Admin By Request

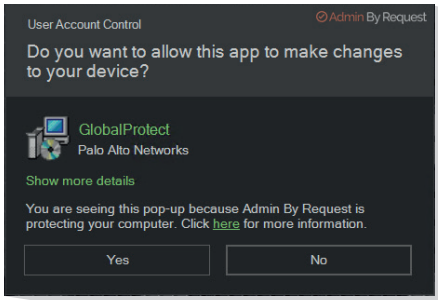
Empower Your Cyber Resilience with Admin by Request

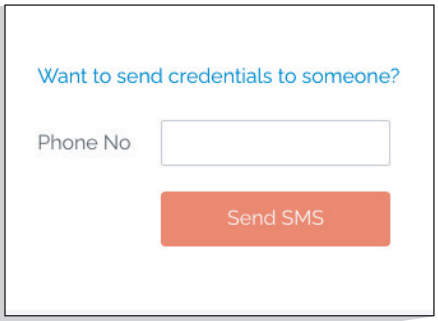
Seamless Compliance & Enhanced Security for the Financial Sector

Seven key Admin by Request features that are particularly relevant and beneficial for organizations looking to comply with DORA regulations:

1. App Elevation:

Ensures that users can perform necessary tasks without having unnecessary administrative rights, which aligns with DORA's emphasis on limiting access rights to reduce cybersecurity risks.
Admin by Request's app elevation feature allows specific applications to run with administrative privileges without granting the user full administrative rights, reducing the risk of malware propagation and data breaches.



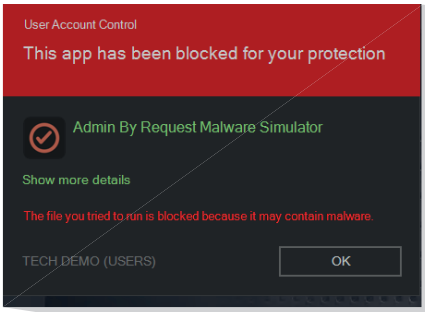


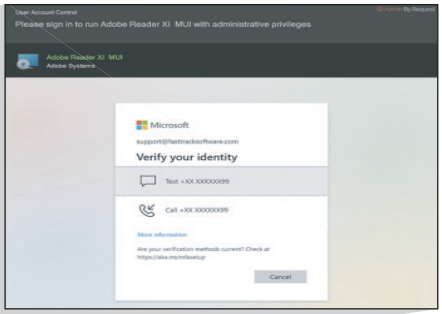
2. Break Glass / LAPS (Local Administrator Password Solution):

Temporary account provisioning supports DORA's requirements for secure and controlled access, enhancing operational resilience by providing emergency access that is auditable and time-bound.
This feature allows for the creation of temporary local admin accounts with a time-limited scope, ensuring that elevated access can be granted in a controlled manner, crucial for maintaining security during urgent situations.

3. Malware Detection:

Directly supports DORA's requirements for robust ICT risk management by detecting and preventing malware threats.
Utilizing over 35 different scanning engines, Admin by Request offers comprehensive malware detection capabilities, significantly reducing the risk of malware infections and enhancing the organization's cyber defence posture.





4. Endpoint MFA/SSO:

Aligns with DORA's focus on secure authentication mechanisms to protect against unauthorized access and enhance digital operational resilience.
By enforcing Multi-Factor Authentication (MFA) and Single Sign-On (SSO) prior to elevating privileges, Admin by Request ensures that only authenticated users can gain elevated access, thereby securing sensitive operations and data.

5. AI Approval & Machine Learning:

Innovative use of AI and machine learning for access management aligns with DORA's encouragement of advanced technological solutions to enhance cybersecurity and AI-driven auto-approval of elevation requests streamlines the process while ensuring security, and the use of machine learning to adapt approval processes over time improves efficiency without compromising security.

Admin By Request

6. GDPR Compliance:

While GDPR is focused on data protection, demonstrating compliance with it shows a commitment to stringent security measures, aligning with DORA's broader goals of ensuring the security and resilience of financial operations.
Admin by Request's adherence to GDPR compliance ensures that all sensitive data handled during the elevation processes is protected, reinforcing the overall cybersecurity framework.

7. Multi-Platform Support & Integrations:

DORA advocates for a comprehensive approach to digital operational resilience, which includes ensuring compatibility and integration across various platforms and tools used within the financial sector.
Supporting multiple platforms (Windows, macOS, Linux) ensures that Admin by Request can be implemented across diverse IT environments. Additionally, integration capabilities with tools like Teams, Slack, Splunk, and more, ensure that Admin by Request can seamlessly fit into and enhance the existing digital ecosystem of a financial institution, promoting resilience and compliance.

Admin By Request Platform Certifications

Being a Software As A Service (SaaS) platform, Admin By Request has two main components, the endpoint agent and the portal. Although endpoints can use Admin By Request to perform application elevations offline, the portal is still required for initial agent registration, centralised logging and settings configuration and deployment.

Customers can configure the type of data they wish to send to the portal, and the duration of which is it stored (3 months to 5 years).

Being a Danish company, Admin By Requests EU datacentre is based between two region locked sites in the Netherlands and the Republic Of Ireland.

ISO/IEC 27001: Information Security Management

This international standard demonstrates that the company adheres to best practices in information security management, ensuring the confidentiality, integrity, and availability of data. It's a hallmark of security excellence that resonates well with DORA's emphasis on cybersecurity and resilience.

SOC 2 (Service Organization Control 2)

SOC 2 certification assures that a service provider securely manages data to protect the interests of the organization and the privacy of its clients. This U.S.-based certification is widely recognized and emphasizes on security, availability, processing integrity, confidentiality, and privacy of a system.

Cyber Essentials (UK)

This UK-based certification demonstrates a company's adherence to fundamental cybersecurity practices, protecting against common cyber threats. It's particularly appealing to UK-based or UK-operating entities concerned with DORA's cybersecurity implications.

GDPR Compliance

Although there's no official "certification" for GDPR compliance, demonstrating adherence to GDPR principles through third-party assessments or certifications related to data protection (like ISO/IEC 27701) can be highly beneficial. It reassures partners and clients of the company's commitment to data privacy and protection, aligning with DORA's focus on secure and resilient digital operations.

Full & detailed compliance information can be found in our Trust Centre, located at www.adminbyrequest.com/en/trustcenter