Browser Isolation for Unmanaged Device Access to Cataloged Resources

The challenge of accessing sensitive resources from non-organization-owned devices is the potential risk of data leakage. The iboss Zero Trust SSE recognizes this concern and addresses it adeptly with the Browser Isolation feature. With the platform's resource catalog, organizations can identify and constantly adapt access to sensitive resources. When users access from organization-owned devices, data remains within a controlled environment. However, when guests or contractors, using personal devices, require access, the data poses a risk. Browser Isolation emerges as the solution, enabling these users to interact with the resources through a pane-of-glass, akin to a VDI interface. As a result, data stays confined to the resource, never venturing onto unsecured devices. With iboss’s capability, any resource within the Zero Trust Resource database can be optimized for access from unmanaged devices. Coupled with tailored configuration options and SAML authentication requirements, it delivers a blend of accessibility and security.

This capability extends and simplifies Browser Isolation configuration by allowing Browser Isolation access to be directly configured within each resource that is cataloged within the Zero Trust Resource Database. This provides clear visibility of which resources have been configured for unmanaged device access.

BENEFITS

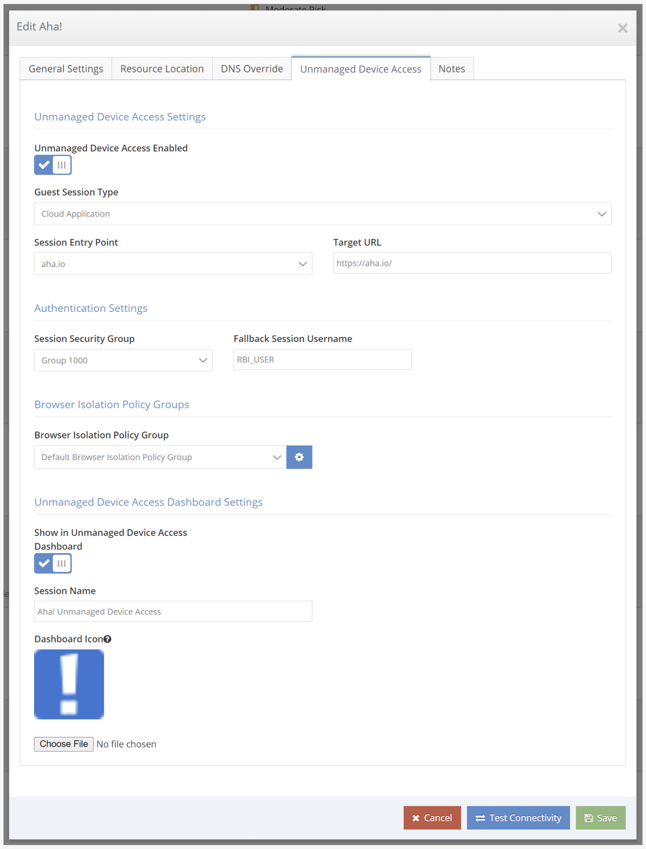
- Resource Cataloging: The iboss platform allows cataloging of sensitive resources for adaptive access decisions.
- Controlled Access: Data accessed on organization-owned devices stays in a controlled environment.
- Pane-of-Glass Interaction: For unmanaged devices, users access resources through a secure pane-of-glass.
- Data Security: Ensures data remains within the resource, preventing potential leaks on unmanaged devices.
- Custom Configurations: Resources in the Zero Trust database can be tailored for unmanaged device access.
- Application Dashboard: Users can view all assigned resources configured for unmanaged device access after authentication.

Browser Isolation for Unmanaged Device Access to Cataloged Resources

The iboss Zero Trust SSE offers Browser Isolation to safely provide access to cataloged resources for users on personal or non-organization owned devices. This capability ensures that sensitive data remains within the resource and doesn't reach the end-user device, significantly reducing potential data loss risks. Browser Isolation can now be configured directly from the Zero Trust Resource Database within each cataloged resource.

Ordering Information

SKU: Included with Browser Isolation



Unmanaged Device Access Settings

Unmanaged Device Access Enabled ☑

Guest Session Type: Cloud Application

Session Entry Point: aha.io

Target URL: https://aha.io/

Authentication Settings

Session Security Group: Group 1000

Fallback Session Username: RBI_USER

Browser Isolation Policy Groups

Browser Isolation Policy Group: Default Browser Isolation Policy Group

Unmanaged Device Access Dashboard Settings

Show in Unmanaged Device Access Dashboard ☑

Session Name: Aha! Unmanaged Device Access

Dashboard Icon

Choose File No file chosen

HOW IT WORKS

- **Catalog Resources:** Resources are cataloged within the Zero Trust Resource Database.
- **Configure Resource Policies:** Resource Polices for cataloged resources are configured to define access and authentication requirements for managed device access.
- **Configure Resources for Unmanaged Device Access:** Edit resources that require access from unmanaged devices and configure Browser Isolation options within the Unmanaged Access tab of the Resource modal.
- **Enable App Dashboard:** Configure resources so that they appear in the App Dashboard for easy access from unmanaged devices.
- **Configure Modern Auth:** Resources can be configured to require SAML authentication