

G-Cloud 15

Unified Identity Management Service for Privileged Access Management (PAM)



Atos

Table of contents

1. What is Unified Identity Access Management Service for Privileged Access Management	3
2. What does it deliver?	5
3. What technology does it use.....	9
4. What terms apply?	11
5. Termination.....	12
6. How do I order?	13
7. Glossary.....	14
8. Why Atos.....	15



1. What is Unified Identity Access Management Service for Privileged Access Management

Atos' Unified Identity Management Service for Privilege Access offers a comprehensive solution and service to manage the onboarding and offboarding of public sector organisation operational or service provider personnel who require system administration (super user) access privileges to manage all organisation SaaS, Cloud and on-premises services and applications.

It is vital for highly trusted public sector organisations to demonstrate that their system administration (or super user) access privileges to their core infrastructure are under strict management processes and can provide a full access audit trail on demand. This is a fundamental element of infrastructure security known as "Privilege Access Management" (PAM).

Many popular PAM solutions offer password vault facilities that lock the system administrator account and passwords in an encrypted repository. System administration or superuser access privileges can only be requested via the PAM solution for legitimate reasons, whether humans or machines made the request.

Each privilege access is fully assessed and authenticated; just enough privilege access is granted in a just-in-time fashion with a specific time limit. The usage of the privileged access is fully monitored and recorded to create a complete audit trail.

With our Unified Identity Service for Privilege Access, we offer a complete end-to-end, automated solution and service to onboard and offboard PAM users, so that their identity and access privilege lifecycle is fully managed without manual intervention.

Benefits of Unified Identity Management Service for Privilege Access are:

Benefits	Outcome	Value
Reduce Cybersecurity Risks • Limit access to sensitive data by removing all permanent user access permissions. • Just-in-time, just enough privilege access with time-bound limits. • Real-time provisioning and removal of privilege access to human and machine users.	Provide Just enough and Just-In-Time privilege system access for each legitimate request.	Reduction in security incidents resulting from the misuse of superuser access.

Benefits	Outcome	Value
Demonstrate compliance with full privilege access audit trail. • Accurate audit and identity analytics for privileged access. • Prescribed risk-based access control based on security policies. • Secured vendor and 3rd party access. • On demand risk and compliance reporting.	Demonstrate to the authority that you are in complete control of your privileged access with evidence.	Real-time access to audit log and compliance status.
Optimise Operational Efficiency • Managed identity lifecycle. • Continuous identity & access discovery. • Reduce risks by better control and visibility.	Knowing who has superuser access to your infrastructure and what they are doing.	100% visibility and control of what super users are doing on your infrastructure.
Enable Digital Business • Automation of manual workflows. • Policy-driven authorisation. • Address cybersecurity audit demands.	Implement and enforce your access policies for the super users with identity lifecycle management automation.	Eliminate manual effort and costs for the administration and enforcement of superuser access.

2. What does it deliver?

AtoS' Unified Identity Management Service for Privilege Access delivers a holistic, integrated, and managed solution in the UK for securing and managing privileged access across a public sector organisation's entire IT ecosystem.

The service combines the capabilities of Evidian's identity and access management products (IDaaS, IGA, EAM, and WAM) with CyberArk's Privileged Access Management (PAM) software to address the complete lifecycle of privileged identities and their access to critical systems and applications.

The service delivers the following key components and benefits:

- **Comprehensive privileged access management:** The service provides centralised control and management of privileged accounts, including the secure storage of credentials in an encrypted password vault, automatic password rotation, and granular access control policies
- **Identity lifecycle management:** Automates the onboarding and offboarding of human and machine entities that require privileged access, integrating with HR systems for streamlined provisioning and de-provisioning processes
- **Single sign-on and multi-factor authentication:** The service enables seamless access to systems and applications through single sign-on (SSO) and enhances security with multi-factor authentication (MFA) capabilities
- **Session isolation and monitoring:** Privileged sessions are isolated and monitored to prevent unauthorised access and provide detailed audit trails for compliance and incident investigation purposes
- **Identity governance and administration:** The service includes access certifications, segregation of duties (SoD), and identity analytics to maintain a compliant and secure state
- **Remote and vendor access management:** It facilitates secure, VPN-less access for privileged users and third-party vendors, simplifying remote access while maintaining strict security controls
- **Integration and extensibility:** The service integrates with various IT systems, such as identity providers and HR applications, and supports the SCIM protocol for integration with IGA platforms. It also offers APIs and SDKs for extending its capabilities to custom applications

- **Managed service model:** Atos' team of experts manages the entire solution, reducing the burden on in-house IT teams and providing access to specialised knowledge and resources
- **Customisation and scalability:** The service is designed to be flexible and customisable to meet the specific needs of each organisation, and it can scale to accommodate growth and changing requirements
- **Enhanced security posture:** By implementing a comprehensive privileged access management solution, organisations can significantly improve their overall security posture, reduce the risk of data breaches, and streamline compliance with regulatory requirements.

In summary, Atos' Unified Identity Management Service for Privilege Access delivers a robust, end-to-end solution for managing and securing privileged access across a public sector organisation's diverse IT environment. By integrating identity and access management capabilities with privileged access management, the service enables organisations to effectively control and monitor privileged access, mitigate security risks, and ensure compliance with industry standards and regulations.

An indicative service scope for a medium-sized enterprise implementation consists of:

- Number of PAM accounts (identity) that need to be managed: 500
- Maximum number of connections to the PAM system: 10
- Number of environments included: 4 (Development, Test, Pre-production and Live).

Our team of service experts will work closely with the organisation to survey and evaluate the scope and service requirements and jointly agree on an implementation approach and timescale.

The detailed service level (e.g. service hours, maintenance period, frequency of service reviews, etc.) will be agreed upon upfront before undertaking any implementation and service take-on.

Service Benefits

Benefits	Outcomes	Value
Enhanced Security • Encrypted password vaults • Granular access control • Real-time session monitoring	Reduced Risk of Data Breaches • Minimise unauthorised access • Protect sensitive data • Prevent financial & reputational damage Enhanced visibility and control • Centralised monitoring of privileged access • Real-time alerting & incident response	Improved Business Agility • Quickly adapt to changing security needs • Securely support new initiatives • Maintain customer trust Enhanced reputation and customer trust • Demonstrate a strong security posture • Differentiate from competitors Cost savings • Reduce costs associated with data breaches • Avoid regulatory fines & penalties
Improve Compliance • Automated Access provisioning • Segregation of duties • Detailed audit trails	Improved audit readiness • Detailed audit trails and reports • Easily demonstrate compliance	Enhance reputation and customer trust • Demonstrate compliance to customers • Build trust with stakeholders Cost Savings • Reduce audit preparation costs • Avoid non-compliance fines and penalties
Increased efficiency • Automated user provisioning • Self-service capabilities	Increased Productivity • Faster access to resources • Minimise access delays Enhanced visibility and control • Centralised IAM & PAM management • Streamlined access governance	Cost Savings • Reduce manual IAM efforts • Reallocate IT resources to strategic tasks Improved Business Agility • Quickly onboard new users and applications • Adapt to changing business needs Reduce IT burden • Minimise IAM & PAM maintenance • Focus on core business objectives

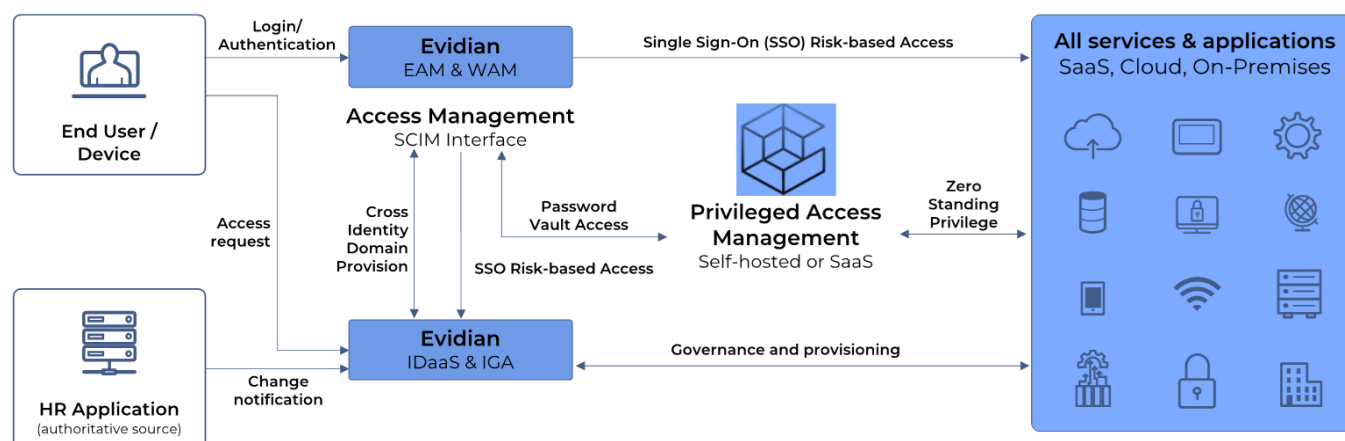
Benefits	Outcomes	Value
Seamless Integration • SCIM protocol support • Easy deployment	Improved audit readiness • Consolidated audit data from IAM & PAM • Simplified compliance reporting	Cost Savings • Reduce integration & maintenance costs • Avoid costs of disparate solutions Improved Business Agility • Quickly integrate new systems & applications • Adapt to evolving IT ecosystem Reduce IT burden • Minimise integration efforts • Focus on strategic initiatives
Scalability and Flexibility • Cloud-based architecture • Diverse deployment models • Customisable integrations	Improved business agility • Quickly scale IAM & PAM capabilities • Adapt to changing business needs Increase productivity • Easily onboard new users & applications • Minimise access delays	Cost Savings • Pay-as-you-go model • Avoid upfront hardware and software costs Enhanced reputation and customer trust • Demonstrate scalable security practices • Meet evolving customer demands Reduce IT burden • Offload IAM & PAM maintenance to Atos • Focus on core competencies



3. What technology does it use?

Atos' Unified Identity Management Service for Privilege Access is built upon a robust foundation of industry-leading technologies and solutions. The service integrates Evidian's identity and access management (IAM) products with CyberArk's Privileged Access Management (PAM) software to create a comprehensive, end-to-end solution for managing and securing privileged access.

The high-level solution diagram for Atos' Unified Identity Management Service for Privilege Access is illustrated in the figure below:



Evidian IDaaS (Identity as a Service): A comprehensive, cloud-based IAM solution that provides authentication, authorisation, identity federation, user lifecycle management, and identity governance functionalities. Supporting single sign-on (SSO), multi-factor authentication (MFA), automated user provisioning/deprovisioning, role-based access control (RBAC), and fine-grained access policies. IDaaS offers a brandable access portal, SDKs for integration, and customisable dashboards and reports. The service is fully managed, scalable, and ensures high availability.

Evidian IGA (Identity Governance and Administration): Manages the onboarding and offboarding of privileged access for human and machine entities. It integrates with HR applications for automated provisioning and deprovisioning, generates access reports and audit trails, and helps maintain compliance through access certifications, segregation of duties (SoD), and identity analytics. IGA can be integrated with Evidian IDaaS for extended governance capabilities.

Privileged Access Management (PAM) with CyberArk: CyberArk is our strategic partner, securing privileged accounts using an encrypted password vault, centralised policy management, and access control. It enables automatic password rotation, session isolation, and monitoring. PAM integrates with identity providers, supports remote and

vendor access management, and facilitates secure, VPN-less access. It includes privileged account discovery, integration with IGA platforms using SCIM protocol, and optional Endpoint Privilege Manager (EPM) for managing endpoint privileges.

CyberArk can be run as a self-hosted or Software as a Service, and the implementation options can be reviewed and confirmed at the beginning of the project.

Evidian EAM (Enterprise Access Manager - Optional): Provides SSO and MFA capabilities for secure access to the PAM system (CyberArk). It serves as an alternative to Evidian WAM.

Evidian WAM (Web Access Manager - Optional): An alternative to Evidian EAM, providing SSO and MFA functionality for accessing the PAM system (CyberArk) through web-based access management capabilities.

To facilitate seamless integration across components, the service utilises the SCIM (System for Cross-domain Identity Management) protocol. SCIM enables efficient and standardised communication between the PAM solution and the IGA platform, allowing for the smooth exchange of identity and access information.

By combining these best-in-class technologies and solutions, Atos' Unified Identity Management Service for Privilege Access provides organisations with a powerful, flexible, and scalable platform for managing and securing privileged access across their entire IT ecosystem. The service enables organisations to streamline IAM processes, enhance security, ensure compliance, and reduce the risk of data breaches and insider threats.



4. What terms apply?

To the fullest extent permitted under G-Cloud 15 Framework Agreement and the Call-Off Contract, Atos will provide the Services in accordance with the Atos Supplier Terms (which will include, but may not be limited to , the Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLAs and Supplier Licence Terms and any applicable Third-Party Terms outlined in this Service Description document and the Order Form) and this Service Description document.

For clarity:

- Atos Supplier Terms may be modified in accordance with the provisions of the Call-Off Contract, and remain effective except where expressly overridden.
- Hyperlinks included in the Atos Supplier Terms and Service Description document remain effective where they point to Atos' or the relevant Third-Party Terms or documents. Should a hyperlink cease to function, Atos will work with the client to update it through the agreed procedure.



5. Termination

Termination shall be in accordance with:

- The G-Cloud 15 Framework terms and conditions
- Any terms agreed within the Order Form of the relevant Call-Off Contract
- For this specific service, by default Atos ask for at least thirty (30) days prior written notice of termination without cause.

Atos commits to the continued provision of services for the duration of the Call-Off Contract subject to the terms and conditions of the G-Cloud 15 Framework Agreement, the Call-Off Contract, the Atos Supplier Terms and the applicable Third Party Agreements (as defined in the Atos Supplier Terms and indicated in the Order Form) related thereto.



6. How do I order?

Please contact our team at: gcloud@atos.net

- We will prepare a quotation for your review, including any applicable volume discounts.
- Once the quotation is agreed, we will issue the necessary documentation (as required by the G-Cloud Framework) and request a purchase order from you.
- Upon receipt of your purchase order, we will configure the services in line with the agreed requirements. Where applicable, you will also receive access to our self-service portal to begin provisioning services.
- If you are a new customer, you may need to complete additional 'new supplier' forms.
- Invoices will be issued to you and to Crown Commercial Service (CCS), quoting the purchase order number, for the services procured.
- We will also submit the required monthly management information reports to Government Procurement.



7. Glossary

Term	Definition
EAM	Enterprise Access Management
EPM	Endpoint Privilege Manager
HR	Human Resources
IAM	Identity Access Management
IDaaS	Identity as a Service
IGA	Identity Governance and Administration
MFA	Multi-Factor Authentication
PAM	Privileged Access Management
RBAC	Role-Based Access Control
SaaS	Software as a Service
SCIM	System for Cross-Domain Identity Management
SDK	Software Development Kit
SoD	Segregation of Duties
SSO	Single Sign-On
VPN	Virtual Private Network
WAM	Web Access Management



8. Why Atos

Atos has been a trusted partner on every G-Cloud iteration since the framework began, helping public sector organisations modernise with confidence. We combine global expertise with deep UK experience, delivering secure, scalable cloud solutions that meet the highest government standards.

As Europe's leading provider of cloud and cybersecurity services, Atos offers end-to-end capabilities - from migration and hosting to SaaS and consultancy - supported by UK delivery centres and strategic partnerships with hyperscalers.

Our focus on innovation, sustainability, and social value ensures that customers not only achieve operational excellence but also contribute to a greener, fairer future. With Atos, you gain a proven partner committed to driving efficiency, resilience, and transformation across public service.



About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands – Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net