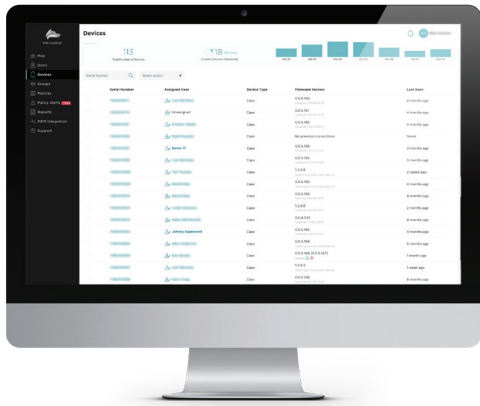


# Privoro Policy Management

Setting and monitoring policy around the use of SafeCase™ and its integrated mobile hardening feature.



## Managing and monitoring SafeCase use

The web-based dashboard serves as the policy management interface for system administrators to assign policies, monitor and gather reporting on SafeCase user actions. Privoro provides the toolbox and the engine, but how administrators choose to “set the dials” is highly flexible inside the framework.

- Configure policies for specific users and groups
- Tie geofences to policies
- Leverage custom MDM attributes
- Get notified of policy violations
- Review SafeCase logs

## Policy engine advantages

The Privoro policy engine makes it possible to monitor actions taken on the SafeCase through independent, hardware-based mechanisms recorded in the customer dashboard. These include everything from engaging and disengaging the camera and microphone protections to removing the smartphone from the SafeCase. Administrators can also monitor SafeCase status, including battery level and location.

The policy engine also allows system administrators to configure use and location-specific policy parameters, like geofencing, and view them in the portal.



### FLEXIBLE CAMERA AND MICROPHONE POLICIES

Instead of disabling cameras or microphones outright, administrators can enable users to utilize these sensors in appropriate work circumstances.



### CUSTOM GEOFENCES

Administrators can establish custom geofences around locations of concern and tie these to policies based on validated location data communicated by the SafeCase.



### TRUSTED REPORTING

SafeCase events are securely reported to the cloud and recorded in a non-repudiable audit log, providing high assurance of the associated mobile device's past and present states.

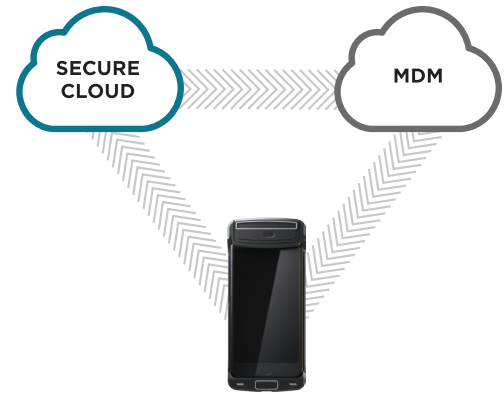


PRIVORO®

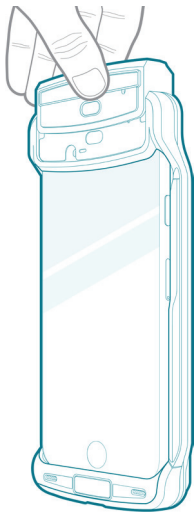
# Privoro Policy Management

## Extending policy enforcement via integrations with existing MDM/UEM solutions

By integrating Privoro's policy engine monitoring and reporting with an organization's existing Unified Endpoint Management or Mobile Device Management solution, administrators can take policy enforcement actions directly on the user's mobile device. These could include sending violation notifications, activating the lock screen or even clearing specific apps so they can't be utilized.



## Anatomy of a policy violation



### USER ACTION

The user makes changes to the condition of the SafeCase (and/or associated mobile device) in violation of policy.

- Exposing the cameras
- Exposing the microphones
- Removing the mobile device from the SafeCase
- Entering a geofence



### REPORTING

SafeCase events are reported to the policy engine over a secure data channel.



### ENFORCEMENT

Privoro's policy engine triggers one or more actions.

- A policy alert may be sent via the policy engine to the administrator, who may investigate the violation
- A challenge-response sequence may be initiated, requiring the user to perform an action on the SafeCase
- The mobile device may be locked or wiped, or a custom action may occur, depending on compliance measures set in integrated MDM solution

