



Claranet UK

Microsoft Intune Deployment Professional Service

Service Description v2.0

1. Introduction

This Service Description describes the service Claranet provides and details the Customer's responsibilities in relation to this Service. The Service Description forms part of the Agreement between the Parties and should be read in conjunction with the terms of the Customer Experience for Managed Services Document ("CXMS") and the Claranet Master Services Agreement ("MSA") set out at www.claranet.co.uk/legal or as otherwise agreed by the Parties and the Parties agree to be bound by such terms. Unless otherwise specified, all terms used within this document are in accordance with the terms to be found in the CXMS and the MSA. Claranet provides the following services as part of its Microsoft Intune Deployment Professional Service. The Service components and features are set out below, along with the related responsibilities for that Service component/feature.

2. Scope of Service Description

The Customer agrees that any services, activities, and deliverables not expressly set out within this Service Description shall be out of scope for the Service. Any components which are described as optional or additional in this Service Description will be chargeable at additional cost and will need to be purchased by the Customer and an Order Form or Statement of Works will need to be signed by the Customer.

Notwithstanding the foregoing, in the event Claranet completes additional services, activities and/or deliverables upon the request or at the direction of the Customer, Customer shall be responsible for the payment of all Fees and expenses associated therewith, whether or not an Order Form or Change Request has been executed.

3. Service Overview

As organisations support hybrid and remote workforces, they're challenged with managing the different devices that access organisation resources. Employees need to collaborate, work from anywhere, and securely access and connect to these resources. Admins need to protect organisation data, manage end-user access, and support users from wherever they work. To help with these challenges and tasks, Claranet advises using Microsoft Intune.

Claranet is a Microsoft Gold Partner with extensive experience delivering cloud solutions for businesses of all sizes and sectors. We have a team of certified experts who can help you design, implement, and manage Intune service according to your specific needs and goals. We can also provide ongoing support and guidance to ensure you get the most out of Intune and optimise your endpoint management strategy. Claranet is your trusted partner for Intune service and beyond.

4. Service Features

Intune is a cloud-based enterprise mobility management (EMM) service that helps enable Customer's workforce to be productive while keeping its corporate data protected. With Intune, the Customer can:

- Manage the mobile devices Customer's workforce uses to access company data
- Manage the client apps Customer's workforce uses
- Protect Customer's company information by helping to control the way its workforce accesses & shares it
- Ensure devices and apps are compliant with Customer's security requirements

Intune integrates closely with Microsoft Entra ID for identity and access control, Microsoft Purview for data protection and Configuration Manager to extend Customer's management capabilities.

4.1. Standard Features

The following table describes the features of the Microsoft Intune Deployment service in more details:

Feature	Description
Advisory & Consulting	During this phase Claranet will gain insight into: - Customer's business requirements, - current device management state - how device and application configuration are delivered to end users. After this discovery Claranet will identify how current processes and management solutions are performing and pinpoint where there are constraints in service delivery that need to be addressed.
Design & Architecture	Using Customer's business requirements, model the desired state, considering different device types, configuration and compliance policies and a migration process sensitive to timescales and risk mitigation.
Enroll users and devices	Claranet helps Customer implement Microsoft Intune to enroll both Organisational and end-user devices effectively. Our expert team assists in creating and enforcing policies for secure access to your organisation's resources across various platforms, including Android, Android Open Source Project (AOSP), iOS/iPadOS, Linux Ubuntu Desktop, macOS, and Windows client devices. Organisation-owned devices are enrolled in Intune for mobile device management (MDM). MDM is device-centric, so device features are configured based on who needs them. For example, the Customer can configure a device to allow access to Wi-Fi, but only if the signed-in user has an organisation account.
App management and protection policies set-up	Intune has a built-in app experience, including app deployment, updates, and removal. Claranet helps the Customer to: - Connect to and distribute apps from Customer's private app stores. - Enable Microsoft 365 apps, including Microsoft Teams. - Deploy Win32 and line-of-business (LOB) apps. - Create app protection policies that protect data within an app. - Manage access to apps & their data.
Automate policy deployment	Claranet helps the Customer to create and assign policies in Microsoft Intune for apps, security, device configuration, compliance, and conditional access. When the policies are ready, the Customer can deploy them to its user groups and device groups. To receive these policies, the devices only need internet access.
Use the self-service features	Claranet helps to configure and customise the Intune Company Portal apps, Company Portal website, and Intune app, so Customer's end-users can use the Company Portal app and website to reset a PIN/password, install apps, join groups with reduced number of support calls.

4.2. Additional/Optional Features

The following features can be purchased on top of the standard service and will be subject to additional charges:

Feature	Description
Advanced endpoint management and security	Microsoft offers Intune Suite as an add-on solution that offers different features, like Remote Help, Endpoint Privilege Management, Microsoft Tunnel for MAM, and more.
Endpoint Analytics Enrollment	Endpoint Analytics provides insights and recommendations to improve your devices' performance, productivity, and user experience. Intune can measure and optimise startup time, battery life, software reliability, and app usage.
Windows Autopilot Deployment	Windows Autopilot for modern OS deployment and provisioning. With Windows Autopilot, the Customer can provide new devices and send them directly to users from an OEM or device provider. For existing devices, the Customer can reimage them to use Windows Autopilot and deploy the latest Windows version.
Integrate with mobile threat defense	Claranet helps integrate Intune with Microsoft Defender for Endpoint and third-party partner services. With these services, the focus is on endpoint security. Claranet helps create policies that respond to threats, perform real-time risk analysis, and automate remediation.
Microsoft Defender for Endpoint	Microsoft Defender for Endpoint helps the Customer prevent, detect, investigate, and respond to threats. In Intune, Claranet helps to create a service-to-service connection between Intune and Microsoft Defender for Endpoint. When they're connected, the Customer can create policies that scan files, detect threats, and report threat levels to Microsoft Defender for Endpoint. Claranet also helps create compliance policies that set an allowable level of risk. When combined with conditional access, the Customer can block access to organisation resources for devices that are non-compliant.
Microsoft 365 Apps in Windows 10/11 devices with Microsoft Intune	Using Intune, the Customer can deploy Microsoft 365 apps to users and devices in its organisation, also when users sign in for the first time. Windows Management allows the Customer to manage Windows 10 and 11 devices using the same platform and interface as mobile devices. Claranet helps to deploy apps and updates, configure settings, and monitor compliance and health of Windows devices.
Intune + Microsoft Copilot Deployment	Copilot in Intune is powered by Copilot for Security. Copilot can summarise existing policies and give you more information about setting them up, including recommended values and potential conflicts. The Customer can also get device details and troubleshoot a device.
Windows Autopatch deployment	Windows Autopatch is a cloud-based service. It keeps software current, gives users the latest productivity tools, minimises on-premises infrastructure, and helps free up the Customer's IT admins to focus on other projects. Windows Autopatch uses Microsoft Intune to manage patching for Intune-enrolled devices or devices using co-management (Intune + Configuration Manager).

Third-party Customer devices and Apps Integration	Claranet offers to connect The Intune admin center to different Customer's services, including: • Managed Google Play for Android apps • Apple tokens and certificates for enrollment and apps • TeamViewer for remote assist
Windows Hello for Business deployment	Windows Hello for Business helps protect against phishing attacks and other security threats. It also helps users sign in to their devices and apps more quickly and easily. Windows Hello for Business replaces passwords with a PIN or biometric, such as fingerprint or facial recognition. This biometric information is stored locally on the devices and is never sent to external devices or servers.
A VPN connection for remote users deployment	Claranet helps to create VPN profiles to connect to VPN servers in Intune. VPN policies give users secure remote access to Customer's organisation network.

Roles and Responsibilities

The Customer, or any appointed third parties, acknowledge and agree to perform their responsibilities. Claranet's delivery, implementation and performance of the Service is dependent upon the timely and effective completion of the Customer's roles and responsibilities and/or as per Claranet's reasonable instructions. If the responsibilities as set out below are not met, and any Service Levels set out herein are impacted, Service Credits will not apply as a result:

Responsibility	Description
Provide a suitable primary contact for the length of the Service.	To ensure smooth delivery of the Service, the Customer must provide Claranet with a primary contact with the relevant knowledge and experience to provide all necessary assistance to Claranet pursuant to this Service Description and/or the SOW.
Access to support, key staff and stakeholders.	The Customer must provide key staff and stakeholders, both internal and external (where relevant), who are available for engineer visits, meetings, and/or workshops. The Customer will provide the necessary access to support and relevant personnel. However, the Customer will be responsible for ensuring all communications to all key or relevant Customer managed stakeholders regarding the Service for the duration, including any technical change and/or approval required.
Provide a safe and suitable working environment.	Where Claranet employees are required to attend Customer and/or third-party premises, the Customer must ensure that Claranet employees are provided with a safe and suitable working environment.

Provide information required by Claranet.	The Customer shall provide any information requested in the format specified by Claranet within five (5) working days, unless agreed otherwise in writing.
Responding to project requests by Claranet.	The Customer shall respond to any project-related request made by Claranet within five (5) working days. Unless agreed otherwise in writing.
Reasonable and timely cooperation	The Customer will provide reasonable and timely cooperation and follow instructions as required by Claranet.
Notifications regarding maintenance	The Customer will inform Claranet of any scheduled maintenance or emergency maintenance within reasonable notice that will affect the Service's performance is scanning, verifying, and identifying vulnerabilities within the Customer's Assets.
Changes to information	The Customer will ensure that technical details are kept up to date by submitting to Claranet to update the relevant details.

Third Party Systems and Integrations

Alongside the Service, the Customer may gain or require access to third party systems or portals, and the details of such systems and the level of access will be confirmed outside of this Service Description. Claranet shall not be liable and cannot guarantee uninterrupted access to these systems.

Note: The Customer's access may vary and may be affected by causes outside of Claranet's control, such as but not limited to, maintenance, updates or patching of third party systems by third parties or the Customer's intentional/unintentional changes to the scope, consumption or size of their Service. This may result in downtime and paused SLAs, as well as additional charges/Fees, including but not limited to, over usage charges.

Pre-Requisites

Before Claranet can commence the Services, the Customer is required to complete the following pre-requisite activities to ensure that the Services can be delivered successfully. If such pre-requisite activities are not met by the Customer, then this may have consequential adverse impact on the delivery of Services and may prevent Claranet from delivering on its obligation and/or require changes in a Change Request Form to remediate any impact.

Pre-requisite Activity

Claranet | Provide a questionnaire to gather information about the Customer's current device management state and business requirements.

Claranet | Provide a spreadsheet template for collecting details on device types, numbers, and applications used by each department or team.

Customer | Complete the questionnaire and return all information requested in the format specified by Claranet within five (5) working days to enable Claranet to deliver the Service.

Customer | Distribute the spreadsheet template to the relevant department or team heads and collect the completed spreadsheets from them within two weeks of receiving the template.

Customer | Provide Claranet with access to Azure AD and Intune Admin Access, and any other systems or platforms that are required for the setup and configuration of Endpoint Manager.

Customer | Assign a project manager or a point of contact who will coordinate with Claranet throughout the onboarding process and facilitate communication and feedback.

Customer | Review and approve the high-level approach, policies, and applications that Claranet will design and implement for Endpoint Manager based on the Customer's business requirements.

Note: In the event a Pre-requisite Activity is not completed, the delivery of Service may be delayed, quality of Service may be impacted and/or additional costs may be incurred to deliver the Services. In addition, the Service shall not be subject to the SLAs or Service Credits (if applicable) and shall be provided on a reasonable endeavours basis until the above activities are completed.

5. Delays and Cancellation Terms

1. Professional Services must be used within 6 months from the date of Customer's signature of the Order Form and at expiry of this period, Claranet may invoice the full remaining Professional Services Fees and the Customer will pay those Fees in accordance with the Agreement. Thereafter, the Customer will have a further 6 months to use those remaining Professional Services, after which they will expire on such date if unused. Unless agreed otherwise, Professional Services are non-refundable.
2. The Customer agrees and acknowledges that Claranet will estimate the time required to complete the Services and that additional days of Professional Services may be required to complete the Services. Claranet shall notify the Customer where it determines in good faith additional days are required to complete the Services and such additional days may then be authorised by the Customer in accordance with Change Request Form or an additional Order Form.
3. Notwithstanding the above, if the project is delayed or put on hold by the Customer (expressly or impliedly) after the date of signature for a cumulative period of:

- a) 1 (one) month, the project status will be reviewed for viability;
 - b) 2 (two) months, the project status and viability will be reviewed, the project will be marked as "at-risk"; and
 - c) 3 (three) months, Claranet reserves the right to cancel the project and invoice the Customer for the greater of (a) any Services delivered up to the point of such cancellation, or (b) the amount payable pursuant to Clause 4.2 of the MSA.
4. If the Customer postpones or cancels a booking (e.g. a workshop, meeting or a call) at short notice, then the following will be charged by Claranet, depending on the amount of notice given:

Notice for Postponement or Cancellation	Postponement or Cancellation Fee
Less than 15 working days but greater than 10 working days	50% of the Fees associated to the booking
Less than 10 working days but greater than 5 working days	75% of the Fees associated to the booking
Less than 5 working days	100% of the Fees associated to the booking

5. If the Customer seeks to cancel a Service/s before the expiry of the Initial Term or Renewal Term, Claranet will automatically invoice and the Customer shall pay for cancellation charges equivalent to the total Fees that would otherwise have otherwise be payable for the remainder of the Initial Term or Renewal Term of the respective Service/s, unless agreed otherwise.
6. Once the cancellation has been processed by Claranet, the Customer shall follow Claranet's reasonable instructions to decommission any hardware and to cease access to relevant systems that the Customer received as part of the Service.

6. Assumptions and Exceptions

Where relevant and to the extent any Service Levels set out herein are impacted by the below, Service Credits will not apply as a result.

1. It is assumed that where required as part of the Service, access to the Customer's IT infrastructure is quickly established and retained for the duration of the Service. Any issues relating to access and permissions may result in work being halted or delayed until such access is resolved, or cause failures in delivery because Claranet personnel are unable to access the Customer's relevant sites.
2. Where software licences are not provided as part of the Service, it is the Customer's responsibility to ensure they have the appropriate subscriptions and licences as required to benefit from the Service. The costs of such licences and subscriptions are not included in the price of the Service as set out in this Service Description unless otherwise provided in the Agreement.

3. Claranet is not responsible for any failure of any component for which Claranet has no control over, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer.
4. Claranet excludes responsibility for meeting any Service Levels to the extent that meeting the Service Level is affected by the following exceptions hereunder and Service Credits will, therefore, not be paid if the outage occurs from such exceptions:
 1. if the Customer is in default under the Agreement;
 2. in the event that the Service is unavailable due to any component, event or situation not wholly within the control of Claranet, including but not limited to a failure of a component that Claranet is not responsible, electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer;
 3. in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;
 4. in the event that the Service is disrupted or unavailable due to viruses, unauthorised users or hackers;
 5. in the event that the Service is unavailable due to changes initiated by the Customer, whether implemented by the Customer or by Claranet on its behalf;
 6. in the event that the Service is unavailable as a result of the Customer exceeding system capacity;
 7. in the event that the Service is unavailable due to viruses, not arising from the failure or breach of Claranet or Claranet's Service;
 8. in the event that the Service is unavailable due to the Customer's failure to adhere to Claranet's implementation, support processes and procedures;
 4. in the event that the Service is unavailable due to the acts or omissions of the Customer and its employees, agents, contractors or otherwise;
 5. in the event that the Service is unavailable due to Customer's third party contractors or vendors or anyone instructed by the Customer gaining access to Claranet's network, control panel or to the Customer's website at its request;
 6. in the event that the Service is unavailable due to a force majeure event;
 7. in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;
 8. in the event that the Service is unavailable due to the Customer's negligence or wilful misconduct or of others authorised by the Customer to use the Services provided by Claranet;
 9. in the event that the Service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer;
 10. in the event that the Service is unavailable due to any failure of local access facilities provided by the Customer;
 11. in the event that the Service is unavailable due to the Customer's negligence or wilful misconduct of the Customer or others authorised by the Customer, to use the Services provided by Claranet;

17. in the event that the Service is unavailable due to any failures that cannot be corrected because the Customer are inaccessible or because Claranet personnel are unable to access the Customer's relevant sites;
18. the Customer's failure to adhere to Claranet's implementation, support processes and procedures;
19. any failure of local access facilities provided by the Customer;
20. any periods of scheduled maintenance or emergency maintenance; and
21. unauthorised users or hackers, or due to any violations of Claranet's Acceptable Use Policy.

5. Terminology

Unless otherwise specified, capitalised terms used in this Service Description shall bear the same meanings as those used in the Master Service Agreement, unless otherwise expressly stated herein. Set out below are a description of key technical terms used in this Service Description.

Terms	Definition
Customer Experience for Managed Services (CXMS) Document	The CXMS document provides a framework for Claranet's core managed support experience and describes what a customer can expect from any standard Managed Service provided by Claranet. It outlines Claranet's and the Customer's responsibilities, including how to log and escalate cases, how SLA targets are prioritised, set, and achieved, and the tools used to perform these functions.
Enterprise Mobility Management (EMM)	A set of services and technologies designed to secure company data on employees' mobile devices.
Mobile Application Management (MAM)	Focuses on securing corporate data at the application level on both company-owned and personal devices.
Mobile Device Management (MDM)	A type of security software used by an IT department to monitor, manage, and secure employees' mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems.
Azure Information Protection	A cloud-based solution that helps an Organisation to classify and optionally, protect its documents and emails by applying labels.
Configuration Manager	A management tool developed by Microsoft for managing large groups of computers, including those running Windows, macOS, Linux, and Unix.

Endpoint Analytics	Provides insights and recommendations to improve device performance, productivity, and user experience.
Windows Autopilot	A collection of technologies used to set up and pre-configure new devices, getting them ready for productive use.
Microsoft Defender for Endpoint	A platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.
VPN (Virtual Private Network)	A service that encrypts your internet traffic and protects your online identity.
Windows Information Protection	Helps to protect against potential data leakage without otherwise interfering with the employee experience.
Microsoft Entra ID	Provides identity and access management solutions, helping to secure access for every user, device, app, and relationship.