

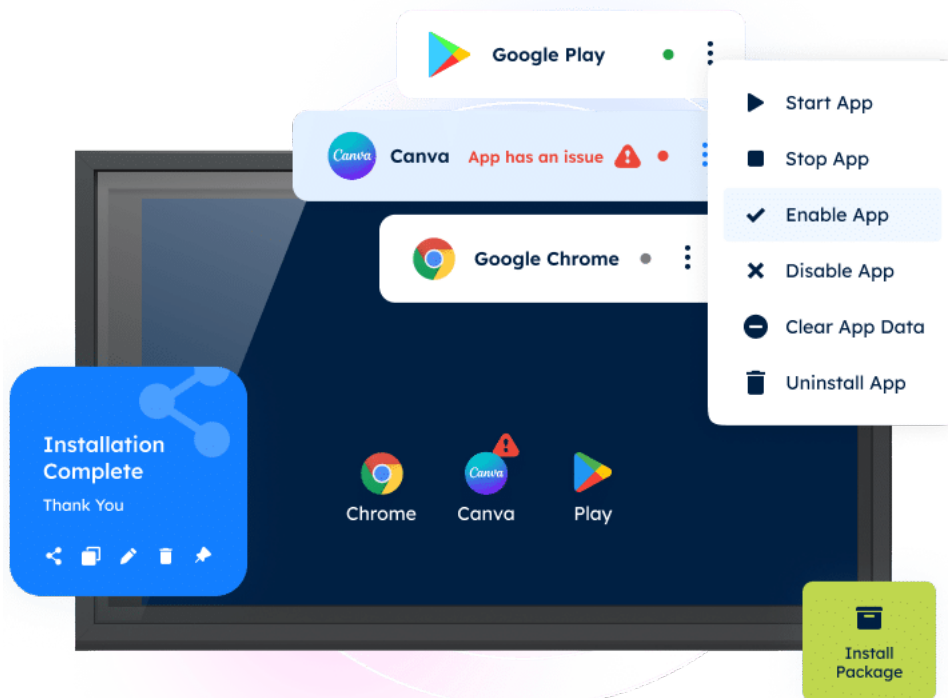
TouchView - Radix Feature Guide



Device Control

1. Cloud/SaaS device management - Radix is described as turnkey SaaS platform for remotely managing fleets of devices without setting up local servers.
2. Multi-OS device management - The platform supports Android, Windows, Apple/iOS and ChromeOS devices; the specific commands available vary by operating system.
3. Central fleet dashboard - The Overview Dashboard provides visibility into enrolled/active devices and users, connected devices, locations, recently enrolled devices, most-used applications, recent commands and OS distribution.
4. Remote Control — attended (live demo/support) or unattended (kiosk-managed) modes
5. Optional user-permission prompt before remote control sessions begin
6. Remote-control screen with rotate, back, home, app-switch, and menu icons
7. Directional pad (D-pad) emulation for game-console-style navigation during remote sessions
8. Volume control during remote-control sessions
9. Remote Execute — run custom command-line arguments or scripts on a device
10. Restart — remotely reboot a device
11. Shutdown — remotely power off a device

12. Wake on LAN — wake a device by Device ID, group name, or filter (requires Ethernet + manual shutdown)
13. Advanced Wake-on-LAN — supports custom Broadcast Address/Port for stricter network setups
14. Sound Siren — trigger an audible alarm on a device (useful for emergencies or locating a device)
15. Clear App Data — remotely clear an app's cache/history to resolve crashes or performance issues
16. Disable/Enable Apps — remotely turn specific apps off or back on
17. Remove Google Accounts — strip Google accounts from an Android device
18. Smart Recovery — restore a device to its last snapshot or factory settings
19. Send Files — push specific files to a device with a defined destination path
20. Send Message — deliver a simple text message (title + body) to a device
21. Change Agent Password — remotely reset a user's device password
- Apple Custom Command — execute a plist (property list) file on macOS devices
22. Kiosk Mode — restrict a device to an approved app allow/block list for single-purpose use



Apps & Policy Management

1. Install Packages — deploy software individually, to a group, or automatically to new devices
2. Uninstall Packages — remove software/apps from a device
3. Package sourcing from URL, local file upload, Google Play Store, or iOS enterprise app
4. Software Policies — blacklist/block apps with security or performance issues
5. Policies configurable per OS (Android, iOS, macOS, Windows, ChromeOS)
6. Device Settings — remote configuration of Wi-Fi, security/login rules, general settings, APN, wallpaper, certificates, panel/power settings, and lock password

7. Install Certificate — push VPN, Wi-Fi CA, or app certificates to a device
8. Workflow — chain multiple commands into one ordered, reusable sequence
9. Workflow drag-to-reorder and Favorites menu for commonly used command sets
10. Timeout command — insert timed delays between steps within a Workflow
11. Scheduler & Trigger — automate command execution by timing, geofencing, Wi-Fi connection, or device startup
12. Timing triggers support one-time, date-range, or perpetual (no end date) execution
13. Group Management — apply packages, settings, or policies to an entire device group at once
14. "New Devices" group automation — auto-install mandatory apps on any newly enrolled device
15. Per-app install-status breakdown across a group (current version / outdated / not installed)
16. VPP Install/Uninstall — deploy or remove apps via Apple's Volume Purchase Program
17. OTA (Over-the-Air) updates — push OS or app updates, or a full OS image, to Android devices
18. DEP Apple Profile — configure and apply Apple Device Enrollment Program profiles
19. Firmware Update — remotely update device firmware for performance/security (device-dependent)
20. Tags — apply/remove tags on devices for easier grouping, filtering, and searching

Messaging & Enrollment

1. Advanced Messaging — rich messages with images, sound, full-screen video, looping YouTube, or interactive HTML forms
2. Message triggers by time, geolocation, network prompt, or third-party API (e.g., emergency alerts)
3. Enroll devices across all supported OSes via QR code, downloadable agent, or Google EMM
4. Apple DEP and Apple VPP support for streamlined enterprise Apple deployment
5. Android for Work (Google EMM) enrollment for secure Android MDM management

User & Access Management

1. Role-based User Permissions — granular, admin-assignable access rights per user
2. Admin vs. standard user distinction (e.g. can delete accounts, or change account-wide settings)
3. Two-step verification (via Google/Microsoft Authenticator) for secure account login
4. Device Pairing — restrict access using a pairing code shared with the remote user