Spec Sheet

Admin By Request
ZERO TRUST PLATFORM

Web Access Management

Product Platform: **Web Access Management**
Product Version: **9.0**
Document Date: **3 August 2026**

Introducing Web Access Management

Admin By Request's **Web Access Management** is an endpoint-based policy layer that gives IT teams centralized control over how users browse the web and download software - without requiring proxy servers, DNS filters, or additional on-premises infrastructure.

Web Access Management enforces policy directly on the endpoint via the Admin By Request agent. Administrators can block or allow websites, govern executable downloads, enforce approved browser versions, require MFA or device compliance before software is allowed through, and scan every download against a multi-engine malware detection service.

Trusted sites and software can be pre-approved to flow without interruption; everything else is blocked, held for approval, or audited according to policy. Sub-settings allow a single Web Access Management tenant to run different policies for different user populations and device groups simultaneously, without separate tenants or duplicate configuration.

Just like Admin By Request's EPM and Secure Remote Access product lines, Web Access Management requires no additional on-premises infrastructure to get started. Sign up for the Free Plan and gain full Web Access Management for up to 25 endpoints - free, forever.

Product Editions

About Web Access Management licensing:

- Web Access Management is a **separate license and SKU** from EPM and SRA. It can be purchased standalone or alongside other Admin By Request products.
- Existing EPM or Secure Remote Access customers do not receive Web Access Management automatically - a Web Access Management plan must be activated separately.
- The same endpoint client software drives Web Access Management, as well as EPM and Secure Remote Access. Version **9.0 +** is required to enable Web Access Management on Windows endpoints.
- The Free Plan is available to all customers regardless of existing subscriptions.

Subscription	Max. Endpoints	License Model	Endpoint OS	Support
Free Plan (WAM)	25	Free	Windows [1]	None
Paid Plan (WAM)	Unlimited	Annual Subscription	Windows [1]	Included

1. The initial release of Web Access Management supports **Windows endpoints only (v9.0 +)**. Mac and Linux support is not yet scheduled.

Security by Design

On-device Inspection

Web Access Management performs all of its work on the endpoint. TLS decryption, policy inspection, and re-encryption happen inside the Admin By Request agent on the device itself, using a root certificate generated locally on that device. Traffic travels straight from the browser to its destination and back; it is never routed out to a cloud proxy, a gateway point of presence, or an on-premises appliance for inspection.

This is the core architectural difference between Web Access Management and traditional cloud Secure Web Gateways (Zscaler, Netskope, Cato, Cisco Umbrella), which backhaul user traffic through the vendor's cloud before it reaches the internet. Enforcing on the endpoint means:

- **No cloud round-trip, no added latency**. Browsing speed is not gated by the distance to a proxy point of presence or the load on it.
- **No infrastructure to stand up or scale**. No proxy servers, PAC files, GRE or IPsec tunnels, or DNS redirection. Enforcement capacity grows automatically with every endpoint added.
- **Decrypted traffic never leaves the device**. Because inspection is local, the plaintext of a user's HTTPS sessions is never sent to a third-party cloud, which supports privacy and regional data-residency requirements.
- **The same policy on-network and off**. Enforcement travels with the agent, so a remote or travelling user is governed identically to an in-office one, with no VPN or tunnel back to a gateway.
- **A minimal footprint**. The on-device filter is under 2 MB and adds negligible CPU overhead.

Because inspection runs on-device, Web Access Management is at its best as the only TLS-inspecting layer on a given endpoint. See "A word on Compatibility" on the next page.

> Certificate-pinned applications bypass inspection by design and can be excluded via the bypass list.

Architecture Compliance

- Downloads held in a secure, user-inaccessible endpoint location until security checks and approval requirements are satisfied - files are released to the user only after all controls pass
- Multi-engine malware scanning via OPSWAT MetaDefender (30+ engines) on every executable
- Real-time file reputation checking; unknown files submitted for cloud-based multi-engine analysis
- MFA re-authentication required at the point of download (Microsoft 365 / Entra ID)
- Device compliance gating via Microsoft Intune integration
- Hard-deny rules applied before any allow logic - blocked downloads cannot be bypassed
- Sub-settings allow strict security controls to be applied to high-risk populations without imposing them on the entire fleet
- Full audit trail of all browsing blocks, download decisions, approvals, and malware detections
- GDPR-compliant regional data hosting (EU, UK, US or Asia)

Deployment & Integration

- Requires Admin By Request agent for Windows, version 9.0 or later
- No additional on-premises infrastructure required
- Managed entirely from the Admin By Request portal
- Policy distributed to endpoints automatically via agent check-in - no manual push required
- Sub-settings scoped by Active Directory groups, Entra ID groups, and/or Organisational Units - no separate tenants needed for population-level policy differentiation
- Entra ID Connector required for MFA-protected downloads, Intune compliance gating, and Entra ID group-scoped sub-settings
- Email integration for approval notifications, outcome alerts, and ITSM/helpdesk routing
- Exportable rule lists (PDF, XLSX, CSV) for audit and compliance reporting
- Inspects HTTPS traffic locally on the endpoint using an agent-installed local root certificate (generated per device); no traffic is sent to an external proxy or cloud for inspection

A word on Compatibility

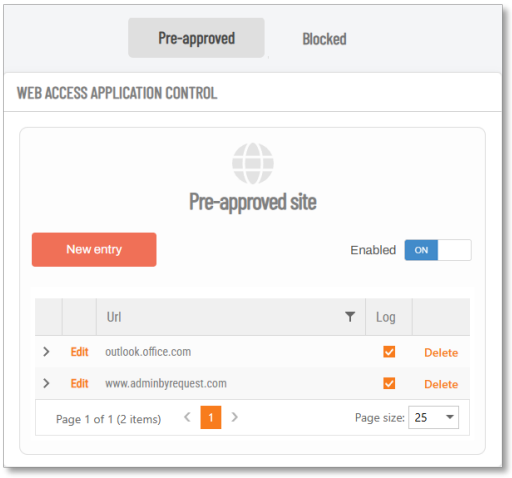
Software that also intercepts or re-signs TLS on the same device (e.g. enterprise secure web gateways such as Zscaler or Cato, next-generation firewall deep packet inspection such as Palo Alto, and some VPN clients or VPN browser extensions) can conflict with local inspection.

Ensure the Web Access Management local root certificate is trusted by that layer, or exclude affected sites via Web Access Management's bypass list. Certificate-pinned applications may bypass inspection by design. Test alongside existing TLS-inspecting tooling before a wide rollout.

Key Features

Browsing Controls

Web Access Management governs which websites endpoint users can reach and which browsers they can use to get there, with policy enforced on the device rather than at a network choke point.



Pre-approved Sites

Trusted destinations that bypass the browsing approval workflow, defined by root URL with optional subpath scoping. Pre-approval does not override explicit blocks: a site on both lists stays blocked.

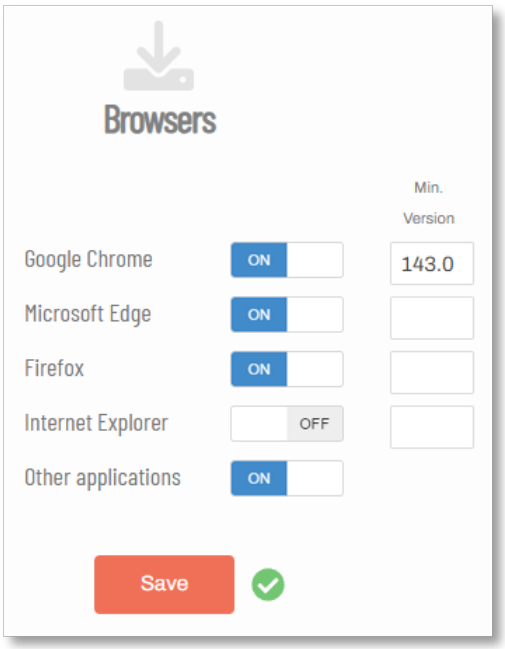
Blocked Sites Enforcement

Deny rules based on root URL, with optional subpath scoping, enforced on the endpoint and applied regardless of where the user is working. Each rule supports a custom blocking message and can be flagged for audit logging individually. Blocked rules take priority over pre-approved rules.

Browsing Permission Controls

Centralized control over which websites endpoint users can access. Browsing can be unrestricted (with explicit block rules applied), or locked down to a pre-approved site list only - suitable for non-interactive or high-security devices.

Users can be permitted to request temporary access to blocked sites, with approval granting a four-hour window. All blocked access attempts are written to the audit log.



Browser Lockdown

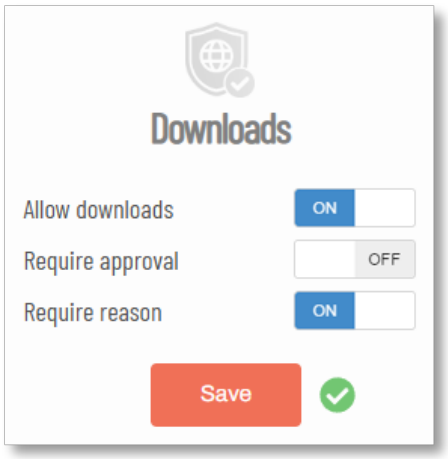
Define which browsers are permitted and the minimum acceptable version for each. Browsers outside the allowlist or below the minimum version are blocked at the endpoint.

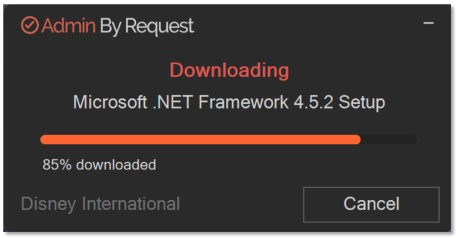
Covers Chrome, Edge, Firefox, Internet Explorer, and in-app (non-browser) controls.

Other applications are browsing capabilities that are embedded into desktop apps running in user space. An example is the "What's new" page in Visual Studio and its in-app updater. Turning this setting **OFF** should be considered only for critical or sensitive equipment.

Download Governance

Executable downloads are intercepted and held in a secure, user-inaccessible area on the endpoint until policy checks and security requirements are satisfied. Downloads can be blocked entirely, permitted freely, or routed through an approval workflow.





Pre-approved Downloads

Rule lists for pre-approving trusted software independently of the broader workflow settings. Rules support five types: source website, direct URL, SHA256 file checksum, vendor digital certificate, and vendor certificate combined with application name.

Pre-approved rules bypass the approval workflow while MFA, compliance checks, and malware scanning remain enforced.

Blocked Downloads

Hard-deny rules using the same five rule types, applied before any allow logic. Blocked rules take priority over every other download permission, including pre-approval. Each rule supports a custom blocking message and per-rule audit logging.

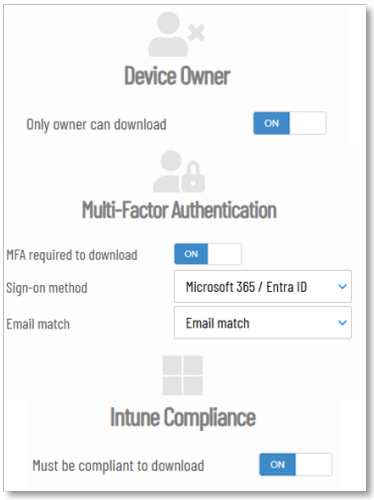
Download Permission Controls

Controls whether executable downloads are permitted, and what a user must do before one proceeds. Both settings can be enabled together.

- **Require approval** - every download held for admin sign-off via the portal
- **Require reason** - user must supply a written justification before the request is submitted

Owner-only Download Restriction

Restricts executable downloads to the recognized device owner, intended for shared-device environments where non-owners should not install software. Other users on the device can still browse normally; only downloads are restricted. Ownership is defined and managed in the endpoint inventory rather than in policy settings.



MFA-protected Downloads

Requires the user to re-authenticate via SSO before an executable download is released. Currently supported through Microsoft 365 and Entra ID, with extensibility for additional providers.

With email match enabled, the authenticated identity must match the email address associated with the endpoint user, or the download is blocked. Requires a connected Entra ID / Microsoft 365 tenant.

Intune Compliance Gating for Downloads

Blocks executable downloads on any device not marked as compliant in Microsoft Intune, even where downloads are otherwise permitted. Browsing is unaffected, so users on non-compliant devices retain web access while the higher-risk action stays blocked until the device is brought back into compliance. Requires the Entra ID Connector.

Intelligent Auto-Approval

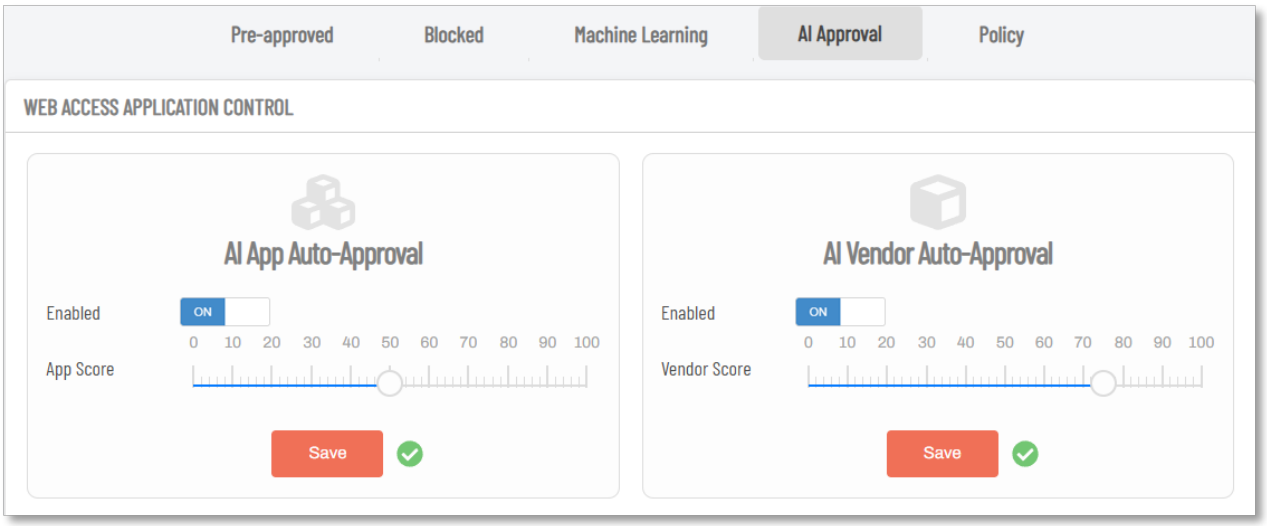
Structured rule lists for pre-approving trusted software and hard-denying disallowed software, independently of the broader workflow settings.

Both lists support five rule types: source website, direct URL, SHA256 file checksum, vendor digital certificate, and vendor certificate combined with application name.

Pre-approved rules bypass the approval workflow while MFA, compliance checks, and malware scanning remain enforced. Blocked rules take priority over all other allow mechanisms

Intelligent auto-approval reduces repetitive admin work without sacrificing control:

- **Machine Learning Auto-Approval** - automatically approves future requests for downloads that have already been manually approved a configurable number of times (threshold: 1–10 approvals)
- **AI App Auto-Approval** - scores downloads on a 0–100 App Score; requests meeting the configured threshold are auto-approved in real time
- **AI Vendor Auto-Approval** - scores software publishers on a 0–100 Vendor Score; all downloads from qualifying vendors are auto-approved



Malware Detection

Every executable that clears download controls is scanned by OPSWAT MetaDefender before execution:

- **Known files are checked** by real-time checksum lookup with no upload required
- **Unknown files are submitted** to MetaDefender's cloud infrastructure for multi-engine scanning
- **Cloud scanning covers files up to 250 MB**; larger unknown files fall through to local endpoint antivirus
- **Malicious files are quarantined** before execution. Detection events appear in the portal.

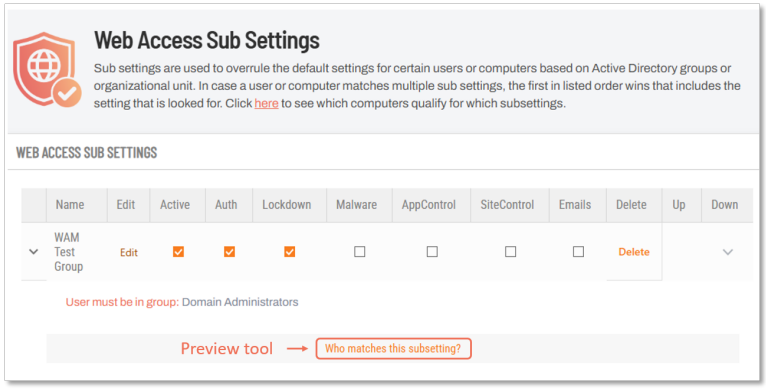
The OPSWAT MetaDefender scanning built into Web Access Management is a pre-release checksum and cloud scan, not behavioural EDR analysis or a continuous monitoring agent. EDR download-blocking features make threat-signal decisions (hash reputation, behaviour); Web Access Management makes policy decisions (user, device compliance, approval, reason). It's good practice to include both approaches when securing endpoints.

Policy and Audit

Sub-Settings (Policy Targeting)

A single Web Access Management tenant can apply different policies to different user and device populations simultaneously.

Sub-settings selectively override any combination of the six policy sections (Authorization, Lockdown, Malware, App Control, Site Control, Emails) for users in specified Active Directory or Entra ID groups and/or devices in specified Organisational Units.



Sections not overridden in a sub-setting fall through to Global Settings. Priority is first-match by listed order, adjustable by reordering groups in the portal. A built-in preview tool shows which sub-settings will be applicable to which devices.

Audit Logging and Notifications

The portal provides a complete audit trail across all Web Access Management enforcement decisions: browsing blocks, download approvals, denials, auto-approvals, rule-based blocks, and malware events.

Per-rule audit logging controls let administrators suppress noise from high-volume trusted traffic while retaining full visibility on unknown or suspicious activity.

Note that Web Access Management does not log ordinary allowed browsing; the browsing entries in the audit trail are blocked-site visits and visits to sites pre-approved with logging on. Every executable download decision is also recorded.

Configurable email templates cover all approval outcomes for both download and site access events. Templates can be overridden per sub-setting, so different populations receive differently worded notifications. A separate ticketing system channel routes Web Access Management events to an external ITSM or helpdesk tool in parallel.

Where Web Access Management fits

Web Access Management is a policy-and-authorization layer for browsing and downloads. It is not a replacement for EDR/XDR or for EPM; it answers a different question at a different point in the timeline.

Layer	Question it answers
Web Access Management	Should this site or download be allowed in the first place, by whom, from where, under what conditions?
EPM	If a downloaded executable runs, should it be allowed to run with elevated rights?
EDR / XDR (e.g. SentinelOne, CrowdStrike, Defender)	If something still executes and behaves suspiciously, detect and respond.

SIEM integration

The initial release of Web Access Management has no native SIEM connector. Web Access Management events route to external systems via the ITSM email channel under **Emails > Ticketing System**. Native SIEM integration is a roadmap item. EPM audit logs have API access today; Web Access Management audit logs are currently portal + ITSM email channel only.

Summary of Benefits by Stakeholder

IT Administrators: Central control over browsing and downloads across the Windows fleet, with no additional infrastructure to manage. Sub-settings allow a single portal to serve the full range of organizational populations - from locked-down kiosk devices to permissive developer environments.

Security Teams: Multi-engine malware scanning, hard-deny rules, browser version enforcement, and a complete audit trail of download and site-blocking decisions. Sub-settings allow high-risk teams (finance, legal, executives) to receive tighter controls without impacting the rest of the fleet.

Compliance Managers: Full download audit log, blocked and pre-approved site logging, MFA enforcement, Intune compliance gating, and GDPR-compliant data hosting.

Helpdesk / Operations: Approval requests appear in the portal and mobile app; ITSM integration via configurable email channel.

End Users: Clear request process for downloads and blocked sites; fast-track for trusted software via pre-approved rules. Policy is appropriate for their role - not one-size-fits-all.

Benefits of using Web Access Management

Reduce Web-Based Risk Without Disrupting Users

Feature	Benefit
Pre-approved sites and downloads	Trusted destinations and software flow without friction
Approval workflow with justification	Accountability for every non-pre-approved download
Browser lockdown	Outdated or unapproved browsers blocked before they become an attack surface
OPSWAT MetaDefender scanning	Malicious files caught before execution, not after

Control Without Infrastructure

Feature	Benefit
Endpoint-enforced policy	No proxy, DNS filter, or firewall changes required
Cloud-managed portal	Centralized configuration with no on-premises servers
Agent-based deployment	Policy follows the device, on-network or off
Automatic policy distribution	Changes reach endpoints without manual intervention
Sub-settings	One tenant, multiple simultaneous policies - no parallel deployments needed

Meet Compliance and Audit Requirements

Feature	Benefit
Full audit trail	Every browsing block and download decision recorded with user identity and outcome
MFA enforcement at download	Mandatory identity verification at the point of risk
Intune compliance gating	Software access tied to device health posture
Exportable rule lists	Pre-approved and blocked rules exportable to PDF, XLSX, or CSV
GDPR-compliant hosting	Choose EU, UK, US or Asia data residency

Intelligent Automation

Feature	Benefit
ML auto-approval	Repeat approvals eliminated for known-safe applications
AI App and Vendor scoring	Low-risk downloads auto-approved without admin involvement
Per-rule audit toggle	Reduce log noise without losing visibility on unknown traffic