



IQ Intelligent System of Work Platform & Experience Description



Table of Contents

1. Intelligent Platform Level	2
1.1 Service Reliability and Access	3
1.1.1 Intelligent Platform Availability	3
1.1.2 Maintenance Windows	3
1.1.3 Backups & Disaster Recovery	3
1.1.4 Access Management	4
1.2 Data Integrations and Connectivity	4
1.2.1 Data Integrations and Connectivity	4
1.2.2 Data Processing, Location and Data Residency	4
1.2.3 Performance	5
1.2.4 Monthly Active Users	5
1.2.5 API Calls	5
1.2.6 File Storage	6
1.3 Cyber Security	6
1.3.1 Core Security Controls and Application Protection	6
1.3.2 Continuous Monitoring, Vulnerability & Patch Management	6
1.4 Compliance	7
2. Intelligent Experience Layer	7
3.1 Intelligent Chat	8
3.2 User Interface	8
3.2.1 Interface Branding	8
3.2.2 Interface Type	8
3.2.3 Interactions with IQ	8
3.2.4 Accessibility	8

This document sets out the minimum level of service to be provided in relation to the Intelligent Experience and underlying infrastructure for SaaS or hosted software (as applicable), referred to as the Intelligent Platform.

The following parameters are OneAdvanced's responsibility in the ongoing support of the Intelligent Platform:

1. Intelligent Platform Level

Capability	Essentials
Service Reliability and Access	Service Reliability and Access
Platform Availability	99.80%
Recovery Time Objective	24hrs
Recovery Point Objective	12hrs
Access Management	Username / Password + MFA + basic RBAC
Data Connectivity and Experience	Data Connectivity and Experience
Data + Processing Residency	Mutually Preferred Data Residency
Performance	Foundational Performance
Monthly Active Users (MAUs)	up to 500 MAUs
API Calls	up to 1m per 24 hrs
File Storage per Customer*	1TB
Data Integrations	x2 Catalogue Integrations
Data Connectivity	As per Intelligent Workflow
Policy Controls	N/A
Language Models	N/A

Cyber Security	Cyber Security
Core Security Controls	✓
Application Protection	✓
Continuous Monitoring	✓
Centralised Security Visibility	Standard
Activity History	Standard logs
Vulnerability remediation	Standard
Proactive Security Testing	Standard
Security Reporting	none
Customer Security Engagement	none

**In addition to any document storage available with the applicable IQ Workflow Package(s)*

1.1 Service Reliability and Access

1.1.1 Intelligent Platform Availability

OneAdvanced shall use commercially reasonable efforts to make the Intelligent Platform available 24 hours a day, seven days a week, excluding planned maintenance.

Target uptime per calendar year is determined by the Customer's Intelligent Service Tier. Essentials is the first available tier.

1.1.2 Maintenance Windows

Routine and emergency maintenance is conducted during windows of least disruption (typically 22:00 to 04:00 GMT/BST). Customers are provided with a minimum of one week's notice for all planned maintenance.

1.1.3 Backups & Disaster Recovery

Backups are performed regularly using technologies such as RDS/EC2 snapshots, Lambda, and Blob/Cloud Storage.

- Recovery Time Objective: The target duration of time within which the Intelligent Platform will be restored following a disaster recovery event.
- Recovery Point Objective: The maximum period for which data might be lost as a result of disaster recovery activities.
- Maximum Restore Period: The maximum period within which OneAdvanced will complete a Customer database restore in a production environment, as set out in more detail in the Technical and Organisational Measures Policy.

1.1.4 Access Management

The Intelligent Platform is protected by multi-layered security and identity management controls, including role-based access control (RBAC) and multi-factor authentication (MFA). OneAdvanced maintains a robust compliance portfolio aligned with applicable UK legal and regulatory requirements, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. For customers operating within health and social care settings, OneAdvanced also maintains compliance with the NHS Data Security and Protection Toolkit (DSPT).

1.2 Data Integrations and Connectivity

1.2.1 Data Integrations and Connectivity

OneAdvanced provides configurable integrations to connect with the systems your organisation already relies on, using a combination of ready-to-use and customised integrations built around your specific needs. The Essentials Tier allows you to choose up to two catalogue integrations. Available catalogue integrations can be found at <https://www.oneadvanced.com/about-us/partners/integrations/>.

Data connectivity gives Customers access to Customer data for insights, reporting and analytics dependent on the Intelligent Workflow Packages ordered and in accordance with the Performance & Experience table above.

1.2.2 Data Processing, Location and Data Residency

OneAdvanced operates three tier three (or equivalent) data centres located in geographically separate sites within the United Kingdom (UK), complemented by residency-compliant public cloud regions.

Customer data is hosted in the region aligned with the Customer's location:

- UK and Ireland customers: data is hosted within the UK and EU regions
- Australia and New Zealand customers: data is hosted within Australia.

This regional alignment ensures that data residency is preserved and that hosting remains within the applicable residency perimeter at all times.

Where AI functionality is embedded in our services, OneAdvanced selects resident AI models as a matter of design principle. For UK customers, this means UK-hosted, UK-jurisdiction models wherever operationally feasible, so that inference and any associated processing remain within the same residency boundary as the underlying Customer data.

OneAdvanced aims to provide resident data services and solutions wherever operationally feasible. Where any change to this position is contemplated, including any extension of access, hosting, or processing arrangements beyond the United Kingdom, OneAdvanced will, in the spirit of transparency, notify affected customers in advance regarding any changes, so that customers can take any necessary steps. Further detail on the artificial intelligence (AI) models we deploy, including the territory in which they are hosted and the purpose for which they are used, is published in our AI Explainability Statements.

Infrastructure includes:

- Private Cloud: Managed infrastructure within our three UK sites.
- Public Cloud: Microsoft Azure (UK South/West), AWS (London/eu-west-2), and Google Cloud Platform (GCP – London/europe-west2).

The hosting infrastructure is provisioned and administered as version-controlled Infrastructure as Code (IaC) by highly trained OneAdvanced engineers.

1.2.3 Performance

Performance is the Intelligent Platform's capacity to receive, queue, and process requests within defined throughput and latency thresholds, ensuring that Services remain consistently available and responsive under anticipated and peak demand conditions.

1.2.4 Monthly Active Users

MAUs are the number of unique users who interact with the Intelligent Platform within a calendar month. Tier limits ensure appropriate compute and resource allocation.

1.2.5 API Calls

An API call is defined as any discrete programmatic request transmitted between the Intelligent Platform and an external or internal software system, service, or component, including but not limited to data retrieval, authentication events, AI inference requests, workflow triggers, and integration handshakes.

Usage is measured at the platform level. Indicative consumption benchmarks are provided for guidance only and do not constitute a contractual commitment: a standard user profile generates approximately 100–150 API calls per 24 hours; an intensive or automated user profile may exceed 500 API calls per 24 hours. Actual usage will vary based on workflow complexity, integration depth, and AI feature adoption.

1.2.6 File Storage

File Storage provides secure dedicated capacity for content and files uploaded directly to the Intelligent Platform. This service is separate from storage used by individual software applications and from data accessed via data connectors. Files uploaded to the Intelligent Platform are stored in its dedicated file storage facility and is measured on a per Customer basis.

1.3 Cyber Security

1.3.1 Core Security Controls and Application Protection

The OneAdvanced Intelligent Platform incorporates built-in, multi-layered security controls designed to protect the platform, its users, and associated data from the point of deployment. Whilst OneAdvanced takes reasonable steps to maintain the integrity of these controls, customers remain responsible for ensuring their use of the platform complies with applicable laws and regulations, including UK GDPR, the Data Protection Act 2018, and, where applicable, the EU AI Act.

Encryption is standardised across all storage layers, utilising TLS 1.2 or above for data in transit and encryption at rest.

1.3.2 Continuous Monitoring, Vulnerability & Patch Management

OneAdvanced utilises an automated, “always-on” security lifecycle to maintain infrastructure health:

Focus	Tooling	Cadence / Action
Vulnerability Scanning	Qualys VMDR	Daily (Critical), Weekly (Full)
Infrastructure Patching	Harness + Nutanix LCM	Monthly (OS), Quarterly (Firmware)
Container Security	Trivy + Harbor	On push + Nightly
Remediation	Microsoft Defender	Immediate auto-quarantine for CVSS ≥ 9.0

Vulnerability Scanning - Intelligent Platform’s vulnerability management programme identifies, evaluates, and mitigates security vulnerabilities. We perform regular agent-based vulnerability assessments and threat analysis. Remediation efforts are prioritised based on risk severity and business impact. This approach is rigorous and provides oversight of all vulnerabilities and remediation performance.

Upgrades and Patching - Upgrades and patches are applied to Intelligent Platform and its supporting infrastructure, during pre-agreed maintenance windows. This will be communicated with as much notice as possible if essential maintenance is required outside of these periods.

Malware Protection - Intelligent Platform uses Endpoint Detection and Response (EDR) tooling across all our assets to detect, investigate, and respond to threats. This capability provides anti-malware capability while supporting a range of other protection mechanisms. We use artificial intelligence and machine learning to identify anomalous behaviour, potential malware, and sophisticated attack patterns.

Infrastructure Penetration Testing - As part of our ongoing security commitment, internal and external penetration testing is undertaken regularly. As a result of this, and other work, OneAdvanced has achieved certification in Cyber Essentials Plus.

Penetration Testing - Formal penetration testing is performed on an application-by-application basis annually by qualified third-party security specialists. Executive summaries are available to customers upon request under NDA.

1.4 Compliance

OneAdvanced is committed to meeting compliance standards and holds a variety of certifications and accreditations. These can be found on the [OneAdvanced Trust Centre](#).

2. Intelligent Experience Layer

Capability	Core
Data & AI	Data & AI
Intelligent Chat	15 Named Users
Sector Specific Agents	N/A
Build Your Own Agent	N/A
Chat Type	Enhanced Chat
Chat Connectivity with your Data	Data uploaded into Customer's Knowledge Bases
User Interface	User Interface

Interface Branding	IQ by OneAdvanced Branded
Interface Type	Software interface with menu navigation
Interactions with IQ	Browser and mobile app interface
Accessibility	WCAG 2.2

3.1 Intelligent Chat

The Intelligent Chat service utilises a private large language model; secure, trusted and hosted in the UK to maintain data residency for all users. Intelligent Chat has an emphasis on privacy; business-grade AI controls that protect data at a user, department and organisation level.

3.2 User Interface

3.2.1 Interface Branding

For the Core Intelligent Experience, the chat interface is aligned to the OneAdvanced IQ brand, giving end users a consistency across all OneAdvanced software.

3.2.2 Interface Type

For the Core Intelligent Experience, a consistent design is applied to industry standards with an intuitive to use interface with menu navigation.

3.2.3 Interactions with IQ

There are two primary methods available. Users can obtain access to the Intelligent Experience service via a web browser or through the OneAdvanced Mobile App, a React Native hybrid mobile application compatible with both iOS and Android devices.

3.2.4 Accessibility

The OneAdvanced Intelligent Experience is designed with reference to the Web Content Accessibility Guidelines (WCAG) 2.2, the internationally recognised standard for digital accessibility published by the World Wide Web Consortium (W3C). WCAG 2.2 defines criteria across four principles — that content must be perceivable, operable, understandable, and robust — against which conformance is assessed at Levels A, AA, and AAA. OneAdvanced targets WCAG 2.2 Level AA conformance, representing the benchmark required under the UK Public Sector Bodies Accessibility Regulations 2018 and referenced by the European Accessibility Act.



Powering the world of work

Our business software is the trusted choice for critical sectors, including healthcare, legal services, and education. We keep the world of work moving.

Speak to our expert consultants for personalised advice & recommendations, & get support on the products you are interested in.

Contact us

 +44(0) 330 343 4000

 www.oneadvanced.com

 hello@oneadvanced.com

OneAdvanced Group Limited is a company registered in England and Wales under company number 05965280, whose registered office is: The Mailbox, Level 3, 101 Wharfside Street, Birmingham, B1 1RF. A full list of its trading subsidiaries is available at <http://www.oneadvanced.com/legal-privacy>