IslandOS: Island Browser as the workspace on company PCs

IslandOS runs Island Browser as the primary workspace on company-owned computers, on Scylos ZeroCore, including aging PCs. Offered to MSPs through PORT1.

November 2026 | PORT1

IslandOS is PORT1's model for running Island Browser as the primary workspace on company-owned computers. Island Browser runs on Scylos ZeroCore, a thin, read-only foundation that keeps no work data on the device. It's part of Island for MSPs, offered through PORT1.

What is IslandOS?

IslandOS turns a company-owned computer into an Island workspace: users power on, sign in to Island and work from the Island homepage. Underneath is Scylos ZeroCore, which keeps no work data on the device.

IslandOS can run kiosk-style, with Island as its single app, or with Island alongside other apps on ZeroCore.

What do users see on an IslandOS device?

On an IslandOS device, users power on, sign in to Island and work from the Island homepage. Because Island Browser is Chromium-based, web apps that work in Chrome or Edge should generally work in it without compatibility testing.

A kiosk-style setup keeps Island as the device's single app, while the alongside setup lets Island run next to other apps on ZeroCore.

How do MSPs manage IslandOS devices across clients?

Scylos Switchboard gives centralized, multi-tenant management of IslandOS devices, so an MSP can manage them across clients. Island itself runs from the Island for MSPs multi-tenant console, where each client has its own tenant with its own users, policies and logs.

Why do MSPs offer IslandOS?

IslandOS gives MSPs a cloud-first option for company-owned computers, with fewer tools to run on each device and less support burden, in PORT1's view. It's also a way to keep aging Windows computers, including PCs that can't run Windows 11, working as Island workspaces after a hardware check.

Which clients and devices fit IslandOS?

IslandOS fits SaaS-heavy users, shared workstations, kiosk-style devices, aging Windows computers (including PCs that can't run Windows 11), MSP admin machines and new hardware for a cloud-first standard. Users who rely on locally installed apps, local data or specialty desktop software are a fit for Island Browser or the Island Extension on Windows or macOS.

In practice, that makes IslandOS a good match for a front desk with shared computers, a team that works almost entirely in web and SaaS apps, or a set of older PCs a client would rather not replace yet.

Can IslandOS give older company PCs a second life?

Often, yes: aging Windows computers, including PCs that can't run Windows 11, are one of the places IslandOS fits. Every IslandOS rollout starts with a hardware compatibility check, where PORT1 reviews make and model details and confirms compatibility with Scylos.

Because ZeroCore is thin and read-only and keeps no work data on the device, an older computer becomes a sign-in point for the Island workspace. Users still power on, sign in to Island and work from the Island homepage, the same as on any IslandOS device.

Does an IslandOS device still need the usual endpoint stack?

PORT1's position is that IslandOS devices don't need the usual endpoint stack, such as endpoint agents, RMM, EDR, vulnerability and patch management, DNS filtering or content filtering, and PC backup. That means fewer tools and less support burden for the MSP. Before removing any tool, MSPs check the client's insurance, compliance and contract requirements.

How is IslandOS licensed and supported?

IslandOS is licensed as an Island Browser license per user plus a Scylos ZeroCore license per device, both through PORT1, and it's available to all active PORT1 partners. For MSP partners, PORT1 supports Island Browser and Scylos ZeroCore on IslandOS devices, while hardware support stays with the MSP, the client or the hardware provider. Partners get PORTER, PORT1's partner platform, for help along the way.

Which Island add-ons work on IslandOS?

Island add-ons work on IslandOS devices, apart from IPA 360. That includes Password Manager, Island Private Access (IPA), AI Protect, AI Browser, DEX, SaaS API and Anonymizer. For example, IPA gives zero trust access to private apps without a VPN for those apps, and AI Browser brings AI into the browser where people work, with the AI providers the organization prefers.

How do MSPs start with IslandOS?

IslandOS starts with a hardware compatibility check, where PORT1 reviews make and model details and confirms compatibility with Scylos. A pilot then installs ZeroCore on a test computer, deploys Island with the client's policies, sets it up kiosk-style or alongside other apps, and reviews the result with real users. That way the client sees IslandOS in daily work before a wider rollout.

How does IslandOS compare with Island Browser and the Island Extension?

All three are part of Island for MSPs, and each fits a different kind of device. The Island Extension covers company-owned, managed computers in the browsers people already use, Island Browser covers personal, BYOD and unmanaged devices, and IslandOS makes Island the primary workspace on company-owned computers. See Island Browser vs the Island Extension for how MSPs match options to devices.

Book an Island demo