Spec Sheet

Admin By Request
ZERO TRUST PLATFORM

Secure Remote Access

Product Platform: **Secure Remote Access**
Product Version: **Jun-25**
Document Date: **23 June 2025**

Introducing Secure Remote Access

Admin By Request *Secure Remote Access (SRA)* is a Zero Trust, browser-based remote access solution designed for modern enterprise environments. With no persistent VPN tunnels or agents required, SRA allows secure just-in-time access to internal resources for IT staff, remote workers, and external vendors.

The solution includes three distinct components: *Unattended Access*, *Vendor Access*, and *Remote Support*, each purpose-built for specific access use cases. All access sessions are logged, auditable, and governed by customizable scopes and approval workflows through a centralized management portal.

What is it?

Secure Remote Access is a solution that enables organizations to grant just-in-time, zero-trust remote access to internal systems without requiring a persistent VPN connection or exposing endpoints directly to the internet. It is designed to securely manage remote administrative sessions, especially for IT staff, vendors, and contractors.

It comprises the following components:

- **Unattended Access** – protocol-level access to endpoints via RDP, SSH, and VNC without end-user interaction.
- **Vendor Access** – browser-based remote access for external vendors via access.work with scope-limited permissions.
- **Remote Support** – live, user-assisted screen-sharing for helpdesk and support personnel using secure WebSocket sessions

Just like Admin By Request's EPM product line, Secure Remote Access requires no additional on-premises infrastructure (servers, VM appliances, databases etc.); all that is required to start a full proof of concept is to sign up to our Free Plan, giving you full remote access to a maximum of **25 endpoints, free, forever** [1].

Product Editions

Subscription	Max. Endpoints	License Model	Endpoint OS	Support
Free Plan (SRA)	25 (10 Remote Support)	Free	Windows or Linux[2]	None
Paid Plan (SRA)	Unlimited	Annual Subscription	Windows or Linux[2]	Included

1. Under the Free Plan, access using the Remote Support component is limited to **10 endpoints**.
2. Remote access for Mac clients is due **Q3 2025**.

Security by Design

Architecture Compliance

- Just-in-time, browser-based access with no standing permissions
- No permanent agents or VPN tunnels
- Session brokering via secure Cloudflare tunnels or self-hosted reverse proxies
- Self-hosted, on-premise gateway option, using Docker-based architecture
- Data transmitted via encrypted channels and fully logged
- Full audit trail support and optional video session recording
- Zero trust access with confirmation, credentials or MFA
- GDPR-compliant regional data hosting (EU, UK or US)
- Customizable approval flows and user scopes
- Session expiry, inactivity timeouts, view-only modes, passwordless login options
- Portal access control for session monitoring and configuration

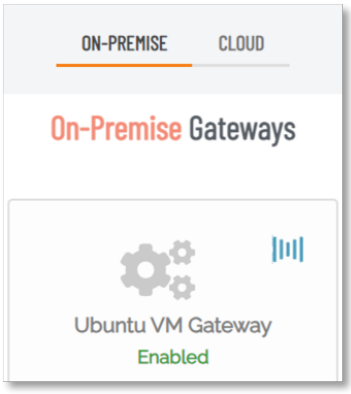
Deployment & Integration

- Easy deployment with Docker Compose for self-hosted gateways
- No additional infrastructure required when using cloud-hosted gateway
- Integrates with Admin By Request agent and portal
- Supports both managed and self-hosted access gateways
- SSO integration with Azure AD, SAML, and Office365
- Flexible user scoping and session approval workflows

Targeted Access Modes

- *Unattended Access* for admin-initiated sessions to enrolled or discovered endpoints
- *Vendor Access* for scoped, temporary access by third-party users
- *Remote Support* for live, real-time sessions initiated by end-users or admins
- Protocol support: RDP, SSH, VNC for WebSocket-based screen sharing
- Device discovery of unmanaged endpoints on internal networks (requires on-prem gateway)

Key Features

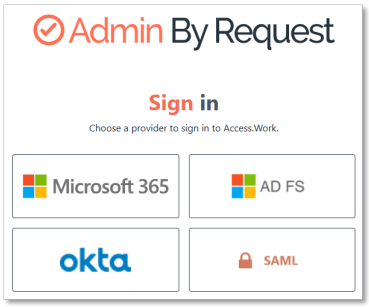


Browser Access via Cloud or On-Premise Gateway

Unattended Access provides internal administrators with secure, browser-only remote access, without needing a user to be present at the endpoint.

The solution can be deployed using either a cloud-hosted or on-premise Docker gateway, eliminating the need for VPN and jump servers, while still maintaining a secure and segregated setup. The solution also supports advanced access scenarios such as reverse proxy routing and non-agent device discovery.

Protocols supported: RDP (Windows), SSH (Linux/Mac) and VNC.



Grant External Parties Internal Access

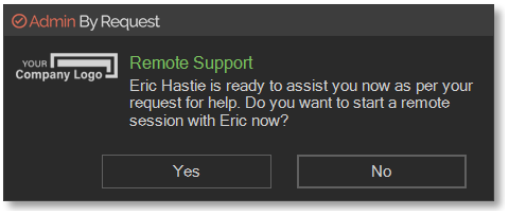
The *Vendor Access* component of Secure Remote Access allows *external* users, such as third-party vendors, to be given secure access to internal devices. This access is managed entirely through their local Internet browser app - there is no need for any additional locally installed software.

Like Unattended Access, the browser creates a secure WebSocket connection to a Docker-based gateway, hosted either in your own infrastructure (self-hosted) or as a managed service (cloud-hosted). Either way, the connection is made via a secure Cloudflare tunnel.

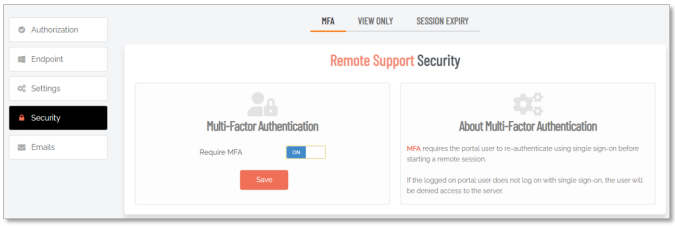
External / third party users login to https://access.work via SSO and connect to internal devices through their browsers without needing access to the Admin By Request portal. Just like internal users, privileged access is controlled according to portal settings and all activity is logged.

Users ask for Help, Admins offer it

Remote Support allows users and/or admins to share screens and remotely control devices recorded in the Admin By Request inventory, while using all of the well-known features of the Admin By Request ecosystem, such as: inventory, auditlog, settings and sub-settings, approval flows etc.



Remote Support allows either end users or IT admins to initiate a secure, just-in-time, remote support session - allowing them to share and control the end-user's device. Once the session is done, everything is dismantled, eliminating any access points for bad actors.



Require MFA

Enabling the "Require MFA" setting requires the portal user to re-authenticate using Multi-Factor Authentication before being able to start any Remote Support session (both end-user and portal-user initiated).

With MFA enabled, portal users are met with the Microsoft account login screen, which is a required step before being able to proceed to initiating the Remote Support session with the endpoint. Using MFA requires users to be logged-in under SSO.

Session Expiry

To prevent sessions from being "forgotten" and therefore running forever, *Session Expiry* can be used, which automatically disconnects after the selected amount of time has expired. Connected users receive a countdown warning when the remaining time gets below 2 minutes.

Optional Session Recording

A full recording of each remote access session can be enabled or disabled from portal settings. Enabling session recordings creates a screen recording of all Remote Support sessions done under the setting scope. Once complete, recordings can be requested directly from the auditlog.

Benefits of using Secure Remote Access

Zero Trust Security Model

Feature	Benefit
No standing access	All sessions are just-in-time and explicitly approved
No VPN or persistent agents	Reduces attack surface by removing always-on connections
Outbound-only communication	Ensures that endpoints do not need to accept incoming traffic, complying with best-practice firewall rules
Cloudflare Tunnel integration	Secure, scalable tunneling via QUIC protocol (UDP port 7844)

Complete Session Visibility and Auditability

Feature	Benefit
Full audit logging	Every session is logged with user identity, start/end times, and protocol used
Optional video recording	Ideal for compliance, forensic review, or internal policy enforcement
Session metadata	Includes contextual data such as user role, target machine, approval trail, and activity duration

No Infrastructure Burden (unless desired)

Feature	Benefit
Cloud-hosted gateway	Requires no on-premises setup. Ideal for fast rollout
Optional on-premises deployment	For organizations that prefer to host their own gateway components via Docker (Connector, Proxy, Discovery)
No browser plugins or local installs	Vendors and support staff access via web browser only

Designed for Enterprise Environments

Feature	Benefit
SSO support	Integration with Azure AD, SAML, and Office365
Zero trust, just-in-time access	Permissions granted only as required, with approval workflow
Session expiry and inactivity timeout	Automatically terminates unused or overlong sessions
Custom user prompts and workflows	Flexible pre-session approval mechanisms

Minimal User Friction

Feature	Benefit
Browser-based experience	Works on Chrome, Edge, and Firefox without installing agents
Passwordless options	Enables modern authentication without credential fatigue
End-user control	For Remote Support, users can approve or reject sessions, enhancing trust

Flexible Network Support

Feature	Benefit
Supports agent-based and agentless access	Managed and unmanaged devices alike
Discovery container (with on-prem gateway)	Optionally scan internal networks to locate unmanaged endpoints
Multi-gateway support	Distribute load or segregate access by department or region

Compliance Ready

Feature	Benefit
GDPR-compliant	Choose EU, UK or US data residency
Audit-ready logging and recording	Supports requirements from ISO 27001, NIST, Cyber Essentials Plus, and more
MFA enforcement	Adds a mandatory verification layer to privileged access actions

Summary of Benefits by Stakeholder

IT Administrators: Fast, secure access to endpoints without needing VPN or firewall changes

Vendors / Contractors: No local install needed; access only what is scoped and approved

Helpdesk / Support Teams: Initiate live support sessions without needing complex tooling

Security Officers: Full audit trail and session control, aligned with Zero Trust policies

Compliance Managers: Supports video capture, GDPR hosting, MFA, session control