Admin By Request
ZERO TRUST PLATFORM

Web Access Management

Frequently Asked Questions

GENERAL

What is Web Access Management?

Web Access Management is Admin By Request's solution for controlling internet browsing and file downloads across your organization's endpoints. It lets you define what users can access and download, enforce policies consistently on the endpoint, scan for malware, and maintain a full audit trail, all managed from the ABR portal.

How does Web Access Management fit with Admin By Request's other products?

Web Access Management extends ABR's Endpoint Privilege Management approach into browser and download security. Where EPM controls local privilege elevation, Web Access Management applies the same control philosophy to internet access, giving you consistent governance across both vectors from a single platform.

Who can configure Web Access Management settings?

Portal administrators configure Web Access Management. End users interact with it through download prompts and access controls enforced directly on their endpoints.

DOWNLOAD CONTENT

Can I block executable downloads across my organization?

Yes. Download permission controls let you block executable downloads globally, require approval before a download proceeds, or allow downloads freely. Applied consistently on the endpoint, so policy is enforced regardless of portal connectivity.

Can I let users download without approval for trusted software?

Yes. Pre-approved downloads let you create exceptions for known-safe software by website root URL, direct download URL, SHA256 file checksum, vendor certificate, or a vendor and application name combination. Matched downloads bypass approval workflows automatically, while other controls (such as MFA requirements, Intune compliance checks, and malware scanning) still apply.

Web Access Management

FREQUENTLY ASKED QUESTIONS

Admin By Request
ZERO TRUST PLATFORM

Can I block specific downloads even when downloads are generally allowed?

Yes. Blocked downloads let you create hard-deny rules using the same criteria as pre-approvals, by website, URL, file checksum, or vendor certificate. Blocked download rules take priority over other allow rules. You can also configure a custom message shown to the user when a block occurs.

How do I block specific websites?

Blocked Sites enforcement lets you define root URL and path-based deny rules that are applied directly on the endpoint. You can configure a custom message for users when a block is triggered, and each rule can be individually logged to the audit trail.

BROWSER CONTROL

How does Web Access Management control what sites users can access?

Browsing permission controls apply your centrally managed site policies directly on the endpoint. This means access rules are enforced consistently. They don't depend on portal connectivity to take effect.

How do I whitelist specific sites?

Use Pre-approved Sites to define trusted websites that users can access without friction. Rules are based on root URL and can include subpaths. Pre-approved sites bypass browsing restrictions for matched destinations, while explicitly blocked sites still take priority.

SECURITY LOCKDOWN

Can I restrict which browsers are allowed on endpoints?

Yes. Browser Lockdown lets you define which browsers are permitted (Chrome, Edge, Firefox, Internet Explorer, and in-app browsers) and set a minimum version for each. Browsers that don't meet your requirements are blocked before they can be used.

Can I require MFA before a user can download an executable?

Yes. MFA-protected downloads require users to complete SSO re-authentication (currently Microsoft 365/Entra ID) before a download is released. You can also enable email matching, which verifies that the authenticated identity matches the endpoint user.

Web Access Management

FREQUENTLY ASKED QUESTIONS

Admin By Request
ZERO TRUST PLATFORM

Can I restrict downloads to the assigned device owner?

Yes. Enabling owner-only download restriction means only the user assigned as the device owner in inventory can download executables. This is particularly useful on shared devices where non-owners should not be able to introduce software. Other users on that device can still browse, depending on your browsing permission settings.

Can I tie download permissions to Microsoft Intune compliance?

Yes. Intune compliance gating blocks executable downloads on devices that aren't Intune compliant, helping you align software access with device health and management posture. This requires the Entra ID Connector to be configured. Browsing access is not affected by this setting.

MALWARE DETECTION

How does malware scanning work?

Web Access Management uses OPSWAT MetaDefender for malware detection. When a download is requested, the file is placed in protected temporary storage on the endpoint, where the user can't reach it, and its checksum is checked against known malware signatures before the file is released to the user. You can also enable cloud scanning, which uploads unknown files for multi-engine analysis to catch threats that aren't yet in local signature databases.

What happens when malware is detected?

You configure the action. At a minimum, quarantine is supported. Detected events are logged and visible in the portal for review.

AUDIT LOGGING

What does Web Access Management log?

Web Access Management builds an audit trail around browsing activity, download decisions, approvals, bypasses, and blocks. Each event captures what happened and why, so administrators can review the record after the fact for security investigations or compliance reporting.

Can I log activity per rule?

Yes. Pre-approved and blocked rules for both sites and downloads include a per-rule audit log toggle, so you can choose which exceptions and enforcements generate log entries.