

WINDOWS 365 CLOUD PC ENABLEMENT AND DEPLOYMENT

Service Definition
G-Cloud 15

REPLY

38 Grosvenor Gardens - London SW1W 0EB - United Kingdom - tel +44 (0) 207 730 6000 - fax +44 (0) 207 259 8600
info@reply.com

www.reply.com



TABLE of CONTENTS

WINDOWS 365 CLOUD PC ENABLEMENT AND DEPLOYMENT ERROR!	BOOKMARK	NOT
DEFINED.		
TABLE OF CONTENTS		2
SERVICE DESCRIPTION		3
ONBOARDING		5
OFFBOARDING		5
SECURITY		6
PERSONNEL SECURITY		6
INFORMATION SECURITY		6
PHYSICAL SECURITY		6
TRAINING & KNOWLEDGE TRANSFER		7
ORDERING AND INVOICING PROCESS		8
CUSTOMER RESPONSIBILITIES		9
ABOUT REPLY		10



SERVICE DESCRIPTION

This service provides an end-to-end capability to design, validate, and deploy Windows 365 Enterprise Cloud PCs, enabling secure and scalable access to corporate systems without reliance on physical devices. The service addresses the challenge of providing controlled, compliant desktop access for flexible workforces while reducing the cost, risk, and operational overhead associated with traditional endpoint provisioning.

We recognise that organisations often need to onboard contractors, temporary staff, and remote users quickly while maintaining strong security controls and consistent user experience. In complex environments, issuing and managing physical laptops can introduce delays, governance gaps, and increased exposure to data loss or misuse.

We provide the capability to establish a cloud-first desktop environment using Windows 365 Enterprise, aligned to organisational identity, security, and governance models. Our service supports organisations from readiness assessment through proof of concept and into production deployment, ensuring Cloud PCs are integrated with existing zero-trust access approaches and managed as part of the wider Microsoft 365 estate.

Intended audience and use cases

This service is intended for organisations seeking to replace or reduce physical device provisioning with centrally managed Cloud PCs. Typical use cases include secure access for contractors and partners; rapid onboarding for temporary or surge workforces; support for bring-your-own-device scenarios; and modernisation of end-user computing in regulated or security-conscious environments.

Scope of service

The service is delivered as a multi-phase engagement on a time-and-materials basis. The scope typically includes:

- Discovery of the Microsoft 365 tenant, identity configuration, and existing zero-trust network access models.
- Definition of Cloud PC architecture and sizing for enterprise user personas.
- Deployment of a trial-user proof of concept using Windows 365 Enterprise.
- Configuration of Microsoft Intune Cloud PC baselines and security hardening.
- Implementation of Conditional Access and identity-based policy controls.
- Alignment to existing zero-trust network access approaches.
- Application deployment modelling and persona-based validation.
- Production rollout using automated Cloud PC provisioning.
- Definition of monitoring, governance, and operational processes.
- Documentation, runbooks, and structured knowledge transfer.

The service focuses specifically on Windows 365 Cloud PCs. It does not include licence procurement, end-user device supply, large-scale application remediation, or wider Microsoft 365 tenant transformation unless agreed separately. On-premise connectivity such as VPN or ExpressRoute is assumed to exist where required and is not implemented as part of this service.

Delivery approach

We take a structured, phased approach designed to reduce risk while enabling rapid adoption. Delivery typically includes discovery and readiness assessment; solution design covering security, identity, and application access; proof-of-concept deployment with real users; and controlled production rollout.

Where appropriate, we leverage Microsoft technologies such as Windows 365 Enterprise, Microsoft Intune, Conditional Access, and Microsoft Entra ID as illustrative components of the solution. You will



typically provide access to relevant tenants, environments, and nominated stakeholders to support design validation and deployment.

Deliverables and outputs

Outputs typically include:

- A validated Windows 365 Enterprise Cloud PC design.
- A configured proof-of-concept Cloud PC environment.
- Intune baselines and security configuration for Cloud PCs.
- Conditional Access and identity policy configurations.
- Application deployment models aligned to user personas.
- Automated provisioning workflows for production rollout.
- Operational documentation and runbooks.

These outputs enable organisations to deliver secure, consistent desktop access while reducing dependency on physical devices and improving operational efficiency.

Review and acceptance

Deliverables are reviewed collaboratively through design walkthroughs, proof-of-concept validation, and production readiness checks. Acceptance is typically confirmed once Cloud PCs meet agreed security, usability, and operational expectations.

Governance and assurance

The service is delivered under project governance with defined oversight, progress reporting, and risk management. Activities are aligned to recognised Microsoft end-user computing and security best practices, with a strong focus on least-privilege access and zero-trust principles. Formal service levels do not apply.

Related services

This service can be followed by broader end-user computing modernisation, device strategy rationalisation, identity and zero-trust maturity services, or ongoing Cloud PC optimisation and enablement engagements.



ONBOARDING

New clients are onboarded through a structured process designed to ensure a smooth transition and immediate value realisation from the service. Initially, a kick off meeting is held to understand the client's specific needs, objectives, and existing infrastructure. In addition, we establish key project stakeholders, educate these stakeholders on essential concepts relevant to data platforms and we propose a way of working that outlines the collaborative effort required for successful implementation and operation. This proposed method is then jointly refined with the client to adapt it to their specific needs, ensuring that the approach is fully aligned with their operational practices and business objectives. Throughout the onboarding process, regular check-ins are scheduled to address any concerns, provide clarity on next steps, and ensure alignment with the project roadmap. This hands-on approach ensures that clients are fully supported from the outset, setting the stage for a successful partnership and seamless experience.

Offboarding

Securing a client's exit or transition to another supplier is approached with careful planning, emphasising smooth and secure service transfer. The process initiates with exit planning to understand the client's needs, including timelines and compliance requirements. Clear communication channels are established to ensure coordination. Data integrity and security are paramount, with protocols for auditing for completeness and securely purging any data from our systems post-transfer. When transitioning to another supplier, we collaborate closely to ensure technical compatibility and provide comprehensive documentation of the client's data platform. Our objective is to minimise operational disruption for the client, ensuring they maintain control and access to their data, and experience a seamless service continuity throughout the transition process. This commitment to a carefully managed exit or transition underscores our dedication to client satisfaction and data security.



SECURITY

Personnel Security

As a Specialist Cloud Service, the capability being offered is not limited to specific Impact levels (as it is not infrastructure, software or a platform) and can be used, subject to personal Security Clearance levels. Reply consultants are mostly Security Cleared (SC), some have higher-level Developed Vetting (DV) clearances. We also have a pool of NPPV3 Consultants for Policing work. The majority of our work for both public and private sector clients is at IL2 but we work in the Official, Secret and Top-Secret domains. Our hard and soft information security processes have been designed and approved by independent CESG CLAS accredited consultants.

Information Security

We are ISO27001, Cyber Essentials certified and our Quality Assurance processes are based upon and compliant with our ISO 9001 accreditation. Our Information Security processes are directly guided by our ISO27001 accreditation. We shall adhere to local information and other security policies and will apply local Security Operating Procedures (SyOPs) as may exist. If such do not exist we shall apply our own SyOPs.

Physical Security

The Main Reply Office (London, UK) is a Police Accredited Secure Facility (PASF) with access controls for each point of entry. All Laptops/Phones must be stored securely overnight. When working on a client-site our consultants adhere to client security policies.



TRAINING & KNOWLEDGE TRANSFER

This service includes structured in-flight enablement to support sustainable operation of Windows 365 Cloud PCs following deployment. We recognise that long-term success depends on internal teams being confident in managing, securing, and scaling the Cloud PC environment.

We enable client teams by working collaboratively throughout delivery. Configuration, policy definition, and operational processes are implemented transparently to support practical understanding and ownership.

Knowledge transfer is delivered through:

- Paired working with client teams during design and deployment activities.
- Walkthroughs of Cloud PC architecture, identity controls, and security configuration.
- Review of Intune management, provisioning workflows, and operational processes.
- Explanation of monitoring, governance, and lifecycle management considerations.
- Provision of documentation and runbooks to support business-as-usual operation.

Formal classroom-based training is not included within the scope of this service. Following completion, we can continue working with you to support further rollout, extended enablement, or targeted training aligned to broader end-user computing and cloud-first strategies.

This approach ensures client teams complete the engagement with a secure, governed Cloud PC capability and the confidence to operate and scale it effectively.



ORDERING AND INVOICING PROCESS

To begin the process, please contact glue.frameworks@reply.com with details of your organisation, role and high-level requirements.

Our Framework Manager will connect you to our experts and from here we will organise an introductory discussion to go into more detail and shape a proposed engagement that suits your needs.

We invoice for both fixed price and time and materials engagements one month in arrears. For fixed price engagements, this takes place upon completion of the deliverable(s), or in stages, if the size of the engagement is greater than £40,000 excluding VAT.

Payment terms are 30 days net of receipt of invoice.



CUSTOMER RESPONSIBILITIES

To ensure successful delivery of our data services, several key inputs from the customer are essential. Firstly, a clear understanding of the customer's business goals, current IT infrastructure, and specific data needs is crucial for tailoring our services effectively. Access to relevant technical documentation and systems is also required to assess the existing environment and design an appropriate data strategy. Active engagement and collaboration from the customer's IT team are vital, both for sharing insights during the planning phase and for effective knowledge transfer throughout the project. Lastly, timely feedback on deliverables and open communication regarding any changes in requirements or challenges faced are imperative for agile project management and ensuring the project remains aligned with the customer's objectives. These inputs are foundational to a successful partnership and the delivery of a solution that fully meets the customer's needs.



ABOUT REPLY

Reply is a company that specialises in Consulting, Systems Integration and Digital Services with a focus on the conception, design and implementation of solutions based on the new communication channels and digital media.

Reply partners with key industrial groups in defining and developing business models made possible by the new technological and communication paradigms such as Artificial Intelligence, Big Data, Cloud Computing, Digital Communication, the Internet of Things and Mobile and Social Networking. In so doing, it aims to optimise and integrate processes, applications and devices.

Reply's offer is aimed at fostering the success of its customers through the introduction of innovation along the whole economic digital chain. Given its knowledge of specific solutions and due to a consolidated experience, Reply addresses the main core issues of the various industrial sectors.

Through its network of specialist companies, Reply supports some of Europe's leading industrial groups in Telco & Media, Industry & Services, Banks & Insurance, and Public Administration to define and develop business models, suited to the new paradigms of Artificial Intelligence, Big Data, Cloud Computing, Digital Media and the Internet of Things.

We make innovation happen.

We started with a small team and a purpose: to help the digital revolution happen. Today, we are a team of more than 14,600 people in 16 different countries but we still have the same DNA, made up of agile, vertical task forces and an inner passion for innovation.

We are a decentralised network of specialised companies.

Among Replyers, you will find passionate geeks, visionary strategists, and creative minds, each with sharp skills in a specific business, who cooperate together and never stop learning from each other.

Make forward, act sustainably.

We know a sustainable future is possible and technology can be a strong asset to reach it. As leaders in digital transformation, we push for change and operate in full accordance with the highest ethical standards and with respect for the rights of future generations