

Privoro Fulcrum Cloud Portal Administrator Guide V1.0

TABLE OF CONTENTS

Section 1: Overview	1
Portal requirements	1
Section 2: Getting started	2
Activate your Portal account	2
Sign in for the first time	5
Section 3: Using the Portal	8
Using the Monitoring Dashboard	8
Navigate to other screens	9
Minimize the navigation menu	10
Sign out	10
Working with lists	10
Search within a list	11
Change the number of results displayed on each page	11
Working with detail panes	12
Receiving success messages	12
Section 4: Initial workflow	13
Section 5: Managing users	14
View user information	14
Adding users	15
Option 1: Add a user individually	15
Option 2: Add users in bulk	16
Edit a user's information	18
Delete a user	18
Section 6: Managing SafeCases	19
View SafeCase information	19
Assign a user to SafeCase	20
Unassign a user from a SafeCase	20
Assign a policy to a user-SafeCase pair	21
Change a user-SafeCase pair's assigned policy	22
Pushing firmware updates	22
Option 1: Push a firmware update to a single SafeCase	23
Option 2: Push a firmware update to all SafeCases	24
Section 7: Managing policies	25
View policy information	25
Create a policy	26
Edit a policy	27
Delete a policy	27
Working with policy alerts	28
Section 8: Submitting a support ticket to Privoro	29

Overview

The Privoro Portal allows you to manage and monitor your organization's SafeCase™ devices.

Through the Privoro Portal, you can:

- Assign SafeCases to users
- Establish policies governing SafeCase usage
- Push firmware updates to SafeCases
- Monitor SafeCase statuses
- Monitor policy violations

PORTAL REQUIREMENTS

For the best experience, the Portal should be accessed using the latest version of the Firefox web browser on a desktop/laptop computer.

Getting started

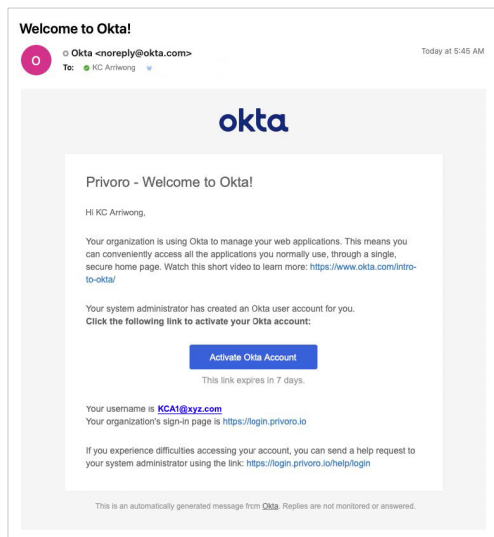
ACTIVATE YOUR PORTAL ACCOUNT

After your Portal account has been established, you will receive an email from Okta (noreply@okta.com) providing you with a link for activating your account.

To activate your Portal account:

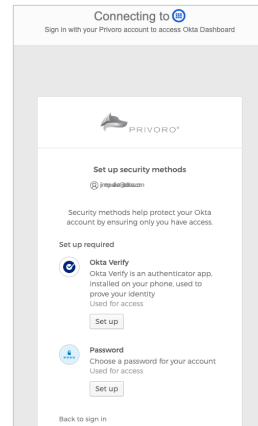
1. In the welcome email, click the link provided.

Note that this link expires after 7 days. If your link has expired, reach out to your Privoro administrator.



The account setup screen will open in your web browser.

2. On the account setup screen, click the **Set up** button under Okta Verify.



You will be prompted to set up two-factor authentication via the Okta Verify mobile app. The Portal will require you to enter a one-time password (a six-digit code) from this app each time you sign in, in addition to your password.

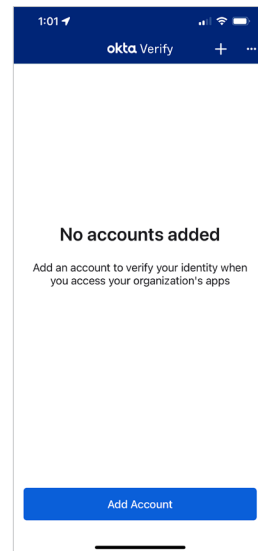
3. Follow the instructions provided on the screen:



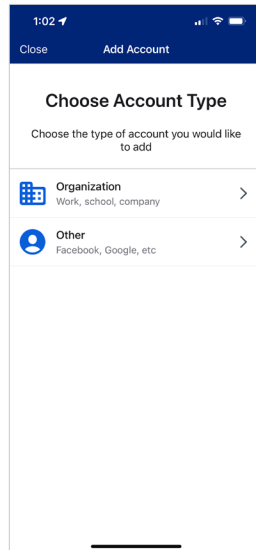
- i. If you don't already have Okta Verify on your smartphone, download and install it via your phone's official app store.

- ii. In Okta Verify:

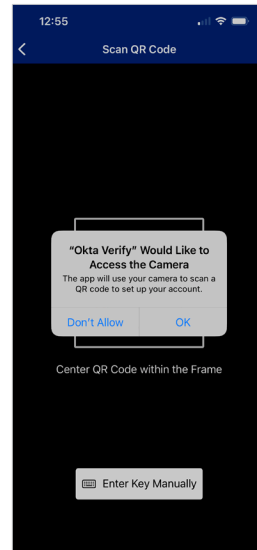
- a. On the main screen, tap the **Add Account** button or **plus (+)** icon.



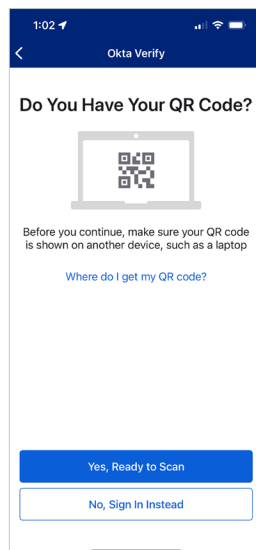
- b. On the Choose Account Type screen, tap the **Organization** option.



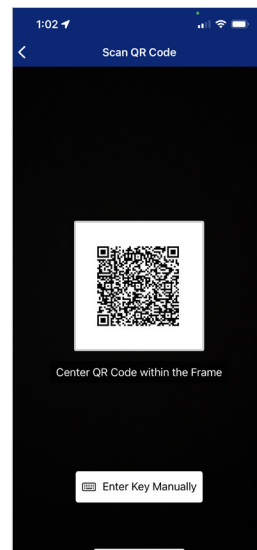
- d. If prompted, grant camera access to the app.



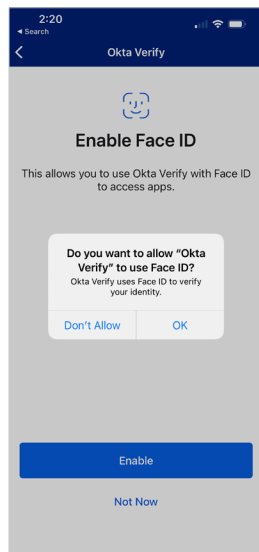
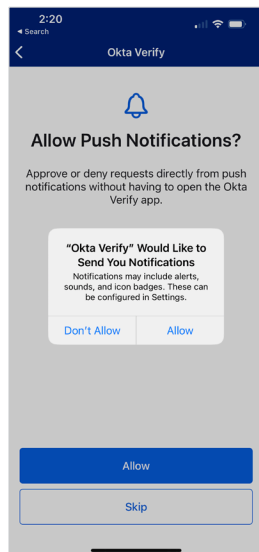
- c. On the Do You Have Your QR Code? screen, tap the **Yes, Ready to Scan** button.



- e. From the Scan QR Code screen, use your phone's camera to scan the QR code that appears on the Okta setup screen.



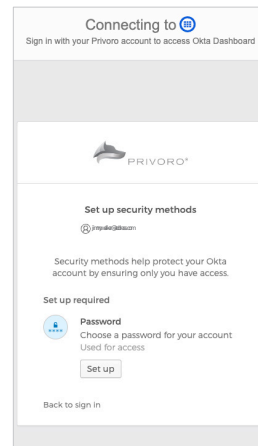
- f. If prompted, grant/deny access for notifications and/or facial authentication to the app.



- g. On the Account Added screen, tap the **Done** button.

In Okta Verify, the Privoro token will be displayed in the app's main screen. In the Portal, the account setup screen will open.

4. On the account setup screen, click the **Set up** button under Password.



You will be prompted to choose a new password for your Portal account. Your password must be at least 16 characters long and include at least one lowercase letter, one uppercase letter, one number and one special character (+_!@#\$%^&*,.). Consider using a password manager to help you generate a sufficiently complex password.

5. Enter a valid password in both the **Enter password** and **Re-enter password** fields and then click the **Next** button.

Connecting to Sign in with your Privoro account to access Okta Dashboard

PRIVORO

Set up password

Password requirements:

- At least 16 characters
- A lowercase letter
- An uppercase letter
- A number
- A symbol
- No parts of your username
- Your password cannot be any of your last 3 passwords
- At least 1 day(s) must have elapsed since you last changed your password

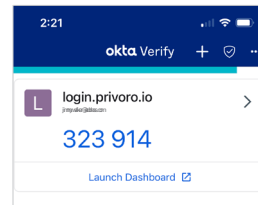
Enter password

Re-enter password

Next

3. On the next screen, enter the one-time password.

- a. In Okta Verify, locate the current six-digit code displayed for the Privoro token. If the code is hidden, tap the eye icon and then authenticate as necessary.



Your Okta dashboard will open.

SIGN IN FOR THE FIRST TIME

To sign into the Portal for the first time:

1. Open the Portal in your web browser.
If using GovCloud, navigate to <https://fulcrum.gc.privoro.com/>; if using Commercial Cloud, navigate to <https://fulcrum.cc.privoro.com/>.
2. On the initial sign-in screen, click the **Sign In** button.

PRIVORO

Username

Sign In

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel recruitment (PR), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PR, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

- b. In the Portal, enter this six-digit code in the **Enter code from Okta Verify app** field and then click the **Verify** button.

The screenshot shows a mobile app interface for connecting to a Privoro account. At the top, it says 'Connecting to' with a gear icon and 'Sign in with your Privoro account to access QA2 Environment'. Below this is the Privoro logo and a circular icon with a checkmark. The text 'Enter a code' is followed by a small Okta Verify app icon. A text input field labeled 'Enter code from Okta Verify app' contains the code '330895'. Below the field is a black button labeled 'Verify'. At the bottom, there are links for 'Verify with something else' and 'Back to sign in'.

4. On the next screen, enter your password in the **Password** field and then click the **Verify** button.

The screenshot shows the same mobile app interface as the previous one, but at the 'Verify with your password' step. It features the Privoro logo and a circular icon with a lock and four asterisks. The text 'Verify with your password' is followed by a small Okta Verify app icon. A text input field labeled 'Password' contains a masked password '*****'. Below the field is a black button labeled 'Verify'. At the bottom, there are links for 'Forgot password?', 'Verify with something else', and 'Back to sign in'.

5. Finally, on the **Update Account Information** screen, enter your email address, first name and last name in the appropriate fields, and then click the **Submit** button.

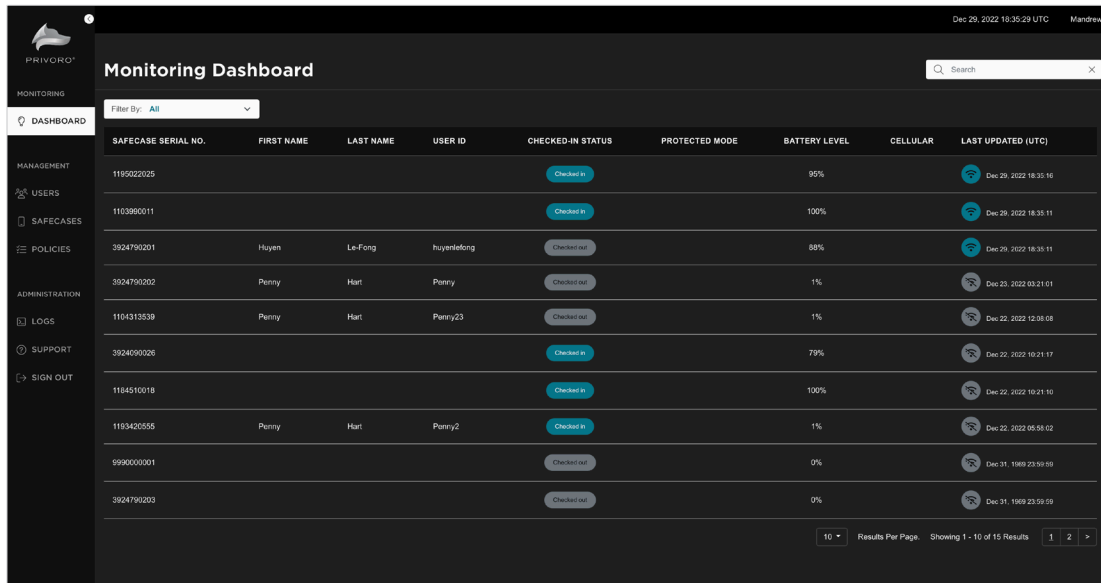
The screenshot shows a web form titled 'Update Account Information'. It has four text input fields: 'Username', 'Email', 'First name', and 'Last name'. Below these fields is a blue button labeled 'Submit'.

Upon successfully signing in, the Monitoring Dashboard view of the Portal will open.

Using the Portal

USING THE MONITORING DASHBOARD

Within the Portal, the Monitoring Dashboard serves as the home screen, presenting key information for monitoring SafeCase activity.



SAFECASE SERIAL NO.	FIRST NAME	LAST NAME	USER ID	CHECKED-IN STATUS	PROTECTED MODE	BATTERY LEVEL	CELLULAR	LAST UPDATED (UTC)
1195022025				Checked in		95%		Dec 29, 2022 18:35:16
1103950011				Checked in		100%		Dec 29, 2022 18:35:11
3924790201	Huyen	Le-Fong	huyenlelong	Checked out		88%		Dec 29, 2022 18:35:11
3924790202	Penny	Hart	Penny	Checked out		1%		Dec 23, 2022 03:21:61
1104313339	Penny	Hart	Penny23	Checked out		1%		Dec 22, 2022 12:56:08
3924090026				Checked in		79%		Dec 22, 2022 10:21:17
1164510018				Checked in		100%		Dec 22, 2022 19:21:10
1193420555	Penny	Hart	Penny2	Checked in		1%		Dec 22, 2022 05:58:02
9990000001				Checked out		0%		Dec 31, 1969 23:59:59
3924790203				Checked out		0%		Dec 31, 1969 23:59:59

The Monitoring Dashboard lists recent SafeCase event data. Events include policy violations, checking into (or out of) a facility and starting (or stopping) a cloud connection.

Within the listing for a single event, you can see the associated SafeCase and user along with SafeCase status information for checked-in mode, policy rules violated (if applicable) and most recent cloud connection.

SAFECASE SERIAL NO.	FIRST NAME	LAST NAME	USER ID	CHECKED-IN STATUS	PROTECTED MODE	BATTERY LEVEL	CELLULAR	LAST UPDATED (UTC)
392479G001	Huyen	Le-Fong	huyentefong	Checked out		88%		Dec 28, 2022 18:36:31
1103990011				Checked in		100%		Dec 28, 2022 18:36:38

To filter by event type, select it from the **Filter By** dropdown menu.

Monitoring Dashboard

Search

Filter By

All

Policy Violations

Checked-in

Checked-out

Online

Offline

SAFECASE SERIAL NO.	FIRST NAME	LAST NAME	USER ID	CHECKED-IN STATUS	PROTECTED MODE	BATTERY LEVEL	CELLULAR	LAST UPDATED (UTC)
1195022025				Checked in		95%		Dec 29, 2022 18:37:08

If filtering by policy violations, you can also filter for the policy rule violated by selecting it from the **Policy Rule** dropdown menu.

Monitoring Dashboard

Search

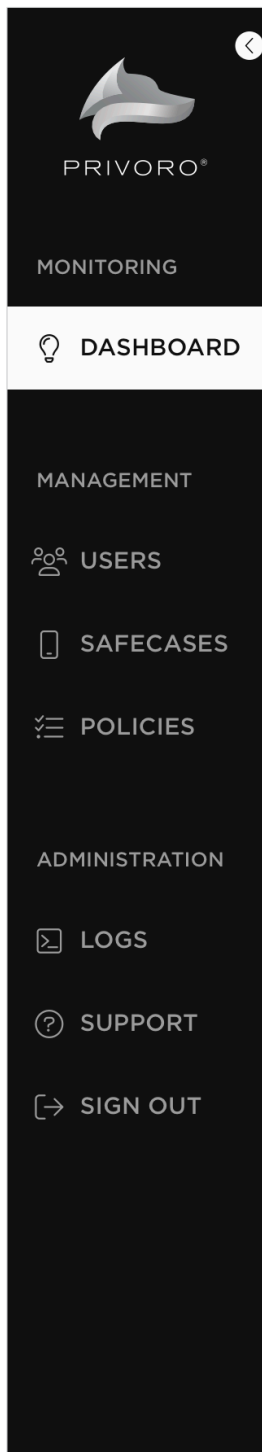
Filter By: Policy Violations

Policy Rule: Protected Mode Disengaged

SAFECASE SERIAL NO.	FIRST NAME	LAST NAME	USER ID	CHECKED-IN STATUS	PROTECTED MODE	BATTERY LEVEL	CELLULAR	LAST UPDATED (UTC)
---------------------	------------	-----------	---------	-------------------	----------------	---------------	----------	--------------------

NAVIGATE TO OTHER SCREENS

You can use the navigation menu on the left side of the Portal to navigate to other screens.

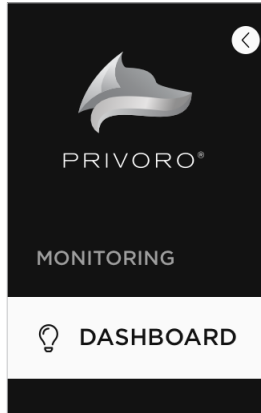


The main screens and their available actions are listed in the following table:

Screen	Actions
Manage Users	<ul style="list-style-type: none">• View all users under your supervision• Search for a user• Add a user (individually or in bulk)• Edit or delete a user
Manage SafeCases	<ul style="list-style-type: none">• View all SafeCases under your supervision• Search for a SafeCase• Assign a user to (or unassign from) a SafeCase• Assign a policy (or unassign from) a user-SafeCase pair• Update firmware for a SafeCase (individually or in bulk)
Manage Policies	<ul style="list-style-type: none">• View all created policies• Search for a policy• Add a policy• Edit or delete a policy
Logs	<ul style="list-style-type: none">• View the statuses of bulk actions (user imports and firmware updates)
Support & Help	<ul style="list-style-type: none">• Submit a support ticket to Privoro

MINIMIZE THE NAVIGATION MENU

You can hide the navigation menu if wanting more workspace. To do so, click the left arrow to the upper right of the menu.



To expand the navigation menu back to full size, click the right arrow to the upper right.

SIGN OUT

To sign out of the Portal, click the **Sign Out** option at the bottom of the navigation menu.



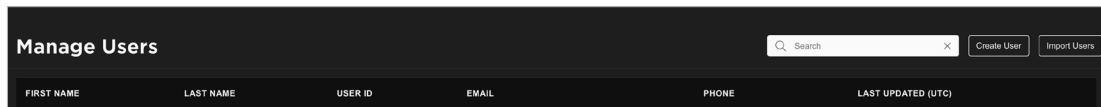
Note that you will be automatically signed out of the Portal after 15 minutes of inactivity.

WORKING WITH LISTS

Items are displayed in list format throughout the Portal, including on the Manage Users, Manage SafeCases and Manage Policies screens.

SEARCH WITH A LIST

To search within a list, enter a pertinent search term in the search box. Partial search terms are acceptable.



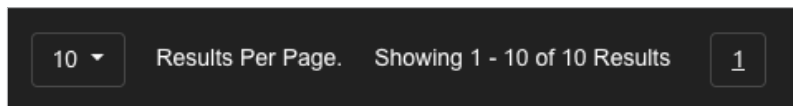
The screenshot shows a dark-themed interface for 'Manage Users'. At the top left is the title 'Manage Users'. To the right is a search bar with a magnifying glass icon, the text 'Search', and a close 'X' button. Further right are two buttons: 'Create User' and 'Import Users'. Below these is a table header row with the following columns: 'FIRST NAME', 'LAST NAME', 'USER ID', 'EMAIL', 'PHONE', and 'LAST UPDATED (UTC)'.

Pertinent search terms are listed in the following table:

Screen	Search term(s)
Manage Users	First name, last name, user ID
Manage SafeCases	SafeCase serial number, user ID, policy name
Manage Policies	Policy name

CHANGE THE NUMBER OF RESULTS DISPLAYED ON EACH PAGE

By default, the Portal displays 10 search results per page. If wanting to display more items, select a new number (20, 50 or 100) from the **Results Per Page** dropdown menu below the results.



The screenshot shows a dark-themed pagination bar. On the left is a dropdown menu with '10' selected and a downward arrow. To its right is the text 'Results Per Page.' followed by 'Showing 1 - 10 of 10 Results'. On the far right is a button with the number '1' inside, representing the current page.

Changing the number of results per page on one screen will apply the change globally.

WORKING WITH DETAIL PANES

Clicking a listing on the three management screens (Manage Users, Manage SafeCases and Manage Policies) will open a detail pane on the right side of the Portal. Here, you can make edits. On a SafeCase detail pane, you can make user and policy assignments.

The screenshot shows the 'Manage Users' interface in the Privoro portal. On the left is a sidebar with navigation links: MONITORING, DASHBOARD, MANAGEMENT, USERS, SAFECASES, POLICIES, ADMINISTRATION, LOGS, SUPPORT, and SIGN OUT. The main area displays a table of users with columns for FIRST NAME, LAST NAME, USER ID, EMAIL, and PHONE. A 'User' detail pane is open on the right, showing fields for User ID, First, Last, Email, and Phone, along with a 'Save Changes' button and a 'Bulk Import' link.

FIRST NAME	LAST NAME	USER ID	EMAIL	PHONE	LAST
John	Doe	JDOE1901	jdoe1901@example.gov	3013213457	Dis
FT	QA01	FTQA01			Dis
John	Silver	John1	johmsilver@gmail.com	608-765-3356	Dis
Mary	Silver	Mary1	marysilver@gmail.com	608-765-3356	Dis
Penny	Hart	Penny2			Dis
Test	One	Test1			Dis
Molly	Green	Molly1			Dis
Penny	Hart	Penny23			Dis
Penny	Hart	Penny			Dis
Fasty	Lady	991100	asdf@example.com	3013213458	Dis

Within a SafeCase detail pane, you can click a section name to expand that section.

To close the detail pane, you can click the X in the upper right corner or click anywhere on the area to the left of the detail pane.

RECEIVING SUCCESS MESSAGES

When you have successfully performed an action within the Portal, such as adding a user, a success message featuring a green checkmark will temporarily display in the lower left corner of the screen. You can click the message to discard it; otherwise, the message will disappear after three seconds.

The screenshot shows the 'SafeCase' detail pane. It contains fields for Serial Number (3924790204), SafeCase Model (iPhone 12 FID), Current SafeCase Firmware (3.4.0.20), and an Update Firmware dropdown menu. Below these fields are expandable sections for 'User' and 'Policy' assignments.

A success message box with a green checkmark icon, the text 'User edited.', and a close button (X) in the top right corner.

Initial workflow

The following is a typical workflow for getting your organization up and running with SafeCase:

1. Privoro adds your organization's purchased SafeCases to the Portal upon order fulfillment.
2. You add all of your organization's SafeCase users to the Portal in bulk (see Section 5: Managing users).
3. You assign a user to a SafeCase (see Section 6: Managing SafeCases).
4. You create one or more policies governing SafeCase usage (see Section 7: Managing policies).
5. You assign a policy to each user-SafeCase pair as necessary (see Section 6: Managing SafeCases).
6. Once SafeCases are in use, you monitor for policy violations via the Monitoring Dashboard (see Section 7: Managing policies).

Managing users

A user is any person who uses or will use a SafeCase.

VIEW USER INFORMATION

The Manage Users screen lists all of the users under your supervision.

Within the listing for a single user, you can see the person's first name, last name, user ID, email address, phone number and time of last user update.

Manage Users					
			<input type="text" value="John"/>	<input type="button" value="Create User"/>	<input type="button" value="Import Users"/>
FIRST NAME	LAST NAME	USER ID	EMAIL	PHONE	LAST UPDATED (UTC)
John	Silver	John1	johnsilver@gmail.com	908-765-3366	Dec 20, 2022 17:38:45

To view additional information about a user, click the user's listing.

The user's detail pane will open.

PRIVORO

MONITORING

DASHBOARD

MANAGEMENT

USERS

SAFECASES

POLICIES

ADMINISTRATION

LOGS

SUPPORT

SIGN OUT

Manage Users

FIRST NAME	LAST NAME	USER ID	EMAIL	PHONE	LAST UPDATED (UTC)
John	Doe	JDOE1951	jdoe1951@example.gov	3013213457	Dec 20, 2022 17:38:45
FT	QA01	FTQA01			Dec 20, 2022 17:38:45
John	Silver	John1	johnsilver@gmail.com	908-765-3366	Dec 20, 2022 17:38:45
Mary	Silver	Mary1	marysilver@gmail.com	908-765-3366	Dec 20, 2022 17:38:45
Penny	Hart	Penny2			Dec 20, 2022 17:38:45
Test	One	Test1			Dec 20, 2022 17:38:45
Molly	Green	Molly1			Dec 20, 2022 17:38:45
Penny	Hart	Penny23			Dec 20, 2022 17:38:45
Penny	Hart	Penny			Dec 20, 2022 17:38:45
Firsty	Lasty	991100	asdf@example.com	3013213456	Dec 20, 2022 17:38:45

10 Results

User

User ID

JohnDoe01

First

John

Last

Doe

Email

name@email.com

Phone

955-555-5555

Save Changes

Bulk Import

ADDING USERS

From the Manage Users screen, you can add users individually or in bulk (via a formatted CSV file).

Option 1: Add a user individually

To add a user individually:

1. On the Manage Users screen, click the **Create User** button in the upper right corner.



A User pane will open on the right side of the Portal.

2. In the the User pane:
 - i. Enter the user's information (user ID, first name, last name, email address and phone number) in the appropriate fields. Note that only the user ID is required. For the sake of simplicity, you may want the user ID to mirror the username from the person's email address.
 - ii. When finished, click the **Save Changes** button.

A light grey vertical pane titled 'User' with a close button (X) in the top right. Below the title is a header section with a user icon and the word 'User'. The main area contains several input fields: 'User ID' (with the value 'JohnDoe01'), 'First' (with the value 'John'), 'Last' (with the value 'Doe'), 'Email' (with the value 'name@email.com'), and 'Phone' (with the value '555-555-5555'). A teal 'Save Changes' button is positioned below the phone field. At the bottom of the pane is a 'Bulk Import' section with a plus icon and a dropdown arrow.

After saving the user, a success message will display.

Option 2: Add users in bulk

You can add up to 1,000 users to the Portal at a time using the bulk user upload feature. This method requires a precisely formatted CSV file that lists all of the users to be added.

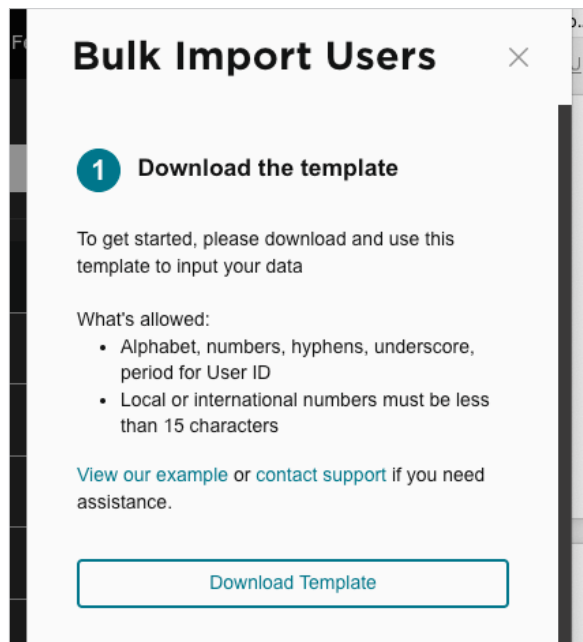
To add users in bulk:

1. On the Manage Users screen, click the **Import Users** button in the upper right corner.



A Bulk Import Users pane will open.

2. If you don't already have a CSV template for bulk user uploads, click the **Download Template** button in the Bulk Import Users pane and then save the file to a desired location.



You may want to create a copy of the template for your bulk user upload so that you have the original for future use.

3. In a spreadsheet program (such as Microsoft Excel):
 - i. Open the new CSV file.
 - ii. Add each user to be added to a new row, making sure to include the pertinent information in the appropriate format under each column. The formatting of this file must be as follows:
 - The column names and order cannot be changed
 - User ID is the only required field
 - For the user ID, acceptable characters include letters, numbers, hyphens, underscores and periods
 - The user ID must be a unique identifier across the organization
 - The phone number must be numbers only (i.e., without spaces or hyphens)
 - iii. When finished, save the file.

	A	B	C	D	E	F
1	User ID	First Name	Last Name	Email	Phone	
2	john.doe	John	Doe	john.doe@example.com	4805550001	
3	jane.doe	Jane	Doe	jane.doe@example.com	4805550002	

4. Back in the Portal:
 - iv. Select the newly created CSV file, either by clicking the **Select File** area and selecting from a file browser or by dragging the file from your computer and dropping into the area.
 - v. Click the **Import File** button.

2 Import File

Drag and drop your file into the uploader below or select and find your file.

Select a .csv file to upload
or drag and drop here

Select File

Import File

After starting the bulk user upload,
a success message will display.

5. Verify that the bulk user
upload was successful.

- i. Navigate to the Logs screen.

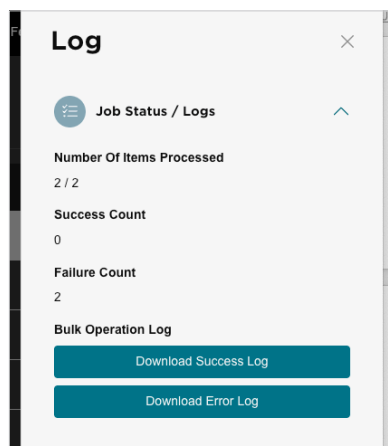
On the Logs screen, a new listing for the bulk
user upload will appear. Under the **Status**
column, the status will be displayed as “In
Queue” before the upload starts, followed by
a progress bar during the upload and finally
“Completed” when the upload has finished.

- ii. When the bulk user upload
has finished, click the listing.

Logs			
TYPE	STATUS	JOB SUBMISSION (UTC)	UPDATED (UTC) ↑↓
USER_IMPORT	✓ Completed	Dec 06, 2022 10:23:56	Dec 06, 2022 10:34:30

A Log pane will open.

- iii. In the Log pane, verify that all
users were successfully uploaded.
If any of the users failed to upload,
click the **Download Error Log** button
to download a CSV file with specifics.

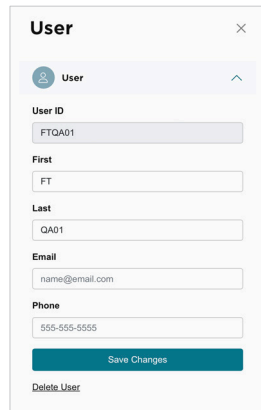


EDIT A USER'S INFORMATION

You can edit a user's first name, last name, email address and phone number. Their user ID cannot be changed.

To edit a user's information:

1. In the user's detail pane:
 - i. Edit any of the available fields.
 - ii. When finished, click the **Save Changes** button.



The screenshot shows a 'User' detail pane with a close button (X) in the top right. Below the title bar is a header with a user icon and the name 'User'. The main content area contains five input fields: 'User ID' (pre-filled with 'FTQA01'), 'First' (pre-filled with 'FT'), 'Last' (pre-filled with 'QA01'), 'Email' (pre-filled with 'name@email.com'), and 'Phone' (pre-filled with '555-555-5555'). At the bottom of the form is a teal 'Save Changes' button and a 'Delete User' link.

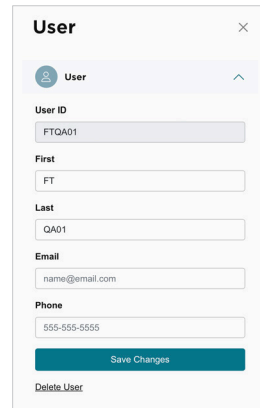
After saving, a success message will display.

DELETE A USER

You can delete a user if they're no longer a SafeCase user or a member of your organization. When deleted, a user's SafeCase will be unassigned.

To delete a user:

1. In the user's detail pane, click the **Delete User** link.



This screenshot is identical to the one above, showing the 'User' detail pane with the 'Save Changes' button and the 'Delete User' link at the bottom.

After deleting the user, a success message will display.

Managing SafeCases

SafeCase is Privoro's security device for mobile devices. SafeCases are added to the Portal by a Privoro administrator upon fulfillment of an order and will remain active in the Portal throughout the license period.

VIEW SAFECASE INFORMATION

The Manage SafeCases screen lists all of the SafeCases under your supervision.

Within the listing for a single SafeCase, you can see the device's serial number, model, firmware version, assigned user (user ID), assigned policy and time of last SafeCase update.

SAFECASE SERIAL NO.	MODEL	FIRMWARE	USER ID	POLICY	LAST UPDATED (UTC)
3924790201	iPhone 12	3.4.0.20	huyenlelong		Dec 29, 2022 19:07:58

To view additional information about a SafeCase, click the device's listing.

The SafeCase's detail pane will open.

The screenshot shows the 'Manage SafeCases' interface in the Privoro portal. On the left is a navigation menu with options like MONITORING, DASHBOARD, MANAGEMENT, USERS, SAFECASES (selected), POLICIES, ADMINISTRATION, LOGS, SUPPORT, and SIGN OUT. The main area displays a table of SafeCases. The right sidebar, titled 'SafeCase', provides detailed information for a selected device, including its serial number, model, current firmware, and an option to update the firmware. It also shows the assigned user and policy.

Additional information includes the following:

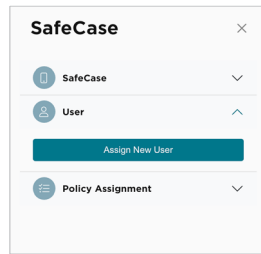
Section	Additional information
User	First name, last name, email address, phone number
Policy	Policy rules

ASSIGN A USER TO A SAFECASE

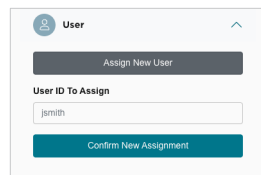
Before assigning a user to a SafeCase, the SafeCase must be added to the Portal by Privoro.

To assign a SafeCase to a user:

1. In the SafeCase's detail pane:
 - i. Click the **User** dropdown menu to expand that section.
 - ii. Click the **Assign New User** button.



- iii. Enter the user's user ID in the **User ID To Assign** field.
- iv. Click the **Confirm New Assignment** button.

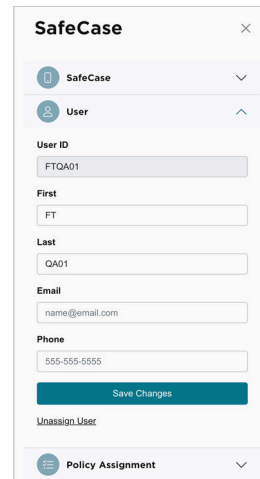


After assigning the SafeCase to the user, a success message will display.

UNASSIGN A USER FROM A SAFECASE

To unassign a SafeCase from a user:

1. In the SafeCase's detail pane:
 - i. Click the **User** dropdown to expand that section.
 - ii. Click the **Unassign User** link.



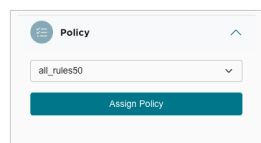
After unassigning the SafeCase from the user, a success message will display.

ASSIGN A POLICY TO A USER-SAFECASE PAIR

Before assigning a policy to a user-SafeCase pair, the policy must be added to the Portal (see Section 7: Managing policies).

To assign a policy to a user-SafeCase pair:

1. In the SafeCase's detail pane:
 - i. Click the **Policy** dropdown to expand that section.
 - ii. Select the policy to assign from the **Select Policy** dropdown menu.
 - iii. Click the **Assign Policy** button.

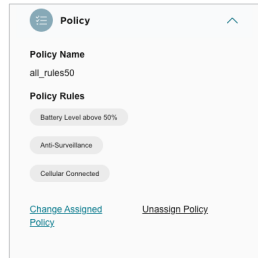


After assigning the policy to the user-SafeCase pair, a success message will display.

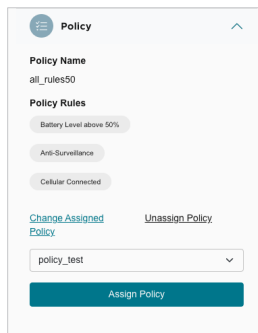
CHANGE A USER-SAFECase PAIR'S ASSIGNED POLICY

To change a user-SafeCase pair's assigned policy:

1. In the SafeCase's detail pane:
 - i. Click the **Policy** dropdown to expand that section.
 - ii. Click the **Change Assigned Policy** link.



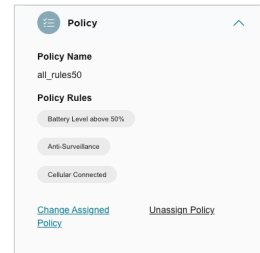
- iii. Select the policy to assign from the **Select policy** dropdown menu.
 - iv. Click the **Assign Policy** button.



After changing the user-SafeCase pair's assigned policy, a success message will display.

To unassign a policy from a user-SafeCase pair:

1. In the SafeCase's detail pane:
 - i. Click the **Policy** dropdown to expand that section.
 - ii. Click the **Unassign Policy** link.



After unassigning the policy from the user-SafeCase pair, a success message will display.

PUSHING FIRMWARE UPDATES

Privoro periodically releases new firmware for each SafeCase model. For security and stability purposes, it is important to keep SafeCase updated with the latest firmware.

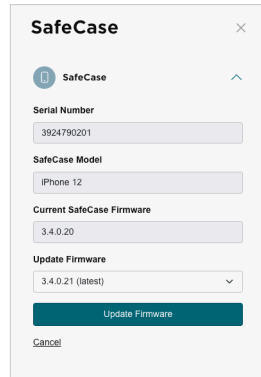
After pushing a firmware update to a SafeCase, the user will receive a push notification via their Privoro app notifying them that an update is about to occur.

From the Manage SafeCases screen, you can push firmware updates to a single SafeCase or to all devices.

Option 1: Push a firmware update to a single SafeCase

To push a firmware update to a single SafeCase:

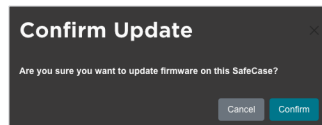
1. In the SafeCase's detail pane:
 - i. Select the desired firmware version from the **Update Firmware** dropdown menu. The most recent version will be marked "latest."
 - ii. Click the **Update Firmware** button.



The image shows a 'SafeCase' detail pane with a close button (X) in the top right. It contains the following fields: 'Serial Number' (3924790201), 'SafeCase Model' (iPhone 12), 'Current SafeCase Firmware' (3.4.0.20), and 'Update Firmware' (a dropdown menu showing '3.4.0.21 (latest)'). At the bottom are 'Update Firmware' and 'Cancel' buttons.


A verification window will open.

2. In the verification window, click the **Confirm** button.



The image shows a 'Confirm Update' dialog box with a close button (X) in the top right. It contains the text 'Are you sure you want to update firmware on this SafeCase?' and 'Cancel' and 'Confirm' buttons at the bottom.

The progress of the update will be displayed under the **Firmware** column for the SafeCase. Once the update is complete, the column will display the new firmware version.

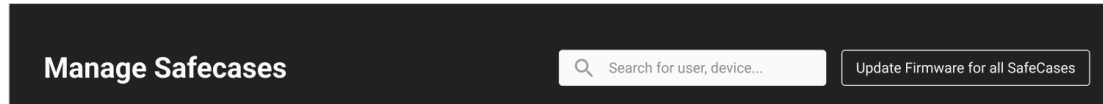
Manage SafeCases					
Search					
Update Firmware for all SafeCases					
SAFECASE SERIAL NO.	MODEL	FIRMWARE	USER ID	POLICY	LAST UPDATED (UTC)
3924790201	iPhone 12	0%  3.4.0.21	huyenlelong	allrules50	Dec 29, 2022 21:03:21

Option 2: Push a firmware update to all SafeCases

Only the latest firmware version can be pushed to all SafeCases.

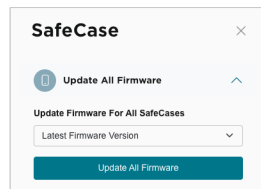
To push a firmware update to all SafeCases:

1. On the Manage SafeCases screen, click the **Update Firmware for all SafeCases** button in the upper right corner.



A SafeCase pane will open on the right side of the Portal.

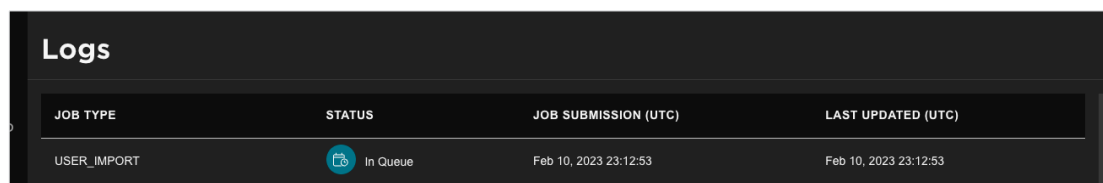
2. In the SafeCase pane, click the **Update All Firmware** button.



After starting the bulk firmware update, a success message will display.

3. Verify that the bulk firmware update was successful.
 - i. Navigate to the Logs screen.

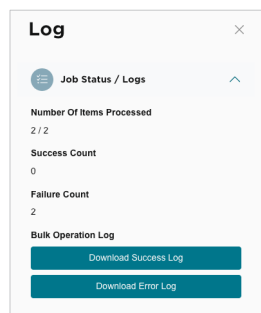
On the Logs screen, a new listing for the bulk firmware update will appear. Under the **Status** column, the status will be displayed as “In Queue” before the update starts, followed by a progress bar during the update and finally “Completed” when the update has finished.
 - ii. When the bulk firmware update has finished, click the listing.



A Log pane will open.

- iii. In the Log pane, verify that all SafeCases were successfully updated.

If any of the SafeCases failed to update, click the **Download Error Log** button to download a CSV file with specifics.



CREATE A POLICY

To create a policy:

1. In the Manage Policies screen, click the **Create Policy** button in the upper right corner.



A Policy pane will open on the right side of the Portal.

2. In the Policy pane:
 - i. Enter a name summarizing the policy in the **Policy Name** field.
 - ii. Check the box for each applicable policy rule: **Protected Mode Engaged** if SafeCase protected mode is required, **Cellular Radio Off** if the phone's cellular radio must be turned off, and **Battery Level Sufficient** if battery level must remain above a specific threshold.
 - If Battery Level Sufficient is selected, select the percentage (10, 20, 30, 40 or 50) from the **Below** dropdown menu.
 - iii. When finished, click the **Save Policy** button.

After saving the policy, a success message will display.

EDIT A POLICY

To edit a policy:

1. In the policy's detail pane:
 - i. Edit the policy's name and/or rules.
 - ii. When finished, click the **Save Policy** button.

Policy [Close]

Create/Edit Policy [Up Arrow]

Policy Name
allrules50

Policy Rules

- ☒ Protected Mode Engaged
- ☒ Cellular Radio Off
- ☒ Battery Level Sufficient
 - Below 50% [Dropdown]

Save Policy

[Delete Policy](#)

After saving the policy, a success message will display.

DELETE A POLICY

Before deleting a policy, ensure that all user-SafeCase pairs assigned to the policy have been unassigned.

To delete a policy:

1. In the policy's detail pane, click the **Delete Policy** link.

Policy [Close]

Create/Edit Policy [Up Arrow]

Policy Name
allrules50

Policy Rules

- ☒ Protected Mode Engaged
- ☒ Cellular Radio Off
- ☒ Battery Level Sufficient
 - Below 50% [Dropdown]

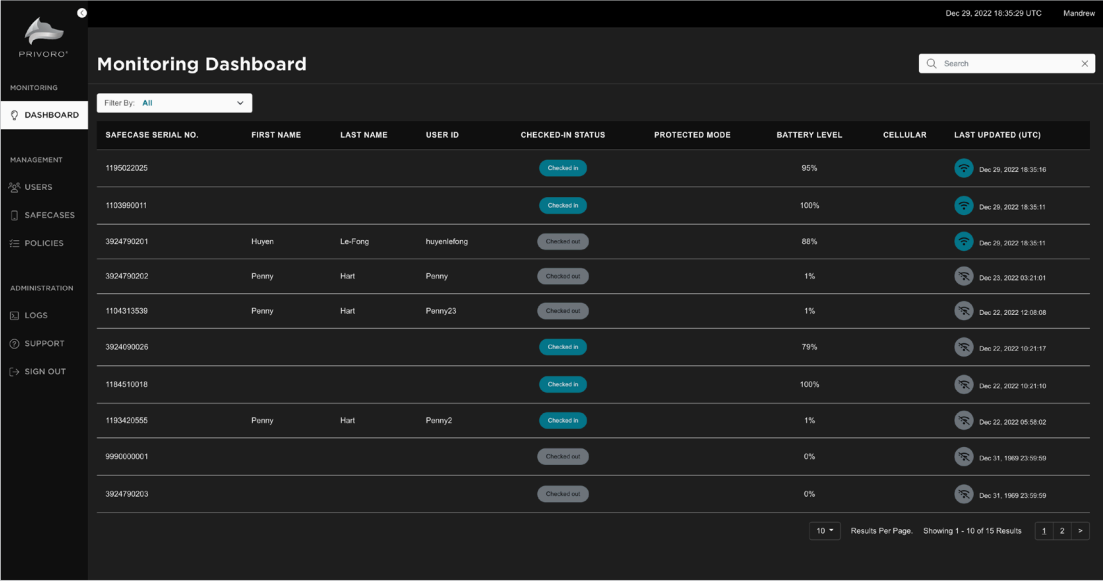
Save Policy

[Delete Policy](#)

After deleting the policy, a success message will display.

WORKING WITH POLICY ALERTS

The Monitoring Dashboard lists recent alerts of policy violations (and other key SafeCase events), presented chronologically.



The screenshot shows the Privoro Monitoring Dashboard. The top header includes the Privoro logo, a notification bell icon, the date and time 'Dec 29, 2022 16:35:29 UTC', and the user name 'Mandrew'. A search bar is located in the top right. The left sidebar contains navigation links: MONITORING (selected), DASHBOARD, MANAGEMENT, USERS, SAFECASES, POLICIES, ADMINISTRATION, LOGS, SUPPORT, and SIGN OUT. The main content area is titled 'Monitoring Dashboard' and features a table of alerts. The table has columns for SAFECASE SERIAL NO., FIRST NAME, LAST NAME, USER ID, CHECKED-IN STATUS, PROTECTED MODE, BATTERY LEVEL, CELLULAR, and LAST UPDATED (UTC). The table lists 10 rows of data, with the first two rows showing 'Checked in' status and the remaining eight rows showing 'Checked out' status. A pagination bar at the bottom indicates '10 Results Per Page. Showing 1 - 10 of 15 Results' with page numbers 1 and 2.

SAFECASE SERIAL NO.	FIRST NAME	LAST NAME	USER ID	CHECKED-IN STATUS	PROTECTED MODE	BATTERY LEVEL	CELLULAR	LAST UPDATED (UTC)
1195022025				Checked in		95%		Dec 29, 2022 16:35:16
1103990011				Checked in		100%		Dec 29, 2022 16:35:11
3924790201	Huyen	Le-Fong	huyentiafong	Checked out		88%		Dec 29, 2022 16:35:11
3924790202	Penny	Hart	Penny	Checked out		1%		Dec 29, 2022 03:21:01
1104313539	Penny	Hart	Penny23	Checked out		1%		Dec 22, 2022 12:08:08
3924090026				Checked in		79%		Dec 22, 2022 10:21:17
1184510018				Checked in		100%		Dec 22, 2022 19:21:10
1193402656	Penny	Hart	Penny2	Checked in		1%		Dec 22, 2022 05:58:02
9990000001				Checked out		0%		Dec 31, 1969 23:59:59
3924790203				Checked out		0%		Dec 31, 1969 23:59:59

Policy violations may also be included in summary data provided to your organization's security information and event management (SIEM) system.

Depending on your organization's procedures, you may choose to follow up on an alert by researching the event within the Portal or SIEM system, reaching out to your security team or contacting the user in question.

Submitting a support ticket to Privoro

If you or a member of your team have an issue using the Privoro Portal, SafeCase or Privoro app or encounter a bug, you can submit a support ticket to Privoro.

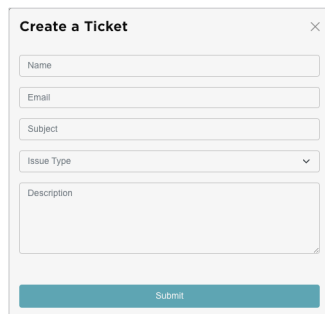
To submit a support ticket to Privoro:

1. On the Support & Help screen, click the **Create a Support Ticket** button in the upper right corner.



A Create a Ticket window will open.

2. In the Create a Ticket window:
 - i. Enter your name and email address in the pertinent fields.
 - ii. Enter a brief summary of your issue in the **Subject** field.
 - iii. Select the pertinent system (SafeCase, Privoro app, or Portal) or category from the **Issue Type** dropdown menu.
 - iv. Enter a detailed description of the issue in the **Description** field. Include step-by-step directions for recreating the issue, if applicable. Also include as many specifics as possible – your browser version if a Portal issue, the serial number if a SafeCase issue or the app version if an app issue.
 - v. When finished, click the **Submit** button.

A screenshot of a 'Create a Ticket' modal window. It contains input fields for 'Name', 'Email', and 'Subject'. Below these is a dropdown menu for 'Issue Type' and a larger text area for 'Description'. A teal 'Submit' button is at the bottom.

After submitting the ticket, a success message will display.

You will receive an email confirmation with your ticket number. A Privoro support member will work on your ticket and get back to you with any updates.



©2024 Privoro LLC or its affiliates. All rights reserved. PRIVORO and the PRIVORO DOG LOGO are trademarks of PPIP LLC, registered in the U.S. and other countries. PVOSJP0291 V03