Roam 1.1.23 - 1 FAQ

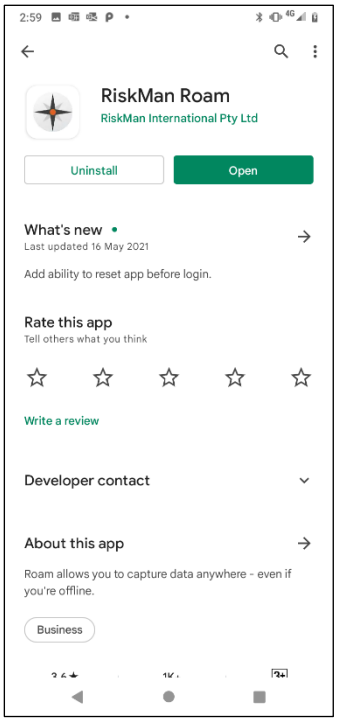
Roam is a simple app designed to enable users to capture new data quickly and easily in the field. The Roam Script Builder is a tool in your RiskMan system where you will define what the Roam app looks like in your organisation. Users will download your script on to their device and capture data to the forms as they require.

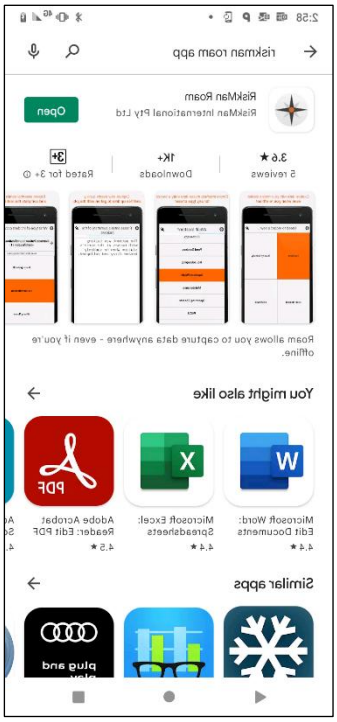
Which devices are supported?

The ROAM app is available for **iOS** (Apple) and **Android** devices – tablets and phones.

The minimum operating system requirements to use Roam on a mobile device are:

- **iOS 14** and up for Apple devices
- **Android or " Vanilla Ice Cream" (Version 15.0)** and up for Android devices





How much does the app cost?

The app is free to download.

Can somebody use the app if I haven't setup Roam on my RiskMan system?

No. Users can download the app, but it cannot be used until you have setup Roam on your system, and communicated the credentials required to sign in to the app to your users.

Can I still record data using the app if I have no active mobile data or Wi-Fi connection?

Yes. You can capture new data while you are offline. The next time your device has an active data connection, it will automatically transmit the new records to your RiskMan system.

Can the app be "forced" on to company-owned devices?

Yes. While the both iOS and Android apps can be deployed through an enterprise deployment process, it also comes with possible limitations.

How does ROAM licencing work?

Each Riskman user that will be using ROAM on their mobile device to enter records into the Riskman system will require a licence. ROAM licences are sold in bulk based on your estimate of how many users will need the ROAM app. The licence is activated in the same way as the register licences.

How does a user sign into the app?

Signing in involves entering a unique, simple, and easy to remember **passkey** then logging into RiskMan with the user's regular username and password. You will need to communicate to your users what the passkey has been set to in your configuration of Roam.

Does the app support all field types for data capture?

No. There are limitations to the types of fields the app supports. Currently the app does not support the following:

- Subforms
- Journals
- Associated risks
- Any other multi-select pop up screens
- Visual selection tools, e.g. the body part selector

How many fields can be captured using the app?

There is no limit to the number of fields you can capture with the app. Depending on how you want to use the app, however, you might want not want to capture *all* the supported fields in a form (e.g. Incident form), in order to provide your users with a fast, easy experience.

Can users record new data 'anonymously' with the app?

No. In order to use the app, the user must have a RiskMan user profile.

Can a user open and modify existing records in the app?

No. The app is designed for data capture only.

Are there any reporting tools available in the app?

No. The app is designed for data capture only.

Can I attach videos using the app?

No. The app only supports attaching images.

Can I use the app on my wearable device?

No. There is no plan to make a version of the app for wearable devices like smartwatches.

Roam Script Builder questions

The Script Builder is the tool in your RiskMan system that allows you to define what a user can record in the Roam app – that is, the types of records they can enter (Incidents, Hazards, Audit, etc.), and the information that you want them to record for each one, based on the existing fields in your RiskMan system.

Who can use the Script Builder?

Access to the Script Builder is controlled by its own user permission, so you can turn it on for any user(s) you want.

Can I have more than one script active at a time?

Yes. You can have multiple scripts available for your users. For example, you might have different scripts available for different facilities in your organisation, or different business units, etc.

Can RiskMan create a script for me?

Yes. RiskMan can engage with you to build the script(s) you need for your organisation. This will be a scoped and quoted project.

Technical questions

Can Roam still be used when my system is hosted by RiskMan?

Yes. From a technical standpoint, it makes no difference where the RiskMan system is hosted, whether it's "in the cloud", or hosted locally at your organisation.

What encryption technique does the app utilise?

Data on the device is stored in browser local storage and is encrypted using the Stanford JavaScript Crypto Library, which uses a symmetric-key authenticated encryption using CCM mode and an AES cipher. This library is considered the most secure library available for encryption in JavaScript.

The encryption keys are randomly generated upon store. The code which does the store is heavily obfuscated.

Any data transferred over the internet is encrypted via HTTPS.

What user authentication standards are supported?

Currently authentication is performed against standard RiskMan accounts, or LDAP-enabled authentication.

Systems where users must nominate their facility or organisation for LDAP login are currently not supported.

There are plans to allow any authentication type that RiskMan can support (such as ADFS, SAML) but currently this is not possible.

The authentication scheme used is a token driven scheme much like any single point sign in but is served by RiskMan and is a proprietary standard.

It is worth noting here that Roam cannot change or review records on the RiskMan site, it is only able to collect information and transmit that collected information into a new record.

How are user credentials managed for the application on the device, e.g. Hashed and stored within the application, iOS keychain, etc.?

The password for the user is never stored on the mobile device and is required to be entered by the user during authentication.

Once authenticated the user is determined dually by the token and device.

Authentication can be put on a strict expiry schedule via Global Settings in RiskMan. The user will be required to re-authenticate when expiration occurs.