



ProofID Technical Support

Service Definition

Prepared for:

GCloud 15



Disclaimer

ProofID Limited makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Copyright

Copyright 2026 ProofID Limited. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of ProofID Limited.

Contact

Questions related to the information contained in this document should be directed to ProofID sales at sales@ProofID.com

Tel: +44 (0)330 808 0785

ProofID Ltd
Suite 2.3
Building 8
Exchange Quay
Salford, M5 3EJ



Table of contents

1.0	Identity and Access Management Technical Support	4
1.1	Identity Management Technical Support Service Highlights	4
1.2	About ProofID	4
1.3	Supported Technologies	4
1.4	What's Covered?.....	5
1.5	Service Level Agreement	6
1.6	Identity Management Technical Support Service Deliverables	7
1.7	Onboarding Process	7
1.8	Service Management	7
2.0	Identity Management Technical Support Pricing	8
2.1	Definitions.....	8
2.2	Pricing Model.....	8
2.3	Marketing Support Discount.....	9
2.4	24 / 7 Access for Priority 1 Incidents (optional)	9
2.5	Additional Items.....	10
2.6	Payment Terms.....	10
3.0	Case Study – Mazars Adopts ProofID's IAM Managed Service	10



1.0 Identity and Access Management Technical Support

In an IT landscape which is increasingly influenced by internet and cloud technologies, identity management is a specialist technology requiring niche technical skills, yet which is at the heart of modern IT operations.

Identity management is an essential element of the IT stack, yet the skills required to deploy and manage identity management solutions are in short supply, which means that many organisations find it difficult to manage their identity management deployment effectively and efficiently. This issue is compounded by the fact that identity management technologies, by their very nature, reach across the whole IT estate, meaning that misconfiguration or outages can have very serious implications, in terms of security and lost productivity.

Building upon many years' experience of delivering complex enterprise identity management solutions, ProofID is ideally placed, to offer highly responsive, expert technical support for its customers' identity management systems. With a team of highly experienced identity management consultants and support professionals, ProofID can provide the assurance that technical issues related to the critical identity management system can be resolved as quickly as possible and normal service resumed.

1.1 Identity Management Technical Support Service Highlights

The Identity Management Technical Support service offers the following benefits:

- Unlimited technical support incidents, providing assistance to customer staff to resolve technical issues with the identity management system, including remote dial-in where necessary to resolve issues
- An optional annual 'consultancy bank' of consultancy hours which can be used for provision of expert identity management consultancy services, such as for a health-check of the identity management system, or implementation of a new identity management connector
- Service backed by strict SLAs

1.2 About ProofID

ProofID is a global provider of managed IAM solutions headquartered in the UK with a US operation in Colorado Springs. We help customers every day in securing enterprise data, manage hybrid cloud environments, secure mobile apps, and provide access to services by partners and customers. All successfully delivered through our methodology driven managed service. Daily we manage over 6 million identities and deliver services to 120 countries. For more information, call +44 (0)330 808 0785

info@proofid.com or visit www.proofid.com.

1.3 Supported Technologies

Proof ID is vendor agnostic and supports a wide array of identity management products, including:

- Microsoft Forefront Identity Manager, ADFS
- NetIQ IDM and Access Manager
- Ping Identity PingFederate, PingDirectory, PingID, PingID, Ping Intelligence and PingAccess
- Shibboleth



- ProofID products
- ideiio
- Thycotic PAM Product Suite

ProofID supports all versions currently supported by the vendor. Support for versions which are no longer supported by the vendor will be on a reasonable endeavours' basis only. ProofID will work with the customer to identify any system components which may be approaching the end of the support lifecycle, and consultancy bank hours may be used to upgrade these components.

1.4 What's Covered?

The following table describes what is covered by the Identity Management support contract:

Situation	Coverage
Break/fix support – i.e. support for incidents where the identity management system is not working as it should.	Covered Unlimited technical support incidents
Support for production and pre-production environments	Covered Unlimited technical support incidents
Support for development environments	Reasonable endeavours basis only Unlimited technical support incidents
General enquiries (e.g. 'how do I do this?')	Covered Consultancy bank on a T&M basis
Changes to configuration / logic, when system is otherwise operational, or general consultancy	Covered Consultancy bank hours on a T&M basis

Technical support incidents may be logged via email, ProofID portal or telephone, by up to six named customer contacts.



1.5 Service Level Agreement

The following Service Level Agreement applies to the Identity Management Technical Support service:

Priority	Response
Priority 1 (P1)	1 working hour
Priority 2 (P2)	2 working hours
Priority 3 (P3)	4 working hours
Priority 4 (P4)	8 working hours

The Priorities referred to in the table above are defined below:

Priority	Description
Priority 1	Complete outage or loss of core component of identity management system affecting whole user population
Priority 2	Low priority issue affecting an individual or small group of users, which causes minor inconvenience but not outage or instability. General enquiries.
Priority 3	Fault which either causes outage of core identity management component for a small section of user population, or causes an intermittent or partial outage for a larger section of user population
Priority 4	Low priority issue affecting an individual or small group of users, which causes minor inconvenience but not outage or instability. General enquiries.

The IAM Technical Support service is subject to the following hours of service:

Activity	Hours of Service
----------	------------------



Service Desk for logging new issues and active progression of existing incidents	Monday to Friday, 08:00 to 18:00 GMT, excluding English Public Holidays
Access to out of hours engineer for Priority 1 incidents (only available via optional 24/7 service)	24 x 7 x 365
Service Portal access for logging of new incidents or to view or update existing incidents	24 x 7 x 365

1.6 Identity Management Technical Support Service Deliverables

The following table details the deliverables of the Identity Management Technical Support service.

Deliverable	Description
Technical Support	Unlimited third line technical support incidents for all technical issues relating to the identity management system, subject to coverage and hours of service specified above. Resolution via remote dial-in will be provided where necessary and with the customers agreement to resolve the technical issue.
Consultancy Bank Hours	Consultancy bank of hours per contract year to be used to provide identity management consultancy services and out of hours work. Consultancy bank hours are consumed on a Time and Materials basis in minimum blocks of half an hour for remote work, and 8 hours for onsite work.

1.7 Onboarding Process

In order to support the Identity Management system effectively, it is essential that ProofID gain an understanding of the technical environment.

To this end, a ProofID will schedule an onboarding conference call with the relevant customer contacts and the ProofID Service Delivery Manager and a senior engineer to gain an understanding of the customers environment and outline the specifics of the service.

ProofID does not charge for the onboarding process.

1.8 Service Management

ProofID will assign a Service Delivery Manager to the customer to assume overall responsibility for the delivery of the contract.

- The Service Delivery Manager will:
- Produce and share quarterly service review reports documenting all incidents during the period and performance of the contract against SLAs
- Arrange quarterly service review calls.
- Single point of escalation for issues related to the support service



2.0 Identity Management Technical Support Pricing

The Identity Management Technical Support service is priced according to the number of identity management components present in the production system.

2.1 Definitions

Identity Management system components are defined as below:

Component	Definition
Connector	A connector is a link between a source r target application and the IDM system which enables provisioning and de-provisioning of user accounts. Examples of terminology used by vendors to describe this include Management Agent (Microsoft FIM) and Driver (NetIQ Identity Manager).
Protected Application	A protected application is one which has been configured to be 'behind' an Access Management product such as NetIQ Access Manager or PingAccess. The user authenticates to the Access Management service which then handles seamless authentication and authorisation to the protected application.
Federated/SSO Application	A Federated Application is one, typically SaaS or externally hosted, which is configured to delegate authentication to an external authentication source, typically a directory service such as Active Directory. The configuration makes use of a federation service such as ADFS, Shibboleth or PingFederate.

2.2 Pricing Model

The pricing model is as per the following table:

Component	1 Year Contract Annual Fee	2 Year Contract Annual Fee	Optional 24/7 Surcharge
'Small' – up to 5 supported system components	£11,500	£11,000	£5,500
'Medium' – 6 to 15 supported system components	£19,850	£18,750	£8,850
'Large' – over 15 supported system components	£30,000	£28,500	11,950



'X Large' – over 25 supported system components	POA	POA	POA
Per additional supported system component	£1,500	£1,350	N/A
Per annual consultancy bank hour	£185	£185	N/A
Per additional named customer contact	£850	£850	N/A

Support fees are inclusive of expenses.

2.3 Marketing Support Discount

A 5% per annum discount applies subject to the customer agreeing to the following terms

- ProofID is permitted to release a Press Release upon receipt of Purchase Order describing the Identity Management Technical Support service and to include contract value
- The customer to collaborate with ProofID on a Case Study following three months of live operation of the Identity Management Technical Support service. ProofID may publish the Case Study as desired.
- ProofID allowed to use the customer' name and logo on promotional material for the Identity Management Technical Support service and on ProofID's website.
- The customer to act as a reference for ProofID's prospective Identity Management Technical Support customers.

2.4 24 / 7 Access for Priority 1 Incidents (optional)

We understand that our customers IAM infrastructure plays a crucial role within their organisation, as such ProofID provide access to an engineer for Priority 1 incidents outside of core hours. This is an optional chargeable service and is subject to the 24/7 contract surcharge.

Work on incidents outside of core hours will consume consultancy bank hours at the following multiplier

Time	Multiplier
Mon-Friday, 18:00 – 08:00	x 1
Saturday	x 1.5



Sunday & public holidays

X 2

Prior agreement with the customer will always be sought before performing work outside of core hours. Where the customer has insufficient remaining hours 'in the bank' ProofID will not leave the customer stranded but retrospectively invoice the customer.

2.5 Additional Items

The following items may be purchased at any time during the contract to 'top-up' services, in which case charges will be applied on a pro-rata basis, or at any time as a 'standalone' item. Volume or marketing discounts do not apply to additional items.

Item	Price
Additional Consultancy Bank Hours	£185/hour
Additional Supported System Component	£1,500
Additional Named Customer Contact	£850

2.6 Payment Terms

- Pricing is exclusive of expenses.
- Pricing is exclusive of VAT.
- IAM Technical Support service fees are invoiced annually in advance. The initial invoice will be raised on receipt of Purchase Order and/or completed GCloud Call-Off Contract.
- Payment terms are 30 days from date of invoice.
- Maximum contract duration under G-Cloud regulations is two years.

3.0 Case Study – Mazars Adopts ProofID's IAM Managed Service

The Challenge

Mazars is a world leading audit, accounting and consulting group with more than 17,000 employees in 77 countries. As a large, globally distributed organisation, it is crucial that Mazars can provide an IT environment which is able to support and encourage collaboration



across all of its territories. With the wider adoption of cloud services, including Office365, Mazars' traditional, on-premise approach to identity management was no longer able to provide a solution. Mazars' needed a solution which would provide a unified authentication framework and a seamless single sign-on experience for its users, regardless of user location or type of application. The solution would need to be able to work with Mazars' global authentication environment, hiding the complexity of multiple directories from end-users. Furthermore, the system would need to have a small technical footprint in order to make deployment across all 77 territories viable.

The Solution

ProofID worked with Mazars to deploy a solution based upon PingFederate, the industry leading federated single sign-on platform. PingFederate's enterprise features and adherence to standards meant that a single resilient cluster deployed in Mazars' Azure tenancy was able to provide federated authentication and single sign-on for all of Mazars' users across all tenancies. Delivered under ProofID's methodology driven managed services framework, the rollout has been streamlined to the extent that a new territory can be integrated within a matter of a few hours; currently the solution has been extended to 35+ territories, allowing those users single sign-on to Mazars' core applications, both SaaS and on-premise.

The solution is enhanced by ProofID's White Pages application, which uses directory aggregation and user provisioning technology to provide a single staff user directory, which can be used to locate and contact colleagues from across the global Mazars family, significantly enhancing cross-territory productivity. The built-in user self-service capabilities ensure that user data is kept up to date and accurate.

The Results

Mazars chose to work with ProofID as its outsourced managed service provider for the expert advice and cost savings it is able to make over the three-year period of the contract. To hire a team internally to do the same job would be expensive, as well as being a hard skill set to find.

"Mazars is a complex organization and has moved to take advantage of cloud based services such as Office365 to foster better collaboration and sense of community to what is a highly-distributed workforce. Given this move our existing identity management service was no longer fit for purpose. Working with ProofID we have rapidly rolled out a new security framework that allows us to integrate new applications and services at pace. The service is transformational for the organisation." explains Jayson Dudley, Group CISO, Mazars.

Tom Eggleston, CEO at ProofID said: "We are proud to have been able to help Mazars on this journey, which shows how ProofID's Identity as a Managed Service approach can underpin transformational technical changes, ensuring the organisation gets the outcome needed, when it's needed."