# Release Notes

Admin By Request
ZERO TRUST PLATFORM

## Release Information

Product Platform: **Windows**
Product Version: **9.0**
Date: **3 August 2026**

# Windows 9.0

## Introduction

Admin By Request for Windows 9.0 introduces **Web Access Management**, an endpoint-based policy layer that gives IT teams centralized control over how users browse the web and download software:

- browser lockdown, blocked sites, pre-approved sites, and browsing permissions enforced on the endpoint
- executable download controls, including owner-only downloads, MFA-protected downloads, Intune compliance gating, and malware detection with OPSWAT MetaDefender

**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.

Also in this release:

- *Extend Active Session Timer*, allowing a user to add time to an Admin Session already in progress
- remote termination of an elevated session from the portal by a portal administrator.

Admin By Request for Windows 9.0 provides improved stability and customer-requested fixes and reflects our ongoing commitment to streamlining privilege management while addressing both user experience and enterprise control.

Refer to Web Access Management for more information on Web Access Management.

Refer to the Admin By Request Documentation Center for full details on any other aspect of Admin By Request.

# In this document



# Prerequisites

Organizations wishing to evaluate endpoints running Admin By Request for Windows 9.0 need the following:

- One or more devices running Microsoft **Windows 10** or higher.
- Credentials to access the Admin By Request portal at **https://adminbyrequest.com/login**.
- Admin By Request for **Windows 9.0** client software (Windows Endpoints), downloaded from the portal and available to each device.

Web Access Management requires the Windows 9.0 client or later. It is activated from the portal on the agent you already deploy, so there is no separate client software to install.

# Web Access Management

**Web Access Management** (WAM) is a policy layer for controlling how users browse the web and download software. It gives IT teams a way to enforce browser restrictions, block or allow sites, govern executable downloads, require stronger authentication or device compliance for risky actions, and scan for malware before software is allowed through.

The aim is to reduce web-based risk without forcing administrators to manage every decision manually: trusted sites and downloads can be pre-approved, while high-risk activity is blocked, audited, or sent through an approval workflow.

Browsing controls in this release:

- **Browser lockdown.** Define which browsers are allowed and what minimum versions are acceptable, so outdated or unapproved browsers can be blocked before they create risk.
- **Blocked sites enforcement.** Prevent access to known unwanted or non-compliant websites by enforcing blocked root URLs and path-based rules directly on the endpoint.
- **Browsing permission controls.** Apply browsing policies consistently on the endpoint, so site access follows centrally managed rules rather than relying on portal settings alone.
- **Pre-approved sites.** Allow trusted websites to bypass browsing approval when they match centrally defined rules, reducing friction for common business destinations. Explicit blocks continue to take priority.

Download controls in this release:

- **Download permission controls.** Govern executable downloads so they can be blocked, approved, or justified before they are written to disk, keeping risky software from reaching the device unchecked.
- **Owner-only download restriction.** Restrict executable downloads to the recognized device owner, which is particularly useful on shared devices where non-owners should not introduce software.
- **MFA-protected downloads.** Require the user to complete MFA before an executable download is allowed, adding a second layer of verification at the point of risk.
- **Intune compliance gating.** Block executable downloads on devices that are not compliant in Intune, aligning software access with device health and management posture.
- **Pre-approved downloads.** Let trusted downloads bypass approval workflows when they match configured allow rules, so known-safe software moves faster without weakening MFA, compliance checks, or malware scanning.
- **Blocked downloads.** Apply hard-deny rules to executable downloads based on URL, checksum, vendor certificate, or similar identifiers, so disallowed software is stopped even where another rule might otherwise allow it.
- **Malware detection with OPSWAT MetaDefender.** Add file reputation and cloud-based scanning, so malicious or suspicious files can be blocked or quarantined before they run with elevated privileges.

**Audit logging and traceability.** WAM builds an audit trail around browsing, download decisions, approvals, bypasses, and blocks, so administrators can review what happened and why.

Refer to Getting Started with Web Access Management for more information.

## Extend Active Session Timer

A non-admin end user can now extend an **already active** Admin Session, without waiting for it to expire and without completing MFA again. This reduces disruption when legitimate elevated work takes longer than the original session duration.

- Adds more time to the current session instead of requiring re-authentication.
- Controlled by policy, using the *Allow session extension* setting under **Windows Settings > Lockdown > Admin Session**.
- Supports limits on how many times a session may be extended, and by how much.
- Logs the extension for auditing and reporting.

In practice this helps users finish longer administrative tasks without interruption, reduces repeated MFA prompts during ongoing work, and gives a better balance between security control and usability.

## Remotely terminate elevated sessions

An authorized portal user can now terminate an ongoing Admin Session remotely from the portal. This is intended for situations where elevated rights should be removed immediately, either because the work is complete or because IT needs to end the session for security or operational reasons.

- Applied immediately when the portal user chooses to end the session.
- Optional **Blackout period**, preventing the user from re-elevating.

- Reuses the existing end-of-session logic on the endpoint, including force-closing elevated applications and processes.
- Can be limited to specific portal roles or permissions.
- Records a full audit trail, including who ended the session.

## Bug fixes and stability improvements

Several bugs and stability improvements have been implemented in this release. Many of these address specific customer reports and have been communicated directly to the customers affected. The broader Admin By Request community will also benefit from general improvements across the Windows product range.

## How does the Update Process work?

Admin By Request software updates are deployed using our Auto-Update process. However, when we release a new version we do not deploy it right away to all customers via auto-update. This is simply to mitigate any unforeseen issues.

Our rule-of-thumb for a new release is to activate auto-update within **4 - 8 weeks** of release, but this is subject to change, depending on feedback and any potential issues that might arise.

Contact us if you wish to receive the latest version right now. You can also raise a support ticket requesting the latest update.

Visit the Download Archive for previous versions of Admin By Request.