PORT1

Island For MSPs

How an MSP can secure its own admin tools with an enterprise browser

An MSP's RMM, documentation platform and admin consoles run as web apps. Here's how an enterprise browser adds access rules, MFA steps and audit trails.

November 2026 | Jason Makevich, CISSP

An MSP can secure its own admin tools by running them in an enterprise browser that adds access rules, an extra MFA step before sensitive actions and an audit trail, without changing the apps. With Island for MSPs, that's Island Browser, which includes changes to web apps without touching their code.

Why does an MSP's own access need extra protection?

An MSP's own access needs extra protection because a compromised MSP can be a path into its customers' networks. A joint advisory from CISA, the NSA, the FBI and their UK, Australian, Canadian and New Zealand counterparts says threat actors can use a vulnerable MSP as an initial access vector to multiple customer networks, and it expects that targeting to continue. See CISA advisory AA22-131A.

The advisory recommends that MSPs implement MFA on all accounts that have access to customer environments and treat those accounts as privileged. It also recommends applying least privilege, disabling accounts that are no longer in use and logging the activity of the infrastructure used to deliver services.

How does Island Browser protect access to an RMM or documentation platform?

Island can add an MFA challenge at sign-in or before a specific action, require an approval step for sensitive changes, hide controls a role doesn't need and keep an audit trail with screenshots and click tracking. Island says this works without API access or changes to the apps. For an MSP, that can mean an extra MFA step before someone opens the password area of a documentation platform or the scripting area of an RMM, with each change tested in a pilot before it's relied on.

Island also applies conditional access inside the browser based on identity, device, network, location and application, and it checks device posture so unsafe devices are kept away from sensitive data. These controls can help an MSP act on the advisory's recommendations for privileged accounts.

Which MSP tools can these controls cover?

These controls work on the web apps MSPs depend on, because Island applies them in the browser instead of inside each app. Island can add automations, extra MFA and other changes to web apps without changing their source code or relying on the app vendor's APIs. It can also hide controls a role doesn't need, so a junior engineer sees fewer risky options than an admin.

How can engineers use shared admin logins safely?

Island Browser can give people the use of shared credentials without exposing the passwords, and Protected Accounts extends single sign-on to apps that don't support it. An engineer can work in a shared vendor or admin account without seeing its password. As of November 2026, Island names Okta, Azure AD (now Microsoft Entra ID) and Ping among the identity providers it works with for single sign-on.

What about engineers on personal or dedicated devices?

Engineers on personal devices can use Island Browser, which needs no agents, MDM enrollment or device imaging: they install it, sign in with their work identity and get the apps they're authorized for. An identity provider can require Island Browser for access to company apps, so opening them in another browser doesn't grant access.

On company-owned, managed computers, the Island Extension brings Island's controls into the browsers engineers already use. For dedicated admin machines, IslandOS runs Island Browser as the primary workspace on company-owned computers, and MSP admin machines are one of the places it fits.

How do MSPs keep client data in admin sessions under control?

Island's data protection is based on context, so data can move between approved work apps while leaks are blocked, for example allowing a paste into Salesforce but not into personal email. Its last-mile controls cover copy and paste, downloads, printing and screenshots, and Island can add watermarks and redact sensitive data on screen.

How do you see what happened in a session?

Island records work activity in the browser in detail for audits and incident response, and it can send that activity to SIEM and analytics platforms. Browser activity logs can be part of the record the advisory asks MSPs to keep of the infrastructure they use to deliver services. For admin work in web apps, Island also keeps an audit trail with screenshots and click tracking.

How do you remove access when someone leaves?

With Island, a person's access is removed in one place when they leave. That can help an MSP act on the advisory's advice to disable accounts that are no longer in use.

How does Island help against attacks on admin sessions?

Island describes built-in protection against malware, phishing, session hijacking and man-in-the-browser attacks, and when it detects a risky site, it stops users from entering company credentials. Island Browser also has browser isolation built in.

The same controls protect contractor access to client apps, and what an enterprise browser adds over a standard browser covers the basics. For everything that's included, see Island Browser.

How do MSPs roll this out?

An Island pilot can start with 1 to 5 users, and PORT1 helps set up the tenant, single sign-on, starter policies and a success checklist, then reviews the results with the partner. Partners get PORTER, PORT1's partner platform, for help along the way. Each change to a web app, such as an extra MFA step in front of a sensitive area, is tested in the pilot before it's relied on.

Sources

- Protecting Against Cyber Threats to Managed Service Providers and their Customers, joint cybersecurity advisory AA22-131A, CISA and partners, May 2022

Book an Island demo