Identity and Access Management

Service Definition Document

January 2026

Document Control

Document Type	Confidential - Customer Facing		
Company	Maple Networks		
Address	The Print Rooms 164/180 Union Street London SE1 0LH		
Primary Contact	Graham Tetley	**Role**	CTO/Lead Consultant
Phone Number	020 3858 0048	**Email address**	gtetley@maplenetworks.co.uk

Revision History

Issue Date	Author	Version	Revision Description
16/12/2025	Rory Leanord	0.1	Initial Draft
08/01/2026	Graham Tetley	0.2	QA for G-Cloud 15
22/01/2026	Jonny Zammer	1.0	Release

Table of Contents

Contents

Services Overview

Maple Networks are next generation Digital and IT service provider in the UK with skills in various areas across the digital landscape. Maple Networks have developed a range of services to support customers in their digital, data and business transformations.

This Document provides overview service definition information for the Maple Networks Identity and Access Management service(s)

Maples IAM service provides end-to-end governance across on-premises, cloud, and hybrid environments. Grounded in Zero Trust and least-privilege principles, the service streamlines access for legitimate users while measurably reducing identity-related risk. Maple designs and operates the policies, processes, and controls that manage the full identity lifecycle (joiner, mover, leaver), enforce strong authentication, and ensure access is appropriate, auditable, and time-bound. The outcome is a secure, frictionless user experience that accelerates onboarding, protects sensitive assets, and strengthens compliance with frameworks and regulations (e.g., ISO 27001, NIST CSF, GDPR).

Service Description

Service Title

Identity and Access Management (IAM) provides the governance and control framework that determines who may access which resources, under what conditions, and for how long. Robust IAM materially reduces both the likelihood and the impact of compromise, because the most prevalent attack paths rely on credentials rather than software exploits.

An NCSC-aligned IAM programme—comprising strong (preferably phishing-resistant) MFA, least-privilege and just-in-time access, rigorous identity lifecycle management, privileged access controls, and auditable activity—delivers measurable risk reduction and strengthens assurance and compliance readiness.

Service Overview

- **Identity Lifecycle & Directories**: Authoritative sources integration (HRIS), identity proofing, automated provisioning/de-provisioning, directory hygiene, and federation for workforce, partners, and customers.
- **Access Governance**: Role- and attribute-based access control (RBAC/ABAC), SoD (segregation of duties), access request/approval workflows, periodic certifications (attestations), exception management, and access recertification cadence.
- **Authentication & SSO**: Multi-factor authentication (MFA), passwordless options, conditional access policies, adaptive risk scoring, and single sign-on for SaaS, on-prem apps, and cloud platforms.
- **Privileged Access Management (PAM)**: Just-in-time/just-enough access, session recording, credential vaulting, break-glass controls, secrets management, and privileged risk reporting.
- **Cloud Entitlements & Non-Human Identities**: CIEM for AWS/Azure/GCP, service accounts, workloads, API keys, certificates, and robotic process automations with lifecycle controls.
- **Monitoring & ITDR**: Identity Threat Detection & Response, anomalous sign-in and privilege use monitoring, SIEM/SOAR integration, and incident playbooks for compromised identities.
- **Third-Party/Supply Chain**: Onboarding/offboarding vendors, least-privilege access for MSPs, and contract-aligned controls for shared environments.

Maple have significant experience across a wide range of organisation types and structures. Across all sectors, Maple have a significant number of examples of delivering similar engagements at different stakeholder levels. Maple aligns our reports and presentations to executive level, as well as to Senior Leadership Teams and Technical staff. Maple's skills at a technical level across multiple platforms and technologies, include:

- Hybrid multi-cloud
- Backup
- Cyber security
- Disaster Recovery
- Business Continuity

This expertise means Maple are well positioned to deliver on such engagements by leveraging all of our accrued experience and knowledge. Maple have developed a proven methodology which has delivered defined outcomes for our customers.

Maple's proven methodology has been developed over several years, leading to successful delivery of large-scale reviews, roadmaps, and implementation projects for many commercial organisations including within the NHS, local government and higher education.

Service Package

Objective	To provide end-to-end governance for Identities and Access management strategy. Ensuring access is restricted to authenticated and authorised users, under determined business conditions.
Description	Maples IAM service provides centralised governance of digital identities and access across cloud and on-premises environments. Grounded in Zero Trust and least-privilege principles, it ensures that only verified users, devices and workloads obtain appropriate, auditable and time-bound access to organisational assets. The service aligns with recognised UK guidance and standards for public sector assurance and delivers a secure, consistent user experience that accelerates onboarding, reduces identity-related risk, and strengthens compliance. • **Identity Lifecycle & Directories**: Authoritative sources integration (HRIS), identity proofing, automated provisioning/de-provisioning, directory hygiene, and federation for workforce, partners, and customers. • **Access Governance**: Role- and attribute-based access control (RBAC/ABAC), SoD (segregation of duties), access request/approval workflows, periodic certifications (attestations), exception management, and access recertification cadence. • **Authentication & SSO**: Multi-factor authentication (MFA), passwordless options, conditional access policies, adaptive risk scoring, and single sign-on for SaaS, on-prem apps, and cloud platforms. • **Privileged Access Management (PAM)**: Just-in-time/just-enough access, session recording, credential vaulting, break-glass controls, secrets management, and privileged risk reporting. • **Cloud Entitlements & Non-Human Identities**: CIEM for AWS/Azure/GCP, service accounts, workloads, API keys, certificates, and robotic process automations with lifecycle controls. • **Monitoring & ITDR**: Identity Threat Detection & Response, anomalous sign-in and privilege use monitoring, SIEM/SOAR integration, and incident playbooks for compromised identities. • **Third-Party/Supply Chain**: Onboarding/offboarding vendors, least-privilege access for MSPs, and contract-aligned controls for shared environments.
Hosted In	• Customers Azure Tenancy
Supported From	All support and management are delivered remotely from the Maple Networks 24x7x365 SOC Remotely from within the UK

Service Features

	Description	Standard / Optional / Customisations
Deployment	Rapid deployment	Standard
Integration into SIEM and Alerting	IAM alerting integrates seamlessly with whatever alerting technology is currently in use, including but not limited to; Messaging Application Notifications, Email, ITSM alerting, SEIM integrations.	Standard
Remediation Support	Remediation support is available through Maples supporting services such as SOC and service desk.	Standard