

Solution Brief

Island for Corrections Institutions

Enabling rehabilitation technology without losing control of the device

The Challenge

Tablets in Corrections: The Security Gap

Tablets have become a fixture in correctional facilities across the country. They are often issued to incarcerated individuals to support education, family communication, and reentry preparation. Research consistently shows that [maintaining family connections during incarceration](#), [participating in continued education](#), and [re-entry programs](#) reduce recidivism. But the reality has become an operational and security headache for corrections IT teams.

Tablets issued on outdated Android operating systems are routinely jailbroken. Once tampered with, a device bypasses all approved content restrictions, connects to contraband Wi-Fi hotspots, and accesses the open internet without visibility or oversight. To combat this, corrections departments confiscate devices, scan for rogue signals, and re-issue hardware, a cycle that costs time and money.

The Island Enterprise Browser can help close the gap and prevent device jailbreaks, ensuring tablets are not misused and serve their continued purpose.

The Gaps in Today's Approach

- **MDM alone isn't enough**

Mobile Device Management tools like Workspace ONE are excellent at managing device enrollment, pushing configurations, and enforcing OS-level policies. But they have limited ability to govern what happens inside a web browser, which is the primary vector for jailbroken tablet misuse. Once a device is compromised at the OS level, MDM visibility and controls are undermined.

- **Binary policies create the black market**

When the only options are full restriction or full access, facilities are forced to lock down too hard, and inmates find ways around it. The inability to allow some access (family communication, approved educational sites) without allowing all access drives the jailbreaking economy.

- **No visibility means no accountability**

Even on compliant devices, corrections IT teams have little insight into exactly what incarcerated users are doing in a browser session, such as which sites were visited, what data was entered, and when. That makes incident response slow and audit trails incomplete.

The Solution

The Way Forward: Island + Workspace ONE

Island, the Enterprise Browser, fills the gap that MDM cannot. When deployed as a managed mobile browser on corrections-issued tablets and enforced as the only permitted browser via Workspace ONE, Island gives IT and security teams precise, policy-driven control over every web session.

Together, Island and Workspace ONE create a layered security model where the MDM controls the device, and Island controls everything that happens on the web.

What This Looks Like in Practice

- **Tamper detection and automatic logout**

Island continuously monitors for signs of device compromise. If a tablet is jailbroken or the OS is modified outside of an approved configuration, Island immediately terminates the browser session and revokes web access. Workspace ONE can then be triggered to wipe or quarantine the device, closing the loop between browser-layer detection and device-layer response.

- **Island as the only browser**

Workspace ONE can be configured to block all other browsers on a managed device, making Island the sole path to web access. This eliminates the ability to sideload alternative browsers or use embedded WebViews to bypass policy.

- **Precise allowlisting of approved content**

Rather than blocking the internet entirely or opening it fully, Island enforces site-level policies, permitting approved destinations like video visitation platforms, educational resources, and reentry services, while blocking jailbreaking websites, social media, messaging apps, and anything outside the approved list.

- **Full audit and visibility**

Every session is fully logged: sites visited, actions taken, time on page. Corrections IT teams gain a forensic-grade audit trail for compliance, incident response, and oversight reporting without requiring any additional monitoring infrastructure.

Key Use Cases for Corrections

Approved communications

Allow video visitation and messaging through vetted platforms while blocking all other communication channels

Educational access

Permit GED prep, vocational training, and approved course platforms with no risk of students navigating outside boundaries

Reentry preparation

Enable access to job search sites, government benefits portals, and reentry resources under policy control

Jailbreak prevention and response

Automatically block access to sites hosting device jailbreaking software and revoke access and alert IT when device tampering is detected



Island is the ideal environment for enterprise work. By unifying modern work requirements into a single Enterprise Platform, Island enables organizations to see, control, and protect work activity while making work itself smooth and simple. Leading enterprises from across major industries are using Island to safely embrace AI, onboard contractors in minutes, enable BYOD, reduce VDI spend, quickly recover from disasters, facilitate M&A, and eliminate unnecessary infrastructure and related expenses. Island is backed by world-class investors including Coatue Management, Insight Partners, Sequoia Capital, and Cyberstarts.

Learn more at island.io

Thinking an enterprise browser could be right for your organization? Take your next step here.

Schedule a demo →