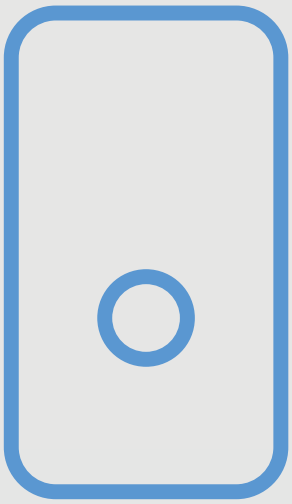


riskband™

ARIES

RiskBand Device User Guide

Version 1.08

August 2020

Published August 2020.

Contents

Preface

Using the RiskBand ARIES™ device you can

- Send emergency alerts to security personnel
- Receive emergency and urgent messages from your organization

RiskBand periodically releases revisions of its software and hardware. Some functions may not be available to all users. Additionally, some functionality described in this document might not be supported by all versions of the RiskBand device and management software.

Contact RiskBand customer support if a product does not function properly or does not function as described in this document: www.riskband.com/support.

11 Quick Start

This chapter describes important functions of the RiskBand device:

- Accepting the Pilot Warning on page 10
- Accepting the End-User License Agreement on page 11
- Sending an Emergency on page 13
- Receiving Messages on page 14
- About Your Privacy and the RiskBand Device on page 16

Additional functionality of the device is described in the chapter Using the RiskBand Device on page 29.

About the RiskBand Device

The key operational and display components of the RiskBand device are:

Accepting the Pilot Warning

If have a received a device that is part of a Pilot or Beta evaluation, the device will display a Pilot warning when it starts up. This warning explains that the device should not be used in any dangerous situations or in an environment where you might be required to trigger and actual emergency. To use the device, you need to accept this warning.

To accept the Pilot warning on the device:

1. 

The Pilot Warning tells you that the devices is an evaluation unit that should only be used in safe, controlled environments for testing purposes.

Note: The Pilot Warning display state is intended to be temporary. While displaying Pilot Warning screen the device will beep and vibrate every minute to remind you to accept the warning.

Accepting the End-User License Agreement

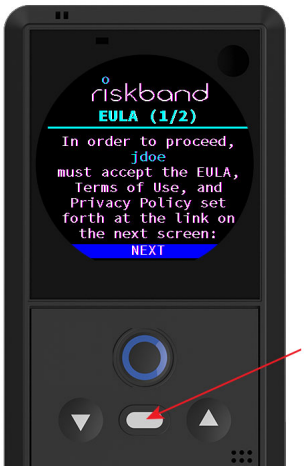
Before using the RiskBand device you must accept the End-User License Agreement (EULA). The EULA consists of

- End-User License Agreement
- Terms of Use
- RiskBand Privacy Policy

The device displays a link to the location of a PDF version of the EULA. You can also review the EULA here: https://us.riskband.com/legal.pdf.

To accept the EULA on the device:

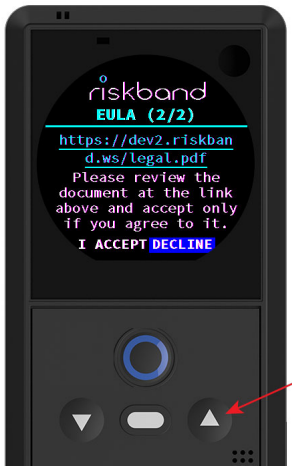
1



After verifying that your username is displayed, press the Menu button to go to the next screen.

Look for your name on the first EULA screen, and then press the Menu button.

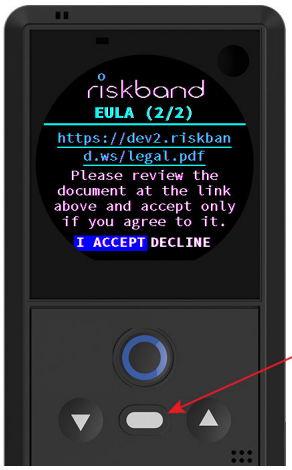
2



Note the URL for the legal agreement. After reading the legal agreement, press the Up button to highlight **I ACCEPT**.

On the second EULA screen, the URL of the EULA PDF file is displayed. You can go to that URL in your browser and read the EULA, or you can read the EULA in the appendices of this document.

3



With **I ACCEPT** selected, press the Menu button to accept the EULA.

Press the Up button to highlight **I Accept**, and then press the Menu button.

4

The device finalizes its configuration, and the assigned screen displays. If you see your user name displayed on this screen, the device is now ready for your use.

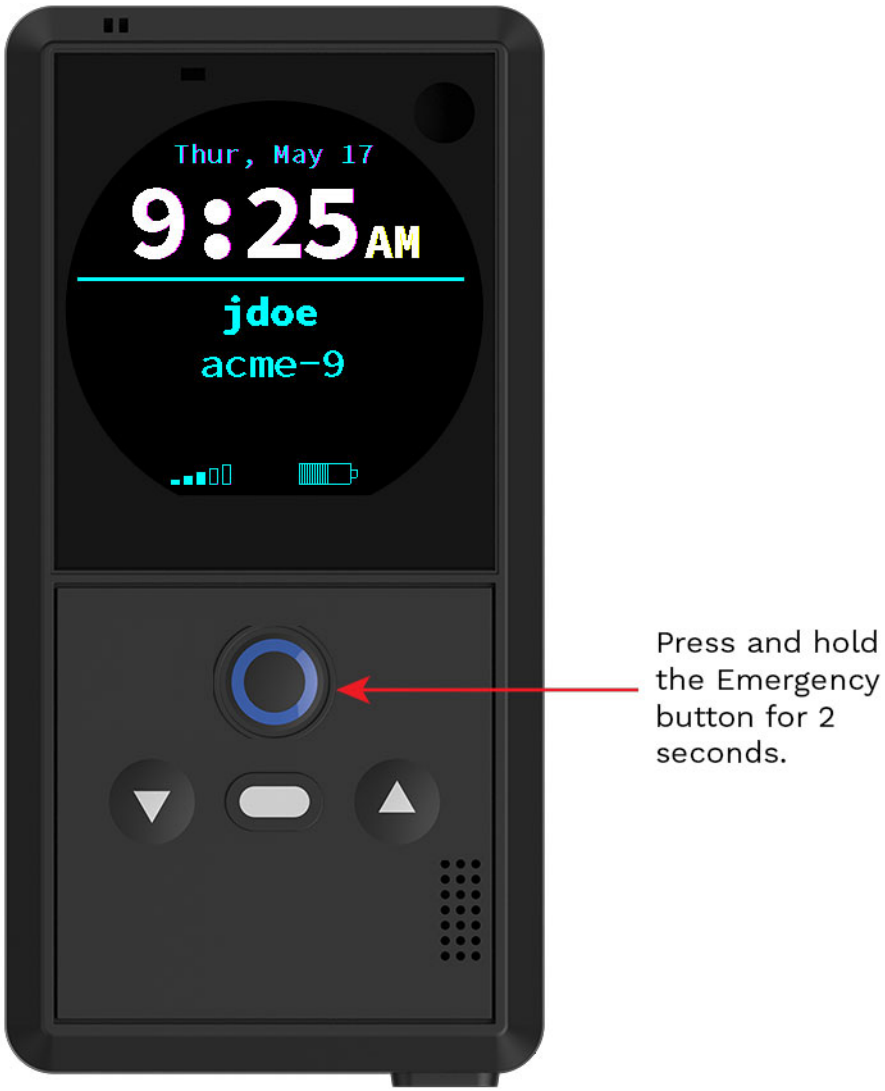
Note: The EULA display state is intended to be temporary. While displaying EULA screens the device will beep and vibrate every minute to remind you to accept the EULA.

Sending an Emergency

When you receive your RiskBand device, it should already be registered and synchronized with the RiskBand servers. You can determine if this is the case by looking to see if your user name is displayed on the device screen. If you see your user name displayed on the screen, it has been configured successfully for your use.

Caution: Do not use a RiskBand device unless you see your user name on the screen. If your user name does not appear on the screen, the RiskBand device may not be able to successfully send an emergency.

To send an emergency, press and hold the Emergency button for 2 seconds.



When the RiskBand servers receive your emergency, your device will vibrate. Following that, at regular intervals throughout the duration of the emergency, the device will vibrate to let you know the emergency continues to be monitored.

If the security personnel responding to your emergency can establish a voice connection to your device, you will feel a rapid vibration pattern. Be aware, however, that after a voice connection is established, the security personnel may choose to just listen with their communication devices on mute.

To experience the vibration patterns that accompany the sending and receipt of emergencies, you can simulate an emergency in Demo Mode. For instructions on how to do this, see Simulating an Emergency in Demo Mode on page 17.

Receiving Messages

The security personnel in your organization can send messages to the RiskBand device. These messages can be Emergency Action Messages (EAMs) or informational Action Messages (AMs). When either type of message is received by the RiskBand device, the device vibrates to alert you that you have a message. The device will also beep if the message is an Emergency Action Message.

Note: After Emergency Action Messages are received, the device will vibrate and beep every 15 seconds until the message is read.

Emergency Action Message

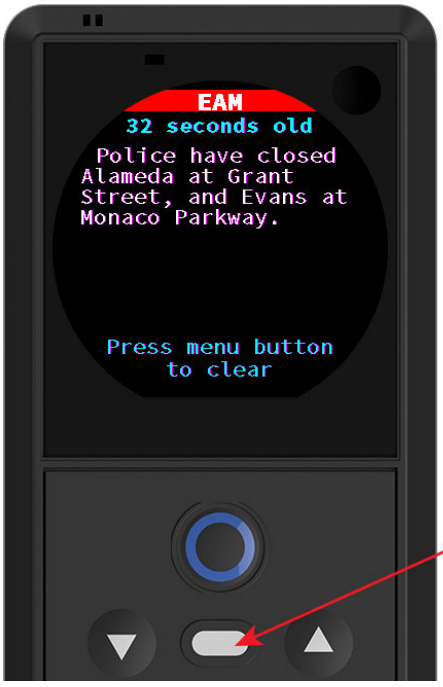
Action Message

To read an Emergency Action Message or an Action Message, press the Menu button.

Press the Menu button to display messages.

To acknowledge a message, clear it, or read the next message on your device, press the Menu button. After all the messages are displayed, the device returns to the main screen.

Note: After a message is cleared, it cannot be displayed again on the device. However, if your organization has provided you with access to the RiskBand ARIES Manager, you can view a history of action messages that have been sent to your device.



Press the Menu button to clear messages after you have read them.

About Your Privacy and the RiskBand Device

While the RiskBand device is capable of taking photos and of creating a two-way voice connection, it only does so when an emergency is triggered. And in the vast majority of cases, you will be the one who triggers the emergency by pressing the alarm button. This means that the RiskBand device cannot be used to spy or eavesdrop on you unawares.

In some deployments, your organization may have the ability to trigger an emergency remotely. That is, the device can be put into the emergency state without your pushing the button. However, in these cases the device still vibrates and displays icons when the emergency in initiated. Even if your organization uses “stealth mode” in emergencies—which means there is no visual display that an emergency is in process—the device still vibrates so you will know the emergency state has been initiated.

Check with your organization administrator to see if either remotely triggered emergencies or stealth mode emergency indicators are enabled for your device. Your organization administrator can tell you exactly how your device will act in an emergency.

2 Simulating an Emergency in Demo Mode

The RiskBand device is programmed with a Demo Mode simulation that allows you to experience how the device handles an emergency first hand. RiskBand strongly recommends that you go through the Demo Mode simulation in order to learn how the device will vibrate and operate during an emergency.

Note: Some organizations my restrict devices from entering Demo Mode.

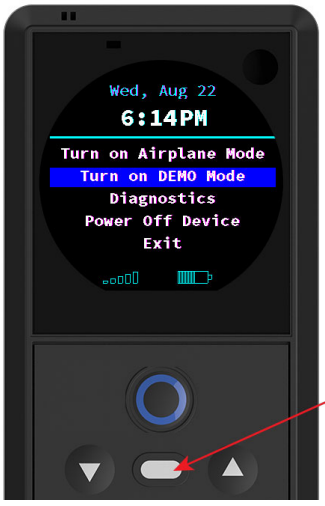
Because this is intended to be a temporary state for the device, the device will beep and vibrate every 15 minutes while in this mode to remind you to exit Demo Mode.

Putting the Device in Demo Mode

To display the device menu, press the Menu button.

Press the Up button until **Turn on DEMO Mode** is highlighted.

3



Press the Menu button to select **Turn on DEMO Mode**.

With **Turn on DEMO Mode** highlighted, press the Menu button.

4

Press the Up button to select **YES**.

Press the Up button to select Yes.

5

Press the Menu button to enter Demo Mode.

With **Yes** highlighted, press the Menu button to enter Demo Mode.

6

The device vibrates and enters Demo Mode. The word DEMO appears on the screen. The color of the word DEMO alternates between red and yellow.

Triggering an Emergency in Demo Mode

1

Press and hold the Emergency button for 2 seconds to simulate an emergency in Demo Mode.

With the device in Demo Mode, trigger an emergency by pressing the Emergency button for 2 seconds.

2

The ring indicates the emergency has been sent but has not yet been acknowledged.

A ring appears on the screen to let you know the emergency has been sent.

3

The device then simulates acknowledgment by the RiskBand servers of your emergency by vibrating briefly. The red GPS icon indicates that GPS coordinates have not yet been established for this emergency.

4

The ring changes to a doughnut, indicating that the emergency has been registered.

The ring changes to a blue doughnut when the emergency is registered with the RiskBand ARIES Manager. After the GPS coordinates are established, the arrow disappears.

5

The ring is completely filled, indicating that the emergency is fully engaged.

When the emergency is fully engaged—it is registered, the GPS coordinates are established, and the voice connection has been made—a blue circle appears on the screen.

6

The device gives a short, rapid vibration. You can simulate closing an emergency demo by pressing and holding the Menu button for 3 seconds. The device vibrates when the assigned screen displays. Every 15 minutes the device will beep twice and vibrate to remind you the device is still in Demo Mode.

7

The blue cloud icon indicates that there are still photos on the device that need to be uploaded.

After an emergency has been closed, if there are photos on the device that need to be uploaded to the RiskBand servers the blue cloud icon appears.

8

The red cloud icon indicates that there are still photos on the device that need to be uploaded, but the battery level is too low to upload photos

If the battery level is low, the device will suspend uploading photos from a closed emergency and display the red cloud icon. It will continue uploading photos after the battery is charged.

Taking the Device Out of Demo Mode

To display the device menu, press the Menu button.

Press the Up button until **Turn off DEMO Mode** is highlighted.

3

With **Turn off DEMO Mode** highlighted, press the Menu button.

4

Press the Up button to select Yes.

5

With **Yes** highlighted, press the Menu button to exit Demo Mode.

6

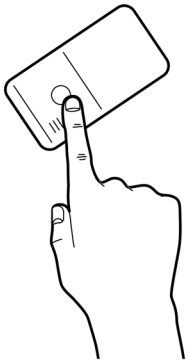
The device exits Demo Mode, and the assigned screen displays.

3 Behind the Scenes with RiskBand

The RiskBand device is designed to not draw attention to itself in an emergency. However, even though the device may not seem to be doing anything, there is a lot happening in the background when you initiate a RiskBand emergency.

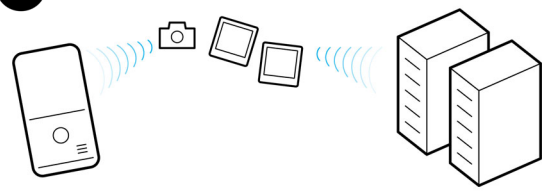
The RiskBand system is very customizable, and not every organization will utilize every feature. The actual response to an emergency will vary according to the policies and procedures of your organization, but as a general rule, here's what happens.

1



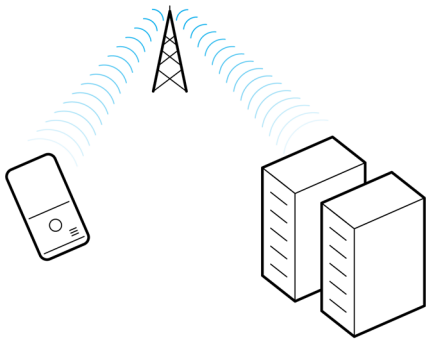
A single press of the Emergency Activation Button on your RiskBand device generates an emergency.

2



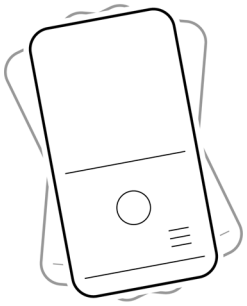
The RiskBand device begins to take photographs and uploads them to the RiskBand servers where they are available to your security personnel. Additionally, your GPS location is immediately updated.

3



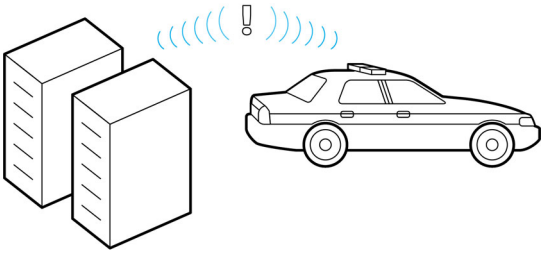
The RiskBand servers receive the alert and immediately attempt to send your device an acknowledgment.

4



The long vibration pattern on your device tells you that the emergency has been received.

5

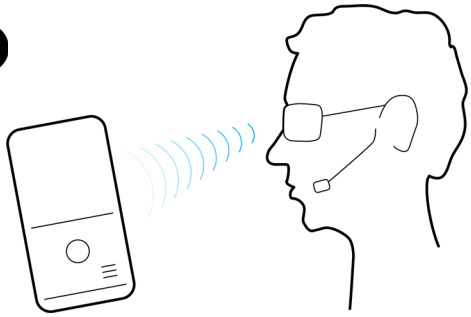


The RiskBand servers send an alert to the security personnel for your organization.

6

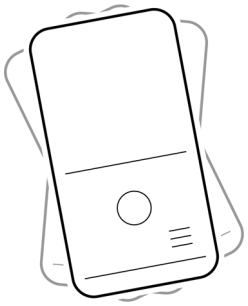
Information about you and your situation is available to security personnel.

7



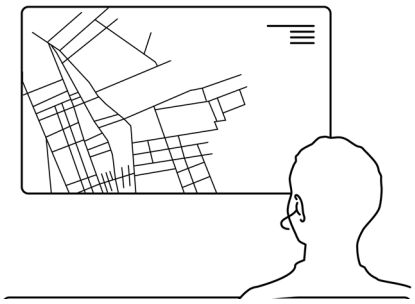
The device will initiate a call to establish two-way voice communication with a designated response team.

8



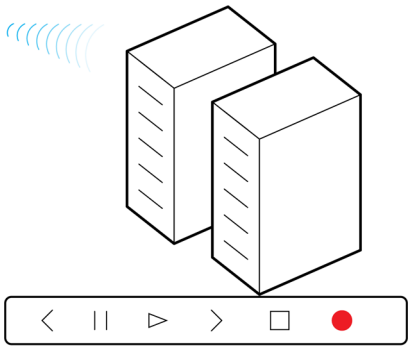
The second long vibration pattern on your device confirms that the voice connection has been established.

9



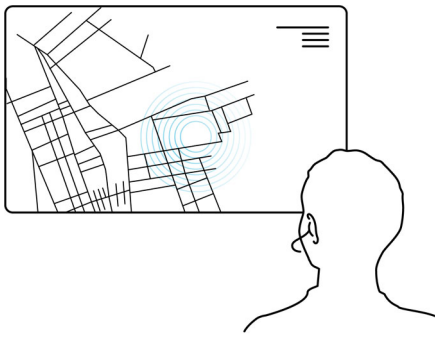
Even though voice communication has been established, designated responders will likely “listen on mute” while learning more about your current situation.

10



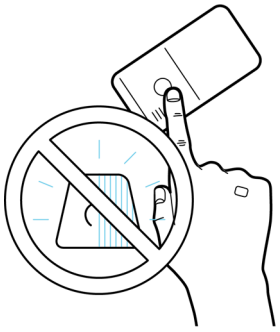
All the audio from this voice connection is recorded.

11



If your organization has enabled GPS on your device, a map showing your exact location is available to the designated responders.

12



If your organization allows self-cancellation, there is a short period of time where you can cancel an emergency by pressing and holding the Menu button. After that only designated responders can cancel the emergency.

4 Using the RiskBand Device

This chapter describes actions that can be performed with the RiskBand device:

Note: Most menu selections require you to confirm your selection.

Triggering and Canceling Emergencies

To trigger an emergency, press and hold the Emergency button for 2 seconds.

To activate an emergency, press and hold the Emergency button for 2 seconds. For additional details on what happens during an emergency, see Sending an Emergency on page 13

To cancel an emergency, press and hold the Menu button for 5 seconds.

Depending on your organization's policies, you may have a brief period of time to self-cancel an accidentally triggered emergency from your device.

If you have successfully self-canceled an emergency, a red line will display across the ring, donut, or filled-in circle.

Note: The ability to self-cancel an emergency is managed by your organization's policies. With some policies, you are not allowed under any circumstances to self-cancel an emergency. With other policies, you may be allowed to cancel an emergency within 20 seconds or 60 seconds of triggering it. Or you may be allowed to cancel up to the point when the emergency is registered with the RiskBand servers.

Triggering an Emergency from Impact Detection

One of the advanced safety options that can be configured on the device is impact and fall detection. If this option is enabled on your device, then abrupt impacts—that might be caused by falling down or being in an automobile—can trigger an emergency. As not every fall or impact results in the need to trigger an emergency, the device beeps and asks you if you are OK. At this device prompt, you can press the menu button to cancel the pending emergency, or you can press the emergency button to trigger an emergency. You can also let the timer on the prompt expire and the emergency will trigger automatically.

Press the Menu button to cancel the pending emergency if you are okay.

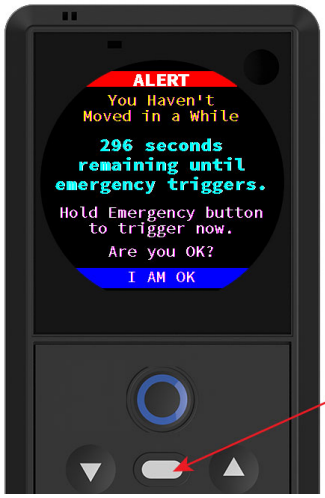
If you experience a fall or impact, but you are not hurt and do not require emergency attention, press the **Menu** button to cancel the pending emergency.

Press the emergency button to trigger an emergency if you are hurt or need assistance.

If you are injured or require attention, press the **Emergency** button to trigger the emergency immediately. Or if you let the time expire, the emergency will trigger automatically.

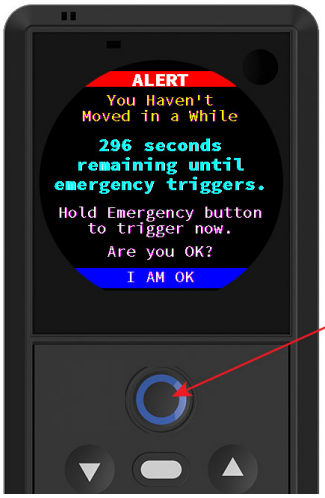
Triggering an Emergency from “Man Down” Detection

Another advanced safety option that can be configured on the device is the “man down” feature. If this option is enabled on your device, then extended periods of inactivity—that might be caused by passing out for a period—can trigger an emergency. As not every period of immobility results in the need to trigger an emergency, the device beeps and asks you if you are OK. At this device prompt, you can press the menu button to cancel the pending emergency, or you can press the emergency button to trigger an emergency. You can also let the timer on the prompt expire and the emergency will trigger automatically.



Press the Menu button to cancel the pending emergency if you are okay.

If you have fainted, dozed off, or otherwise have not moved for a period of time, but you are OK and do not require emergency attention, press the **Menu** button to cancel the pending emergency.



Press the Emergency button to trigger an emergency if you are hurt or need assistance.

If you are not OK or require attention, press the **Emergency** button to trigger the emergency immediately. Or if you let the time expire, the emergency will trigger automatically.

Reading and Clearing Messages

For additional information on displaying and clearing messages, see Receiving Messages on page 14.

To read a message that has been sent to the RiskBand device, press the Menu button.

After you have read a message, pressing the Menu button will clear the message and then display the next message. Or if there are no other messages, the device will display the assigned screen.

Accessing the RiskBand Device Menu

To access the options on the RiskBand device menu, press the Menu button.

To access the options on the RiskBand device menu, press the Menu button.

When the option you want is selected, press the Menu button.

Device Menu: About Airplane Mode

Airplane Mode on the RiskBand device is similar to Airplane Mode on mobile phones. It temporarily deactivates the connection to the cellular network. While the RiskBand device is in Airplane Mode, the device will not receive any messages and your security personnel will not be able to trigger an emergency remotely. However, while the device is in Airplane Mode, you can trigger an emergency by pressing and holding the Emergency button for 2 seconds.

Note: Some organizations do not allow devices to go into airplane mode.

Putting the Device in Airplane Mode

Press the Menu button to enter Airplane Mode.

With the RiskBand device menu displayed and with the **Turn on Airplane Mode** option selected, press the Menu button to enter Airplane Mode.

While the device is in Airplane Mode, the airplane icon appears on the screen.

Note: When triggering an emergency when the device is in airplane mode, there can be a delay of up to 90 seconds for the device to reconnect to the network and register an emergency with the RiskBand ARIES Manager. This delay can be even longer if there is no network or data connectivity in your location.

Taking the Device out of Airplane Mode

With the RiskBand device menu displaying and with the **Turn off Airplane Mode** option selected, press the Menu button to turn off Airplane Mode.

The device exits Airplane Mode, and the airplane icon is removed from the screen. The assigned screen appears.

Device Menu: Turning Demo Mode On and Off

For additional information on Demo Mode, see Simulating an Emergency in Demo Mode on page 17.

With the RiskBand device menu displaying, and with the **Turn on DEMO Mode** option selected, press the Menu button to enter Demo Mode.

With the RiskBand device menu displaying, and with the **Turn off DEMO Mode** option selected, press the Menu button to turn off Demo Mode. The device will return to the main screen.

Device Menu: About Diagnostics

To support troubleshooting issues that may arise with using the RiskBand device, the device menu provides access to the following diagnostic tools and screens:

- Synchronize with Server
- About this Device

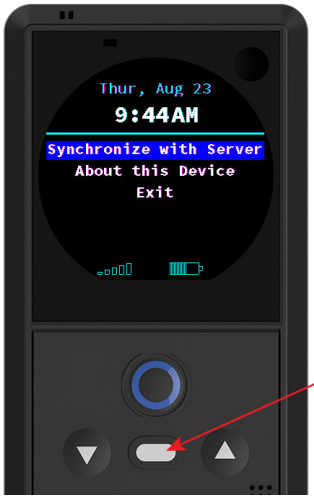
Press the Menu button to display diagnostic tools and screens.

With the RiskBand device menu displayed, and with the **Diagnostics** option selected, press the Menu button to display the diagnostic tools and screens.

Select a diagnostic option and press the Menu button.

Synchronizing with the RiskBand ARIES Manager

The RiskBand device automatically syncs with the RiskBand server. However, if instructed to do so by RiskBand customer support, you can force your device to synchronize.



Press the Menu button to synchronize the device with the server.

With the RiskBand device menu displayed, and with the **Synchronize with Server** option selected, press the Menu button to synchronize your device with the RiskBand servers.

Any pending messages or emergencies on the server will be sent to your device, and your GPS coordinates will be updated.

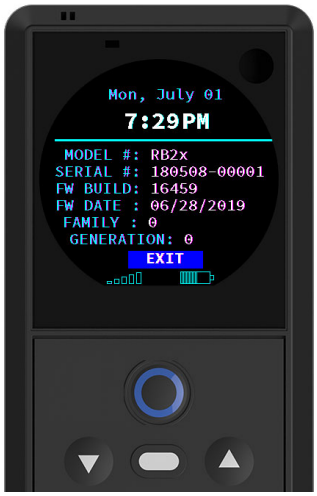
The device initiates a “call home” operation and displays the Synchronizing screen. After the synchronization request is sent to the RiskBand ARIES Manager, the device displays the assigned screen.

Displaying Device Information

In some cases, customer support or security personnel may need detailed information about your device like the serial number or SIM card number. This information can be displayed by selecting the **About this Device** option from the device menu.

Press the Menu button to display device information.

With the RiskBand device menu displayed, and with the **About this Device** option selected, press the Menu button to display information about the device.



This is an example of the device information that is displayed. From this screen, press the Menu button to return to the assigned screen.

Device Menu: Powering Off the RiskBand Device

The ability to power off your device is dependent upon the security policy that has been assigned to it. If your organization allows devices to be powered off, you can select **Power Off Device** from the device menu.

Note: If your device is unresponsive, and you are not able to access the device menu, you can restart the device manually. See Restarting the Device Manually on page 40. If restarting the device does not allow you to access the device menu, contact customer support for instructions on how to proceed.

With the RiskBand device menu displayed and with the **Power Off Device** option selected, press the Menu button to power off the device.

To Power On the device, hold the Menu button down for three seconds. After you feel a short vibration on the device, release the menu button.

Caution: It can take 1-2 minutes for the device to power on completely. Do not use a RiskBand device unless you see your user name on the screen. If your login name does not appear on the screen, the RiskBand device may not be able to successfully send an emergency.

Device Menu: Restarting the Device

If your organization does not allow devices to be powered off, the device menu displays the option to **Restart Device**.

Note: If your device is unresponsive, and you are not able to access the device menu, you can restart the device manually. See Restarting the Device Manually on page 40. If restarting the device does not allow you to access the device menu, contact customer support for instructions on how to proceed.

Press the Menu button to Restart the device.

With the RiskBand device menu displayed and with the **Restart Device** option selected, press the Menu button to restart the device.

The device restarts, and the assigned screen displays.

Caution: It can take 1-2 minutes for the device to fully reset. Do not use a RiskBand device unless you see your user name on the screen. If your name does not appear on the screen, the RiskBand device may not be able to successfully send an emergency.

Restarting the Device Manually

In rare situations the device may become unresponsive, and you may not be able to access the device menu to restart the device. If this situation occurs, you can reset the device manually by pressing and holding the up and down arrows for seven seconds.

Note: If your device does not restart after seven or eight seconds, contact customer support for instructions on how to proceed.

Press and hold the Up and Down buttons for 7 seconds to reset the device.

To reset the device, press and hold the Up and Down buttons for 7 seconds.

When the device restarts it returns to the assigned screen.

Caution: It can take 1-2 minutes for the device to fully reset. Do not use a RiskBand device unless you see your user name on the screen. If your name does not appear on the screen, the RiskBand device may not be able to successfully send an emergency.

About Sending Diagnostics

In situations where your device may not act as expected or may appear to malfunction, RiskBand technical support personnel can request that the device send diagnostic information to the RiskBand ARIES Manager. When this happens, an action message will display on the device to inform you that the device will be sending diagnostics. This process uses a lot of the device resources, and, while you can continue to use the device, it may exhibit sluggish response times and poor performance.

Press the Menu button to read the action message.

After a the device receives a request to send diagnostics to the RiskBand ARIES Manager, an action message displays on the device. Press the menu button to read the message.

Press the Menu button to clear the message after you have read it.

The message informs you that the device performance will be poorer than usual while the diagnostic upload is in progress. Press the menu button to clear the message.

While the diagnostics icon is displayed, the device may exhibit poor performance.

The diagnostics icon displays while the device sends the diagnostic information to the RiskBand ARIES Manager. When it has finished, the icon disappears.

About Device Updates

Occasionally, RiskBand updates the software that runs the RiskBand devices. These software updates are called firmware updates, and they are created to fix bugs and to add new features and new functionality to the device.

Each organization has a firmware policy that determines which updates are appropriate for your device as well as when the update should occur. When the RiskBand ARIES Manager determines that your firmware policy requires your device to be updated, it sends a message to your device telling you that the device will be updated the next time it is plugged in to a charger. The update will happen automatically; you do not have to do anything except connect the device to the charger.

On occasion, the software in your device may need to be updated. The need for an software update, and the schedule for deploying that update, is determined by your organization administrators. Software updates for your device are download in the background, and when the update has been fully downloaded to the device and is ready to be installed, an action message displays on your device. This message instructs you to connect the device to the charger in order to apply the update.

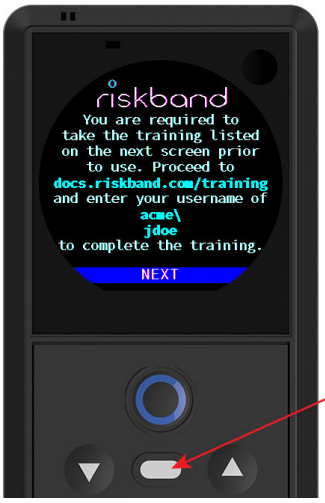
After a software update for the device has been fully downloaded, an action message displays on the device. Press the menu button to read the message.

The message informs you that the next time you connect the device to a charger, the update will be installed. Press the menu button to clear the message.

After the device is connected to a charger, the firmware update will be downloaded and applied, and then the device will then restart. After restarting, the device will display the assigned screen, which displays your user name.

About Required Training

In some organizations, online training may be required before people are allowed to use the RiskBand device. If online training is required by your organization, then any device assigned to you will check during startup to see if you have completed the training. If you have not completed the training, the RiskBand device will remind you that training needs to be completed. The device will not start up beyond these reminder screens until the RiskBand ARIES Manager has been notified that you have successfully completed the course.



Press the Menu button to see the list of required training courses.

The device reminds you that training is required before using the device. The device displays your full user name, which you will enter into the training program after you have successfully completed the course.

After taking note of the required courses click the Menu button to select OK.

After you have reviewed the list of required training modules and select **OK**, the device will power off. After completing the training, power the device on. (Devices that are not allowed to power off will restart.)

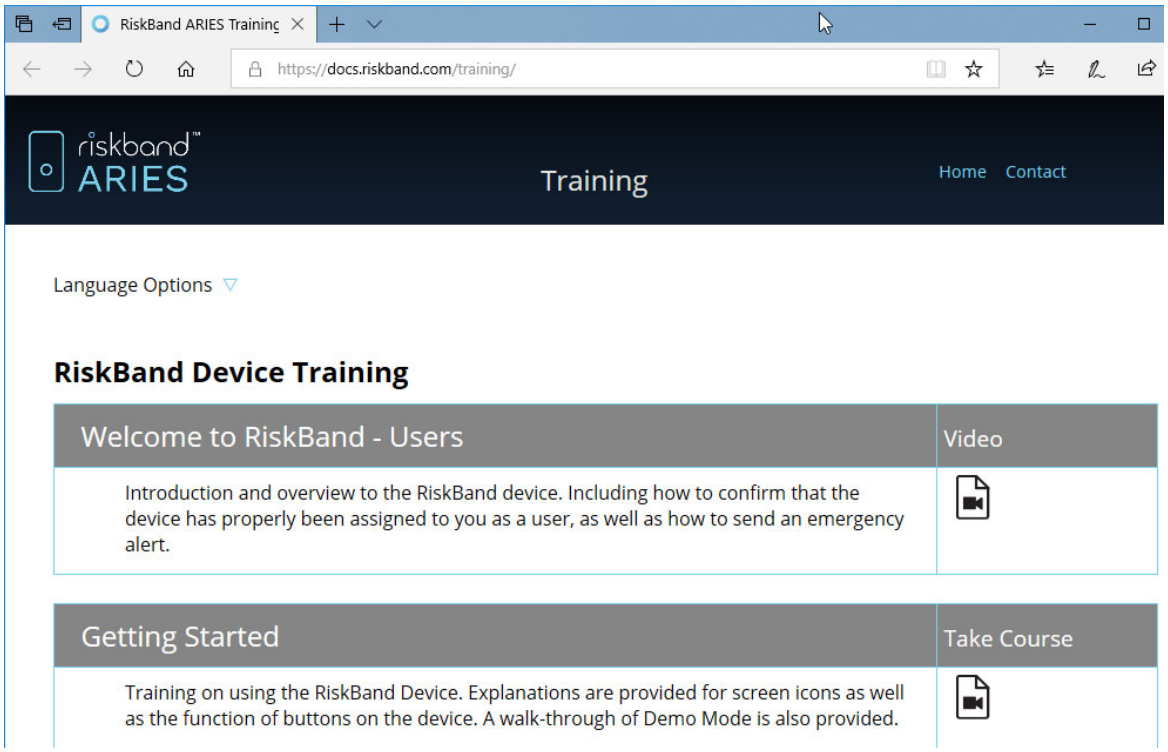
Hold the Menu button down for 3 seconds to Power On the device.

To Power On the device after completing the training, hold the Menu button down for three seconds. After you feel a short vibration on the device, release the menu button.

After the device reaches the normal assigned screen, and you can see your user name displayed on the device, the device is ready for use.

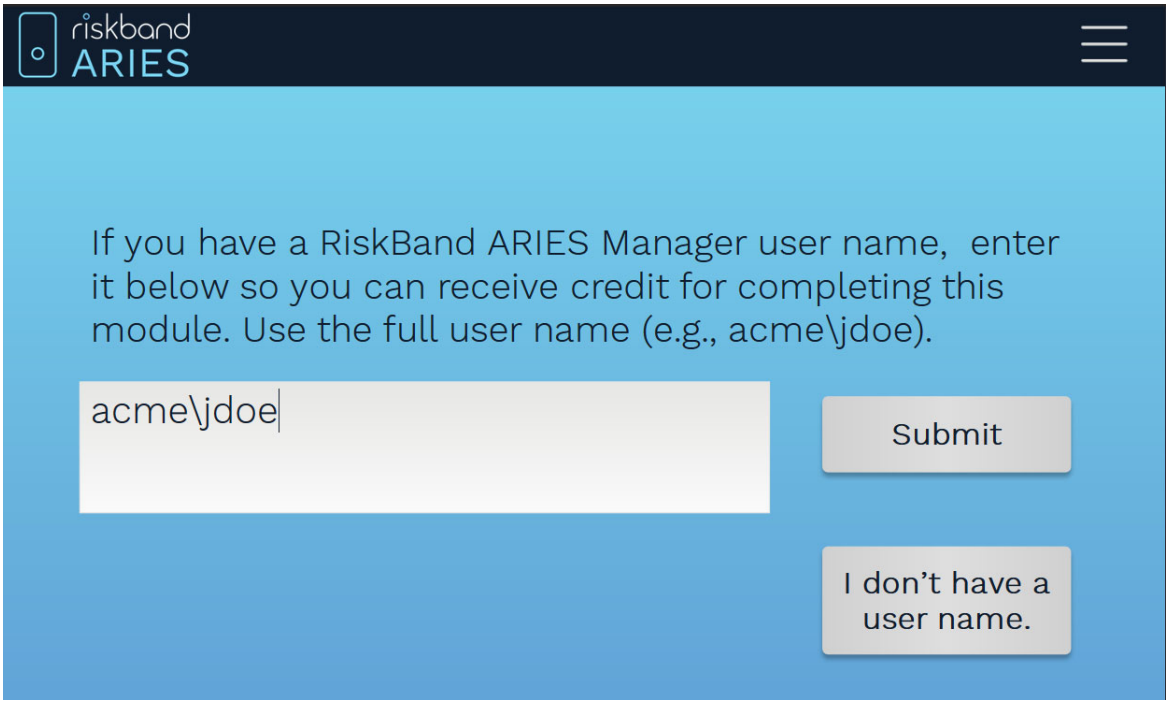
Taking Training Course from the RiskBand Training Website

A list of RiskBand training modules can be found at docs.riskband.com/training. Clicking on the **Take Course** icons on that page will launch the online training modules.



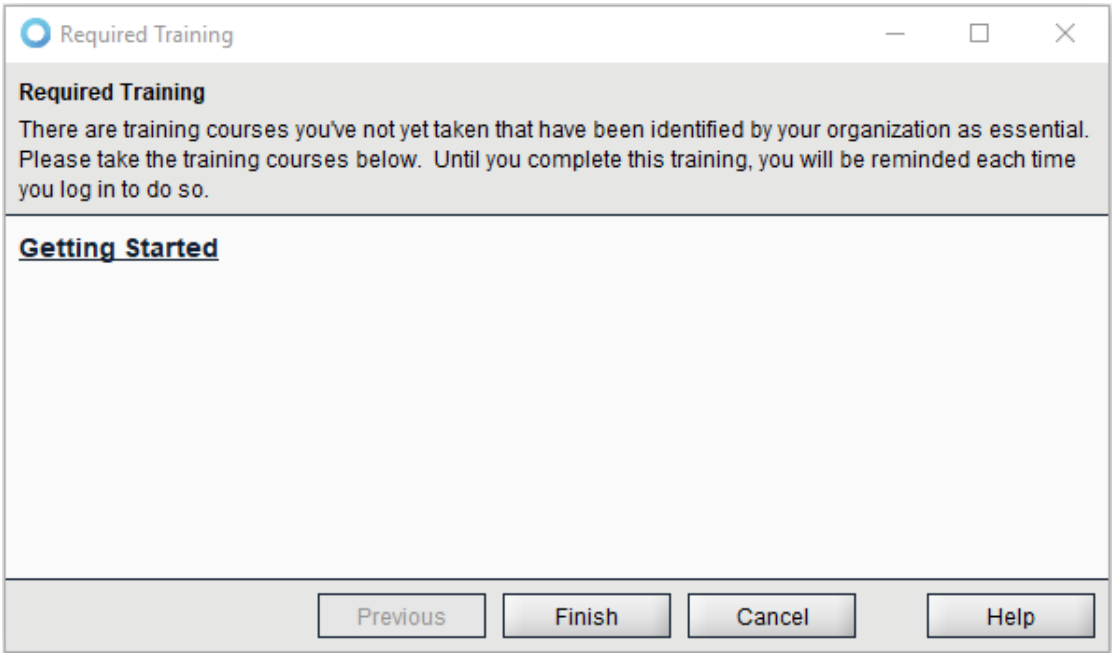
After you have successfully completed the course, the training module will prompt you to enter your user name. This is the user name that is displayed on the reminder screen on your device. It is your user name combined with your organization's prefix. For example, if a user was part of the Acme organization whose prefix was "acme", and their user name was "jdoe", then he or she would enter **acme\jdoe** in the User Name field on the final screen of the training. After clicking **Submit**, the training module will send a course

completion notice for your user name to the RiskBand ARIES Manager. After all required training modules are completed, you can restart your device and it will display your user name on the assigned screen, and you can use the device.



Taking Training Courses from the RiskBand ARIES Manager

If you have been sent an email or text message providing you with log in credentials, you can log in to the RiskBand ARIES Manager to take required training courses. When you first log in to the RiskBand ARIES Manager, a dialog box displays that provides links to required training. Clicking on a link launches the training module, and successful completion of the module is automatically recorded in the system.



5 Charging the RiskBand Device

Caution: Customers must use the RiskBand-supplied charger for charging devices. Unsupported chargers which may supply too much or too little current can damage the device or the charger. Using an unapproved charger and cable will void the RiskBand warranty.

Caution: Do not allow devices to discharge completely. The self-discharge of batteries for an extended period of time at low battery levels can damage the battery. Devices that are not going to be charged (or that will not be used) for 1-2 days, should be powered off using the device menu. See Device Menu: Powering Off the RiskBand Device on page 38.

RiskBand recommends that you avoid the critical power state on devices. When devices are not in use, connect the devices to the supplied charging units. Use the charger and cable that are supplied with the RiskBand device for charging the device's battery. If the device is charging, the charging LED displays on the device, and the charging icon will appear on the LCD.

Figure 1: Device charging LED with cable connected

Note: RiskBand recommends that you do not remove the device from the charger until the LED displays green. Removing the device from the charger before the green LED indicates it is fully charged, or removing the device from the charger when the LED is off, will result in the device being unable to accurately report remaining battery life.

About the LED Charging Light

While the device is physically connected to the charger, the LED charging light will be displayed (see Figure 1). If the device is charging, the LED will be red, and if the device is fully charged it will be green. Charging times for the device can vary, but generally the device can be fully charged within 6 hours. In cases where the device senses it might be overheating, it may stop charging and turn the charging LED off. However, after the temperature drops to a safe level, charging will restart and the LED will display again.

Note: If after 6 hours of charging, the charging LED is still red, disconnect the device from the charger and then reconnect it. If after 6 more hours, the charging LED does not turn green, contact customer support.

About Device Performance While Charging

The RiskBand device can be used while connected to the charger. However, the device can experience reduced cellular connectivity and/or reduced GPS performance while it is actively charging.

Should a situation arise where you need to trigger an emergency with a device while it is charging, RiskBand recommends that, after triggering the emergency, you take the extra step of disconnecting the device from the charger.

6 More about the RiskBand Device

This chapter provides additional information about your RiskBand device:

About the RiskBand Display

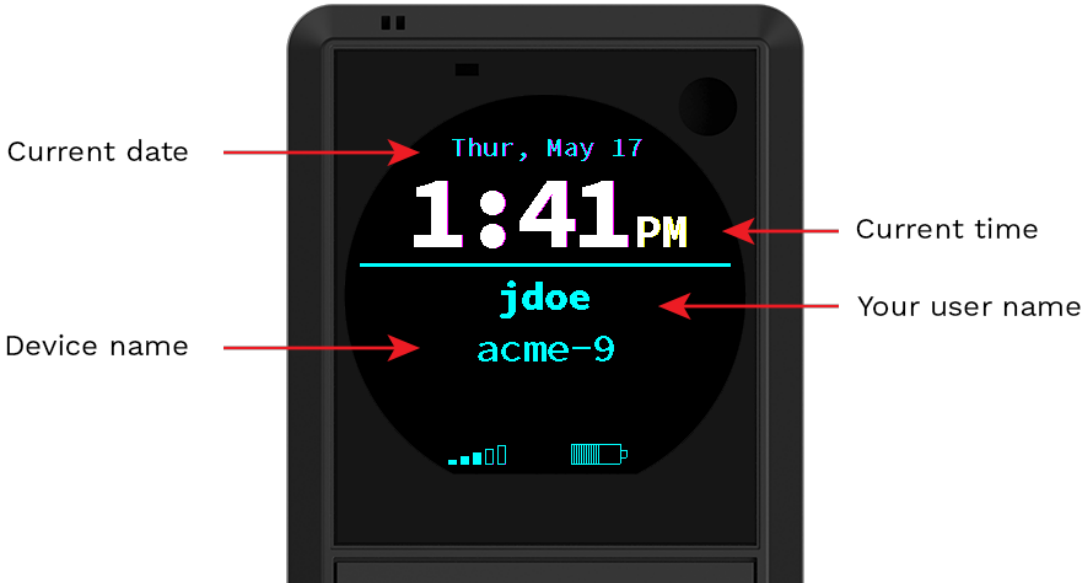
There are three general kinds of information or icons displayed on the RiskBand screen:

- General Device Information
- Emergency Indicators
- Device State Icons

General Device Information

On the main screen, the RiskBand device displays the following information:

- Time — the current time. The time is set through the cellular connection.
- Date — the current date.
- Your User Name — this indicates that information about you has been registered with the RiskBand servers.
- Device Name — this is the name of the device. It is the device prefix of the organization, division, or group combined with a number.

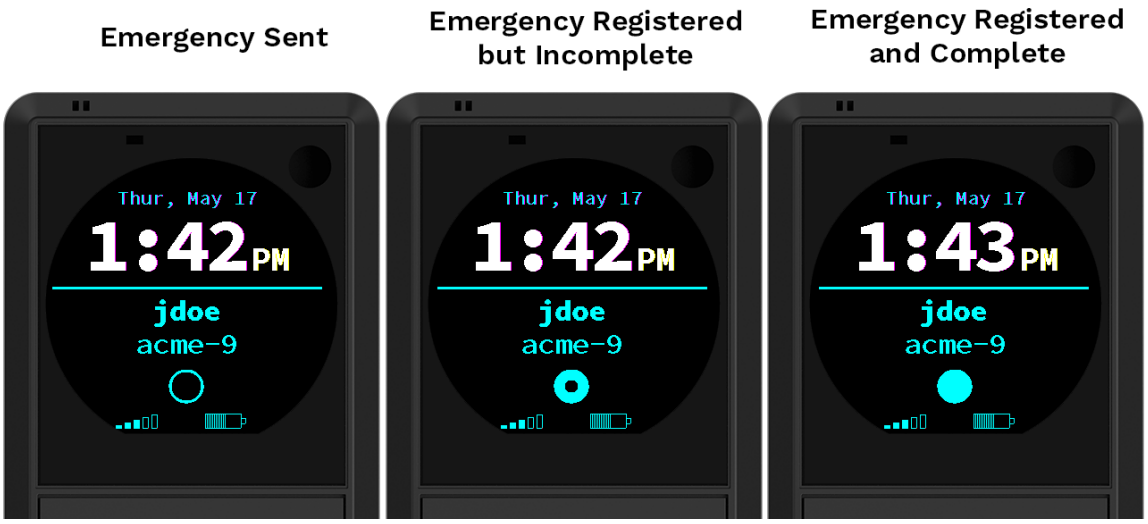


Emergency Indicators

Your RiskBand device is configured to respond to emergencies in one of the following modes:

- Stealth Mode — there is no visual indication on the screen that an emergency is in progress. A series of vibrations on the device will signal you that the emergency has been initiated and a response has started.
- Discreet Mode — the following emergency indicators are displayed to signal the state of the response:
  - Ring — the emergency has been initiated. The RiskBand servers have not yet acknowledged the emergency.
  - Doughnut — the RiskBand servers have registered the emergency, but the voice connection has not yet been established. If the red GPS indicator also appears, it means that the device has not established GPS coordinates since the emergency was initiated.

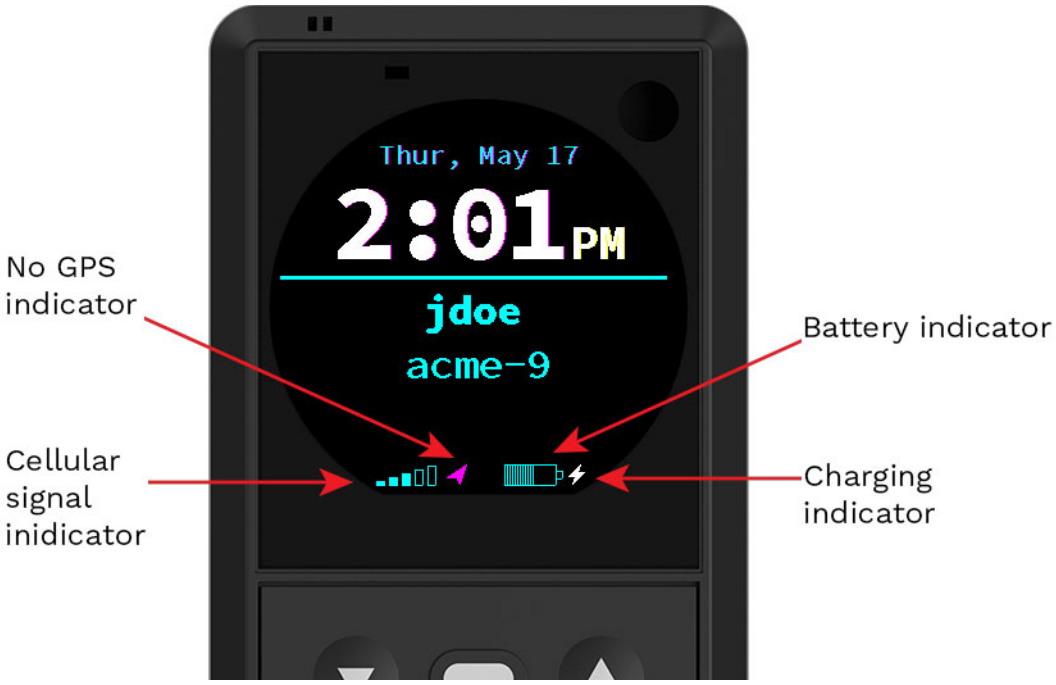
- Blue Dot — the RiskBand servers have registered the emergency, and the GPS coordinates have been established. If voice connections are allowed by your organization's policy, the voice connection has also been established.



Device State Icons

In addition, there are several icons that may appear on the screen:

- Cellular Connection Indicator — indicates the signal strength of the device's cellular connection.
- GPS Signal Indicator — indicates that your GPS coordinates cannot be established.
- Battery Charge Indicator — indicates the percentage of battery life remaining.
- Charging Indicator — indicates the device is connected to power and is charging.



More about the Battery Life Indicator

The battery displays an estimate of the percentage of battery life remaining.

More about the GPS Signal Indicator

The GPS signal indicator might be better described as the "no GPS signal indicator." It only appears when your GPS coordinates cannot be established. If your organization does not use GPS, or if your device is successfully acquiring GPS coordinates, the GPS icon will not appear.

The device may be unable to successfully send GPS coordinates for a number of reasons. However, as a general rule, the no GPS signal indicator lets you know either:

- that the device is at least two minutes late acquiring GPS coordinates as specified by the power management policy, or;
- the device has not yet acquired one set of GPS coordinates since an emergency was triggered.

About RiskBand Device Buttons

The following buttons are available on the RiskBand device:

- Emergency
- Menu
- Up
- Down

The following actions can be initiated using the buttons:

- Emergency — pressing the Emergency button for 2 seconds
- Cancel Emergency — if your organization's policies allow it, pressing the Menu button for 3 seconds cancels an emergency. (The device menu is unavailable during an emergency.)
- Display Menu — pressing the Menu button. (The device menu is unavailable during an emergency.)
- Device Reset — pressing the Up and Down buttons simultaneously for 7 seconds.

Any button when pressed—except for the Emergency button—turns on the backlight on the LCD for 7 seconds.

About the RiskBand Device Startup Process

When a RiskBand device starts up, one of the first things it does is try to figure out who it has been assigned to and what it should do in an emergency. The device gets this information by connecting to the RiskBand ARIES Manager on the Internet. Consequently, the device needs a data connection on the cellular network.

If you turn on or restart a device in a location where the device can't get a connection to the cellular network, the device will display the "No cell data connection" screen. If you see this screen, move the device to a location where there is a strong cellular network signal.

After connecting to the cellular network, it is possible the data portion of that connection may be poor. If that is the case, the device will display the "Poor cell data connection" screen. If you see this screen, move the device to a location where there is a stronger cellular connection and a better data connection.

If, after moving to different locations where there is better cellular connectivity, the device never moves off these two screens, contact customer support.

Caution: Do not use a RiskBand device unless you see your user name on the screen. If your user name does not appear on the screen, the RiskBand device may not be able to successfully send an emergency.

About Poor Cellular Connectivity and GPS Performance

As you move around with your RiskBand device you may encounter and pass through areas of poor cellular connectivity or be in areas where GPS performance is limited. This is a normal situation, and it is expected in the normal operation of the device. After the initial device startup process, and the device reaches a state where it correctly displays your user name on the assigned screen, it continues to function even with occasional periods of no cellular connectivity or poor GPS performance.

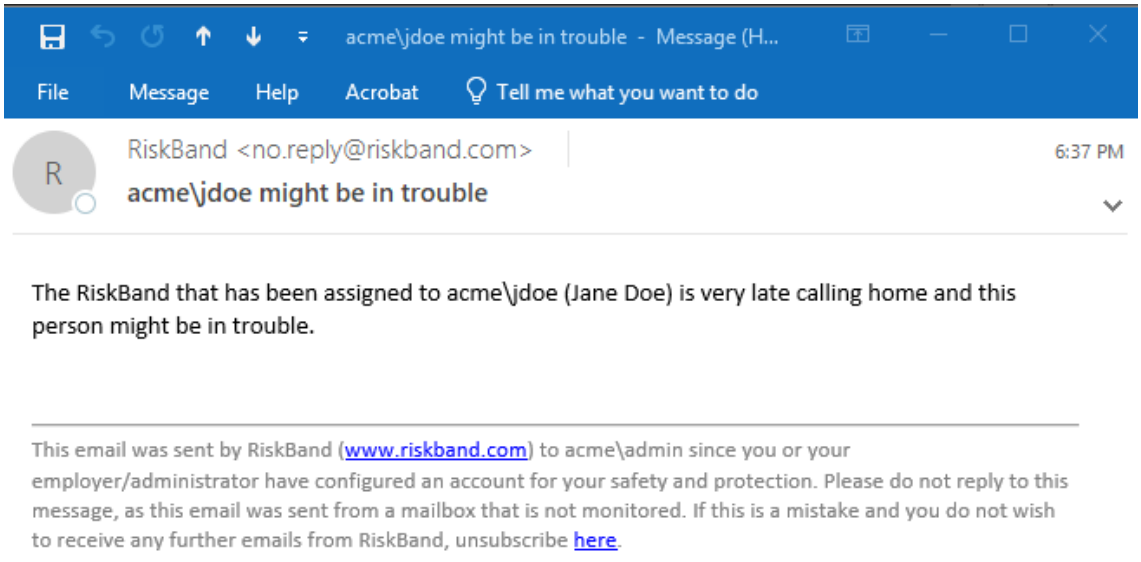
Even in situations where the device has no network data connectivity, or even no cellular network connectivity, the device continues to provide useful services. For example,

- No data connectivity — even though the RiskBand ARIES Manager cannot be immediately notified of a triggered emergency, the device can still call out to emergency responders.
- No cellular connectivity — even though the device cannot call out or connect to the RiskBand ARIES Manager during a triggered emergency, it still takes photos and collects GPS coordinates, which will be uploaded as soon as connectivity is restored.
- In both of the situations above, the RiskBand ARIES Manager can determine that the device is not communicating as it should, and it sends notifications to designated administrators or monitors telling them that you might be in trouble. See Figure 2: Example of a Late Calling Home Notification on page 55.

The following things can be done to prevent reduced cellular connectivity and poor GPS performance:

- Keep the device battery charge above 10%.
- Do not use the device while it is connected to the charger
- Do not use devices in close proximity to each other. GPS performance is the area most likely to be affected by proximity to other devices. Devices will work best if separated by 1-3 feet.

Figure 2: Example of a Late Calling Home Notification



About Low Power States

The battery charge indicator on the device provides an approximation of the amount of battery power remaining.

When the battery has approximately 20% of it's battery life remaining, the battery charge indicator will turn yellow and starts to blink.

When the battery has approximately 10% of it's battery life remaining it enters a critical battery state. In this state the battery charge indicator turns red and blinks. Additionally the critical battery warning displays on the device.

In the critical battery state the device will stop taking GPS coordinates and will stop calling home to the RiskBand ARIES Manager in order to save power for triggering an emergency. If an emergency is triggered while the device is in the critical battery state, the device will resume full operation at full power and continue to do so until the emergency is closed or until it runs out of power.

A Note About GNSS and GPS

The RiskBand device uses the Global Navigation Satellite System (GNSS) to obtain location information. GNSS is comprised of a number “regional” satellite-based navigation systems including GPS, which is the satellite system created by the United States. Depending on the power management policy in use, RiskBand devices can obtain location information from any of the satellites in any of the following systems:

- GPS (USA)
- Galileo (Europe)
- GLONASS (Russia)
- BeiDou (China)
- SBAS (Europe)
- QZSS (Japan)

While the term GPS is frequently used in RiskBand documentation as a general term to describe location and positioning features of the device, be aware that the location acquisition capabilities of the device are truly global.

7 Accessing the RiskBand ARIES Manager

Note: Even if you have been assigned a RiskBand device, you may not need to log in to access the RiskBand ARIES Manager. The steps in this chapter only apply to users who have received RiskBand ARIES Manager log in credentials in an email or text message.

In addition to the RiskBand device, there are some features and services that are available through a RiskBand software program referred to as the RiskBand ARIES Manager client. This chapter describes how to install the RiskBand ARIES Manager client and access the features in the RiskBand ARIES Manager.

Installing the RiskBand ARIES Manager Client

To access the RiskBand web services, you need to install the RiskBand ARIES Manager client. Download the installer that matches the operating system of the computer you will be using. The following installers are available for download from https://docs.riskband.com/downloads/.

- RiskBand-installer-mac.zip
- RiskBand-installer-unix.zip
- RiskBand-installer-win-x64.msi (for 64-bit Windows operating system)
- RiskBand-installer-win-x86.msi (for 32-bit Windows operating system)

Currently, the 64-bit Windows client is the only officially supported version of the RiskBand ARIES Manager. The system requirements for this version are

- Windows 64-bit operating system
- 4 GB of RAM
- 150-200 MB free disk space
- Network connection to the Internet

Installing the RiskBand ARIES Manager on Windows

To install the RiskBand ARIES Manager on the Windows operating system:

1. Download the `RiskBand-installer-win-x••.msi` file that is appropriate for the operating system on your computer.
2. Double-click **RiskBand-installer-win-x••.msi**.
3. On the Welcome screen click **Next**.
4. To install to the default location, click **Next**.

   To install in a different location, click **Browse** and then navigate to the installation folder you prefer, or create a new installation folder. After you are finished, click **OK**. Then click **Next**.
5. Click **Install**.
6. If asked if you want to allow the installation program to modify your device, click **Yes**.

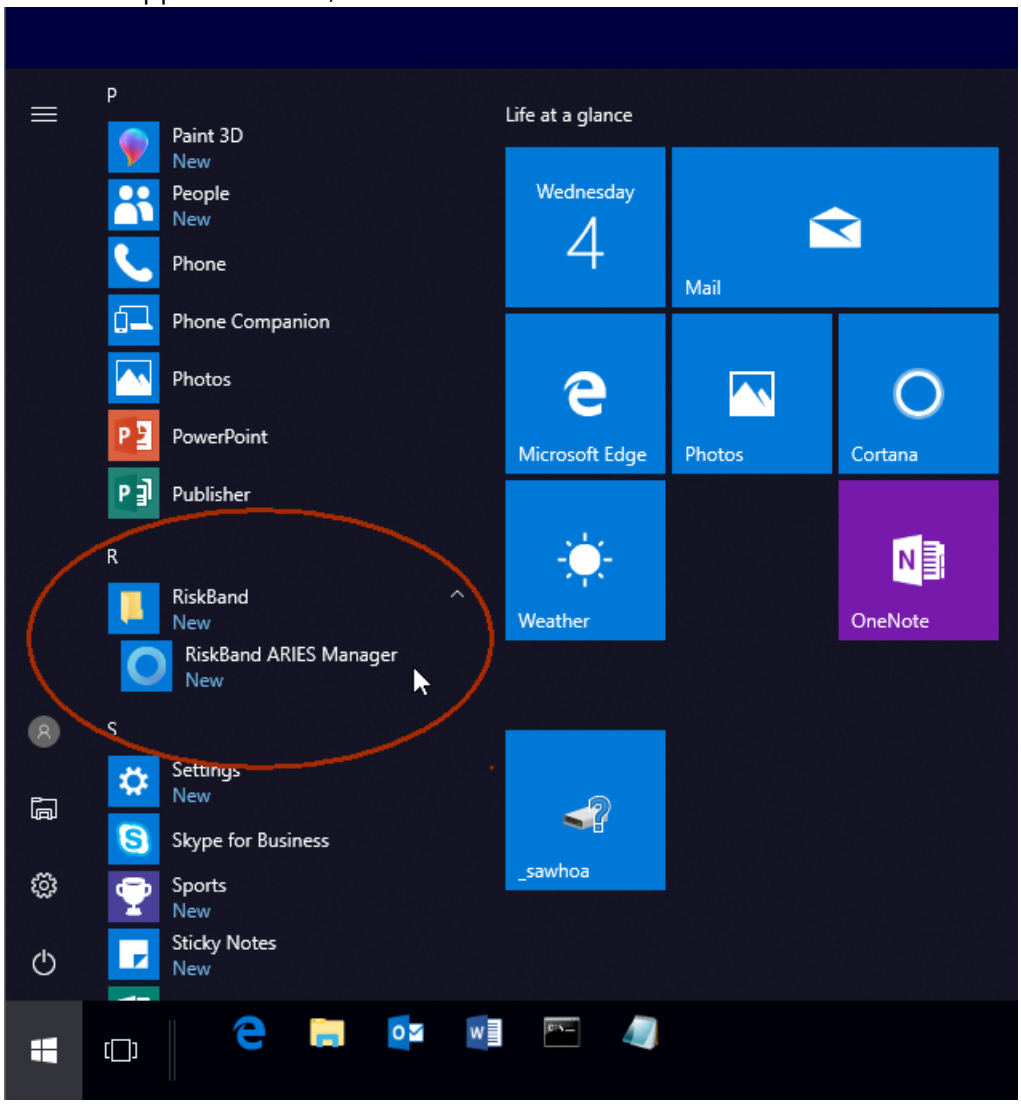
   The RiskBand ARIES Manager client is installed on your computer.
7. After the installation completes, click **Finish**.

The RiskBand ARIES Manager is now installed and ready for use.

Launching the RiskBand ARIES Manager on Windows

To log in to the RiskBand ARIES Manager:

1. Click **Start** on the Windows desktop.
2. In the applications list, scroll down to RiskBand and click **RiskBand ARIES Manager.**



The RiskBand ARIES Manager login screen appears.

Installing the RiskBand ARIES Manager Client on Mac OS

Note: You may need to create an exception to your Mac's security policy to allow it to run applications downloaded from the Internet.

To install the RiskBand ARIES Manager client on Mac OS:

1. Download `RiskBand-installer-mac.zip` to a directory where you want to install the RiskBand ARIES Manager client.

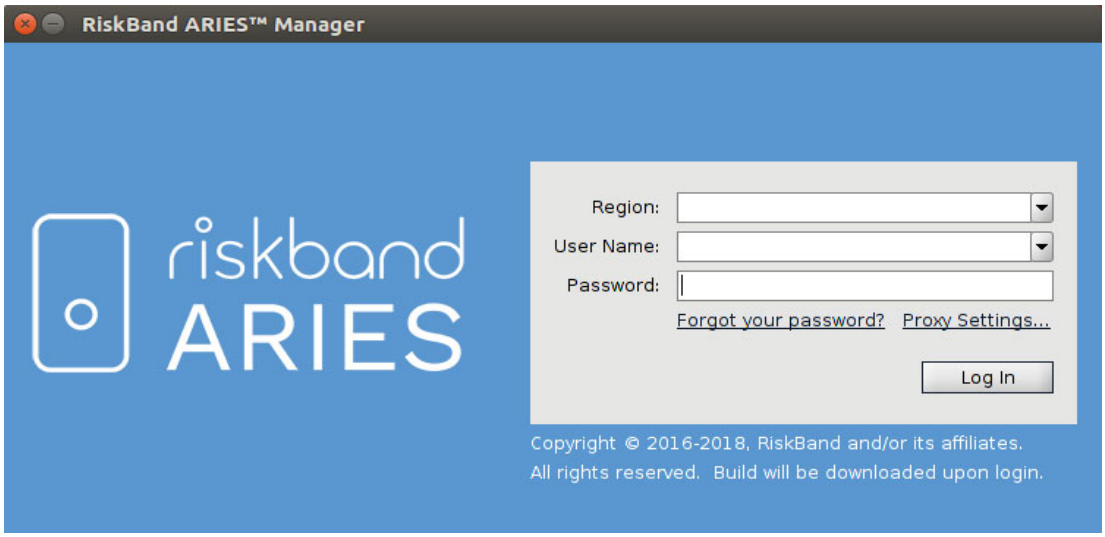
2. In the directory where you downloaded the installer, double-click **`RiskBand-installer-mac.zip`**

   Mac OS unzips the file and creates a directory called `RiskBand ARIES Manager`. Some versions of Mac OS will automatically unzip the downloaded file for you.

3. In the `RiskBand ARIES Manager` folder, double-click **RiskBand ARIES Manager**.

   The RiskBand ARIES Manager login screen appears.

4. Using the information that was sent to you in the invitation email from your organization, log in to the RiskBand ARIES Manager.



Installing the RiskBand ARIES Manager Client on UNIX/Linux

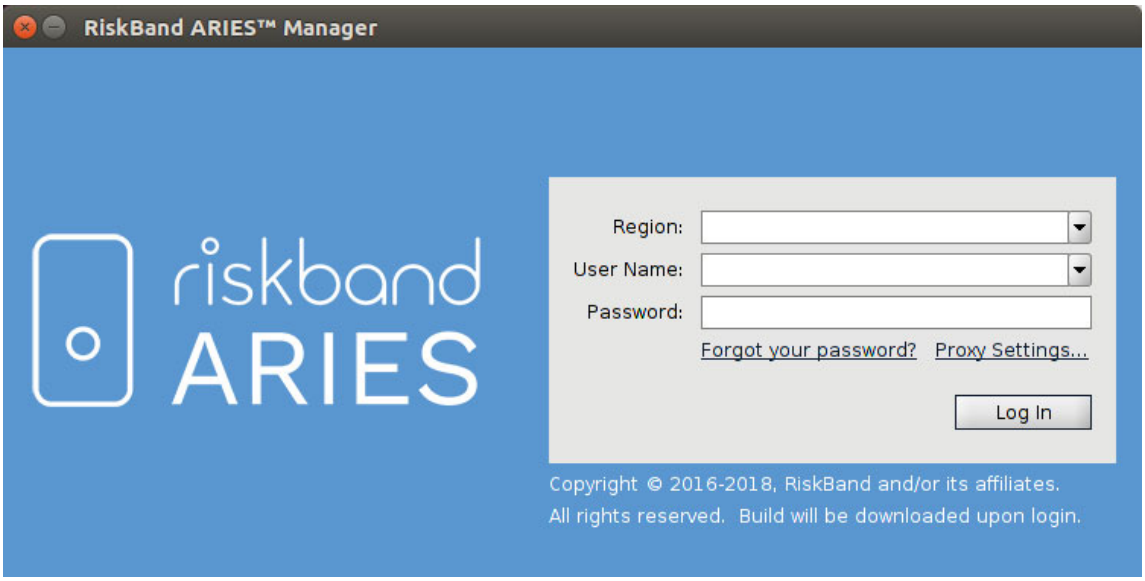
Note: Before installing the RiskBand ARIES Manager client on your UNIX/Linux or machine, you must have Java installed on your computer. Enter **`java -version`** on the command line to determine if Java is installed.

To install the RiskBand ARIES Manager client on a UNIX/Linux operating system:

1. Download `RiskBand-installer-unix.zip` to a directory where you want to install the RiskBand ARIES Manager client.
2. In the directory where you downloaded the installer, type **`unzip RiskBand-installer-unix.zip`**
3. Type **`chmod 755 runRiskBandGui.sh`**
4. Type **`./runRiskBandGui.sh`**

   The RiskBand ARIES Manager login screen appears.

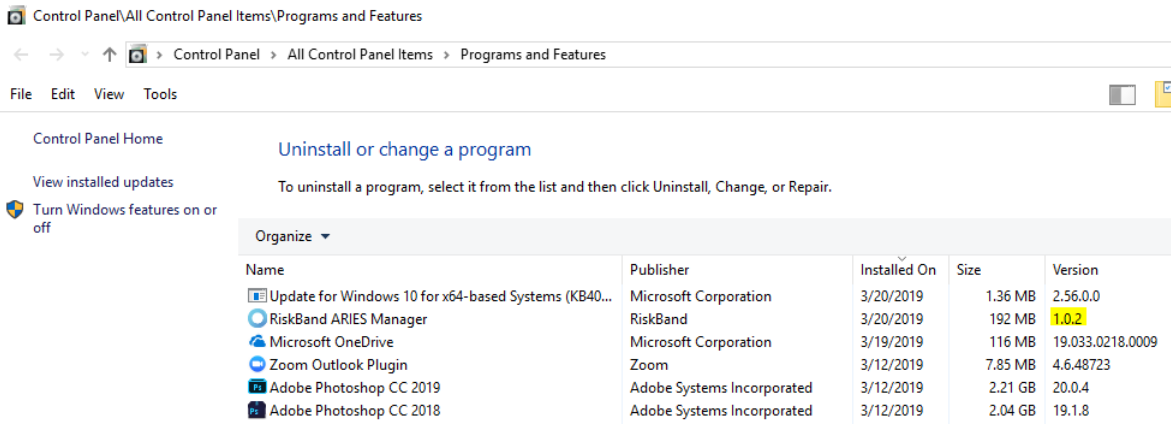
5. Using the information that was sent to you in the invitation email from your organization, log in to the RiskBand ARIES Manager.



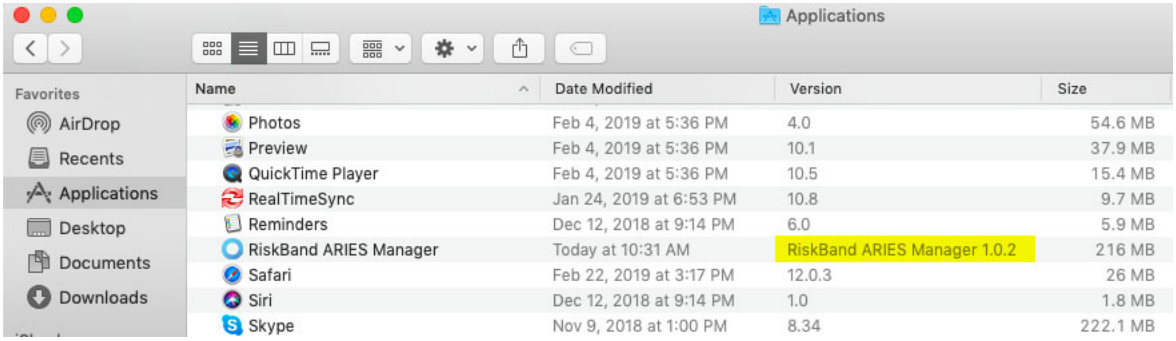
Determining the Version of the Installed Client Software

The current version of the RiskBand ARIES Manager client is 1.0.2. You can determine which version of the RiskBand ARIES Manager you have installed on your computer in this way:

- **Windows** — the version of the RiskBand ARIES Manager reported in the Programs and Features dialog box. In the example shown here, the installed version is 1.0.2.



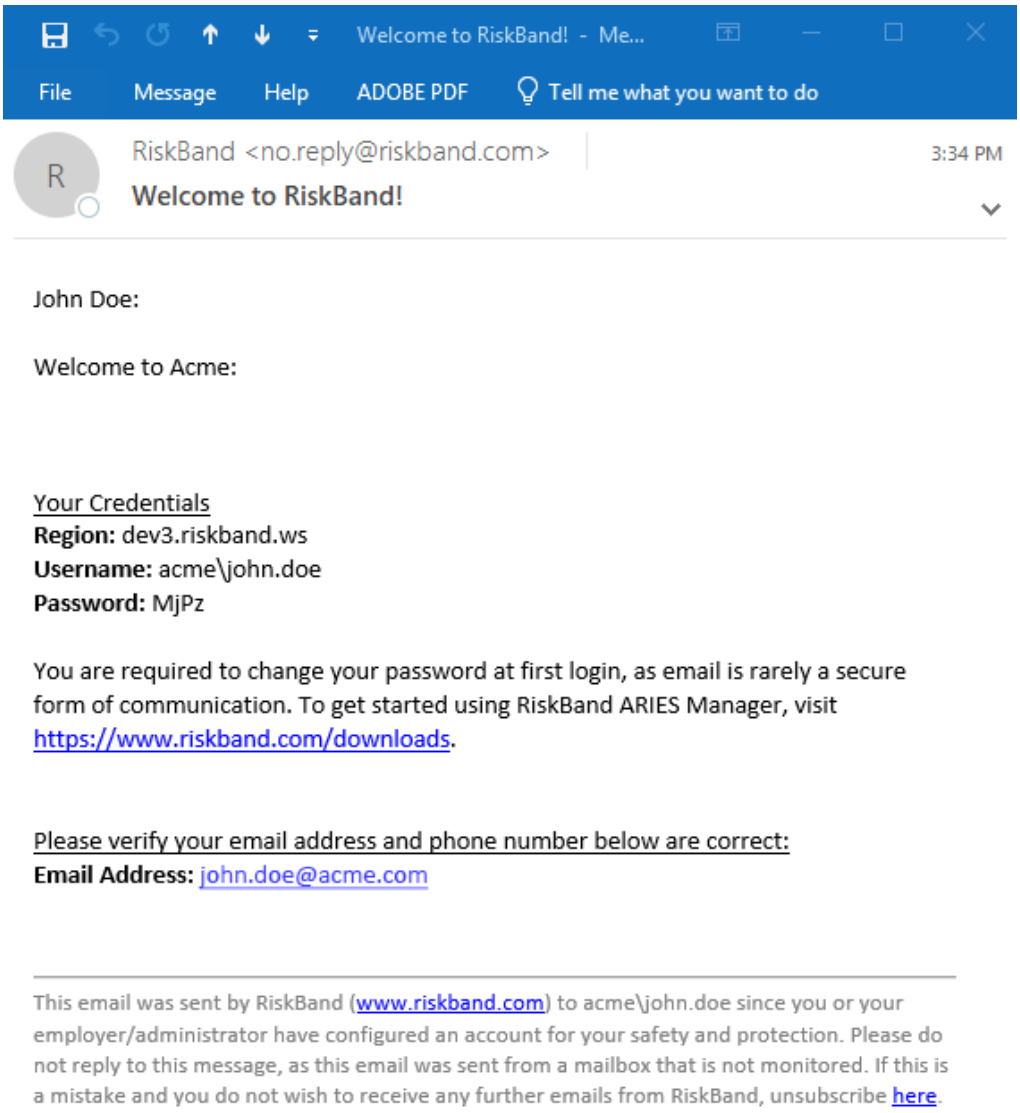
- **Mac OS** — in the Finder window the version should display in the Version column. In this example the version number is 1.0.2.



- **Linux** — the version number is determined by the date of the `guirb-Dev.jar` file. Version 1.0.2 has a date of 3/13/2019 or later.

Logging in to the RiskBand ARIES Manager

In the process of assigning you a device, a user ID was created for you in the RiskBand system. Your user ID and login credentials were emailed to you. The email may have looked something like this:



Welcome to RiskBand! - Me...

File Message Help ADOBE PDF Tell me what you want to do

R RiskBand <no.reply@riskband.com> 3:34 PM

Welcome to RiskBand!

John Doe:

Welcome to Acme:

Your Credentials
Region: dev3.riskband.ws
Username: acme\john.doe
Password: MjPz

You are required to change your password at first login, as email is rarely a secure form of communication. To get started using RiskBand ARIES Manager, visit https://www.riskband.com/downloads.

Please verify your email address and phone number below are correct:
Email Address: john.doe@acme.com

This email was sent by RiskBand (www.riskband.com) to acme\john.doe since you or your employer/administrator have configured an account for your safety and protection. Please do not reply to this message, as this email was sent from a mailbox that is not monitored. If this is a mistake and you do not wish to receive any further emails from RiskBand, unsubscribe here.

Use the information in this welcome email to log in to the RiskBand ARIES Manager.

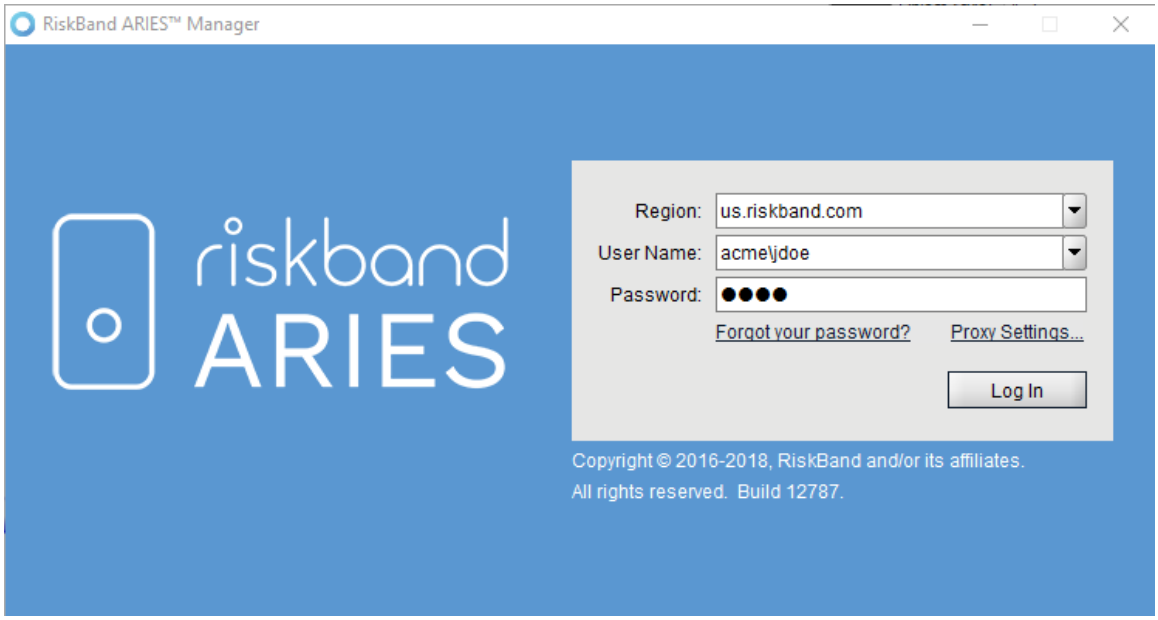
To log in to the RiskBand ARIES Manager:

1. Open the RiskBand ARIES Manager by clicking **Start > All Programs > RiskBand > RiskBand ARIES Manager.**

   The RiskBand ARIES Manager Log In dialog box appears.
2. In the Region field, enter the Region included in your welcome email.
3. In the User Name field, enter your full user name.

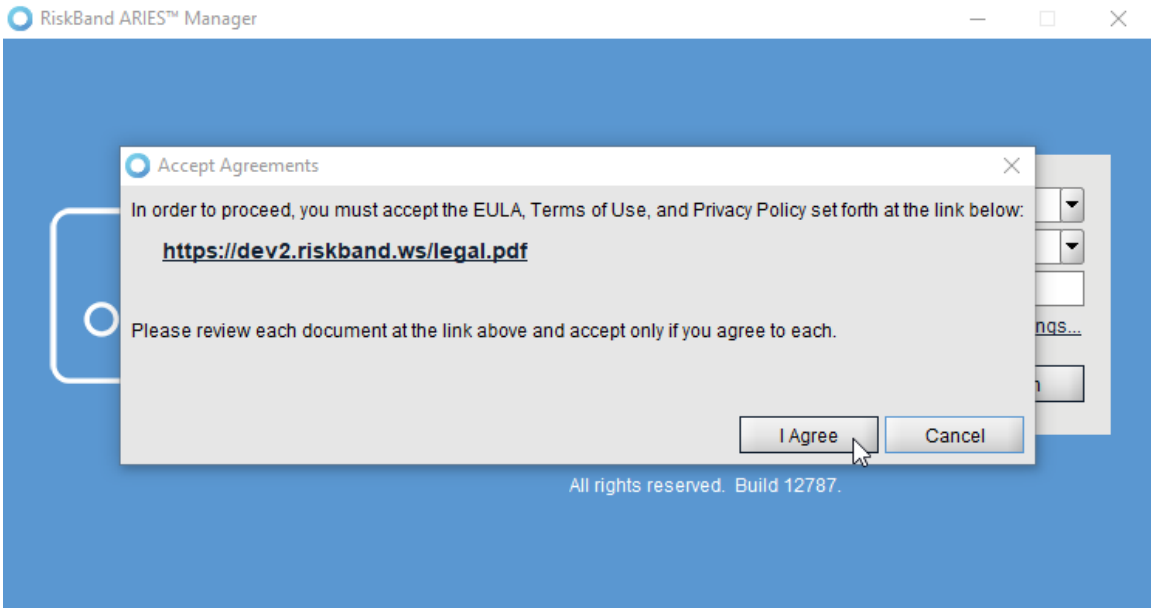
   Include the domain prefix with your user name. In the illustration above, the domain prefix is “acme” so you would enter **acme\jdoe** in the User Name field.
4. In the Password field, enter your password.

5. Click **Log In**.



6. If you have entered valid login credentials, the program will determine if the version of the RiskBand ARIES Manager that is being used on your computer matches the current version on the server. If it does not, then the latest version of the RiskBand ARIES Manager is downloaded to your computer. After it has been downloaded, you will need to repeat steps 4 and 5 to log in again.

   The first time you log in to the RiskBand ARIES Manager the Accept Agreements dialog box appears. You will need to accept the EULA, Terms of Use, and Privacy Policy.



7. Click on the link to view the agreements.

   The agreements can also be viewed at: https://us.riskband.com/legal.pdf.

8. After reading the agreements, click **I Agree**.

You are logged in to the RiskBand ARIES Manager.

If you are unable to connect to the RiskBand ARIES Manager, here are some possible reasons:

- Your company firewall is preventing the connection. If this is case, contact your IT group and ask if them to open up outgoing TCP/IP on port 443.
- Your company uses a proxy server. If this is the case, see the “Configuring Proxy Server Settings” section of this guide.

Note: After logging in, the RiskBand ARIES Manager displays any required training that you need to complete. You can click **Finish** to close the dialog box and take the training later (see Viewing and Taking Training Modules on page 72). Or, you can click a link that is displayed to take the training immediately.

Configuring Proxy Settings

If your organization uses a proxy server that allows users to connect to the internet, you can provide proxy server settings to the RiskBand ARIES Manager.

Note: Contact your organization’s network administrator to get the proxy settings for you network.

To set proxy server settings:

1. From the RiskBand ARIES Manager login screen, click **Proxy Settings**.

   The Proxy Settings dialog box appears.
2. In the HTTPS Proxy Host field, enter the network name or IP address of your organization’s proxy server.
3. In the HTTPS Proxy Port, enter the port that your proxy server communicates on.
4. In the HTTPS Proxy User Name, enter a user name that is authorized to use the proxy server.
5. In the HTTPS Proxy Password field, enter the password for the user.
6. Click **OK**.

The RiskBand ARIES Manager now has the proxy server information necessary to communicate over the Internet.

Note: The RiskBand ARIES Manager does not validate any of the information entered in the Proxy Settings dialog box. If you get a “connection refused” error, verify that the information you entered is correct.

Recovering Forgotten Passwords

If you have forgotten your password for the RiskBand ARIES Manager, you can reset it with the Reset Password Wizard. Depending on how your organization has been configured, you will need the following information:

- email address — this is the email address that is associated with your user name in the RiskBand ARIES Manager.
- phone number — this is the phone number that is capable of receiving SMS text messages that is associated with your user name in the RiskBand ARIES Manager.

However, if your organization is configured so that password self-recovery is “Allowed via Email,” you do not need to enter a phone number.

Note: If you do not know your user name you cannot use this wizard to recover your password. You will need to contact your organizational administrator to get your user name and password.

To recover a forgotten password:

1. From the RiskBand ARIES Manager login screen, click **Forgot your password?**

   The first screen of the Reset Password Wizard appears. This screen contains important information about the password recovery process.

2. Click **Next**.

   The Enter Your Information dialog box appears.

3. In the Your User Name field, enter your user name.

   The user name should include the organization domain. For example, in an organization where the domain was “acme,” the user name “jdoe” would be entered as “acme\jdoe.”

4. In the Your Email Address field, enter your email address.
5. In the Your Phone Number field, enter your telephone number.

   This field is optional if your organization is configured to allow password self-recovery with just an email address.

6. Click **Next**.
7. Click **OK**.

   The Password Reset Request Accepted screen appears.

8. In the Password Reset Code Sent via Email field, enter the code that was sent to your email address.
9. In the Password Reset Code Sent via SMS Text field enter the reset code sent to your phone.
10. Click **Next**.
11. Click **OK**.

    The Password Reset Complete screen appears.

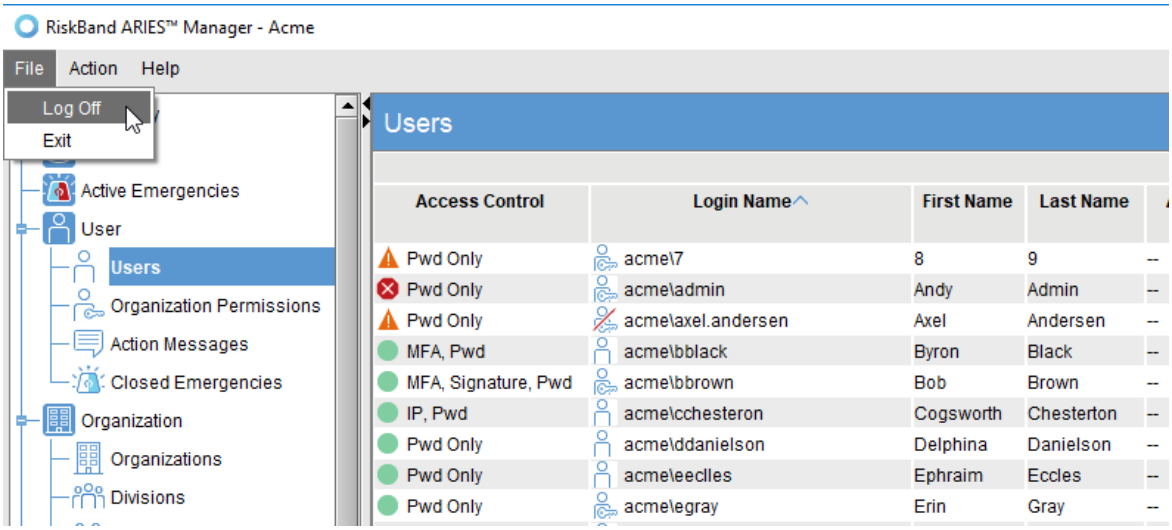
12. Click **Finish**.

The RiskBand ARIES Manager sends an email to you containing your new credentials.

Closing the RiskBand ARIES Manager

When closing the RiskBand ARIES Manager, you have two options:

- Log Off — closes the session and returns you to the login screen. To log off, click **File > Log Off**.
- Exit — closes the program completely, and returns you to your operating system's desktop. To exit the RiskBand ARIES Manager completely click **File > Exit**.



About Passwords

Note: After logging in to the RiskBand ARIES Manager for the first time, RiskBand strongly recommends that you change your password.

User passwords can be set to one of following modes or types:

- Memorized — these passwords are traditional passwords that a user creates and can use to log in to the RiskBand ARIES Manager.
- Cryptographic — these passwords are generated by the system and are 40 characters long.

Table 1 shows some of the feature and vocabulary differences between these two types of passwords.

Table 1: Differences between password types

Memorized Passwords	Cryptographic Passwords
User created (must comply with your organization's User Password Strength Policy)	System Assigned
Up to 40 characters long	Exactly 40 characters long

Table 1: Differences between password types

Memorized Passwords (cont.)	Cryptographic Passwords (cont.)
Requires the use of sessions for programmatic access to RiskBand APIs.	Can be used for programmatic access to RiskBand APIs.
Selecting “Auto-generate password” in the Reset Password dialog creates a memorized password that is emailed to the user.	Configuring an account for “secret key” access in the Reset Password dialog displays the cryptographic password on the Secret Key Configured dialog, where you have the opportunity to cut and paste it to a location where it can be saved.
Memorized Secret Authenticator (Encrypted)	Cryptographic Secret Key (for session-less programmatic access.

About Password Strength Policies

Password strength policies are defined as follows:

- Maximum — Passwords must be 12 characters in length and contain at least three of the following four types of characters: lowercase, uppercase, numerical, and special characters. Additionally, complexity requirements are enforced, which means that dictionary words, and slightly masked dictionary words, are not allowed.
- Strong — (Default) Passwords must be 8 characters in length and contain at least two of the following four types of characters: lowercase, uppercase, numerical, and special characters. Additionally, complexity requirements are enforced, which means that dictionary words, and slightly masked dictionary words, are not allowed.
- Standard — Passwords must be 8 characters in length and contain at least two of the following four types of characters: lowercase, uppercase, numerical, and special characters.
- Weak — Passwords must be 4 characters in length.

The RiskBand ARIES Manager provides a password strength indicator to indicate the strength of the password entered. The password strength policies roughly correspond to the following visual indicators:

- Maximum — 

- Strong — 

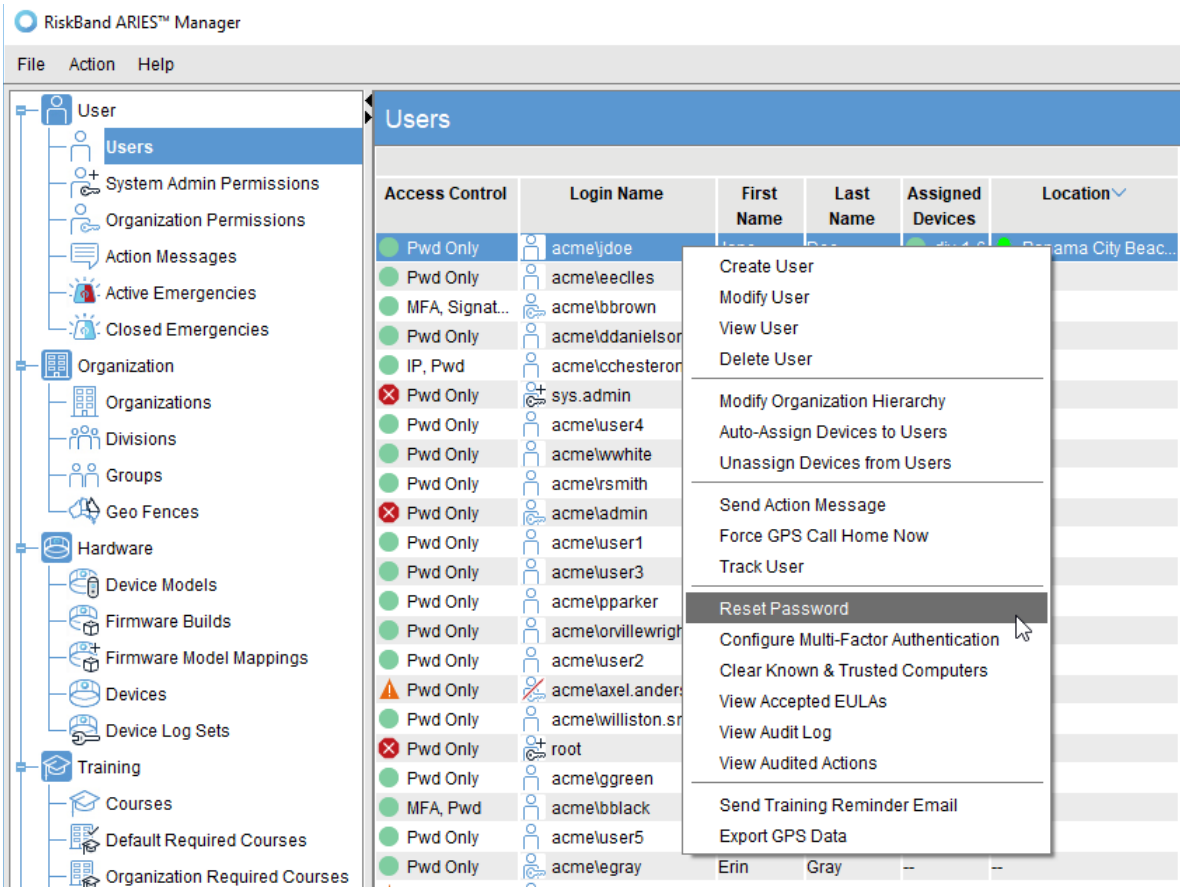
- Standard — 

- Weak — 

Resetting Passwords

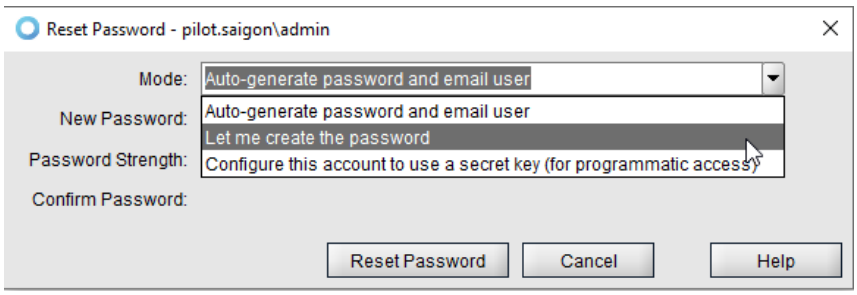
To reset a user password:

1. In the navigation pane, under the User section, click **Users.**
2. From the Users content pane, right-click the user whose password you want to reset and select **Reset Password**.



The Reset Password dialog box appears.

3. In the Reset Password dialog box, choose the Mode or type of password you want to create. There are three choices:
   - Auto-generate password and email user (creates a memorized type password)
   - Let me create the password (creates a memorized password)
   - Configure this account to use a secret key (creates a cryptographic password)



4. Click **Reset Password**.

The user's password is reset.

If you chose to auto-generate a password, the password will be emailed to the user. After the user logs in with the new password, the user will be immediately required to change their password.

If you chose to configure the account to use a secret key, the secret key is displayed in the Secret Key Configured dialog where it can be copied and saved for later use.

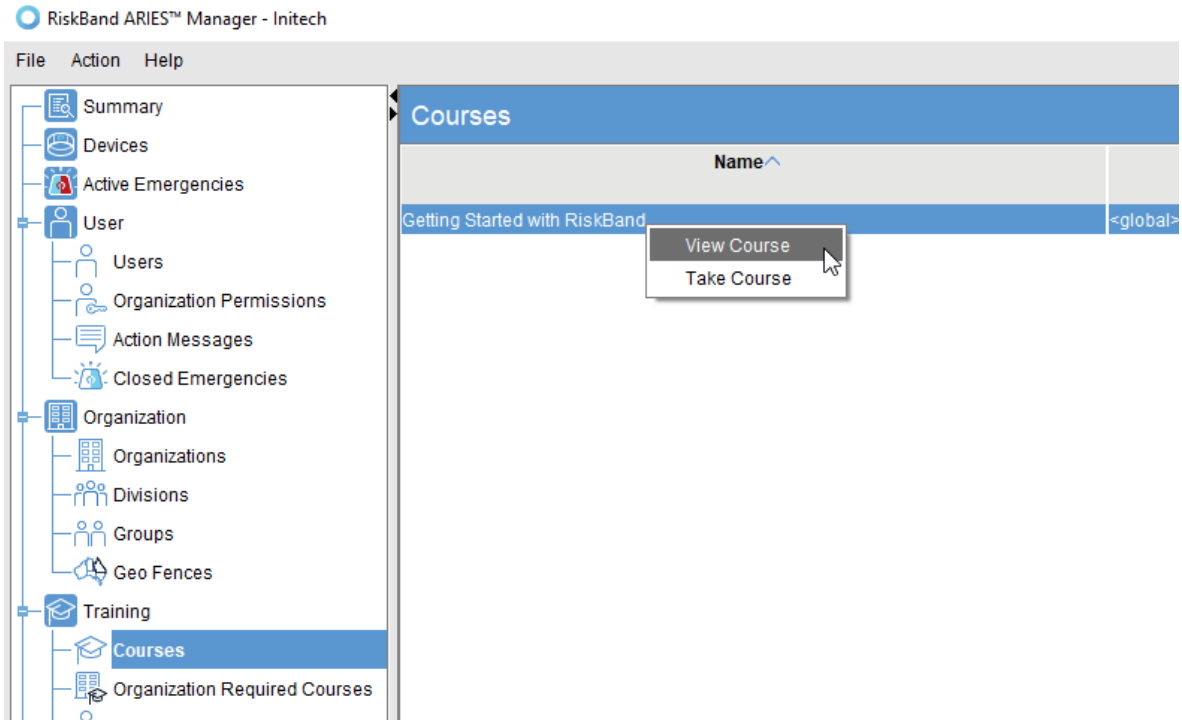
Viewing and Taking Training Modules

From the RiskBand ARIES Manager you can view the training modules that are available. You can also launch training modules by right-clicking on them and selecting **Take Course**.

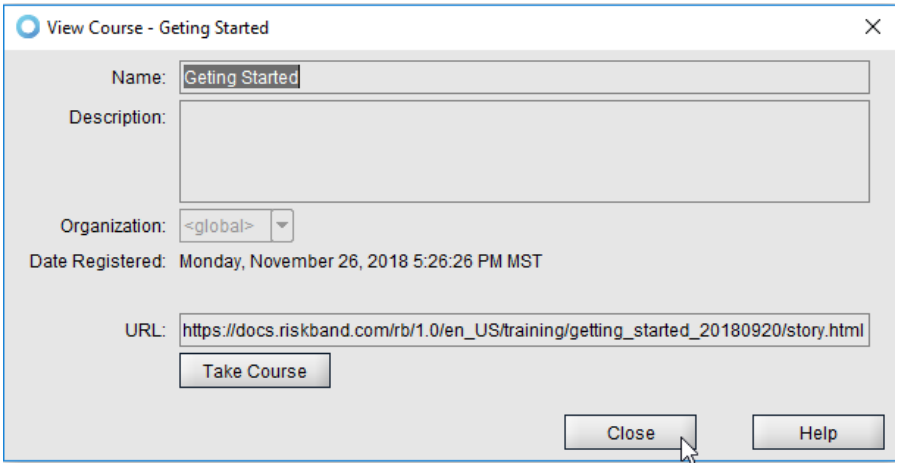
Viewing Training Courses

To view a training course:

1. In the navigation pane, under the Training section, click **Courses**.
2. In the Courses content pane, right-click the course you want to view and select **View Course**.



The View Course dialog box appears.



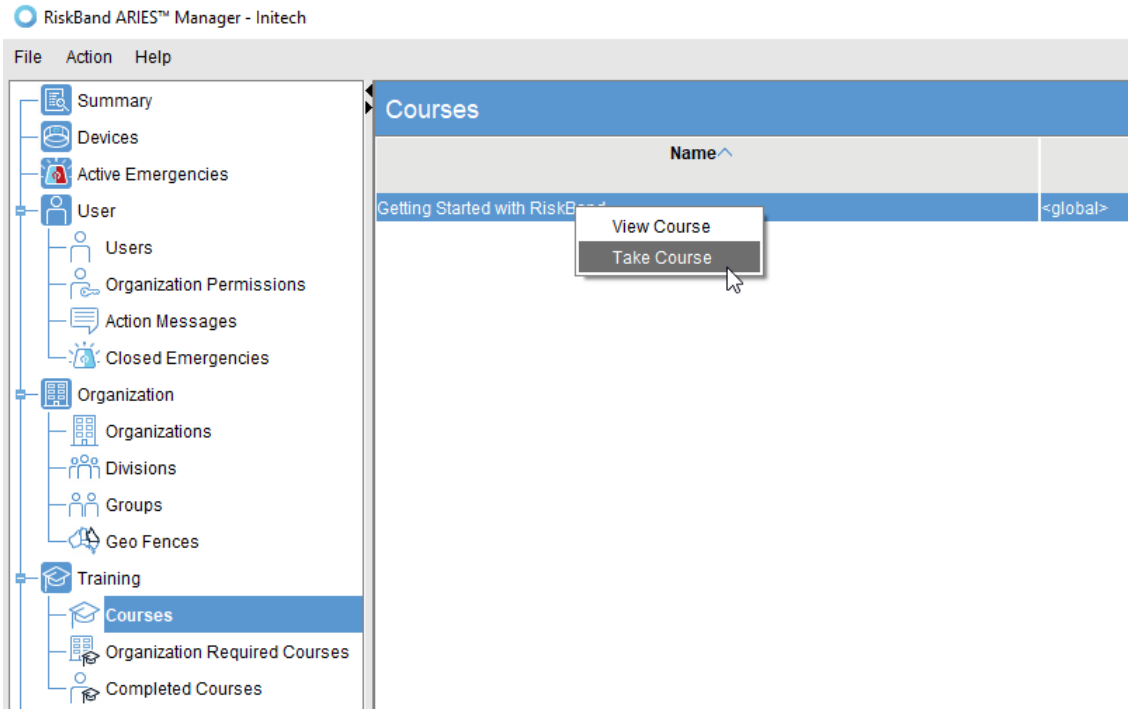
3. After you are finished viewing the information about the course, click **Close**.

The View Course dialog box closes.

Taking Training Courses

To take a training course:

1. In the navigation pane, under the Training section, click **Courses**.
2. In the Courses content pane, right-click the course you want to take and select **Take Course**.



   The Take Course dialog box appears informing you that the browser has been launched to display the training course.

3. Click **Close**.

You can now go to the browser window that was launched and take the training course.

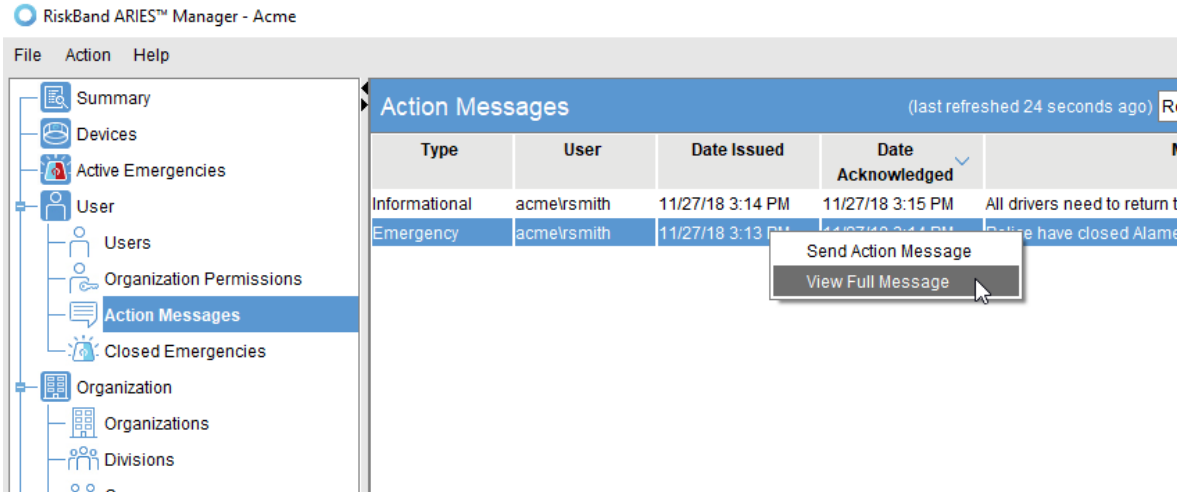
Viewing a History of Action Messages

To view the full text of an action message that has been sent:

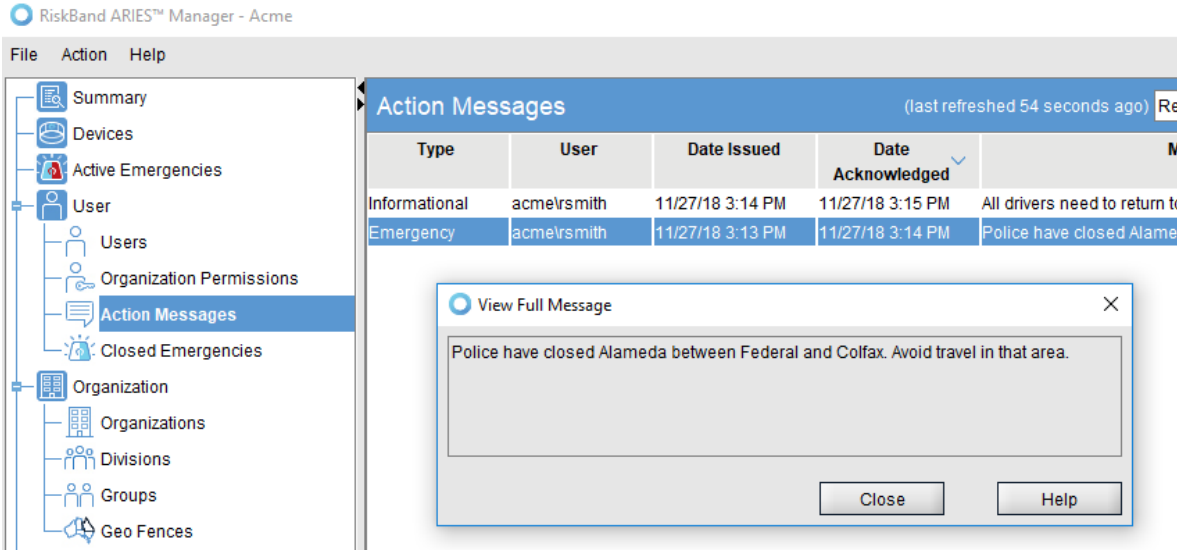
1. In the navigation pane, under the Users section, click **Action Messages**.

   The Action Messages content pane appears.

2. From the Action Messages content pane, right-click the row that contains the action message you want to view and select **View Full Message**.



The View Full Message dialog box appears.



3. After viewing the message, click **Close**.

The View Full Message dialog box closes.

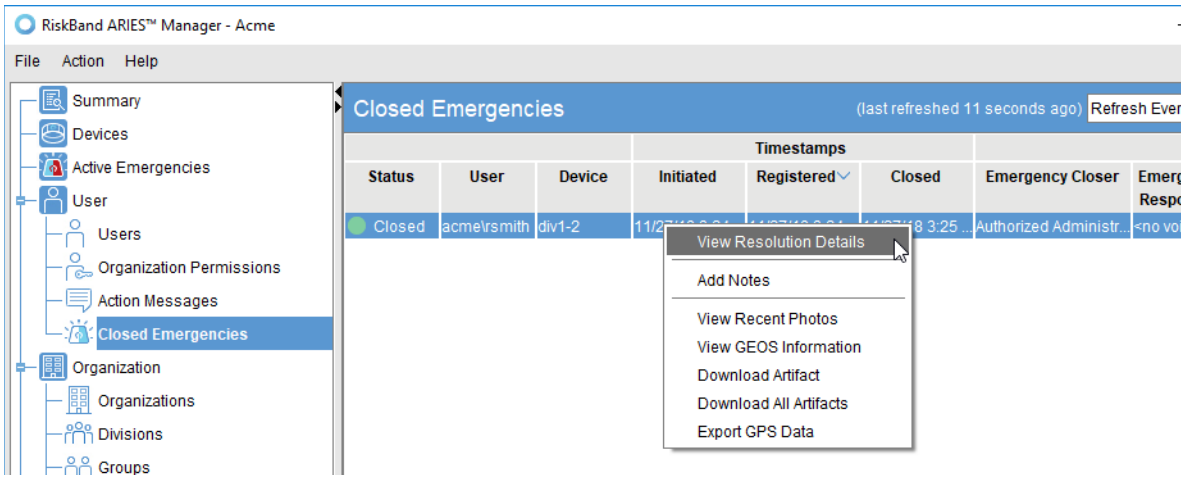
Viewing Closed Emergencies

To view the resolution details of a closed emergency:

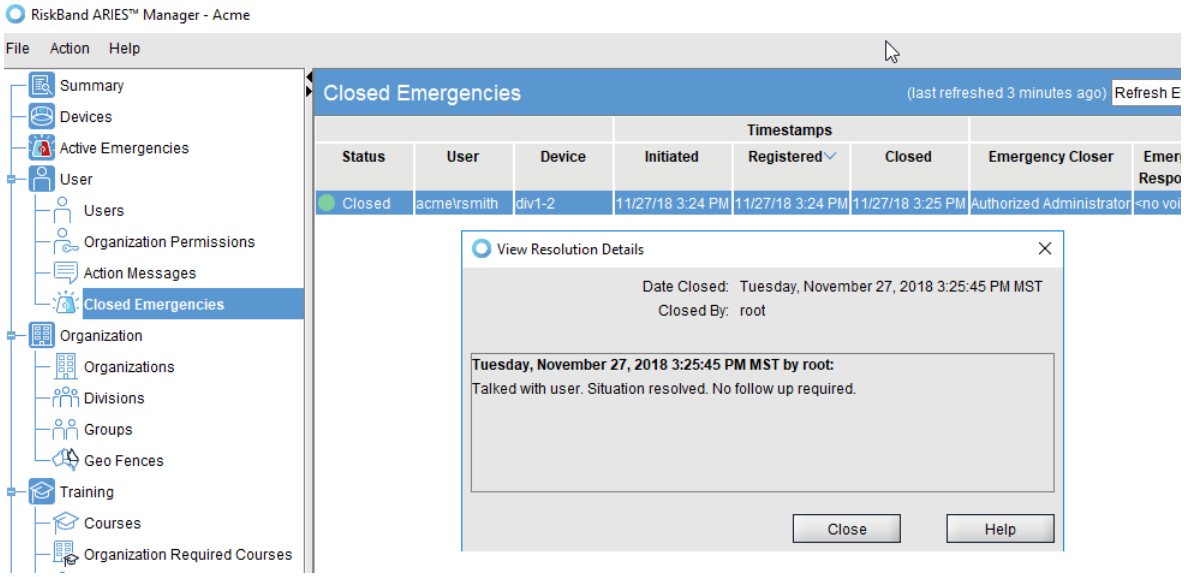
1. In the navigation pane, under the Users section, click **Closed Emergencies**.

   The Closed Emergencies content pane appears.

2. From the content pane, right-click the row that contains the emergency whose resolution details you want to view and select **View Resolution Details**.



The View Resolution Details dialog box appears.



3. After viewing the resolution details, click **Close**.

The View Resolution Details dialog box closes.

A Safety

This chapter describes safety considerations for the RiskBand.

Handling

When wearing or handling the RiskBand consider the following:

Wearing the Device on a Lanyard

If wearing or carrying the RiskBand device with a lanyard, only use breakaway safety lanyards.

Using the Buttons

Do not use excessive force when pressing the buttons on the RiskBand.

Exposure to Dust and Liquid

The RiskBand device has an ingress protection rating (IP rating) of 67, which means it is fully protected from dust and can be submerged in three feet of static water for 30 minutes. Avoid submerging the device completely in water.

Cleaning and Care

Clean the RiskBand device with a cotton cloth and distilled water if it comes in contact with substances that leave stains or obscure the LCD screen.

Repairing

Do not attempt to repair a RiskBand. Return the device to RiskBand for servicing. Information on returning a device to RiskBand can be found at www.riskband.com/support.

Charging

Caution: Customers must use the RiskBand-supplied charger for charging devices. Unsupported chargers that may supply too much or too little current can damage the device or the charger. Using an unapproved charger and cable will void the RiskBand warranty.

Caution: Do not allow devices to discharge completely. The self-discharge of batteries for an extended period of time at low battery levels can damage the battery. Devices that are not going to be charged (or that will not be used) for 1-2 days, should be powered off using the device menu.

Avoid charging the RiskBand under the following conditions:

- Extreme heat conditions
- Environments where flammable gases or particles may be present

Replacing the Battery

If the RiskBand device stops working or develops a short battery life, do not attempt to replace the battery. Return the device to RiskBand for servicing. Information on returning a device to RiskBand can be found at www.riskband.com/support.

Radio Frequency Interference

Avoid using the RiskBand in environments where radio devices are restricted. In these situations, the RiskBand device can be temporarily placed in Airplane Mode.

Medical Device Interference

The RiskBand can emit electromagnetic fields that can interfere with medical devices. If you are using a medical device, consult with a physician before wearing or using the RiskBand.

B Regulatory and Compliance Notices

This chapter describes the regulatory and compliance information for the RiskBand device.

FCC Verification Statement

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Certification

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

- FCC ID: 2AHZ7100602018
- Equipment Product Code: RBD10060

Declaration of Conformity

This device complies with Part 18 of FCC Rules.

Disposal and Recycling

RiskBand devices should not be disposed of in household waste. Contact customer support at www.riskband.com/support for information on returning RiskBands for disposal.

Contacting RiskBand

Contact RiskBand customer support in the following ways:

Support Site	www.riskband.com/support
email	customercare@riskband.com
Telephone Number	877-475-2263 (87RISKBAND)
Company Website	www.riskband.com