



Purple Service Definition

Managed guest, public & staff WiFi



Service Description: Managed guest, public & staff wifi

Scalable cloud-native platform providing identity-based access for staff, guests, and residents. It utilises cloud RADIUS infrastructure for SSO integration (Microsoft/Google/Okta) and Passpoint encryption. Replaces shared passwords with unique per-user keys and automated SCIM revocation. Includes centralised management and occupancy analytics to optimise estate utilisation.

Service Overview:

Scalable cloud-native platform providing identity-based access for staff, guests, and residents. It utilises The Purple platform provides an Identity-Based Networks solution that replaces traditional, insecure authentication methods like shared passwords and captive portals with identity-driven access. The software is an overlay solution that works with any existing RADIUS-compatible network hardware, preventing vendor lock-in and eliminating the need for on-premise servers.

The system functions by binding network authentication to a verified identity source. For staff and students, it integrates directly with an organisation's trusted Identity Provider (IdP), such as Microsoft Entra ID, Google Workspace, or Okta. For guests and visitors, it uses certificate-based provisioning to create a secure, encrypted connection from the first packet, removing the risks associated with open networks.

Public sector entities face unique challenges regarding security compliance, large-scale visitor management, and efficient resource allocation.

Elimination of security gaps in staff networks

Traditional staff WiFi often relies on shared passwords that are rarely changed, creating a massive security risk when employees leave. Purple uses SCIM integration to sync with the organisation's directory, ensuring that network access is revoked automatically and instantly when a staff member is disabled in the HR system.

Mitigation of open network risks for the public

Public sector venues often provide guest WiFi over open networks, which are insecure by design and vulnerable to "evil twin" attacks. Purple provisions Passpoint (Hotspot 2.0) profiles that encrypt traffic from the very first packet and use trusted root certificates to ensure devices only connect to legitimate access points.

Reduction in IT helpdesk burden

Public sector IT teams often spend significant time on WiFi-related troubleshooting. By automating the onboarding process through the Purple application, organisations typically see an 80% reduction in WiFi-related support tickets.

Secure management of residential and multi-tenant environments

In government-managed housing, care homes, or student accommodations, standard WiFi often leads to a lack of privacy. Purple creates a Private Area Network (PAN) for each resident, allowing their devices to communicate securely while remaining invisible to other users on the same infrastructure.

Data-driven building and estate optimisation

The platform provides detailed workplace analytics regarding building utilisation and occupancy patterns. This data allows facilities teams to optimise real estate usage, resulting in an average 35% reduction in real estate costs through informed space management.

Compliance with rigorous security standards

The platform supports Zero Trust architectures by providing unique encryption keys per user and maintaining complete audit trails. Purple is ISO 27001 and ISO 9001 certified, as well as GDPR and CCPA compliant, meeting the high security and data sovereignty standards required for public sector contracts.

Key Features and Benefits

The Purple Identity-Based Networks platform provides a range of technical capabilities designed to enhance security, reduce operational costs, and deliver actionable insights for public-sector infrastructure.

- **IDP and SCIM integration.** Connects directly to directories such as Microsoft Entra ID or Okta to automate user provisioning. This allows for the instant revocation of network access when staff leave the organisation.
- **Unique per-user encryption keys.** Assigns unique WPA2/3-Enterprise session keys to every individual user. This implementation ensures traffic is isolated even on shared access points to prevent local data interception.
- **Passpoint (Hotspot 2.0) provisioning.** Installs secure profiles that enable devices to connect automatically with enterprise encryption from the first packet. This mitigates vulnerabilities in open networks and protects users from evil twin attacks.
- **Private area networks (PAN).** Uses mDNS reflection and iPSK to create virtual network bubbles for residents in housing or care settings. This allows personal devices to communicate with each other while remaining invisible to neighbours.
- **Cloud-native radius architecture.** Operates on a high-availability global infrastructure, eliminating the cost and technical debt of maintaining on-premise authentication servers.
- **Vendor-agnostic interoperability.** Functions as an overlay compatible with any RADIUS-supporting hardware, including Cisco, Aruba, and Meraki. This prevents vendor lock-in and allows for unified management across mixed estates.
- **Real-time utilisation analytics.** Tracks WiFi connection data to generate occupancy and building utilisation reports. Facilities teams use these insights to optimise space, resulting in an average reduction of 35% in property costs.
- **Centralised management dashboard.** Provides a single interface to manage all users, locations, and policy changes globally. This centralised control reduces WiFi-related IT support tickets by 80%.
- **Security and compliance certifications.** Maintains ISO 27001 and ISO 9001 certifications alongside full GDPR and CCPA compliance. This ensures all authentication and data handling meet rigorous government security standards.

Onboarding & Offboarding

Onboarding:

The onboarding process is a structured journey designed to move a customer from initial planning to a live environment. The process begins with Requirements Gathering to collect network specifications, hardware details, and design preferences, followed by a Kick-Off Call to align stakeholders and outline the project timeline. Implementation then moves into Hardware Setup, where access points and controllers are configured, and Platform Setup, where the Purple portal is customised and integrated with existing systems.

Before the final launch, rigorous Testing and Quality Assurance are conducted, including connectivity checks and User Acceptance Testing (UAT) to ensure the service meets all functional requirements. The journey concludes with the Go Live phase, where the portal is transitioned to a live environment and formal support is handed over to the Purple support team for ongoing maintenance.

Ongoing skills transfer and training is managed through a series of webinars and or virtual workshops, ensuring staff remain proficient as system requirements evolve

Summary of onboarding process:

- Requirements Gathering: Collecting network, hardware, and design assets
- Kick-Off Call: Aligning project goals, milestones, and responsibilities
- Hardware Setup: Configuring APs, WiFi controllers, and content filtering
- Platform Setup: Portal configuration and system integrations
- Testing and QA: Functional testing, UAT, and connectivity checks
- Go Live: Deployment to the live environment and final handover

Offboarding:

The offboarding process involves a few steps to ensure a smooth transition and the secure handling of data in accordance with regulation and compliance. Here's a general outline of our off-boarding process:

Purple manages customer offboarding through a framework aligned with ISO 27001 and UK GDPR standards. Client confidential data is removed at the end of the relationship or immediately upon request, while end-user personal data is automatically anonymised or deleted after 13 months of inactivity.

In accordance with standard data processing obligations, Purple commits to the secure destruction of all customer data and associated copies within four business days of the processing end date, unless specific legal obligations require further retention. To ensure a seamless transition, customers may request the return or transfer of their data in a structured, machine-readable format (such as .csv) within two business days of the contract's conclusion. These files are accessible through the self-service portal, the RESTful API, or via secure transfer. Throughout this transition, Purple maintains strict logical data separation to prevent cross-contamination, ensuring that all administrative access and user rights to the customer's specific environment are promptly revoked.

The final data destruction is executed using industry-standard methods to ensure all information is rendered completely unrecoverable. To maintain a robust audit trail for compliance purposes, the completion of these activities is formally recorded, providing transparent verification that all data handling obligations have been met.

Service Levels and Support

Purple provides a comprehensive Service Level Agreement (SLA) to ensure high availability and responsive support for all G-Cloud customers.

Service Availability

- Uptime Commitment: 99.9% availability for the Purple Cloud Platform (excluding scheduled maintenance).

Support Hours (Standard)

- Hours: 07:00 – 23:00 (GMT/BST), Monday to Friday.
- Exclusions: UK Public Holidays.
- Note: Enhanced 24/7 support and SLA are available via our Support+ and Guest Support add-ons.

Response Times

We categorise support requests by impact and urgency, with the following target response times during Support Hours:

Priority Level	Description	Target Response Time
P1 – Critical	Total loss of service or major system failure.	2 Hours
P2 – High	Severe degradation of service or key functionality.	4 Hours
P3 – Normal	Minor system issues or general "how-to" queries.	1 Business Day
P4 – Low	General requests, cosmetic issues, or feedback.	2 Business Days

Support Channels

Customers can log and track tickets via our 24/7 online support portal, which also provides access to our extensive knowledge base and technical documentation.

Technical Requirements:

Purple's solution is a cloud-hosted, responsive web application requiring a web browser for portal access and captive page negotiation. All web traffic is transmitted via HTTPS (over TCP port 443), ensuring compatibility with standard web clients on desktop and mobile devices. The service does not require a specific internet speed for end-users, a stable internet connection, such as 50mbps, is ideal for high-performance activity and smooth delivery of service, the platform functions across standard WiFi and/or Ethernet network infrastructures. There is no requirement for specific client-side software for general use. Technical integration requires hardware capable of communicating via RADIUS authentication and accounting protocols (using UDP ports 1812 and 1813).

Information Assurance:

Purple operates an ISO 27001 certified ISMS that governs all aspects of information security, ensuring confidentiality, integrity, and availability. This framework is underpinned by a comprehensive suite of policies, including an Access Control and Password Policy that enforces RBAC and MFA to strictly limit system access. We adhere to a Secure Development Policy requiring peer reviews and automated testing throughout the software lifecycle, alongside a Vulnerability and Patch Management Policy that mandates regular scanning and annual CREST-accredited penetration testing to proactively address threats. To ensure robust data protection, we implement a Cryptographic Controls Policy utilising AES-256 encryption for data at rest and TLS 1.2+ for data in transit. Our operational resilience is maintained through Business Continuity and Incident Response Plans, which are tested annually. Furthermore, we align with Cyber Essentials Plus standards and GDPR requirements, conducting regular internal audits and DPIAs to mitigate risks associated with processing activities. Purple hosts customer data on Google Cloud Platform (GCP), providing three distinct regional instances dependent on customer location. These are the Netherlands, the United States (California), and Australia (Sydney). Data is stored and processed within the specific region where it is captured to maintain residency compliance. In accordance with ISO 27001 standards and internal data protection policies, customer data is logically separated and is not transferred outside of its designated region.

Backup & Disaster Recovery:

Purple protects data within its network by enforcing strict network segmentation and firewalling to isolate critical components, ensuring that database connections remain internal-only. We apply the principle of least privilege through granular Role-Based Access Control (RBAC), limiting staff access strictly to role requirements. Additionally, all data at rest, including disks and backups, is encrypted using AES-256. To further secure the environment, we utilise automated vulnerability scanning, patch management, and endpoint detection and response (EDR) agents on all compute instances to actively prevent and detect malicious activity. Complementing these protections, customer data is backed up constantly to Google Cloud, providing the capability to roll back to any point in time within the past 24 hours, with snapshots retained for up to one month. Our disaster recovery framework defines a maximum Recovery Time Objective (RTO) of four hours for service restoration and a Recovery Point Objective (RPO) of four hours for data. Adhering to ISO 27001 best practices, these recovery procedures are tested at least annually through full restoration exercises to validate system integrity and ensure that restoration capabilities align with our service commitments.

Constraints:

Maintenance windows are scheduled outside of UK business hours. Customisation of splash pages is limited to HTML/CSS standards supported by modern browsers. Exact functionality may be limited by your network vendor, authentication options or network configuration.

Standard Support Hours: Our standard technical support is available from 07:00 to 23:00 (GMT/BST), Monday to Friday, excluding UK Public Holidays.

Ordering & Invoicing:

Ordering is via the G-Cloud digital marketplace using the standard call-off contract. Invoices are issued annually in advance, payable within 30 days



Visit: www.purple.ai

Email: info@purple.ai