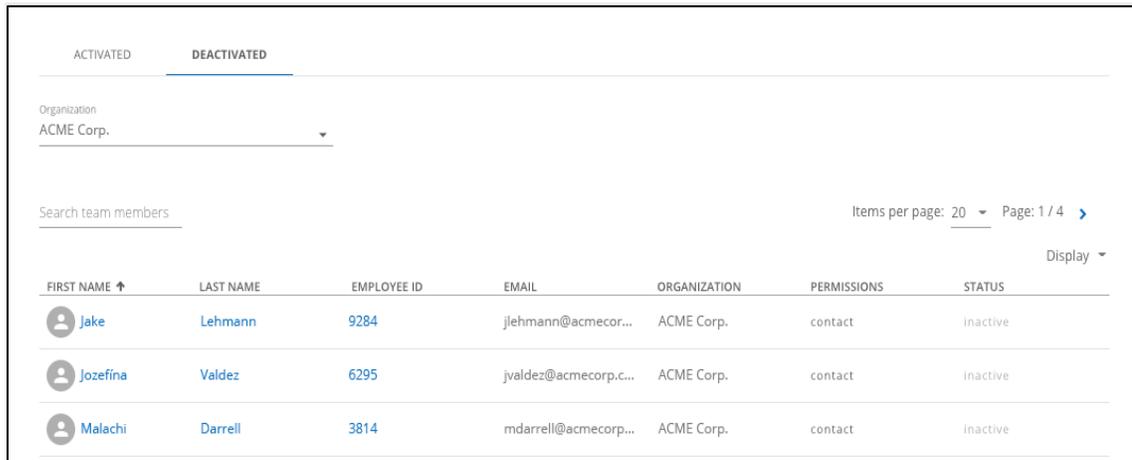


The screenshot shows the same 'Team member profile' form as above. In this view, the 'DEACTIVATE' button (in red) is highlighted, while the 'CHANGE TO CONTACT' button is not.

2. In the confirmation dialog box that opens, select **DEACTIVATE**.
3. The team member's profile will automatically be 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.



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@acmecor...	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 deactivated tab, open the team member details page and select **Activate**.



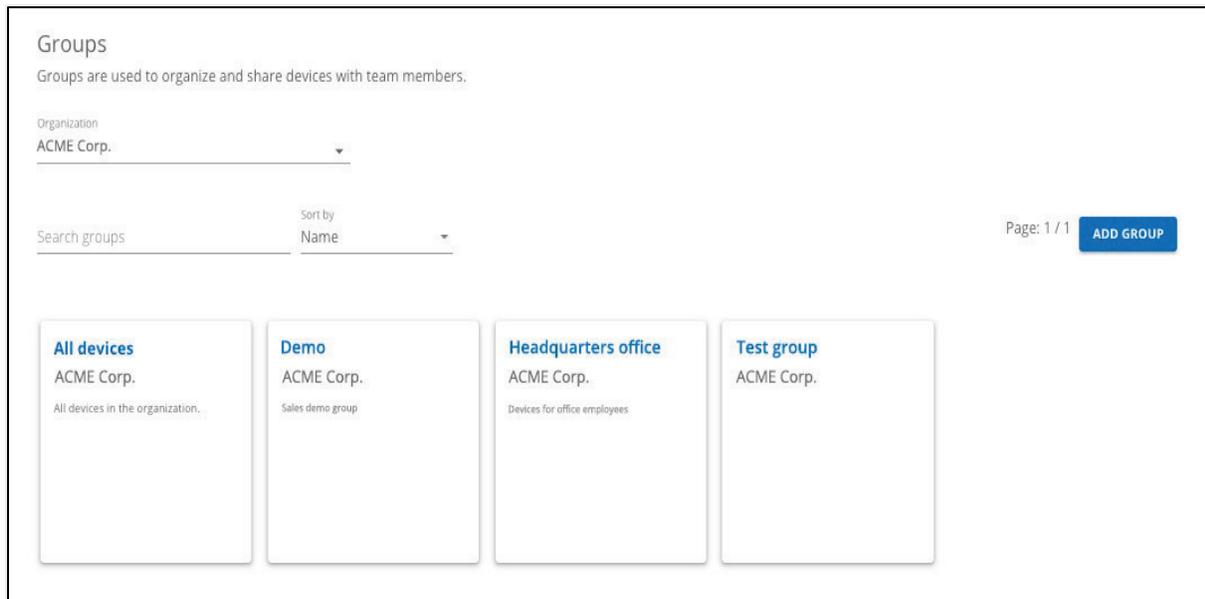
Deactivated team member profile ACTIVATE

Enter your team member's information

2. The team member's profile will automatically be made active in Blackline Live.

6 MANAGING GROUPS

The Groups page lists all 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. The group list can be searched and sorted by name. For more information on group structure, roles, and permissions, refer to [Group Membership](#).



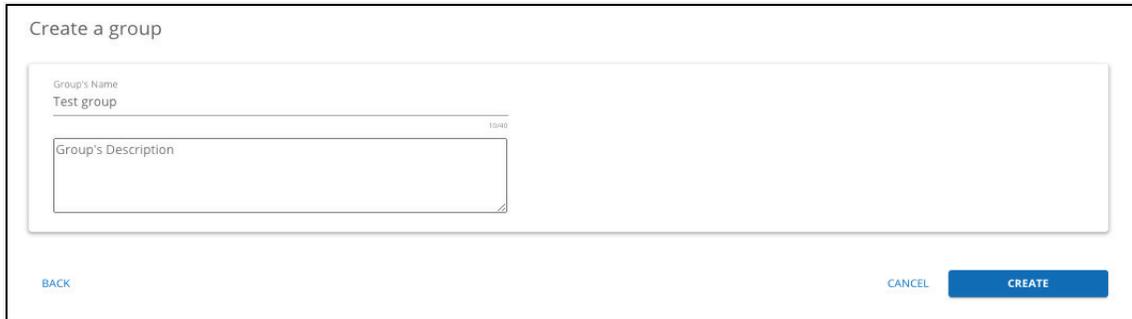
IMPORTANT: Each organization has a default group called the All devices group. This group collects all the devices in the organization and represents the whole organization. The All devices group allows administrators to easily grant Account users access to resources in an organization.

The title, description, and device list of the All devices group cannot be edited. The group managers of the All devices group can be edited.

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 available, a description for the new group.



Create a group

Group's Name
Test group

Group's Description

BACK CANCEL CREATE

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, refer to Editing Group Details.

6.2 EDITING GROUP DETAILS

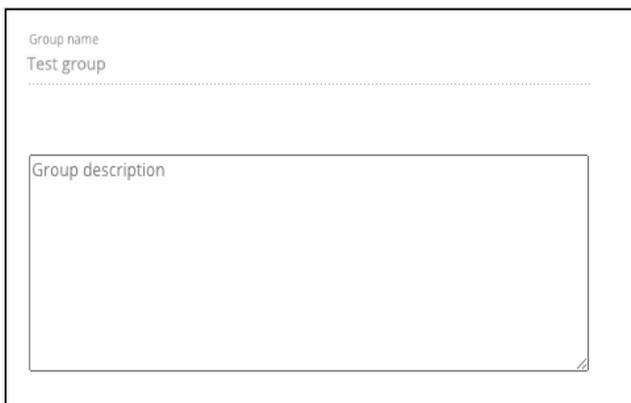
Update the group description, manage team member permissions for the group, and assign devices to the group by editing the Group details page.

NOTE: To open a section for updating, 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.



Group name
Test group

Group description

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 and 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 on the available group roles, refer to [Group Roles and Permissions](#).

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.	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.	

Display ▾

Group devices — Manage the devices assigned to a group:

G7 AND LONER **G6**

Search devices _____ Only show devices in this profile (5)

Devices selected: 5 Columns ▾

<input type="checkbox"/>	DEVICE NAME	DEVICE ID	FIRST NAME	LAST NAME	EMPLOYEE ID
<input type="checkbox"/>	Unit 3455000102	3455000102	Anita	Kunkel	2848WD
<input checked="" type="checkbox"/>	Unit 3455000123	3455000123	Cheryl	Smith	Y6DUYW
<input type="checkbox"/>	Unit 3455000124	3455000124	Gerhard	Brent	HR9JR3
<input type="checkbox"/>	Unit 3455000126	3455000126	jake	Lehmann	TN3E56
<input type="checkbox"/>	Unit 3455000347	3455000347	Leon	Breiner	PGR238
<input type="checkbox"/>	Unit 3455000445	3455000445	Leon	Mein	23WRT4
<input checked="" type="checkbox"/>	Unit 3455000546	3455000546	Miguel	Vemulakonda	BT3T2E
<input type="checkbox"/>	Unit 3455000547	3455000547	Poncio	Macías	093LK3
<input type="checkbox"/>	Unit 3455000548	3455000548	Shireen	Bousaid	YT230U
<input type="checkbox"/>	Unit 3455000589	3455000589	Vivi	Henson	23HTR4

Items per page: 10 Page: 1 / 2 >

- Add devices to the group by selecting new devices you would like to include in the group.

NOTE: The device list can be searched and sorted 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 AND LONER** tab 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 will no longer have access to this group.

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

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

To delete a group:

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



2. In the confirmation dialog box that 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.

STATUS	CHECK-IN REMINDER	ASSIGNED TEAM MEMBER	ORGANIZATION	DEVICE ID	DEVICE NAME	CONFIGURATION PROFILE	ALERT PROFILE	LAST COMMUNICATION
	not configured	Team member	ACME Corp.	123456789	Unit 123456789	Demo G7	G7 alert profile	20 days ago
	00 : 20 : 10	Team member	ACME Corp.	123456789	Unit 123456789	ACME G7 config	G7 alert profile	20 days ago
	00 : 14 : 12	Team member	ACME Corp.	123456789	Unit 123456789	ACME G7 config	G7 alert profile	20 days ago
	not configured	not assignable	ACME Corp.	123456789	Unit 123456789	Default	G7 alert profile	20 days ago
	not supported	select to assign	ACME Corp.	123456789	Unit 123456789	EXO config	EXO alert profile	20 days ago

The device list can be searched and sorted. Filter the device list by device type by selecting the **G7 AND LONER** tab 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 check-in reminder configured 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** — Unique device identifier.
- **Device name** — Device name.
- **Configuration profile** — The device's assigned configuration profile.
- **Alert profile (G7 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	Kiki Wash	ACME Corp.	2334000123	Unit 2334000123	ACME G6 config	not supported	23 minutes ago
	not supported	Cherilyn Weiss	ACME Corp.	2334000124	Unit 2334000124	ACME G6 config	not supported	16 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 configuring team members, refer to [Managing Team Members](#).
 - 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, refer to [Editing Device Details](#).
 - 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, refer to [Maps \(Live View\)](#).

7.2 EDITING DEVICE DETAILS

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

NOTE: To open a section for updating, 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
Shared G6 123

13/64

Organization
Blackline UX Test

Assigned team member
Kiki Wash

G6

Unit ID: **3570001777**

Activation code: **P89SCG**

For more information about assigning an organization to a device, refer to [Moving Devices between Organizations](#).

For more information about assigning devices to team members, refer to [Assigning a Device to a Team Member](#).

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, refer to [Updating a Device Configuration Profile](#).

For more information on editing a G7 device’s assigned alert profile, refer to [Changing the Alert Profile for a Device](#).

For more information on editing a device’s assigned notification profile, refer to [Changing the Notification Profile](#).

Groups — Manage the groups the device is assigned to.

Sort by

Name ▼

All devices

ACME Corp.

All devices in the organization.

Headquarters office

ACME Corp.

Devices for office employees

blacklinesafety

Groups are used to 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, refer to [Managing Groups](#).

7.3 ASSIGNING A DEVICE TO A TEAM MEMBER

There are multiple pages in Blackline Live that enable you to assign devices:

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

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

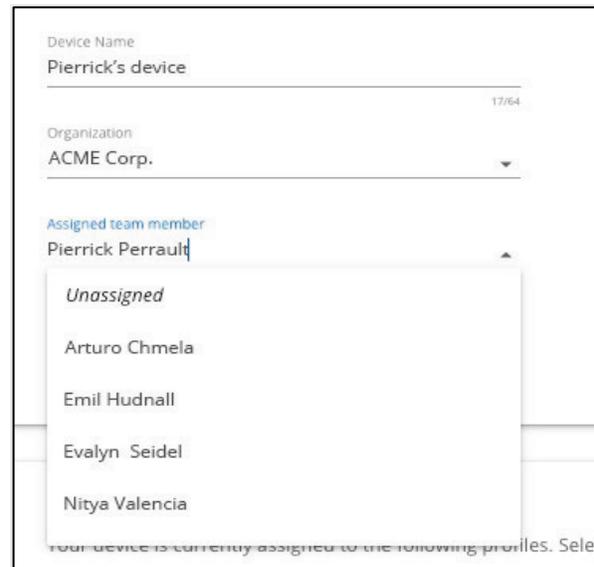
NOTE: To open a section for updating, select **EDIT**. To save your updates and stop editing the card, select **SAVE**. To cancel your updates without saving your changes, select **CANCEL**.

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

From the Device details page:

1. In the Device description card, select a name from **Assigned team member** dropdown.

The devices description card displays the new assignment.



The screenshot shows a form for device details. The 'Device Name' field contains 'Pierrick's device'. The 'Organization' dropdown is set to 'ACME Corp.'. The 'Assigned team member' dropdown is open, showing a list of team members: 'Unassigned', 'Arturo Chmela', 'Emil Hudnall', 'Evalyn Seidel', and 'Nitya Valencia'. The current selection is 'Pierrick Perrault'.

7.3.3 ASSIGNING A DEVICE USING THE QUICK ASSIGN PAGE

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

To use the Quick assign page, you will need:

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



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

- **Scannable identifier for each team member (e.g., an ID card)** Before using the Quick assign page, you will have to ensure your team members are set up with a team member ID. The team member ID can be any combination of letters and numbers, as

long as it corresponds to a scannable code that represents them — the most common example of this would be a company ID card.

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*.
3. 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**.
4. In the **Employee ID** field, type the employee ID to assign to the device.
5. 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:

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

NOTE: 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:

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 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 update a device configuration profile:

From the Device details page:

1. Select your 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, refer to [Editing Configuration Profile Details](#).

7.6 CHANGING THE ALERT PROFILE FOR A DEVICE

IMPORTANT: G6 does not support alert profiles.

To change the assigned alert profile for a device:

From the Device details page:

1. Select your 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, refer to [Editing Alert Management Profile Details](#).

7.7 CHANGING THE NOTIFICATION PROFILE FOR A DEVICE

NOTE: 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 change the notification profile for a device:

From the Device details page:

1. Select your 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, refer to [Editing Notification Profile Details](#).

7.8 MOVING DEVICES BETWEEN ORGANIZATIONS

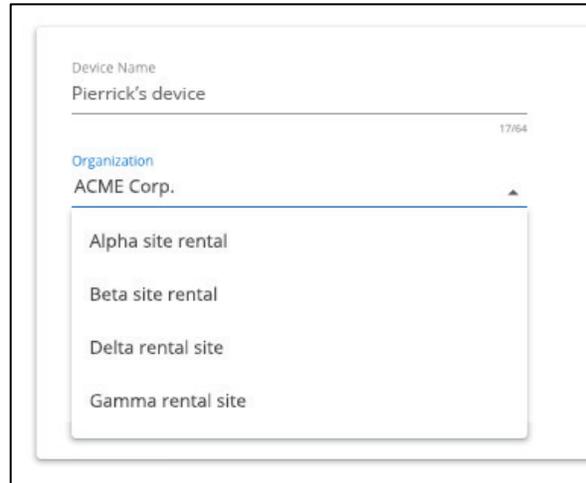
To move devices between organizations, an Account user needs to have either a group or organization admin role over the All devices group of both organizations.

In general, distributors will need to move devices, either when they are setting up a new customer and transferring devices from their own organization to the customers or when they are facilitating rentals and need to move devices back and forth between their own organization and multiple rental organizations.

NOTE: 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 move devices between organizations:

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



7.9 MARKING A DEVICE AS UNDER REPAIR

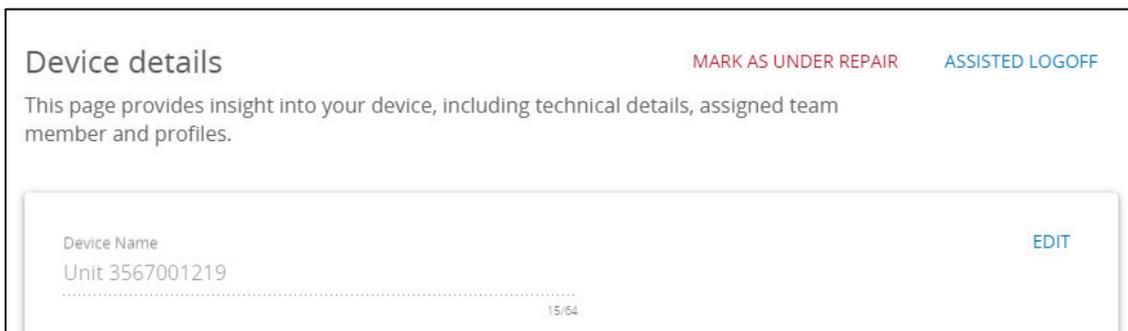
Marking a device as under repair disables the ability to assign the device to team members.

NOTE: Devices marked as under repair require return merchandise authorization (RMA) and should not be used in the field.

To mark a device as under repair:

From the Device details page:

1. Select **MARK AS UNDER REPAIR**.



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 will be 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**.
2. 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. It is used by monitoring personnel during troubleshooting when the device cannot properly power down. It does not power down the physical device.

IMPORTANT: 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 device's new status as under repair. The device cannot be assigned 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:

From the Device details page:

1. Select **SEND ACTIVATION CODE**.
2. 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.

NOTE: The Account administrator group receives updates regarding all three of the other categories

8.1 ADDING TEAM MEMBERS TO CONTACT GROUPS

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

To add team members to contact groups:

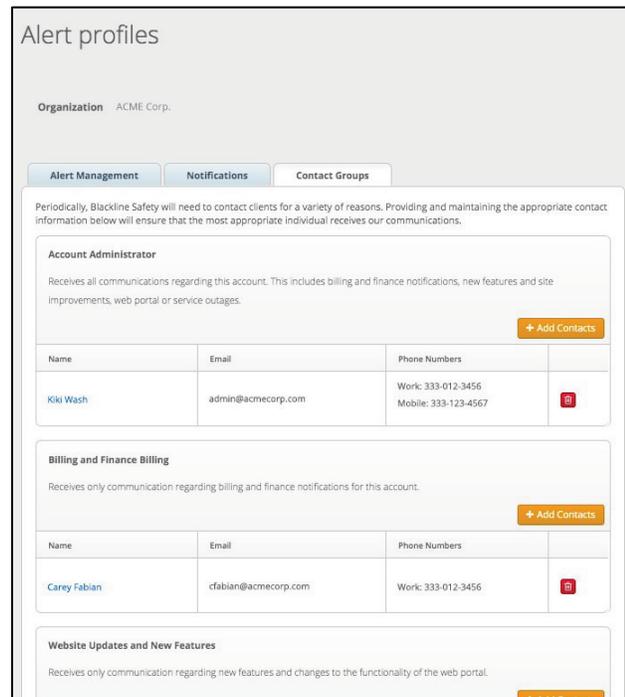
1. From the main menu, select **Alert profiles**. The Alert profile page opens.
2. Select the Contact Groups tab.
3. For the contact group of interest, select **Add Contacts**.

The Choose a Contact dialog box opens.

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.



9 MANAGING CONFIGURATION PROFILES

Configuration profiles define how a device will behave in the field, manage which features are enabled, and allow users to adjust the settings related to these features. Device configurations can be changed over-the-air (OTA), without having to power cycle the device. The configuration profiles list can be searched and sorted.

G7 AND LONER		G6			
DEVICE TYPE		CONFIGURATION NAME ↑		ORGANIZATION	NUMBER OF DEVICES
 G7c	Alpha site G7c	ACME Corp.	135		
 G7c	Beta site G7c	ACME Corp.	60		
 G7 EXO	Alpha site EXO	ACME Corp.	10		
 G7 EXO	Beta site EXO	ACME Corp.	25		
 G7c	Demo G7c	ACME Corp.	15		

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, refer to [Editing Configuration Profile Details](#).

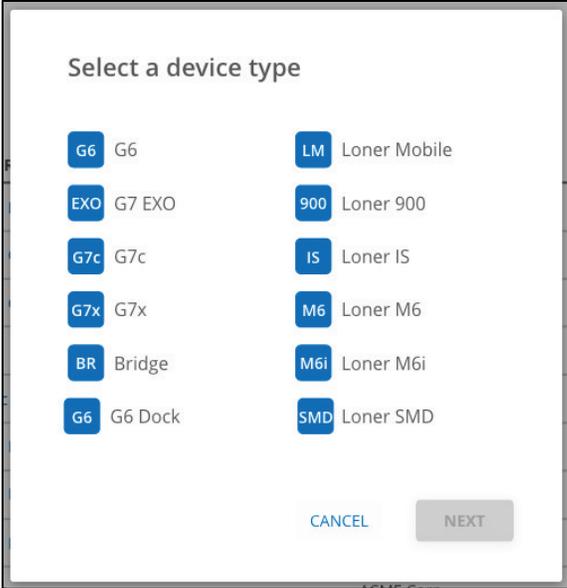
9.2 CREATING A NEW CONFIGURATION PROFILE

To create a new configuration profile:

From the Configurations profile page:

1. Select **ADD CONFIGURATION**. The device type dialog box opens.
2. Select the device type that the profile will apply to.

NOTE: You cannot change the device type associated with a configuration profile after it is selected.



3. Select **NEXT**. The Configuration profile details page opens.
 For information on how to update information related to a configuration profile, refer to Editing Configuration Profile Details.
4. To save the new profile settings, select **SAVE**.

9.3 EDITING CONFIGURATION PROFILE DETAILS

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	G7 EXO
Description	✓	✓	✓
Operating mode		✓	✓
Functional settings	✓	✓	✓
Gas sensor settings	✓	✓	✓
Pump inlets			✓
Interface ports			✓
Assigned devices	✓	✓	✓
Last profile change	✓		

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, select **CANCEL**.

IMPORTANT: Because configuration profile updates impact device behavior in the field, you will always be asked to 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.

Operating modes (G7 and G7 EXO) — Configure the functional and gas 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, refer to [Editing Configuration Profile Mode Settings](#).

Modes

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.

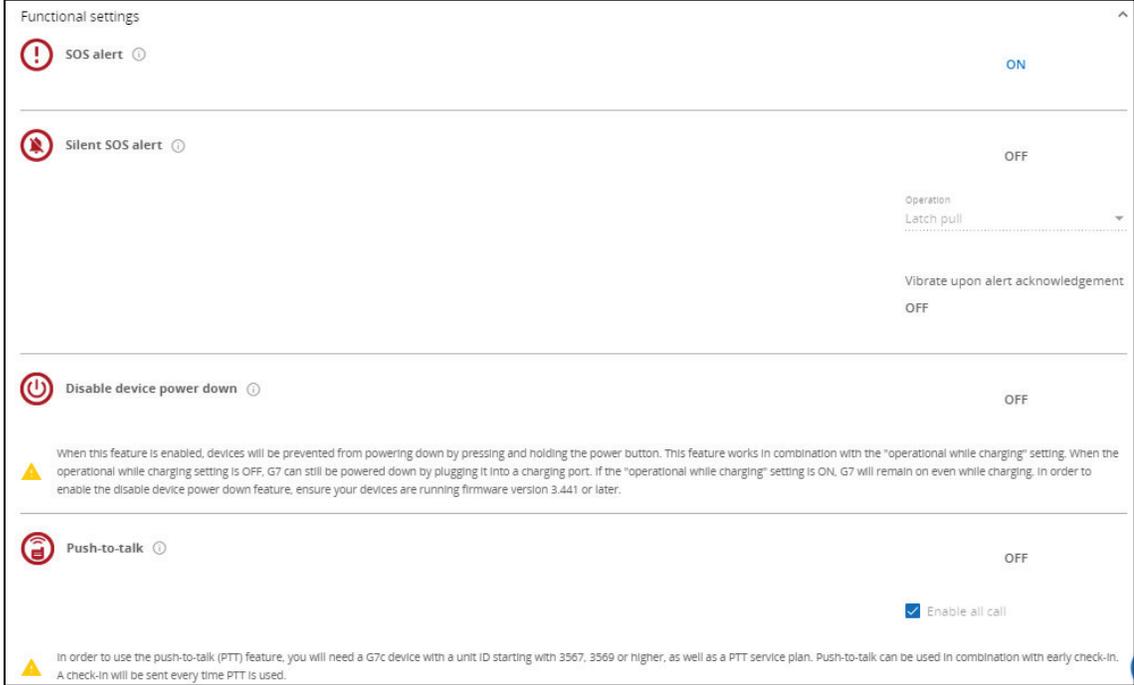
NORMAL OPERATION	PRE ENTRY	HIGH RISK	LEAK CHECK	PUMP RUN	SCBA
-------------------------	-----------	-----------	------------	----------	------

Functional settings ▼

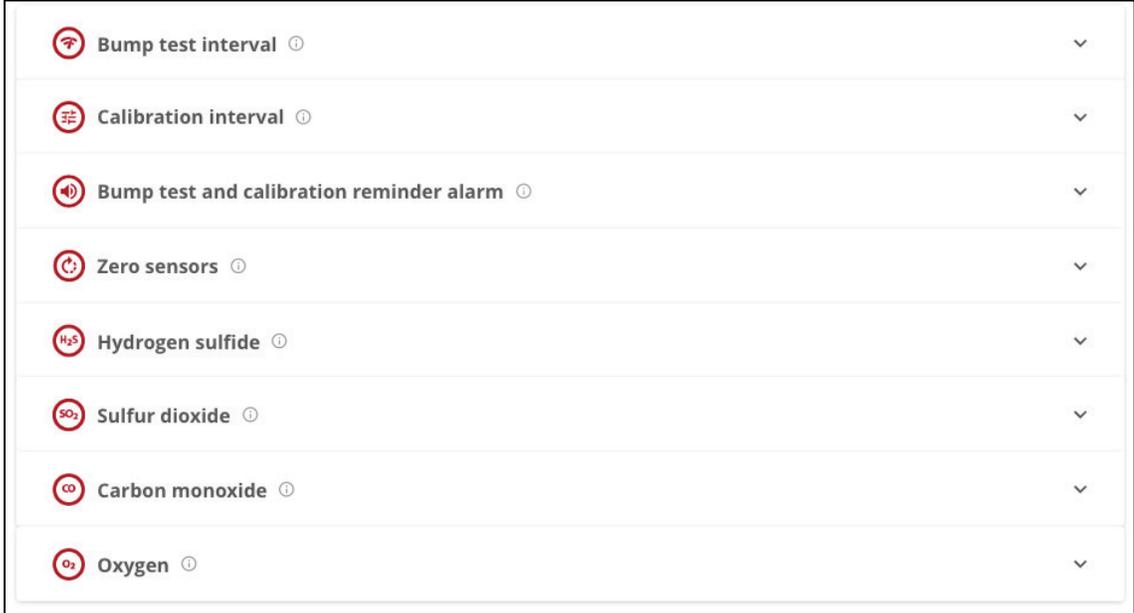
Gas sensor settings ▼

⚠ 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).



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



Pump Inlets (G7 EXO) — Configure G7 EXO’s pump module. For each inlet, select the Inlet function (Disabled, Gas sampling, or Self bump test and calibration). If Self bump test and calibration is selected, enter the gas cylinder details (gas cylinder lot number, gas type, expiry date, gas type, gas concentration). Toggle the inlet Default to ON upon start up on or off. If multiple inlets are used for gas sampling, enter the Sampling schedule (minutes).

NOTE: A multi-inlet sampling setup implies that G7 EXO will not be continuously monitoring any single environment.

The interval entered indicates the amount of time G7 EXO will pump gas into each inlet. There will be a 2-minute buffer period in between each sample to allow time for the gas from the first inlet to be replaced with gas from the next inlet.

Inlet 1

Inlet Function
 Self-bump test and calibration ▼

Inlet setting

Gas	Concentration		
H ₂ S	25	ppm	
	<small>Range: 0.5 - 50ppm Increment: 0.1ppm</small>		
Gas	Concentration		
LEL - CH ₄	50	%LEL	✘
	<small>Range: 4 - 60%LEL Increment: 1%LEL</small>		
Gas	Concentration		
CO	100	ppm	✘
	<small>Range: 5 - 500ppm Increment: 1ppm</small>		
Gas	Concentration		
O ₂	18	%vol	✘
	<small>Range: 0.1 - 19%vol Increment: 0.1%vol</small>		
Gas	Balance		✘
N ₂			

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.

Gas cylinder

Lot number

Expiry date

Additional notes

0020

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

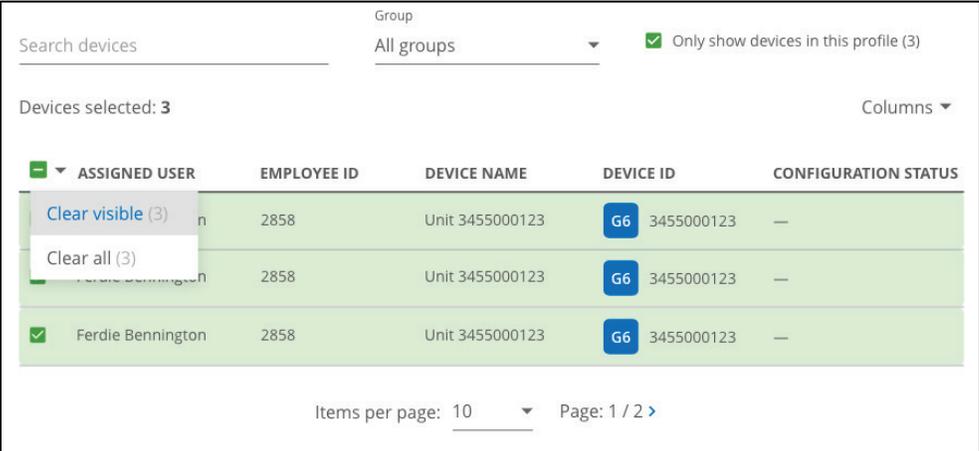
©2023 Blackline Safety Corp
2023-03-15

Blackline Live Technical User Manual | 50
Rev. 02-2 BETA

Interface Ports (G7 EXO) — Review the function of G7 EXO's interface ports. Use the settings to set up G7 EXO up to communicate a signal to an external device (e.g., a horn or light) when it goes into a low gas event or high gas alert.



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



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

9.4 EDITING CONFIGURATION PROFILE MODE SETTINGS (G7 AND G7 EXO ONLY)

Use configuration profile mode settings to manage G7 and G7 EXO device 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 device type. Blackline Live currently offers the following configuration modes for each device type:

Mode	G7c	G7x	G7 EXO
Normal Operations	✓	✓	✓
Pre entry	✓	✓	✓
Pump run	✓	✓	
High Risk	✓	✓	
Leak Check	✓	✓	
SCBA	✓	✓	

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

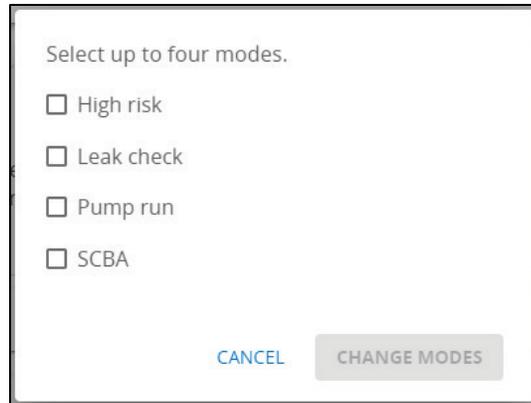
Some modes (Pre entry, Leak Check, SCBA) have a mandatory mode time out feature, which will prompt the user to confirm they are still using the mode after the countdown reaches zero. Because many of the configuration modes modify alert and alarm behavior, this time-out ensures that, in the case the user cannot respond, the device will exit the configuration mode and notify 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:

In the Configuration profile modes card:

1. If you are configuring G7c or G7x:
 - 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 [Blackline Live](#).
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 is required to enter the mode and the pump will start running when the mode is entered on the device.

IMPORTANT: Pump run mode will always run the pump cartridge.

Loner Mobile Configurations

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

If you are using Loner DUO with 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. Alert profiles can be applied to any kind of device type if the emergency protocol contacts are the same for all the devices.

IMPORTANT: If your organization is monitored by Blackline's Safety Operations Center (SOC), you will not be permitted to 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 when an alert is occurring.

IMPORTANT: 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, refer to [Editing Alert Management Profile Details](#).

10.2 CREATING A NEW ALERT MANAGEMENT PROFILE

To create a new alert management profile:

From the Alert management profiles page:

1. Select **Create Alert Profile**. The Alert Management profile details page opens.

For information on how to edit information related to an Alert Management profile, refer to [Editing Alert Management Profile Details](#).

10.3 EDITING ALERT MANAGEMENT PROFILE DETAILS

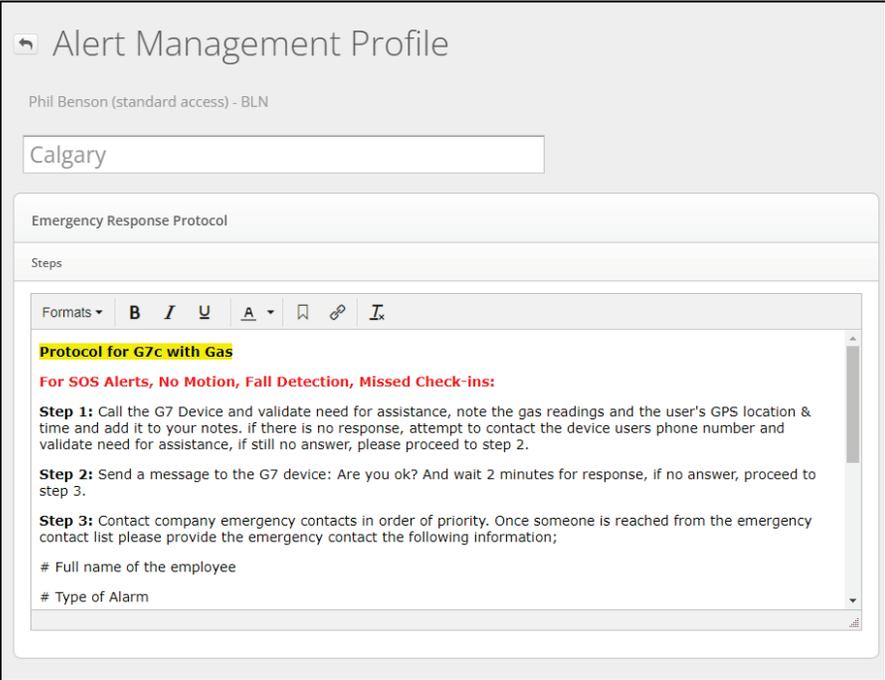
Update an alert management profile by editing cards on the Alert management details page. The page is composed of multiple sections, including emergency response protocol, emergency response contacts, notified contacts, device alerts, and device users.

To edit configuration profile details:

- 1. From the Alert management profile details page, edit any of the following:

Emergency Response Protocol – Review the standard steps monitoring personnel will take in the case of an emergency.

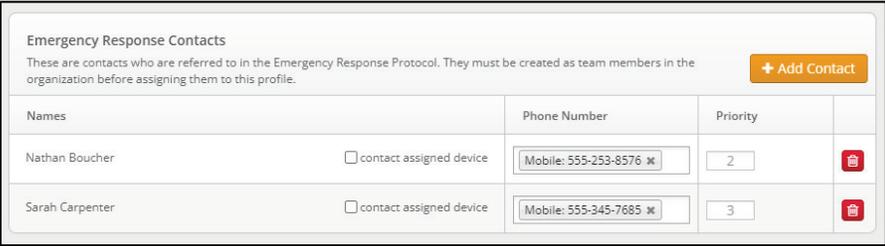
IMPORTANT: Organizations monitored by Blackline’s Safety Operations Center (SOC) will work with Blackline Safety SOC administrators to review and build a protocol. Emergency response protocols should not be modified without consultation with SOC administrators.



Emergency Response Contacts – Manage the emergency response contacts who should be contacted in case of an emergency. Their information will be made available to monitoring services when a device in the alert profile goes into alert, and they will be listed in order of priority of who to call.

NOTE: Ensure that any team members listed as emergency contacts have up-to-date phone numbers in their team member profiles.

IMPORTANT: Always enter phone numbers using a 10- or 14-digit phone number format.



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

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

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

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 alert (Emergency alert)	<input checked="" type="radio"/>	<input type="radio"/>
Silent SOS alert (Silent alert)	<input type="radio"/>	<input checked="" type="radio"/>
Fall detected alert	<input checked="" type="radio"/>	<input type="radio"/>
No motion alert	<input checked="" type="radio"/>	<input type="radio"/>
Missed check-in alert	<input checked="" type="radio"/>	<input type="radio"/>
Tumble alarm (G7 EXO only)	<input type="radio"/>	<input checked="" type="radio"/>
Pump blocked (G7 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"/>
Gas sensor over limit alert	<input type="radio"/>	
High gas alert	<input type="radio"/>	
STEL gas alert	<input type="radio"/>	
TWA gas alert	<input type="radio"/>	

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

IMPORTANT: If any devices require a different protocol or emergency response contacts, put them into separate alert profiles

Device Users			+ Add User
Users	Device Name		
Unassigned	Unit 3566000638		
Angie Hunt	Unit 3567001219		

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

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

For information on how to edit information related to a notification profile, refer to [Editing Notification Profile](#).

11.2 CREATING A NEW NOTIFICATION PROFILE

To create a new notification profile:

From the Notification profiles page:

1. Select **Create Notification Profile**. The Notification profile details page opens.

For information on how to edit information related to a Notification profile, refer to [Editing Notification Profile Details](#).

11.3 EDITING NOTIFICATION PROFILE DETAILS

Update an alert management 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 will result in a notification in Blackline Live by toggling each event type on or off.

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

Device Notification		
Notifications	On	Off
SOS alert (Emergency alert)	<input type="radio"/>	<input checked="" type="radio"/>
Silent SOS alert (Silent alert)	<input type="radio"/>	<input checked="" type="radio"/>
Fall detected alert	<input type="radio"/>	<input checked="" type="radio"/>
No motion alert	<input type="radio"/>	<input checked="" type="radio"/>
Missed check-in alert	<input type="radio"/>	<input checked="" type="radio"/>
Tumble alarm (G7 EXO only)	<input type="radio"/>	<input checked="" type="radio"/>
Pump blocked (G7 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"/>

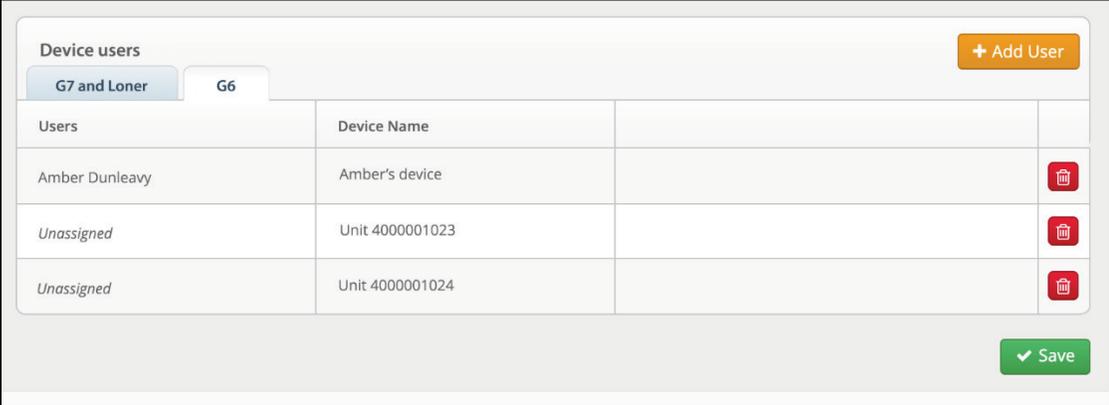
Notified contacts — Manage who should be notified when an alert occurs. Notified contacts will be sent an email, SMS message, or both. Existing contacts can be removed by selecting .



Notified Contacts		+ Add Contact
Names	Contact Method	
Nathan Boucher	SMS	
Doris Knight	All	

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

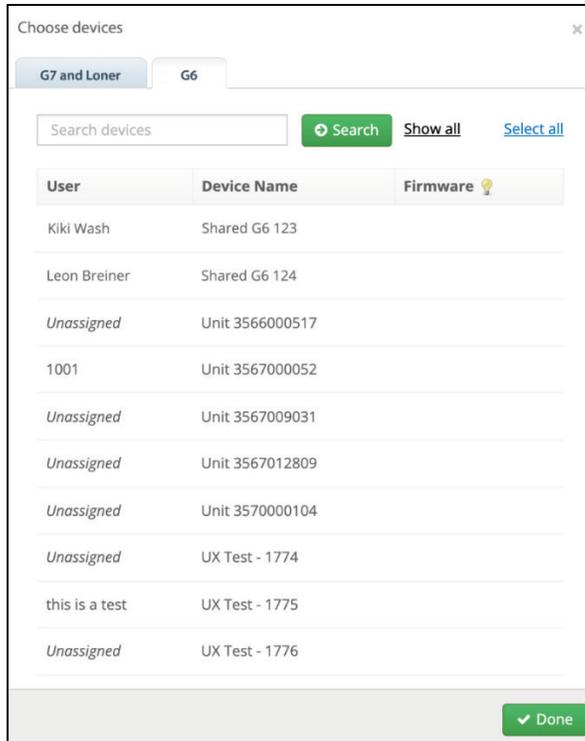
Device users — Add multiple device users to a notification profile so that they share the same notification protocol.



Device users		+ Add User
Users	Device Name	
Amber Dunleavy	Amber's device	
Unassigned	Unit 4000001023	
Unassigned	Unit 4000001024	

[Save](#)

Select [+ Add User](#) to add device users to the notification profile. Existing device users can be removed by selecting .



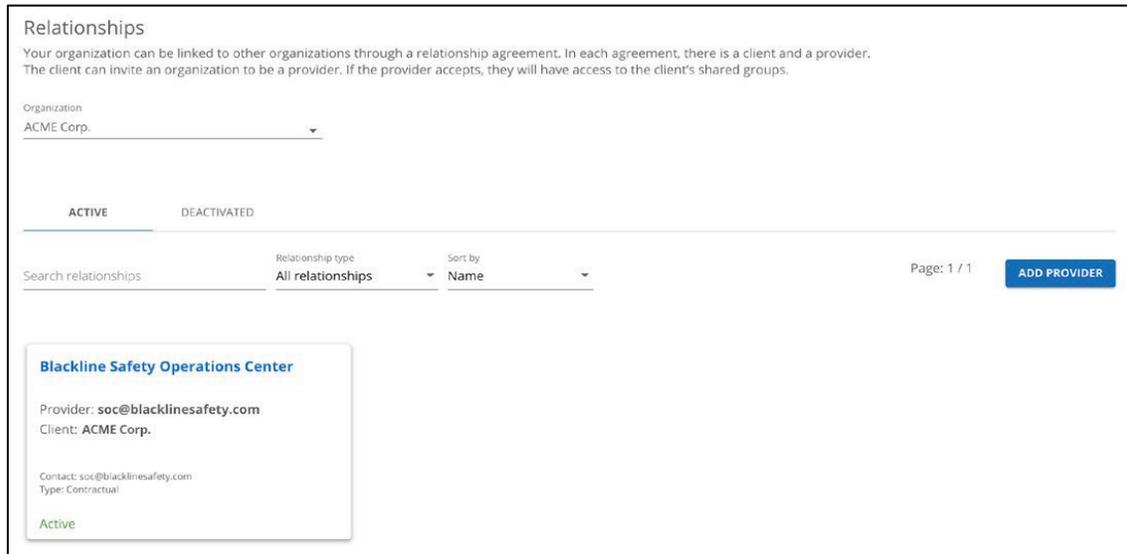
12 MANAGING RELATIONSHIPS

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 will have access to your shared groups.

For more information on relationship structures, refer to [Relationships](#).

12.1 VIEWING ACTIVE RELATIONSHIPS

The Relationships page lists relationships that involve your organization.



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, refer to Editing Relationship Details.

12.2 VIEWING DEACTIVATED RELATIONSHIPS

To view deactivated relationships:

From the Relationship page:

1. Select the **DEACTIVATED** 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 access that the provider will have. If you would like to give another organization access to your resources, you can invite them to be your provider.

To create a relationship:

From the Relationships page:

1. Select **Add Provider**. The Agreement details page opens.
2. Update the agreement details.

You will need to provide a unique relationship name and the email of the Organization admin that will be facilitating your shared resources.

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

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. Contractual relationships cannot be changed by either party after they are agreed upon and require Blackline's [Technical Support](#) team to edit or deactivate the agreement.

For more information on relationship types, refer to [Relationships](#).

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 will automatically have 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 will appear on the Relationships page with a pending status. Once the provider accepts the agreement, this status will change 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 have not been accepted by the provider. Contractual relationships cannot be changed by the client or provider. Contact the Blackline Safety [Technical Support](#) team to make changes or deactivate the relationship.

NOTE: To open any card for editing, 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 e-mail, client, type, and status.

Relationship name
Blackline Safety Operations Center

Contact email
soc@blacklinesafety.com

Provider: soc@blacklinesafety.com
Client: **ACME Corp.**

Type: Contractual

Active

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

G7 and Loner | G6

Search devices

User	Device Name	Firmware
Kiki Wash	Shared G6 123	
Leon Breiner	Shared G6 124	
<i>Unassigned</i>	Unit 3566000517	
1001	Unit 3567000052	

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 all the G6 and G7 docks in your organization and their current configuration status. The list can be searched and sorted.

Docks

This page lists all of the docks you have access to. To update a G7 Dock's settings, select the dock in the list below and edit its profile. To update a G6 Dock's settings, go to the [Configurations](#) page and create or edit a G6 Dock configuration 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 DOCK G6 DOCK

Search devices Columns ▾

DOCK TYPE	DOCK NAME ↑	ACTIVATION CODE	DOCK ID	ORGANIZATION	CONFIGURATION STATUS
 G7 Dock	Dock B12NRJ	B12NRJ	7583	ACME Corp.	active
 G7 Dock	Dock B6HY78	B6HY78	9024	ACME Corp.	active
 G7 Dock	Dock KQHIN8	KQHIN8	1503	ACME Corp.	pending update ⓘ

Items per page: 10 ▾ Page: 1 / 1

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 DOCK** or **G6 DOCK** tab.
3. To open the Dock details page for a dock, select the **DOCK NAME** in the dock list.

For information on updating information for a dock, refer to [Editing Dock Configuration Details](#).

13.2 EDITING DOCK CONFIGURATION DETAILS

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

NOTE: To open any card for editing, 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.



The screenshot shows a form with the following fields and values:

- Dock name***: North shack dock (with a character count of 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).

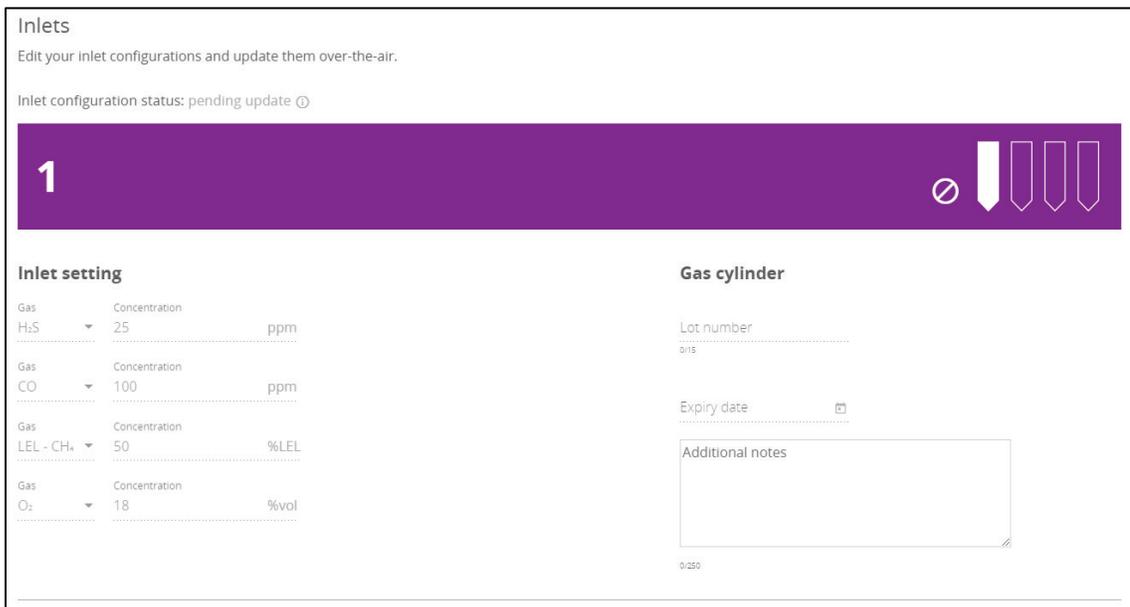
G7 Dock has four gas inlets and one exhaust outlet. Each of the four inlets are represented in the dock configuration page with a diagram indicating where it is located on the device.

NOTE: Docks are pre-configured with common calibration gases when they are shipped out, but this configuration can be updated 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 will cause tests from G7 Dock to fail.

IMPORTANT: Updated docks will 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 and select **Update Dock** from the device menu.

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



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.



blacklinesafety

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 will cause tests from G6 Dock to fail.

NOTE: 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 a web interface for configuring the dock's inlet. At the top, it says "Inlet" and "Edit your inlet configurations and update them over-the-air." Below this, it indicates the "Inlet configuration status: pending update" with a refresh icon. A yellow progress bar is shown. The main configuration area is divided into two sections: "Inlet setting" and "Gas cylinder".

Inlet setting		Gas cylinder
Gas	Concentration	Lot number
H ₂ S	25 ppm	4894038403493
		Expiry date
		11 / 03 / 2021
		Cylinder notes

At the bottom right, there are "CANCEL" and "SAVE" buttons.

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

The screenshot shows a box titled "Last profile change" containing the following information:

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

14 MANAGING LOCATION BEACONS

Location beacons can be set up throughout your work facility to provide more accurate locations in areas with poor GPS coverage, such as inside buildings or in areas with metal scaffolding.

Location beacons represent a single GPS coordinate and transmit this information to nearby G7 devices. When a G7 connects with the beacon, it assumes it is in the location the beacon is transmitting. This location will be sent to Blackline Live in any communication G7 sends while it is in the vicinity of the beacon.



The Beacons page lists all 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	1369000039	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.

For information on updating beacon information, refer to [Placing Location Beacons](#).

14.2 PLACING LOCATION BEACONS

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

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

To place a location beacon:

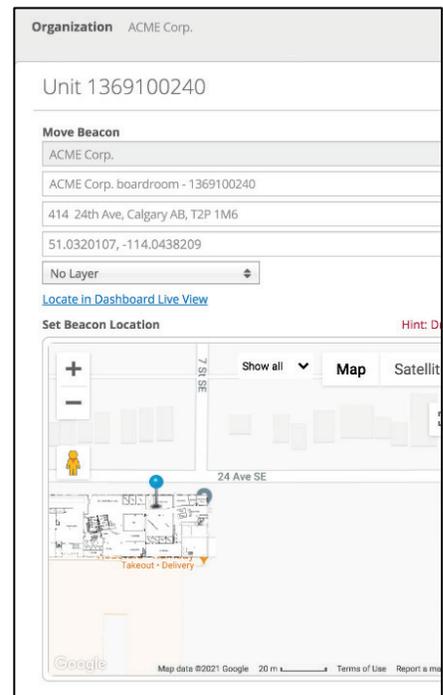
From the Beacons page:

1. 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 floor plans:** Select the layer that corresponds with the floor plan the beacon is on.

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

If you are not using floor plans: Select **No Layer**.

6. After map coordinates are entered, 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, allow monitoring agents to 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 layouts, including rooms, hallways, and doors on the map.

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

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](#).

The floorplan files you provide to Blackline Live for implementation should:

- 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.

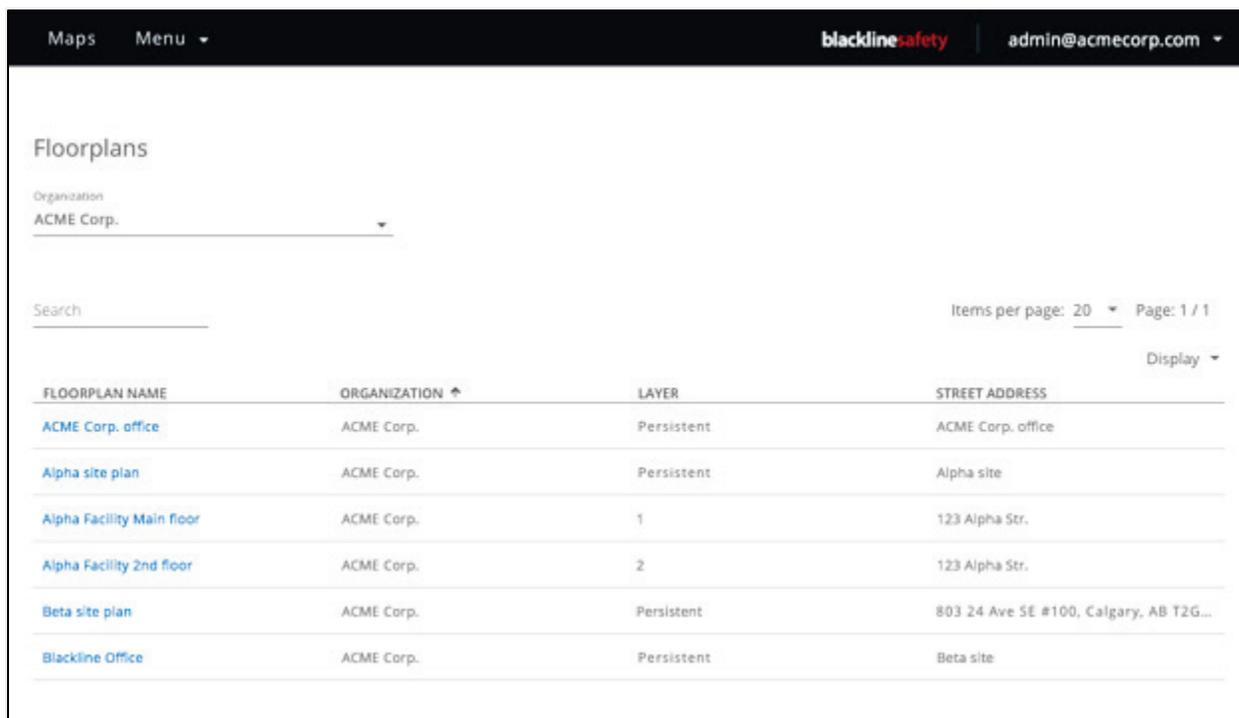
Google Earth files can be created through professional GIS software, or for free using Google's My Maps tool. You can create lines, shapes or markers and place them directly on a map.

Once all the assets have been created, you can export them as an 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

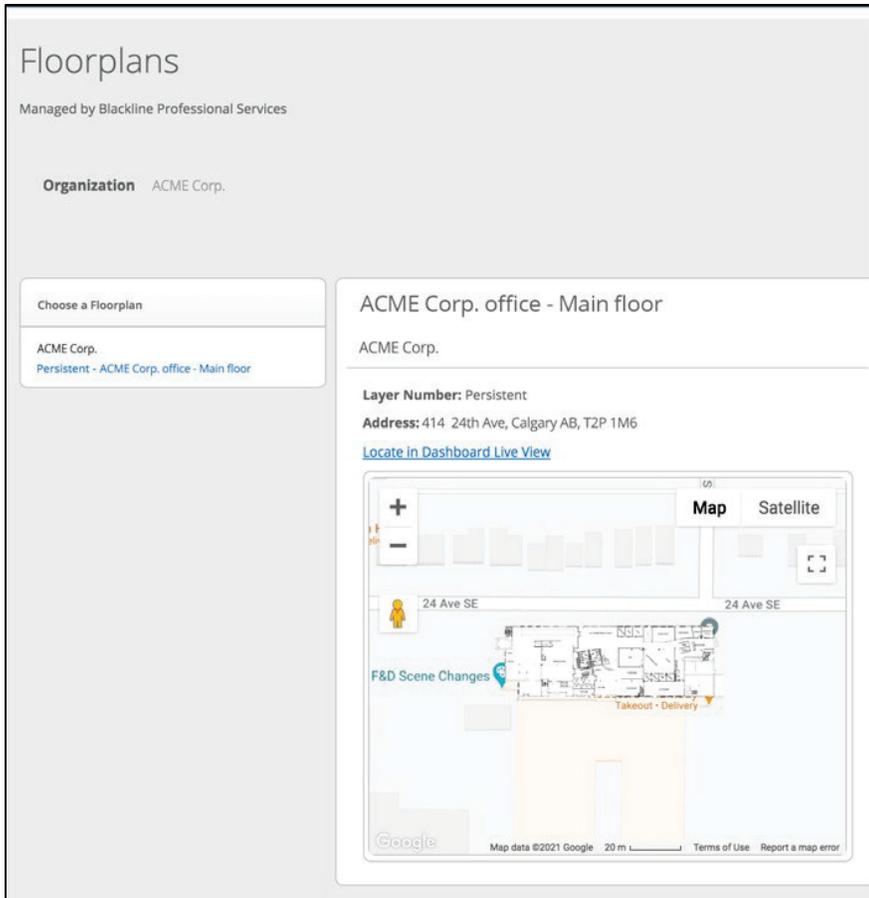
The Floorplans page lists the floorplan name, site address, and the map layer it has been placed on. The list can be searched and sorted.



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:

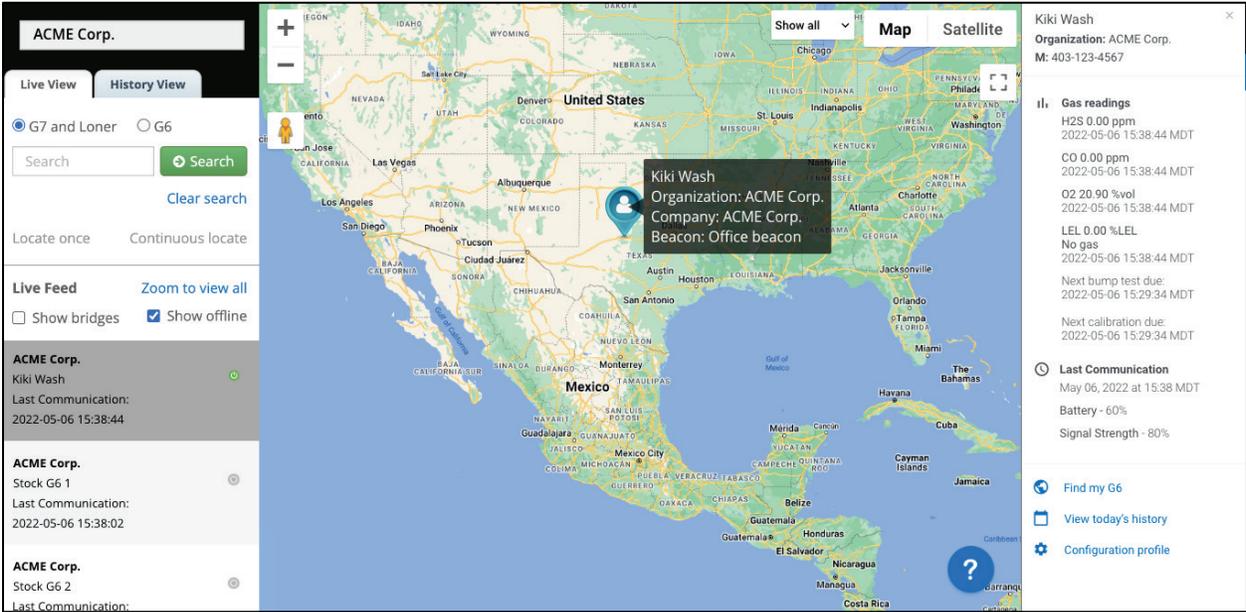
1. From the main menu, select **Floorplans**. The Floorplan page opens.
2. To open the Floorplan details page, select the **FLOORPLAN NAME** in the list. The Floorplan details page opens.



3. 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)

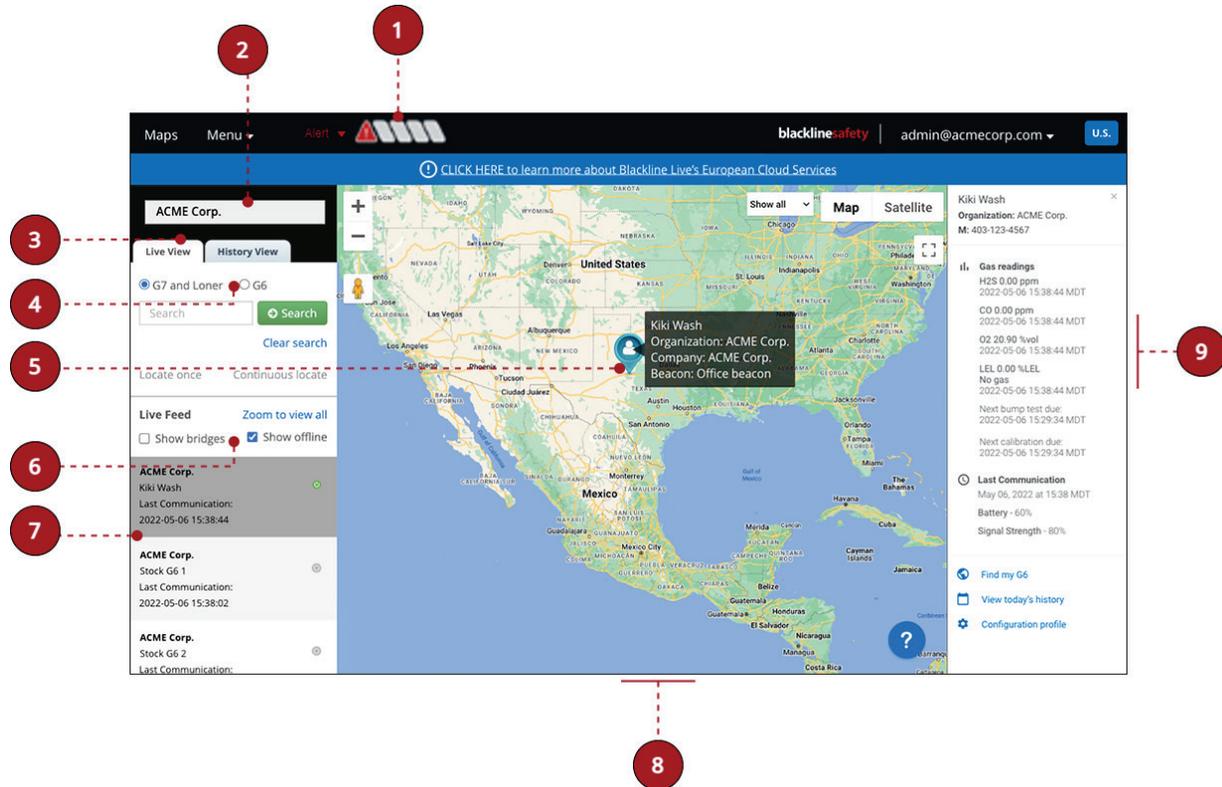
The Maps Live view displays the last known location of online devices and is useful for monitoring the current status and location of your fleet.

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 on 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 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 are also automatically shown at the top left-hand side of the page so that they are easy to identify.



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

6

Display disconnected devices on the Live map view.
NOTE: G6 devices are disconnected by default.

7

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

8

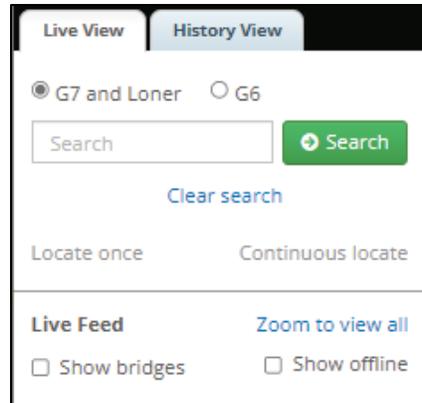
The Maps Live view displays the last known location of online devices and is useful for monitoring the status and location of your organization's devices. The map display can be navigated, minimized, and enlarged as needed.

9

The Info panel displays detailed information about the selected device.

16.1.1 LOCATING DEVICES

By default, the Live map view displays all G7 and Loner or G6 devices in your organization. The device list can be searched and filtered to locate specific devices on the map.



To locate a single device:

In the Live map view menu panel:

1. 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 5 seconds for 10 minutes.

To locate a group of devices:

In the Live map view menu panel:

1. To filter based on device type, select either **G7 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:

In the Live map view menu panel:

1. 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 will list the assigned user's name, or their ID if a name is not available. If the device is not assigned, the info panel will list 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:

- Allows you to message (✉) or call (☎) the device.
NOTE: Taking either of these actions will require an alert to be created. Once redirected to the alert management page, you can use the message text box to send a message or use the provided phone number to initiate a 2-way call with the device.
- Displays the device's alert profile (⚠) and assigned configuration profile (⚙). Selecting either of these links will open the respective profile page.

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**

- Allows you to view a device’s daily history (📅). Selecting the link will direct you to the device in the map history view.

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

- Assigned user name 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 will list the assigned user’s name, or their ID if a name is not available. If the device is not assigned, the info panel will list 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:

- Allows you to activate **Find my G6**.
- Allows you to view a device’s daily history (📅). Selecting the link will direct 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.

16.1.3 MESSAGING A G7 DEVICE

You can send a message device.

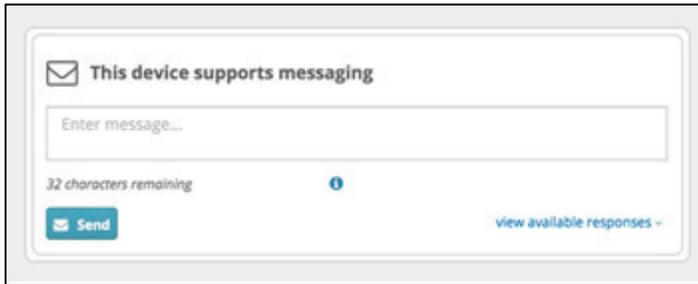
IMPORTANT: If you message a device, an alert will automatically be created.

To message a device:

1. Open the device’s Info panel and select **Message this device**.

An alert will automatically be created and the Alert management page for the device will open.

2. Enter a message and select **Send**.



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

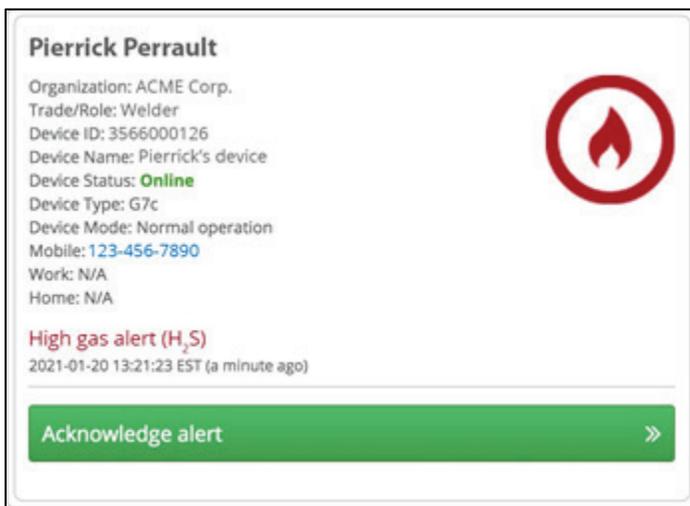
16.1.4 CALLING A G7 DEVICE

You can initiate a 2-way call with a device.

IMPORTANT: If you call a device, an alert will automatically be created.

To call a device:

1. Open the device's Info panel and select **Call this device**.
An alert will automatically be created and the Alert management page for the device will open.
2. Initiate a 2-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 and select the device's configuration profile.



The Configuration profile detail page opens, displaying the device's details. For more information on the configuration profiles, refer to [Viewing Configuration Profiles](#)

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, refer to [Viewing Alert Management Profiles](#).

16.1.7 ACCESSING A DEVICE'S HISTORY

To access a device's history:

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



The Map (Historical View) will open, displaying the device's historical information for the previous 24 hours. For more information, refer to [Accessing Device Information in the Map History View](#).

16.1.8 FINDING A G6 DEVICE

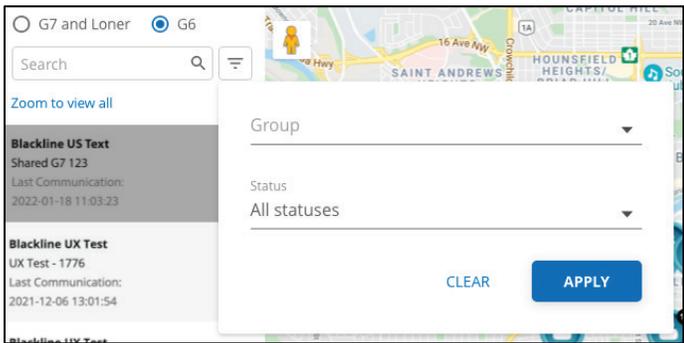
Use Find my G6 to locate missing G6 devices. Devices with this feature toggled on communicate their locations to Blackline Live every 30 minutes for 2.5 hours.

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

To turn on Find my G6:

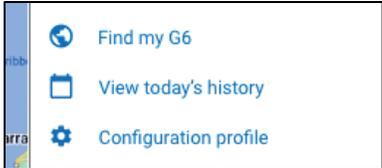
- 1. In the Live map view, locate and select the missing G6 device.

Search for specific G6 devices or filter your device list to display only G6 using the search and filtering tools in the Live map view.



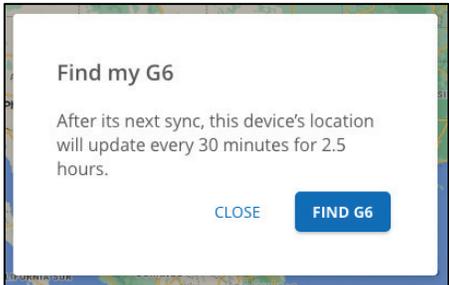
The device's info panel will open, displaying the last known details for the device. The device location pin will indicate the device's location the last time it connected to Blackline Live.

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



The Find my G6 dialog box opens, informing you that the device will connect 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.

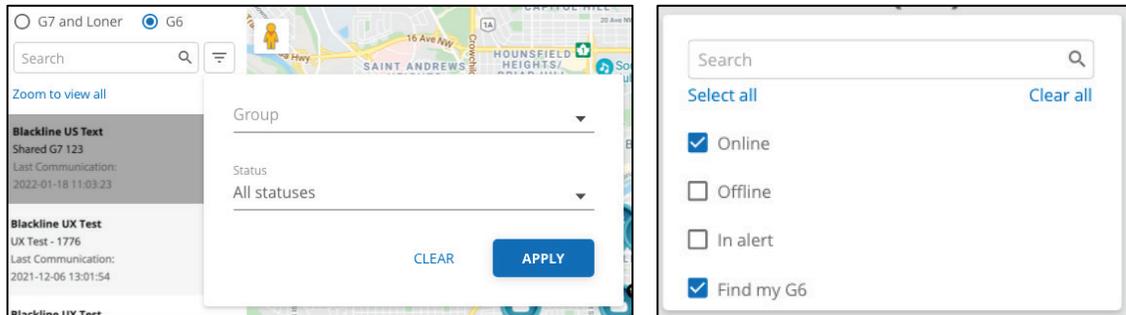


To turn off Find my G6:

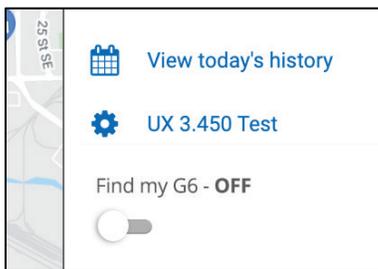
1. In the Live map view, locate and select the G6 device.

The device's info panel will open, displaying the last known details for the device. The device location pin will indicate the device's location the last time it connected to Blackline Live.

NOTE: You can filter for G6 devices with **Find my G6** turned on, using the search and filtering tools in the Live map view.

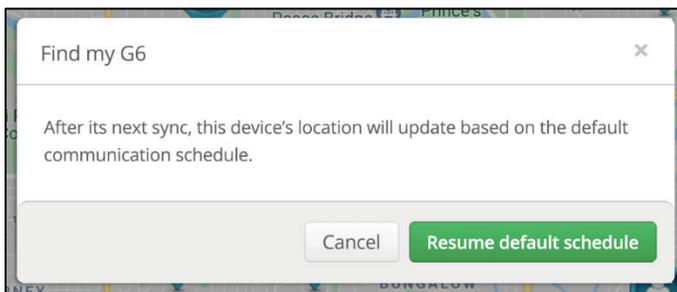


2. In the selected device's Info panel, toggle off Find my G6.



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

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

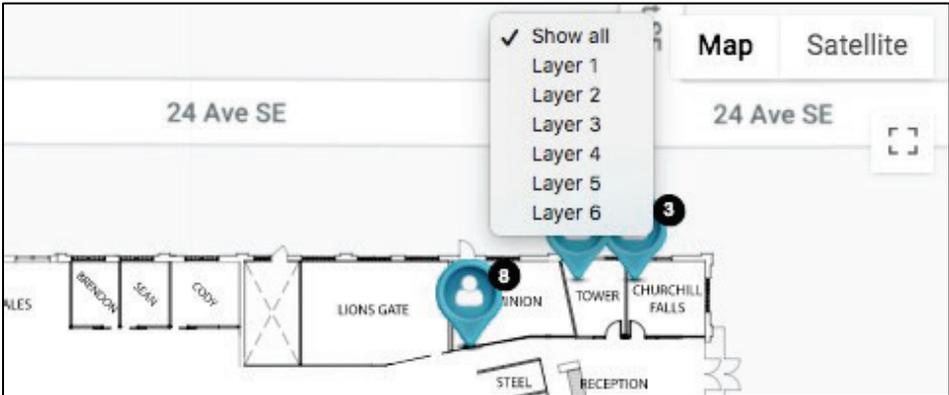


16.1.9 DISPLAYING FLOORPLANS

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



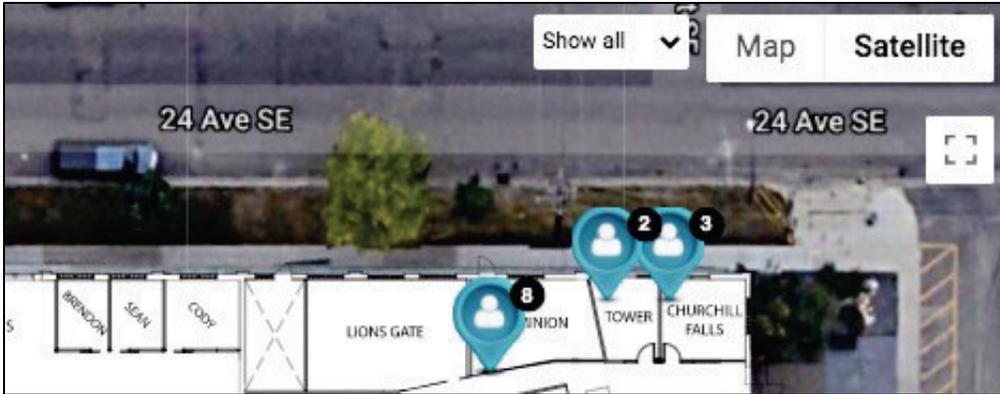
If your organization uses layered floorplans, you can also filter the map view to a particular layer. When filtered, only floorplans and devices communicating with beacons on this layer will be displayed.



TROUBLESHOOTING TIP: If you see a device being 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 if you would prefer to see your floorplans and devices overlaid on detailed satellite images. For workforces operating in remote areas, satellite imagery will provide geographical details and landmarks that may not display in the simplified map view.

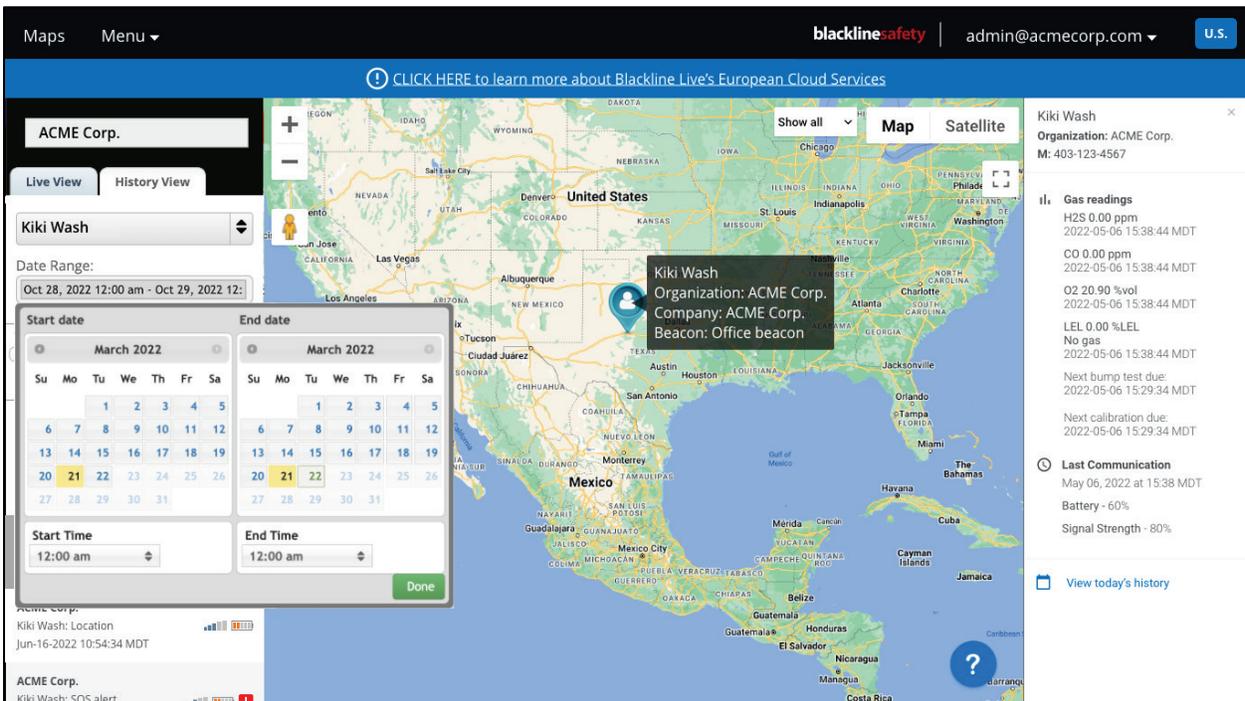


To display satellite imagery:

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

16.2 MAPS (HISTORICAL VIEW)

In the case you need to investigate an incident, track where a device has gone over time, or troubleshoot an issue with the device, you can use History View to learn more about what happened to a particular device. In addition, the page provides several tools for viewing historical data and analytics information:



16.2.1 ACCESSING DEVICE INFORMATION IN THE MAP HISTORY VIEW

To access device information in the Map History View

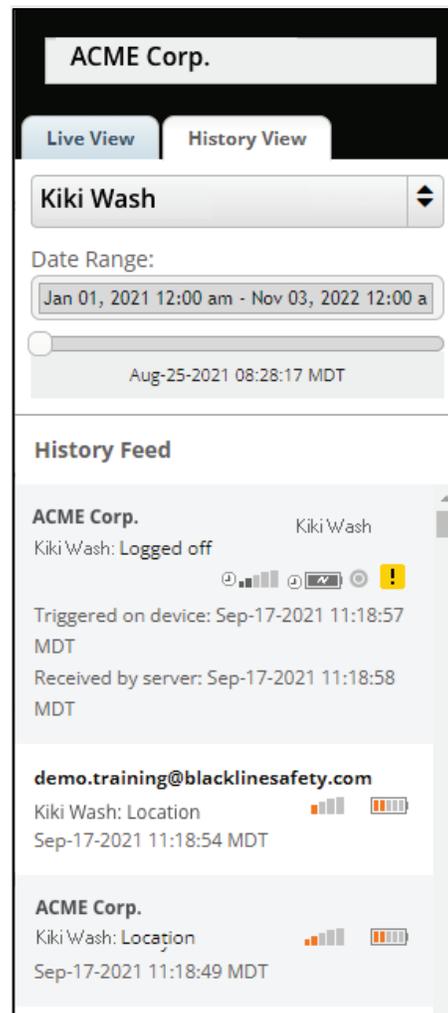
1. From the Maps page, select the **History View** tab.
2. Select a device in the Map.
3. To set a time interval to review for the selected device, select **Date Range**.

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

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 will have their own icons to differentiate them — a check-in will have an  icon, while a message will have an  icon.



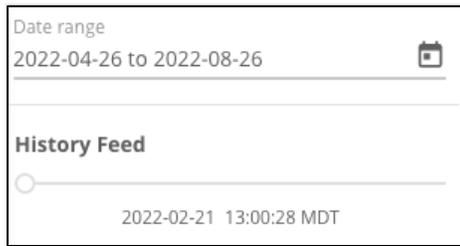
16.2.2 NAVIGATING DEVICE EVENTS IN THE MAP HISTORY VIEW

To navigate device events in the map history view:

1. Hover over the event icon to view the device event summary.
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 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

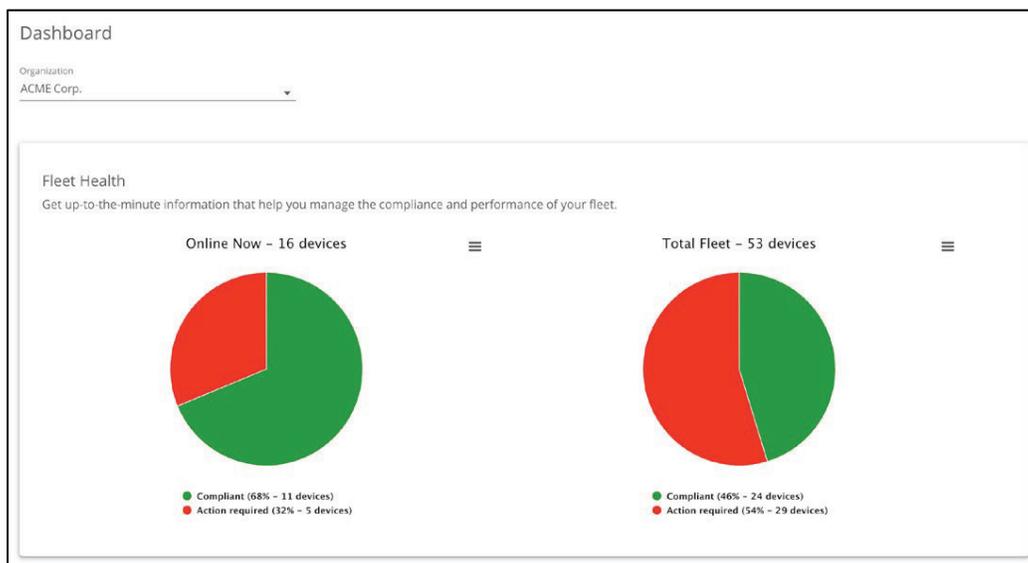
The live dashboard provides a snapshot of the compliance of your entire fleet. Devices that are non-compliant are listed with a description of the issue and the recommended resolution.

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

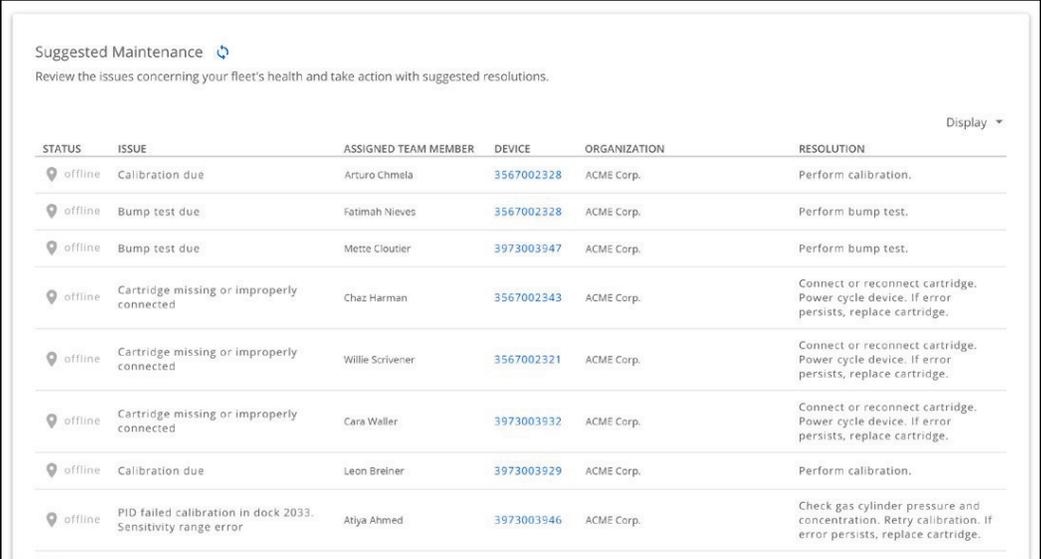
To view the Fleet health dashboard:

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. The information displayed can be printed or downloaded (JPEG, SVG, or PDF).



Suggested Maintenance – The suggested maintenance card displays a list of devices that require maintenance and the maintenance they required (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.

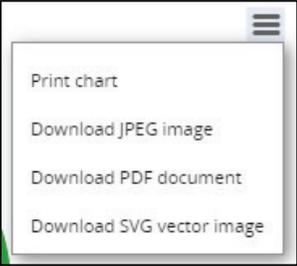
Display 

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:

- 1. In the Fleet health section, select .
- 2. Select the desired download format from the shortcut menu.



To access device details from the dashboard:

From the Compliance Dashboard page:

- 1. 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, refer to [Managing Devices](#).

18 COMPLIANCE CERTIFICATES

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

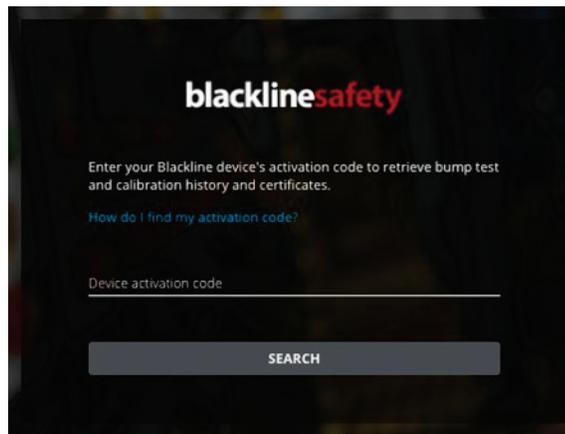
The certification page shows a device's most recent bump test and calibration results. It allows you to view up to 125 days (U.S.) or 7 days (Europe) of device history.

NOTE: The Certification page is hosted independently from Blackline Live and 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/>



2. On the sign in page, enter the activation code of the device.

The Bump test and calibration certifications page will open, 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	Display
2020-11-24 08:00:05 MST	Bump Test	Pass	10123	

Last calibration

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

LOAD MORE

To view more test results, select **LOAD MORE**. All the tests that were performed within the last 125 days (U.S.) or 7 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	Display
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	

3. To view a summary of a specific test, select the timestamp **DATE/TIME** of the test. The summary will display 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.

H ₂ S: Pass	Bump test readings
CO: Pass	H ₂ S: 17.7 ppm
O ₂ : Pass	CO: 91 ppm
LEL: Pass	O ₂ : 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**

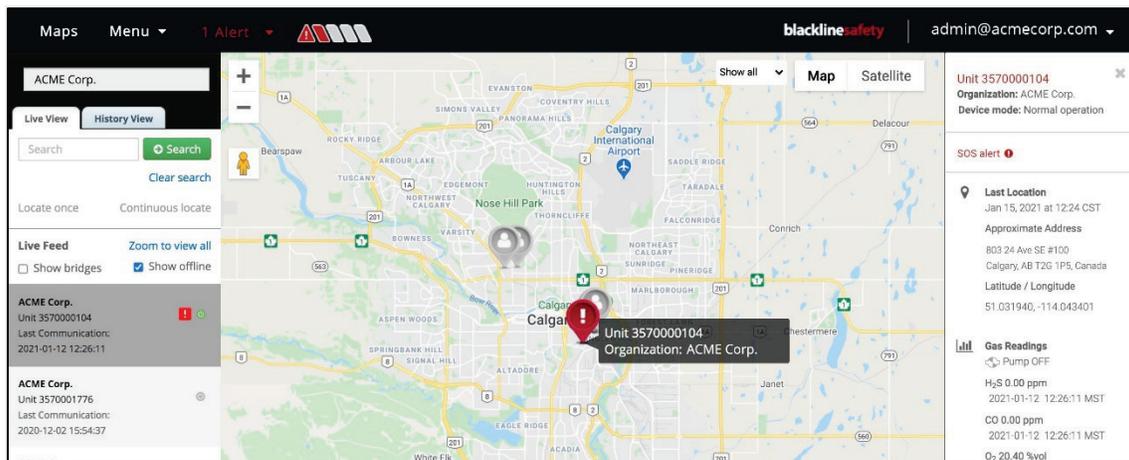
Lights test result: **Pass**
Vibrator test result: **Pass**
Sound test result: **Pass**

Sensor test results: **Pass**
A bump test has passed when the sensor detects 50% of the calibration concentration.

H₂S: **Pass**

19 G7 DEVICE ALERTS

When a G7 device goes into alert, Blackline Live will inform you with a notification in the navigation bar and a loud siren sound. The device in alert will be shown with a red map pin on the Maps page and will appear at the top of the left-hand sidebar.



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

IMPORTANT: Alerts from G6 devices will not be displayed in the Alerts page, will not trigger the Alert banner in Blackline Live, and will not have any alert histories or alert management pages associated with them. For more information on G6 notifications, refer to [G6 Device Notifications](#).

19.1 VIEWING DEVICE ALERTS

The Alerts page 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.



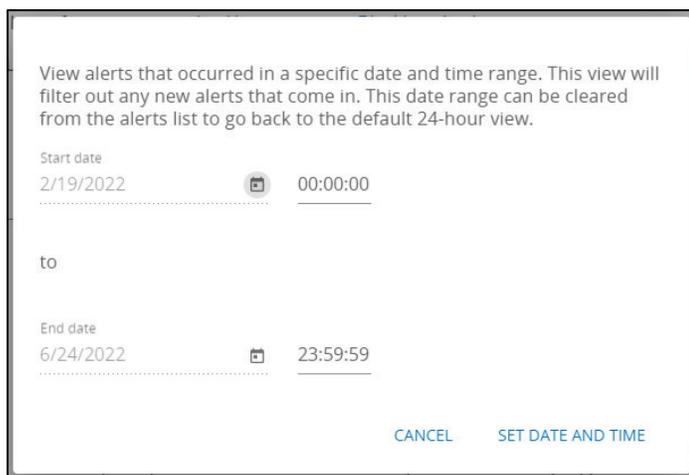
DATE/TIME ↓	STATUS	ALERT TYPE	ASSIGNED TEAM MEMBER	DEVICE ID	DEVICE NAME	ORGANIZATION	OPERATOR	RESOLUTION REASON
2021-01-19 15:00:25 MST	Unacknowledg...	High gas alert (H2S)	Pierrick Perrault	G7c: 3566000126	Pierrick's device	ACME Corp.	--	--
2021-01-19 13:27:23 MST	Resolved	Missed check-in alert	Pierrick Perrault	G7c: 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 have 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:

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

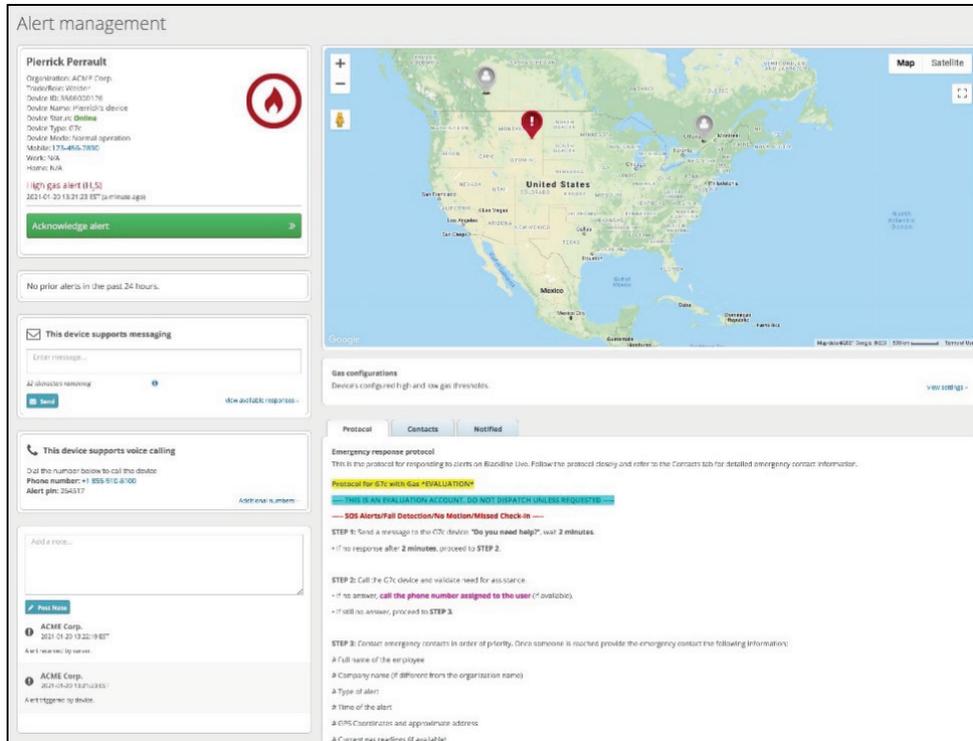


DATE/TIME ↓	STATUS	ALERT TYPE	ASSIGNED TEAM MEMBER	DEVICE ID	DEVICE NAME	ORGANIZATION	OPERATOR	RESOLUTION REASON
2021-01-19 15:00:25 MST	Unacknowledg...	High gas alert (H2S)	Pierrick Perrault	G7c: 3566000126	Pierrick's device	ACME Corp.	--	--
2021-01-19 13:27:23 MST	Resolved	Missed check-in alert	Pierrick Perrault	G7c: 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.



- 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. For more information, refer to [Acknowledging Active Alerts](#).



3. If the alert is **Resolved**, the Alert history page opens, which displays a snapshot of the device's state when the alert occurred, as well as information regarding how and when it was resolved. For more information, refer [Viewing Alert History](#).

19.3 ACKNOWLEDGING ACTIVE ALERTS

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

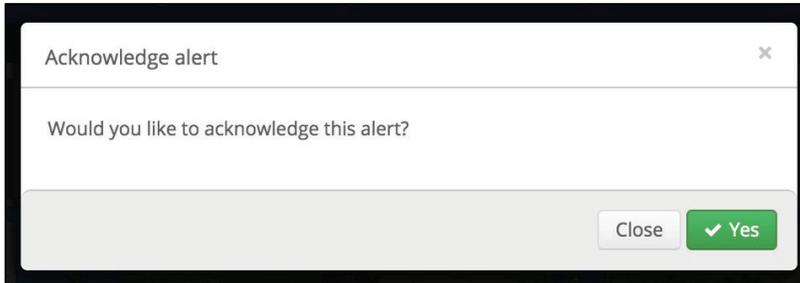
If your organization is self-monitored, or if your organization uses Blackline Live to monitor other organizations, your Account users will be responsible for managing and responding to alerts.

If your organization is monitored by Blackline Safety's SOC or another monitoring service, do not attempt to manage active alerts. Giving Account users the **Contact admin**, **View only**, or **Analytics only** roles will prevent them from being able to interact with alerts. For more information, refer to [Group Roles and Permissions](#).

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.



IMPORTANT: 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.

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
 Organization: ACME Corp.
 Trade/Role: Welder
 Device ID: 3566000126
 Device Name: Pierrick's device
 Device Status: **Online**
 Device Type: G7c
 Device Mode: Normal operation
 Mobile: 123-456-7890
 Work: N/A
 Home: N/A
High gas alert (H,S)
 2021-01-20 13:21:23 EST (a minute ago)

Acknowledge alert >

No prior alerts in the past 24 hours.

This device supports messaging
 Enter message...
 32 characters remaining
Send [view available responses](#)

This device supports voice calling
 Dial the number below to call the device
Phone number: +1 855-910-8100
Alert pin: 264517 [Additional numbers](#)

Add a note...
Past Note

- ACME Corp. 2021-01-20 13:22:19 EST
Alert received by sender.
- ACME Corp. 2021-01-20 13:21:23 EST
Alert triggered by device.

Gas configurations
 Device's configured high and low gas 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 Alerts/Fail Detection/No Motion/Missed Check-in -----

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**.

STEP 3: Contact emergency contacts in order of priority. Once someone is reached provide the emergency contact the following information:
 # Full name of the employee
 # Company name (if different from the organization name)
 # Type of alert
 # Time of the alert
 # GPS Coordinates and approximate address
 # Current gas readings (if available)

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 have occurred on the same device with the same user in the last 24 hours.

Select **Acknowledge alert** to start investigating the alert.

Pierrick Perrault
 Organization: ACME Corp.
 Trade/Role: Welder
 Device ID: 3566000126
 Device Name: Pierrick's device
 Device Status: **Online**
 Device Type: G7c
 Device Mode: Normal operation
 Mobile: 123-456-7890
 Work: N/A
 Home: N/A
High gas alert (H,S)
 2021-01-20 13:21:23 EST (a minute ago)

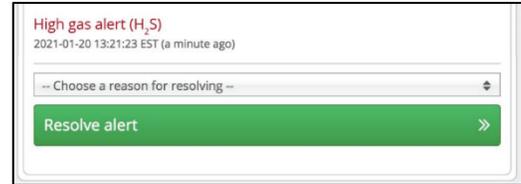
Acknowledge alert >

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 will be cleared from the device, and the device will no longer be 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.

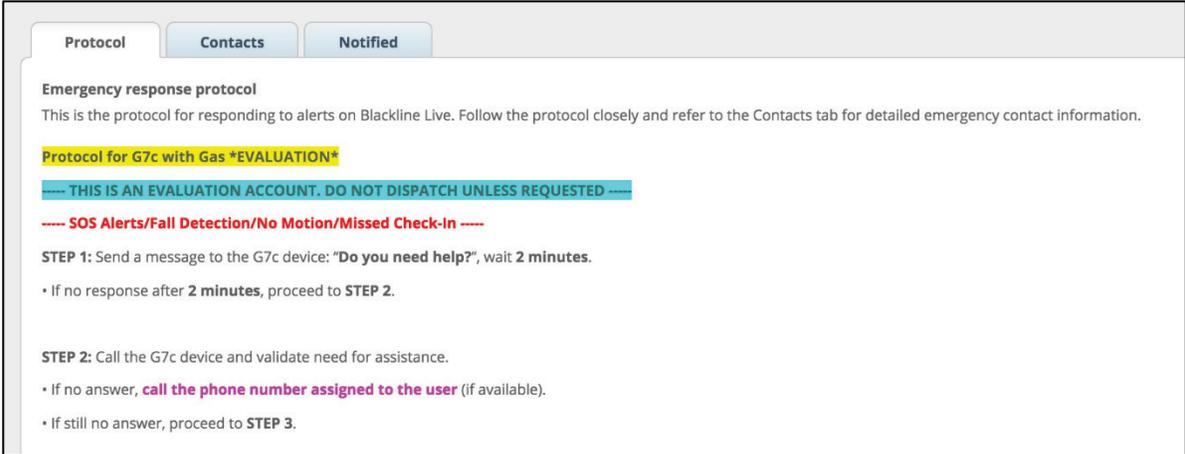
Use the map to identify nearby workers who may be able to help or allow you to provide directions to response or dispatch teams.



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.

IMPORTANT: The information provided is assigned to the device’s configuration profile. It is important to ensure 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](#).



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.

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

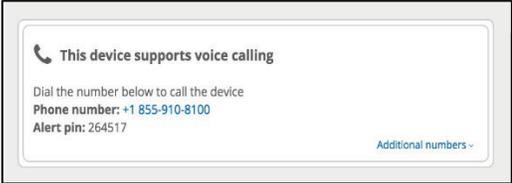


Two-way voice call:

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

If the alert on the device has not been acknowledged 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 is not required to do anything to accept the voice call, and the call will only end when the person on the phone hangs up.



Gas configurations:

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: [G7x Configuration Settings](#)
Configuration version: 4

<p>H₂S Low threshold 5.00 ppm</p> <p>High threshold 10.00 ppm</p>	<p>CO Low threshold 35.00 ppm</p> <p>High threshold 200.00 ppm</p>	<p>O₂ Enrichment Low threshold ↑23.50 %vol</p> <p>Enrichment High threshold ↑25.00 %vol</p> <p>Depletion High threshold ↓18.00 %vol</p> <p>Depletion Low threshold ↓19.50 %vol</p>	<p>LEL Low threshold 10.00 %LEL</p> <p>High threshold 20.00 %LEL</p>
---	---	--	---

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 and selecting **Post Note**.

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

Add a note...

Post Note

ACME Corp.
2021-01-20 13:22:19 EST

Alert received by server.

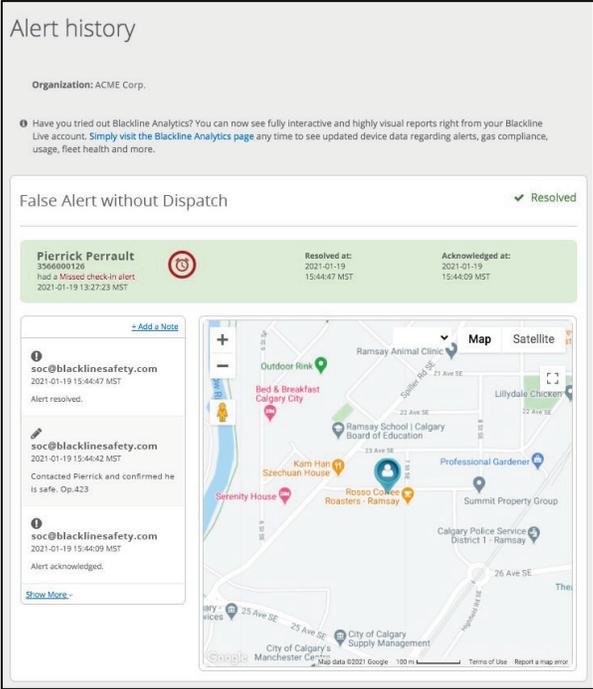
ACME Corp.
2021-01-20 13:21:23 EST

Alert triggered by device.

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



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, refer to [Managing Notification profiles](#).

IMPORTANT: Notifications from G6 devices will not be displayed in the Alerts page, will not trigger the alert banner in Blackline Live, and will 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)

blacklinesafety

Bob Smith
has a **High gas alert (H₂S)**

Employee Id: 00123
Device ID: 1234567890
Device Name: 302 - Bob
Organization: Example Org

Site Address
3004-3041 34 Street Southwest, Calgary, AB T3E 2X1, Canada

Last Known Location (2013-12-10 10:55:03 MST)
IMPORTANT: Located by cellular tower location, not GPS. (location is approximate)



Latitude & Longitude
[51.0318, -114.7537](#)

Hardware Failures

- No failures
- Testing list

Gas Errors

- No gas errors
- Gas Errors Test

Triggered by Device
2013-02-04 05:46:33 MST

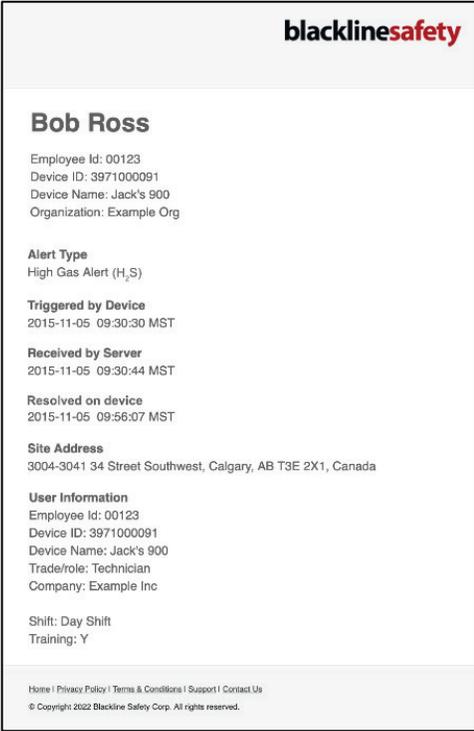
Received by Server
2013-02-04 05:45:59 MST

User Information
Employee Id: 00123
Device ID: 1234567890
Device Name: 302 - Bob
Trade/role: Technician
Company: Example Inc

Shift: Day Shift
Training: Y

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)



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



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

Text Message
Today 12:07 PM

Kiki Wash
Resolved: High gas alert (H₂S)
Time: 2021-11-12
10:07:41
Blackline Live
Notification
Org: Blackline UX Test

21 MASS NOTIFICATIONS

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

IMPORTANT: G6 does not support mass notifications.

Mass notifications

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

Organization
ACME Corp. ▼

Device group *
All devices ▼

Evacuate the
area

Enter up to two lines of 16 characters. %, ^ and accented characters are not supported. 16/32

21.1 SENDING MASS NOTIFICATIONS

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

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.
IMPORTANT: The message must be split into two lines with a maximum of 16 characters on each line.
4. Select **SEND**. The message will be sent to all devices in the specified group.

22 BLACKLINE ANALYTICS

Blackline Live includes a built-in suite of analytics reports that help you to 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 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 Analytic reports are available by default.

Report	G7	G6	G7 EXO
Usage and compliance Displays 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.	✓ (emailed)	✓	✓
Bump tests and calibrations Review your fleet's bump tests and calibrations. Over a chosen period of time, see how many tests are performed, the number of devices tested, how many docks are being used and the overall success rate. Use this report in combination with the usage and compliance report to determine whether compliance trends coincide with bump test and calibration frequency and success.	✓	✓	✓
Devices and cartridges 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 devices cartridges are being used and maintained regularly.	✓	✓	✓

Report	G7	G6	G7 EXO
Docks Delivers information on the locations and usage of docks. Use the map to see where a dock was last used and track each dock's bump test and calibration results to track performance and ensure regular maintenance.	✓	✓	
Device assignment history Tracks 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.	✓	✓	
Alerts (emailed) Full breakdown of alerts occurring on devices. See which device user is triggering the most alerts, when and where alerts are occurring and what types of alerts are most common. Additionally, if you are using our real-time monitoring services you can see the time it takes for alerts to be resolved, resolution trends and the most common resolution reasons.	✓	✓	✓
Events 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 alarms and see when events occur over time.	✓		✓
Events map Explore the locations of your data events. Multiple occurrences of the same type of event might indicate a recurring issue that may require investigation.	✓		✓
Location beacons Communicates 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.	✓		
Device logs Review data from all device alerts from the past seven days. Data from this report can easily be exported by clicking the three dots icon in the top right corner of the table and selecting "export data".	✓		✓
Worker safety analytics Review worker safety trends such as: alerts by device, by day of the week, alerts over a worker's shifts, impact of longer shifts on alerts, alert types by month, and compare alert trends against planned operations and maintenance events. These trends will allow you to narrow down possible root causes and continually improve worker safety.	✓		

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