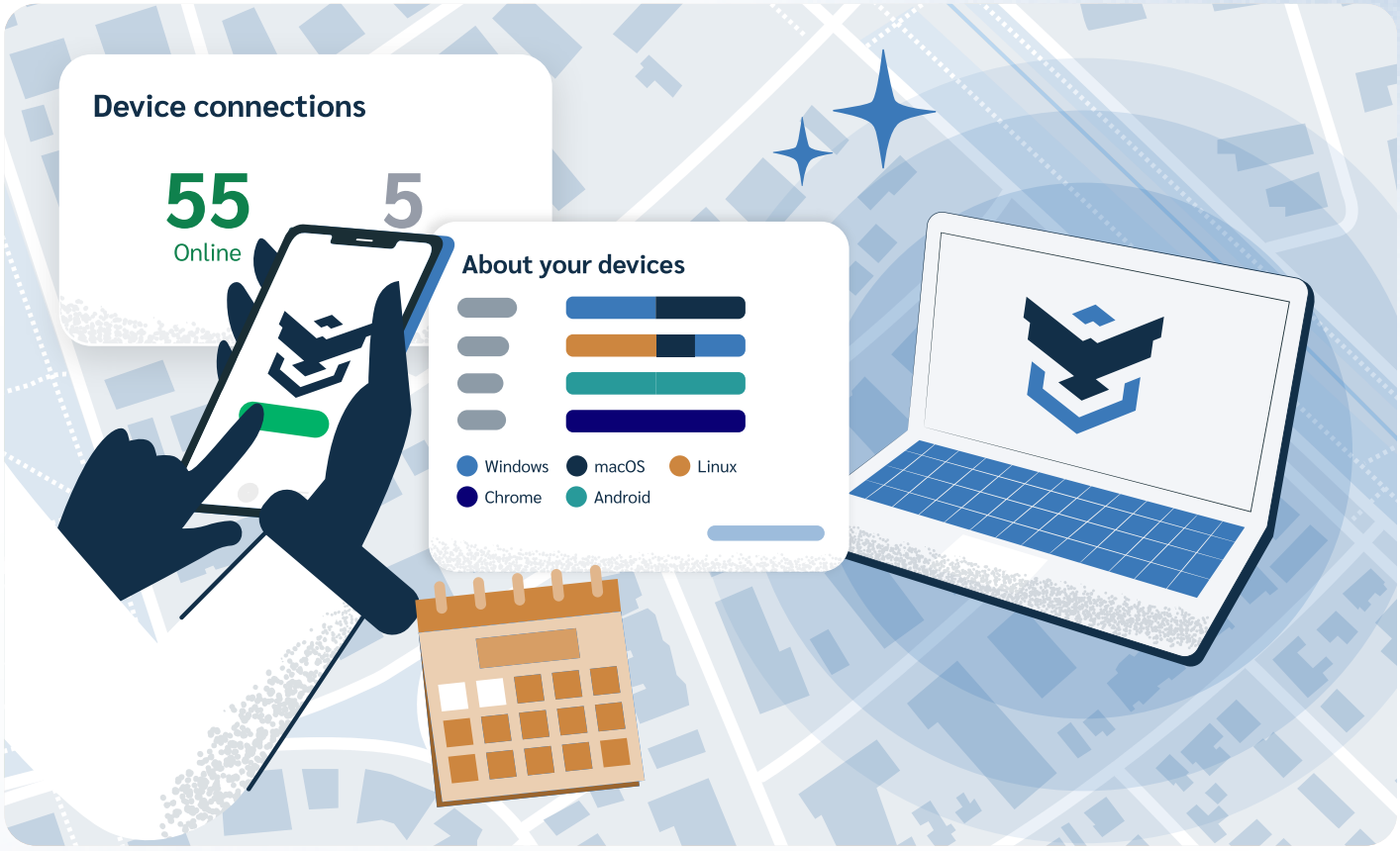
Prey's end-of-year security and readiness

CHECKLIST

Prey Inc.

Prey end-of-year security & readiness checklist



A fresh year deserves a fleet that is just as fresh. This is the perfect moment to declutter your account, confirm that everything is running smoothly, and make sure your devices are ready to take on whatever chaos January brings.

1. General account & organization health

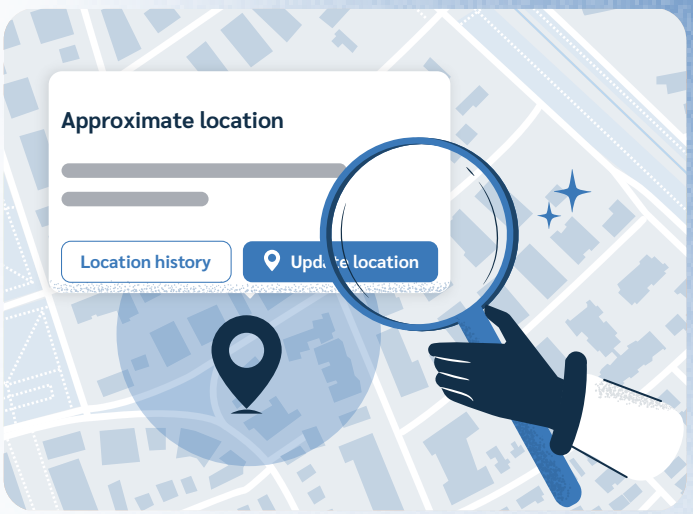
Your Prey account is the command center of everything. Keeping users, permissions, and access clean means fewer headaches later. This step makes sure the right people have the right access, no old logins hanging around, and your account is safe from the inside out.

Account security

Your devices might be in the field, but your Prey account is home base, and it needs to be locked down tight. This section is all about reducing human error and closing the front door on unnecessary risk.

- [ ] Verify that every user has **2FA** enabled.
  (Users must activate it themselves from their profile settings.)
- [ ] Use the Audit Log (Full Suite) to review recent device actions, admin changes, and critical events.
- [ ] (Optional) Password rotation for users with elevated permissions.
  Tip: If changed by an admin in the Panel, notify users so they can log back in.

2. Device tracking & monitoring



If a device goes off the grid and nobody notices... did it even happen? This section will make sure your tracking setup is running smoothly, so you're not caught off guard when someone leaves a laptop in a taxi, or worse.

Tracking setup

Tracking only works if it's actually tracking. Sounds obvious, but it's easy to assume things are fine until they're not. These checks make sure devices are talking to the Panel, sending location data, and updating regularly, especially if you're relying on Aware Tracking to keep tabs passively.

- [ ] Confirm that Tracking is active on all devices using filters in the Panel.
- [ ] Validate whether Aware Tracking is enabled when continuous location updates are required.

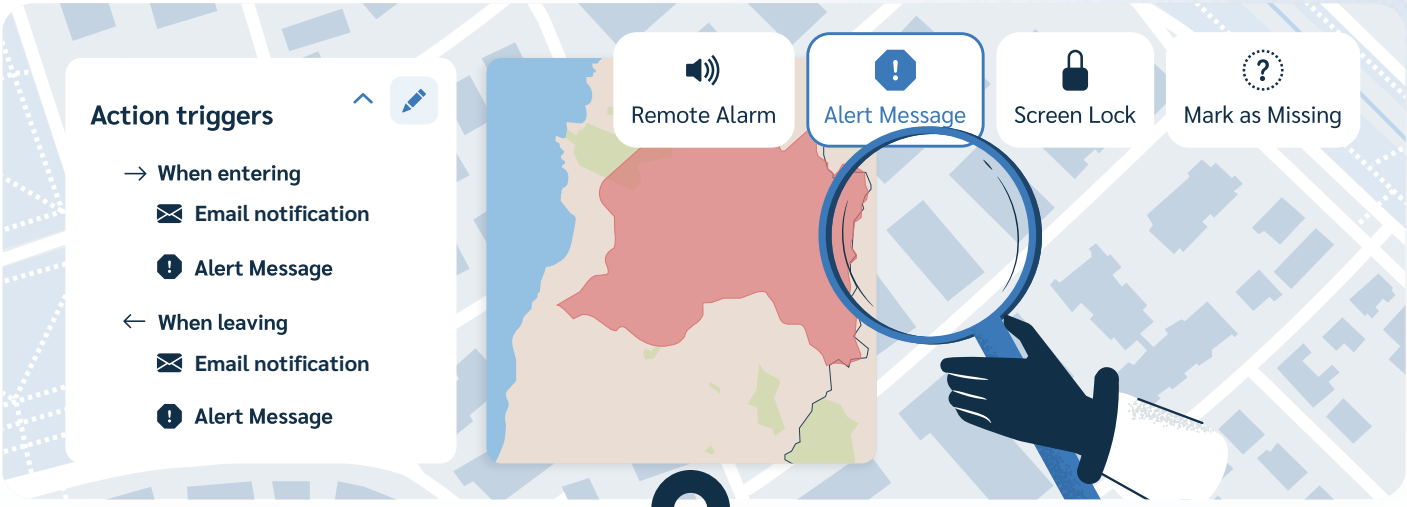
Location History Visibility

Knowing where a device is right now is useful, knowing where it's been is powerful. Before you kick off the new year, take a scroll through your devices' past locations. This helps spot red flags, verify usage, or just confirm that everything's been where it should be.

- [ ] Review and **export Location History** to confirm regular reporting from devices.
- [ ] Flag devices that show long periods without connection or reporting anomalies.

3. Geofencing Adoption & Validation

Geofences let you know when a device leaves the building, enters a restricted zone, or just ends up where it shouldn't be. This section helps you check if you've got geofences set up and actually doing something: sending alerts, running actions, and keeping your fleet in bounds.



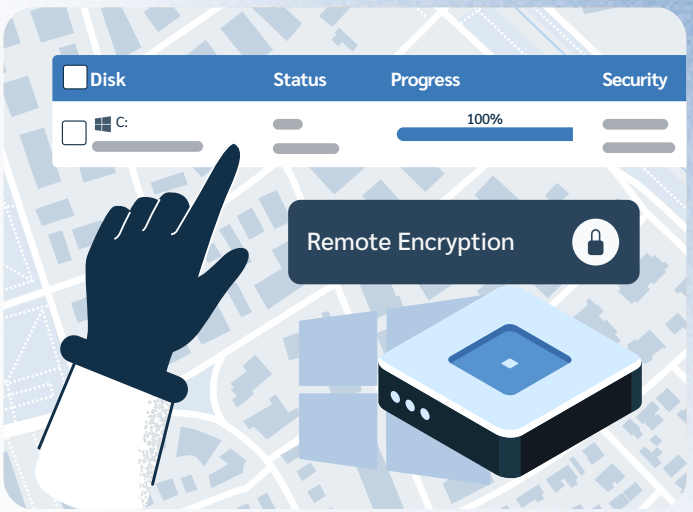
- [ ] Verify that **Geofences** are configured for key locations (e.g., offices, schools, warehouses).
- [ ] Ensure **devices are assigned** to the correct geofences.
- [ ] Validate that **email alerts** are set for entry/exit notifications.
- [ ] Confirm that **triggers** (automated actions) are configured and tested where needed.

Fleet visibility

Keeping your device fleet visible and connected ensures that remote actions work when they're needed most. These checks help spot connection issues early, confirm that security commands can reach devices, and that you're not flying blind when something goes wrong.

- [ ] Verify that firewall, antivirus, proxy, and other security tools are whitelisting Prey traffic, preventing blocks to the agent's communication with Prey servers.
- [ ] Confirm that all devices are visible in the Global Map and have recently connected to the Panel.
- [ ] Audit **device last seen, connection status, and battery percentage.**
- [ ] **Enable "Identify devices when linking"** to prevent duplicate device entries when re-installing or reassigning equipment. *This is only available on Windows, macOS, and Ubuntu.*
- [ ] Check for **unusual location patterns** or offline devices.

4. Device security & protection



Lost or stolen devices happen. What matters is how ready you are when it does. This section is all about making sure your security tools are in place before something goes sideways, so you can act fast, protect sensitive data, and avoid a bigger mess.

Data protection (OS-dependent)

Some devices hold sensitive data, credentials, or access to other systems. These steps help you double-check that encryption is enabled where it should be, and that you're able to wipe things clean if needed. Better to have the safety net and not need it than the other way around.

- [ ] Test **Remote wipe** functionality on a test device.
- [ ] **Use the Encryption filter to identify devices that support encryption and those storing sensitive data that must be encrypted.**
- [ ] Export the **BitLocker Recovery Keys CSV** for Windows devices and archive it securely.

5. Device management

Device management is about making sure everything is organized, updated, and cleaned up so you're not dragging around outdated records or ghost devices from three semesters ago.

Inventory review

When was the last time you took stock of what's actually out there? This is your chance to double-check that every device is accounted for, running the latest version of Prey, and not secretly collecting dust somewhere.

- [ ] Ensure that **all devices have the latest Prey version** installed.
- [ ] Export a full device inventory CSV to verify hardware data integrity and detect anomalies.
- [ ] Remove or archive **decommissioned and inactive devices** from the account.

Organization & labels

Group devices in a way that reflects how your organization actually works, by team, department, location, or loan program. Smart labels and groups save time, reduce confusion, and prevent endless scrolling later.

- [ ] Confirm that labels and groups reflect current structure: teams, departments, campuses, or loan programs.

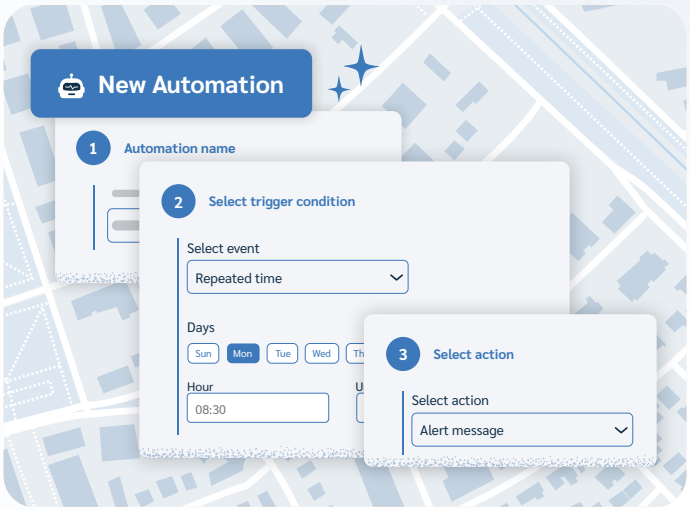
Mass actions and Automations (Full Suite only)

Want to lock 20 laptops at once without breaking a sweat? That's what mass actions are for. This section also includes Automations, which are your hands-free helpers for repetitive events ike flagging devices with low battery or taking action when a laptop hasn't connected in days.

- [ ] Test **Mass actions** like Lock, Message, and Alarm actions in a few test devices.
- [ ] Validate that **Automations are** correctly scheduled (low battery, device offline, etc.).

6. Scheduled Automations

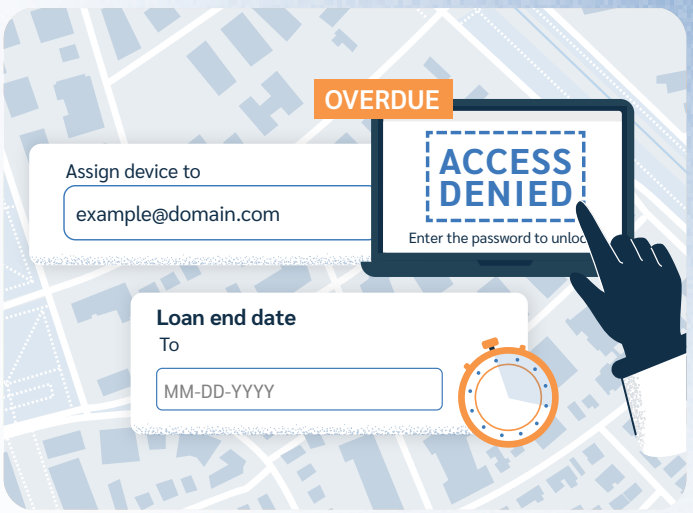
Automations let you set smart rules that kick in when certain things happen, like low battery, missed check-ins, or hardware changes, so nothing slips through the cracks. Once they're set, they've got your back.



- [ ] Review and test **Automations** configured for events such as:
  - Low Battery
  - Device Offline *(device has not connected to Prey after a specified number of days)*
  - Hardware Changes
  - Start/Stop Charging
  - Scheduled Time

7. Device Loan Management (Full Suite)

This section is about making sure your loan system is under control, due dates are checked, devices are assigned, and overdue returns don't go unnoticed.



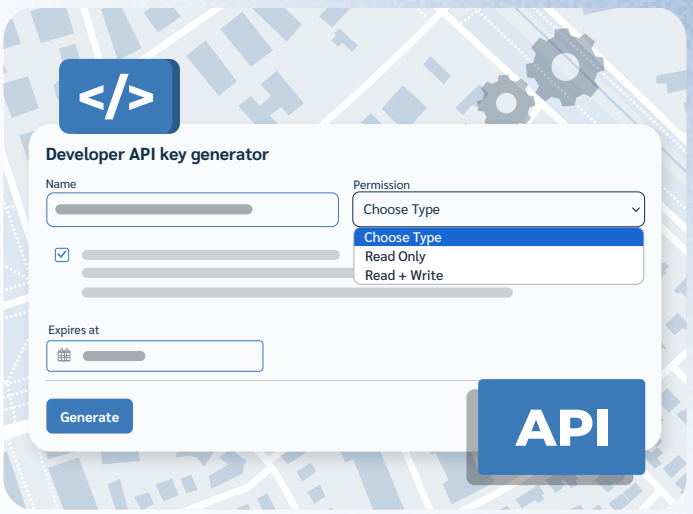
Loan Manager

Loan Manager makes it easy to assign devices, follow up on returns, and add a bit of automation to the process. With alerts, security actions for overdue gear, and clear visibility, it keeps things organized without adding extra overhead.

- [ ] Review and clean up **user assignments**, ensuring each device has an assigned user.
- [ ] Review all **active loans** and check due dates.
- [ ] Ensure **notifications** for overdue devices are being triggered and received.

8. Developer Integrations & API

(Full Suite)



If you're using Prey alongside other tools, like your ticketing system or internal dashboards, this section is for making sure everything's still talking to each other. A quick check here helps avoid broken workflows, expired tokens, or surprise gaps in your integrations.

Developer Tools

The API and integrations give you more control and flexibility, but they do need occasional maintenance. This is your reminder to double-check token health, clean up anything unused, and make sure your connected systems are still running smoothly.

- [ ] Rotate any API Keys that are unused.
- [ ] If you have integrations enabled, **review their status and verify they are functioning as expected.**

9. Breach Monitoring
(bonus track)

Credentials have a bad habit of ending up in the wrong places, especially when no one's looking. If you're using Prey's Breach Monitoring feature, this section helps you make sure it's set up, catching what it should, and giving you the insights you need to act fast.

Exposure Awareness

A quick peek at your Breach Monitoring dashboard can tell you a lot: which emails have popped up on the dark web, what data was exposed, and how frequently it's happening.

- [ ] Review **Breach Monitoring Dashboard** for any exposed credentials, PII, and other relevant data.
- [ ] Download and archive the latest exposure report for compliance.
- [ ] Check if **domain-wide monitoring** is enabled (for larger organizations).

10. End-of-Year Readiness

You made it to the finish line! This last section is your final sweep, tying up loose ends, testing your response actions, and giving your team a clean slate to start the new year strong.

Final Checks

Before wrapping things up, it's a good idea to make sure devices are still checking in, remote actions work as expected, and your team knows what to do if something goes wrong. A little time here now saves headaches down the line.

- [ ] Use the **Device View** to ensure all devices have reported activity within the last 30 days.
- [ ] Clean up users, geofences, automations, and inventory for a fresh operational start.
- [ ] Run a **test of remote actions** (lock, alarm, message).
- [ ] Ensure that all team members are familiar with emergency procedures (wipe, lock, etc.).

About Prey

Prey is a cross-platform **Device Tracking & Security** tool to stay in control of remote assets. It's a service that protects over 8 million devices and their data every day, all around the world.

Prey started in 2009 as a small tech company with a sole purpose: helping people keep track of their devices. 15 years later, our service evolved into a trusted multi-tool for both people and businesses. We are experts at tracking, protecting and managing your work and play tech tools. And a proud team of people willing to support you.

Prey for: **People** | **Businesses** | **Schools**

Prey Spa. © Santiago, RM Chile