



## **Intune Advanced Integration Service**



# Advanced Integration Service

Comprehensive Device Management with Enhanced Features and Automation

## Service Overview

The Advanced Integration Service is designed for organizations that need a comprehensive solution to manage a wide range of devices including Windows, macOS, iOS, Android, and Linux using Microsoft Intune. This service includes advanced management, security, and compliance features, ensuring that your entire IT infrastructure is optimized, secure, and ready to scale with your business needs

## Why choose Advanced Integration?

- **End-to-End Management:** Leverage advanced management features to optimize and control your IT environment effectively
- **Tailored Flexibility:** Our solution is designed to adapt to your specific business needs, providing you with the control and flexibility to manage your IT infrastructure seamlessly

## Why choose Reply?

- **Advanced Expertise and Customization:** Reply brings deep expertise in device management, delivering tailored solutions that address the unique complexities of managing a diverse IT environment. Each integration is customized to ensure that your organization's specific requirements are met with precision
- **Seamless Integration and Long-Term Scalability:** With a focus on seamless integration, Reply ensures that your device management setup is both robust and scalable, allowing your IT infrastructure to grow and adapt effortlessly as your organization evolves

## The Result

- Unified Device Management:
- Enhanced Security
- Customized User Experience
- Comprehensive Compliance
- Streamlined Application Deployment & Management
- Optimized IT Operations

## Key Components

- Intune Setup
- Cross-Platform Device Enrollment
- Security Settings
- Advanced Configuration Profiles
- Advanced Compliance Policies
- Automated Patch Management
- Microsoft Defender Deployment (Configuration is not included)
- Application Deployment (Up to 10 Applications)
- Autopilot Deployment
- Role-Based Access Control (RBAC)
- Conditional Access Policies

## Requirements

- Microsoft Intune License (Microsoft 365 E3/E5 or EMS E3/E5)
- Azure Active Directory (on-premises or Azure AD)
- Microsoft Defender for Endpoint (optional, for advanced security)
- IT Manager / Stakeholder

## Effort / Price (blanket price)

- Up to 500 Devices = 60 days by 53000.- € plus tax
- Up to 1000 Devices = 80 days by 69500.- € plus tax
- Larger packages to be discussed



# Advanced Integration Service

## Assessment and Planning

Explore the advanced capabilities of our Advanced Integration Service, designed to deliver comprehensive device management with enhanced security, compliance, and automation, ensuring your IT infrastructure is both robust and flexible to meet growing business needs.

### End-to-End Management:

- **Cross-Platform Device Support:** Manage Windows, macOS, iOS, Android, and Linux devices with enhanced management features
- **Unified Management Console:** Oversee all devices from a single, integrated platform, simplifying administration and ensuring consistency

### Enhanced Security Features:

- **Advanced Security Policies:** Implement comprehensive security policies that adapt to the latest threats and organizational requirements
- **Microsoft Defender Integration:** Deploy Microsoft Defender for advanced threat detection and response, ensuring all endpoints are secure. Configuring Microsoft Defender is not included in the package

### Customization and Flexibility:

- **Tailored Solutions:** Customize the integration to fit the unique needs of your business, from specific security configurations to specialized compliance requirements
- **Scalability:** Easily scale the solution as your business grows, whether managing 500 or 10,000 devices



# Advanced Integration Service

## Implementation Process

Our implementation process for the Advanced Integration Service is structured into detailed phases, ensuring a seamless transition while maximizing security and efficiency.

### Assessment and Planning:

- **Comprehensive Evaluation:** Conduct a detailed assessment of your current IT environment, identifying potential risks and areas for improvement
- **Strategic Planning:** Develop a tailored plan that addresses your organization's specific security, compliance, and management needs, ensuring a smooth deployment

### Deployment Phases:

- **Phase 1: Intune and Defender Setup:** Configure Microsoft Intune, RBAC and integrate Microsoft Defender across devices for unified management and advanced security
- **Phase 2: Device Enrollment and Policy Implementation:** Enroll devices across all platforms and deploy advanced security and compliance policies tailored to your organization
- **Phase 3: Application and Autopilot Deployment:** Deploy critical applications and use Windows Autopilot to automate device setup, ensuring a streamlined and consistent deployment across all users
- **Phase 4: Full Deployment:** Complete deployment with ongoing monitoring and adjustments

### Support and Training

- **Ongoing Support:** Receive continuous support during implementation
- **Training Resources:** Offer in-depth training and resources for your IT staff, ensuring they are fully equipped to manage the new systems

