Frequently Asked Questions

Introducing TRUCE

Welcome to TRUCE! You may have heard that TRUCE is a mobile app that stops mobile device distraction. You're probably wondering though, what exactly does that mean and what does that look like in practice?

Put simply, TRUCE™ is like a safety switch for mobile devices. It uses contextual awareness — meaning it recognizes where and how a mobile device is being used — to automatically enforce policies in hazardous or risky work environments, including driving a vehicle or operating heavy equipment.

At TRUCE, we are about ensuring your safety, but never at the expense of your privacy. We've created this guide to answer the most common questions about how the TRUCE app works on your device and what it means for your personal information.

Frequently Asked Questions

What personal information is the TRUCE application able to see or access on a mobile device?

TRUCE respects your privacy. It never collects or stores personal data such as credit card information, passwords or photos. Call details, texting information and emails are not accessed or read. And, information is never collected on what apps are being used or what the apps are being used for.

Can the TRUCE system access data from other applications on my mobile device?

No, TRUCE does not have access to your other applications, only the ability to enable or suppress access to them based on your company's policy. All your sensitive information like passwords, phone numbers, SMS, and emails, are inaccessible by the TRUCE app.

Will TRUCE ever sell or share my information with a 3rd party?

No data is ever shared with or sold to a 3rd party by TRUCE Software. Keep in mind, no personal data is accessible by the application in the first place.

Will TRUCE use up my mobile data or drain my phone battery?

We know battery life and data usage is important to every mobile device user. That's why on average, TRUCE only uses about 40-70mb of data per month, and 1%-2% of battery power per hour when active.

Will my employer be able to tap into my phone, even when I'm not at work?

TRUCE is designed to protect your privacy. The app does not tap, listen in, or record any personal usage of your mobile device. Ever.

Android Permissions and Device Settings

Location REQUIRED

This setting allows TRUCE to recognize when you are entering a vehicle or any managed zone. This is how TRUCE enforces device policy only in the places it should, and never where it shouldn't. The location setting is not used to track your movements outside of a managed zone.

Accessibility Services REQUIRED

This setting allows the TRUCE app to enable approved applications while in a managed zone. It also prevents the app from being uninstalled.

Draw Over Other Apps REQUIRED

This setting allows the TRUCE app to manage your access to applications based on your company's policy configuration.

Call Log REQUIRED

(Android devices running OREO 8.0 and later)

This setting is used to manage incoming and outgoing calls based on company policy configuration and allowed whitelisted phone numbers.

Do Not Disturb REQUIRED

(Android devices running OREO 8.0 and later)

TRUCE uses this setting to manage incoming notifications, both audio and visual, based on your company policy.

Device Admin

This permission supports the no uninstall policy setting.

SMS

This setting allows TRUCE to auto-respond to SMS messages while your device is in a managed zone.

Write Settings

This setting helps to reduce the TRUCE app's battery power usage.

Contacts

This setting enables the TRUCE app to allow calls from certain whitelisted numbers and support auto-responding to SMS messages. This will also allow for access to your contact list while in a managed session based on your company policy.

Camera

This setting is used within a vehicle zone, and only if the Passenger Mode feature is allowed. When initiated, the front and rear camera is used to determine that you are not driving the vehicle and deactivates the policy during the managed vehicle session. No photos are taken, and no images are stored.

iOS Permissions and Device Settings

Location Services REQUIRED

This setting must be set to 'ALWAYS ALLOW'. Doing so allows TRUCE to recognize when you are entering a vehicle or any managed zone. This is how TRUCE enforces device policy only in the places it should, and never where it shouldn't. The location setting is not used to track your movements outside of a managed zone. This permission also helps to minimize battery usage.

Bluetooth REQUIRED

This device setting allows the TRUCE app to connect and communicate with beacons. Communicating with beacons is how TRUCE knows when to enter an active policy mode. The TRUCE app requires your Bluetooth setting to be on at all times, however Bluetooth uses no energy unless it is paired to a device.

Bluetooth Sharing REQUIRED

This permission allows for your device to be more efficiently managed in a zone where more than one managed device is present.

Contacts

This setting allows the TRUCE app to allow calls from certain whitelisted numbers and support auto-responding to SMS messages when in a managed zone. TRUCE never modifies or records any of your contact information.

Camera

This setting is used within a vehicle zone, and only if the Passenger Mode feature is allowed. When initiated, the front and rear cameras are used to determine that you are not driving the vehicle and deactivates the policy during the managed vehicle session. No photos are taken, and no images are stored.

TRUCE