Technical Note

Admin By Request
ZERO TRUST PLATFORM

Product Platform: **All platforms**
Product Version: **All versions**
Document Date: **8 May 2026**
Document Version: **1.1**
Classification: **Public**

Integrations: An Overview

Introduction

Admin By Request's Zero Trust Platform is built to fit into your existing infrastructure, not the other way around. Our solutions connect with the identity providers, endpoint management tools, SIEM platforms, ticketing systems, and communication apps your teams already use, so security workflows stay connected across your entire stack.

This document provides a summary of every available integration, organized by category. For full setup instructions, each section links to the relevant documentation page.

In this document

New integrations

We're continuously adding new integrations. If something your organization relies on isn't listed here, let us know and we'll see what we can do.

This technical note is available online:

Integrations: An Overview

Notifications

Microsoft Teams

Documentation: Microsoft Teams Integration Overview

The Microsoft Teams integration adds a custom Admin By Request app to a dedicated Teams channel, allowing IT admins to approve or deny elevation requests directly from Teams without needing to open the portal or mobile app. Real-time notifications are pushed to the channel the moment a user submits a request.

One thing worth noting: access granted through the Teams integration overrides portal sub-settings. Anyone with access to the configured channel can approve or deny requests, so it's important to keep that channel restricted to authorized personnel only.

Slack

Documentation: Slack Integration

The Slack integration brings Admin By Request EPM's Requests feature into your existing Slack workspace. When a user submits a request for elevated access, the request details and the user's stated reason are pushed directly to a dedicated Slack channel, where IT admins can approve or deny without opening the portal or mobile app. The integration uses your Admin By Request API key to connect to a custom Slack app, and setup is self-service via a downloadable configuration guide.

The same caveat as Teams applies: channel-level access overrides portal sub-settings, so only authorized users should be added to the dedicated channel.

Mobile Application

Documentation: Mobile Application

The Admin By Request mobile app is a free companion to the web portal, available for iOS and Android. It gives IT admins on-the-go access to the auditlog, pending requests, and approval workflows. The moment a user submits an elevation request, a real-time push notification is sent to the admin's phone, and approvals can be granted or denied in seconds directly from the notification itself. Apple Watch is also supported for push notifications.

The app is free and available in both the Apple App Store and Google Play.

SIEM Tools

Microsoft Sentinel

Documentation: Microsoft Sentinel Integration Overview

For organizations using Microsoft Sentinel as their SIEM, this integration forwards Admin By Request Auditlog and Events data to a Sentinel Log Analytics Workspace in real time. It uses Azure Logic Apps to consume the Admin By Request public REST API and pipe data through. Admin By Request provides pre-built Logic App JSON templates to get you up and running quickly with minimal configuration required. Once the data is in Sentinel, it's available for threat detection, investigation, and automated response workflows.

Splunk

Documentation: Splunk Integration

The Splunk integration routes Admin By Request Auditlog data to your Splunk environment in real time using a combination of Splunk's HTTP Event Collector (HEC) and Admin By Request webhooks. Once configured, events like privilege elevation requests and software installs are pushed to a Splunk HEC endpoint as they happen, rather than requiring you to pull data on a schedule. Setup involves three steps: creating a Splunk HEC channel with an authorization token, configuring a webhook in the Admin By Request portal pointed at that endpoint, and then verifying events are coming through. A self-service setup guide is available for download on the documentation page.

Power BI

Documentation: Power BI Integration

For organizations that use data visualization as part of their security or business strategy, Admin By Request offers a plug-and-play Power BI template that pulls your portal data into Microsoft's BI platform. The template covers seven pages: a general Dashboard, Inventory, Approvals, Malware, Load (when users are most active), Settings, and Events (new in version 2.0). Each page surfaces a different slice of your privilege management data through interactive charts, graphs, and tables that can be filtered by date, request type, user, and sub-settings.

All data can also be configured to generate scheduled reports that are automatically emailed to relevant users from within Power BI. The template is available as both a downloadable file and a template app.

Webhooks

Documentation: Webhooks

Webhooks are the push-based alternative to the pull-based public API. Rather than polling the API on an interval, you subscribe to specific events and Admin By Request sends the data to a public web server endpoint of your choice in real time as those events occur. The data structure is identical to what the API returns, so if you're already familiar with the API, the transition is minimal.

Webhooks are configured in the portal under Settings \> Tenant Settings \> Data \> Webhooks. Common use cases include routing events into tools like Splunk, or triggering notifications in Teams or Slack via a pointed webhook URL. Note that webhooks are push-only: you'll still need the API if you want to approve or deny requests programmatically.

Public API

Documentation: Public API Overview

Admin By Request offers a free REST API included with all plans, covering five separate endpoints: Auditlog, Requests, Inventory, Events, and PIN Code. The API returns data in JSON format and mirrors the structure of what you see in the portal, making it straightforward to pipe into a SIEM, a custom backend, or a ticketing system of your choice.

Authentication is handled either via an apikey header or standard basic authentication. A daily quota of 100,000 API calls applies per tenant, with automatic blocking until the next business day if exceeded. The API also supports approving and denying elevation requests programmatically, which is useful for building custom approval workflows in external systems. For organizations not using a pre-built integration like ServiceNow or Jira, the API is the flexible alternative for building out exactly what you need.

Other Portal Access

Azure AD SSO

Documentation: Single Sign-On (general information), Entra ID Connector (specific details)

Azure AD SSO (via Microsoft 365 / Entra ID) lets portal users authenticate using their existing Microsoft 365 credentials. No extra configuration is needed beyond selecting it as the sign-on method when adding a portal user. Users need to be permitted to consent to apps in your Entra ID Admin Center for the initial login. After that, the option can be disabled without affecting future sessions.

ADFS

Documentation: ADFS Single Sign-On

Active Directory Federation Services (ADFS) lets your on-premises AD users log into the Admin By Request portal using their standard Windows credentials via SAML authentication. Once configured, portal users don't need a separate password, and if your ADFS setup supports IdP-initiated login, they won't even need to know their username. Setup involves creating a Relying Party Trust on your ADFS server and uploading the federation metadata to the portal. MFA can be enforced at the ADFS level as part of the same flow.

Okta SSO

Documentation: Okta Single Sign-On

Okta SSO lets portal users authenticate using their existing Okta credentials via SAML, connecting your in-house Active Directory to the Admin By Request portal without requiring a separate password. Setup involves creating an Admin By Request application directly from the Okta App Catalog, which makes configuration fairly straightforward. Once configured, you assign users to the application on the Okta side, download the IdP metadata, paste it into the portal, and then update each portal user's sign-on method to Okta SSO.

Note that if you're planning to use SCIM with Okta, SSO needs to be configured first before provisioning can be set up.

SAML

Documentation: Generic SAML Single Sign-On

For identity providers not covered by the dedicated Microsoft 365, ADFS, or Okta integrations, Admin By Request supports generic SAML 2.0 SSO. This covers a wide range of providers including DUO, F5, NetScaler, OneLogin, Idaptive, and RSA, among others. Setup follows the same general flow as other SSO options: create a SAML entry in the portal, configure your IdP using the provided service provider metadata (or manually with the Consumer URI and Entity ID), download the federation metadata XML, and upload it to the portal.

SCIM

Documentation: SCIM Overview | SCIM (Entra ID / Azure AD) | SCIM (Okta)

SCIM (System for Cross-Domain Identity Management) automates the provisioning and deprovisioning of portal users by syncing directly from your identity provider. Rather than manually creating and managing portal user accounts, you handle it all from your IdP (Entra ID or Okta), with changes automatically pushed to Admin By Request when the provisioning cycle runs. Supported operations include Create, Update, and Delete for both users and groups.

Portal user roles and permissions are assigned based on IdP group membership, so you can manage access centrally without touching the Admin By Request portal directly. SCIM-provisioned users authenticate via Microsoft 365 (for Entra ID) or Okta, and this authentication method is set during SCIM setup and cannot be changed afterward. Full setup guides are available as downloadable PDFs for both Entra ID and Okta.

Endpoints

Active Directory

Documentation: Active Directory Integration

On domain-joined machines, Admin By Request EPM works directly with Active Directory to manage local admin rights. Upon installation, the Domain Users group is removed from the local administrators group immediately. From that point on, admin rights are only retained by accounts that meet specific configured conditions, such as being on an exclusion list or belonging to a privileged domain group like Domain Admins.

Sub-settings (policy overrides for specific user groups or OUs) are supported natively using AD groups, so you can apply different elevation rules to different teams without extra legwork. The solution also functions offline, caching group and OU data locally and syncing back to the portal when connectivity is restored.

Entra ID Connector

Documentation: Entra ID Connector

For organizations using Azure AD-joined or Entra ID-managed devices rather than traditional on-premises AD, the Entra ID Connector allows Admin By Request to query your Azure Active Directory for user and device group memberships. This is what makes sub-settings work correctly in cloud-only and hybrid environments. Without it, the platform can't differentiate privilege policies between different user groups.

Setup requires an Azure App Registration with Directory.Read.All permissions. Once connected, the portal also pulls inventory data including full names, phone numbers, and group memberships from Entra ID, and correctly identifies Global and Device Administrators so their tray icon reflects their admin status.

Intune

Documentation: Working with Intune

Microsoft Intune is supported for deploying and managing the Admin By Request client across Windows and macOS endpoints. For Windows, the MSI installer is packaged into the .intunewin format using Microsoft's Win32 Content Prep Tool, then deployed silently to device groups through the Intune Admin Center with no end-user interaction required. For macOS, a configuration profile is created in Intune to grant the necessary permissions.

Beyond deployment, Intune compliance status can also be used as a condition within Admin By Request. Devices that fall out of Intune compliance can be blocked from using privilege elevation entirely.

MetaDefender

Documentation: OPSWAT MetaDefender

Admin By Request's malware detection capability is powered by OPSWAT's MetaDefender Cloud Service. Whenever a user requests to elevate a file, its SHA-256 checksum is submitted to MetaDefender and checked against a database of over 40 billion entries using 30+ anti-malware engines, including Bitdefender, CrowdStrike, ESET, McAfee, Microsoft Defender, Sophos, and more. The lookup takes less than a tenth of a second, so there's no noticeable delay for the user.

If a file's checksum isn't in the database (roughly 25% of cases), there's an option to upload the file itself for a real-time cloud scan, which typically completes in under 10 seconds. Flagged files can be automatically blocked or placed in quarantine for review, depending on your portal settings. This integration is built into the Admin By Request agent and requires no additional software.

Ticketing Systems

Generic Ticketing System

Documentation: Generic Ticketing System

This integration allows the Admin By Request portal to push notifications into virtually any ticketing system that accepts inbound email, including Zendesk and others. When configured, elevation requests and completed sessions trigger emails to your ticketing system's inbound address, automatically creating tickets with all relevant detail.

The email template is fully customizable using dynamic tags (user name, reason, applications run, etc.), and lines with empty tag values are automatically removed, so you don't need separate templates for different event types. You can also subscribe to specific events (such as requests submitted, approved, denied, or completed) to control the volume of tickets generated.

Jira

Documentation: Jira Integration Overview

The Jira integration connects Admin By Request EPM with Jira Service Management (cloud), allowing elevation requests to flow directly into Jira as issues. IT admins can optionally approve or deny requests from within Jira itself, and Jira automation rules can be configured to further streamline how tickets are handled and updated throughout the request lifecycle.

Setup requires API tokens from both platforms. Note that this integration is supported for Jira Cloud only. On-premise Jira Data Center is not currently supported.

ServiceNow

Documentation: ServiceNow Integration Overview

Admin By Request has a custom-built ServiceNow application that lets IT teams manage elevation requests and review audit activity directly within ServiceNow, without logging into the Admin By Request portal. The app is installed from the ServiceNow store and authorized using an Admin By Request API key. Once connected, elevation requests flow into ServiceNow and can be approved or denied from there, with configurable flows to control how tickets are handled throughout the lifecycle.

The integration supports ServiceNow up to and including the Yokohama release (Q2 2025). Note that this is a first-time install guide only; upgrading from a previous version requires a few additional manual steps around flow cleanup.

Admin By Request Portal

ChatGPT

Documentation: ChatGPT in the Portal

The ChatGPT integration gives IT admins a quick way to look up information about any file a user has requested to run with elevated privileges. When a Run As Admin request comes in, an AI Assistance button appears alongside it in the portal, allowing admins to get a plain-language description of the file or executable in question before deciding whether to approve or deny. The same capability is available from the Auditlog, where admins can click "Ask ChatGPT what this is" on any Run As Admin entry regardless of its current state.

Note that this feature is available for Run As Admin requests only, not Admin Session requests, and can be disabled by contacting your Account Executive. No data is sent to ChatGPT beyond the filename and vendor. All queries go server-to-server, so OpenAI has no visibility into who is making the request.

VirusTotal

Documentation: VirusTotal

In addition to OPSWAT MetaDefender, Admin By Request submits files to VirusTotal for scanning and analysis. This happens from within the Admin By Request portal, where IT admins can select a file from the auditlog for further checks. VirusTotal applies these checks via more than **70** antivirus scanners and URL/domain blocklisting services, as well as using a number of tools to extract information from the submitted content.

VirusTotal not only advises whether or not a given antivirus solution detected a submitted file as malicious, but also displays each engine's detection label (e.g., I-Worm.Allaple.gen). It does the same for URL scanners, most of which will discriminate between malware sites, phishing sites, suspicious sites, etc. Because the results of analysis are immediately available to the submitter, IT admins can take appropriate action without leaving the portal, including ignoring (for false positives), quarantining or adding to the allow list.