

Device Management

2-Week Assessment

Simplify user experience and maintain security standards across every device in Microsoft 365.

Overview


Does your team work remotely, from multiple locations and across a variety of devices?

If so, you're probably familiar with the challenges of this working model, particularly when it comes to managing and securing company devices. These challenges can be resolved in Microsoft 365, using tools like Intune and Enterprise Mobility + Security suite to manage all devices and applications securely.

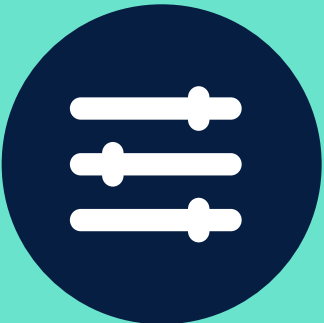
Getting it right requires careful consideration and implementation. That's where Ogi Pro can help. During this two-week engagement, our friendly experts will simplify device management for your organisation, helping you adopt best practices and choose the appropriate licenses to manage device and application security across a range of platforms and user scenarios.




Key benefits




Streamline and simplify user experience across multiple devices




Implement a baseline standard configuration for all users on setup – ideal for new starters and hybrid workers



Unify updates across all enrolled devices, and easily lock down devices when lost or stolen to prevent unauthorised access



Demonstrate professional security policies in the event of an audit or security breach



Provide central control for remote users and devices, while also enabling flexible BYOD policies

This engagement includes:

- Active Directory/Entra ID integration
- Device management options built into Microsoft 365 services
- Device management using Intune
- Mobile application management
- Defender for Windows 10/11
- Advanced threat protection
- Cloud app security
- Integrations with third party management platforms (Android, iOS, MacOS) and tools (e.g. Samsung Knox)

Complementary add-ons for this engagement include:

- Identity management
- Securing content in SharePoint and OneDrive

Scope

This engagement is focussed on Device and Application Management in Microsoft 365. The intention is to keep the scale and complexity of the Engagement to a minimum in order to quickly provide the defined benefits to the customer and end-users. For larger, more complex organisations the engagement can be run multiple times with a new set of user stories or success criteria.

Examples of circumstances where this may be appropriate are:

- Separate engagements for devices management/ application management
- Separate engagements based on device types or user scenarios e.g. all Windows devices first, or a separate exercise for BYOD

Assumptions

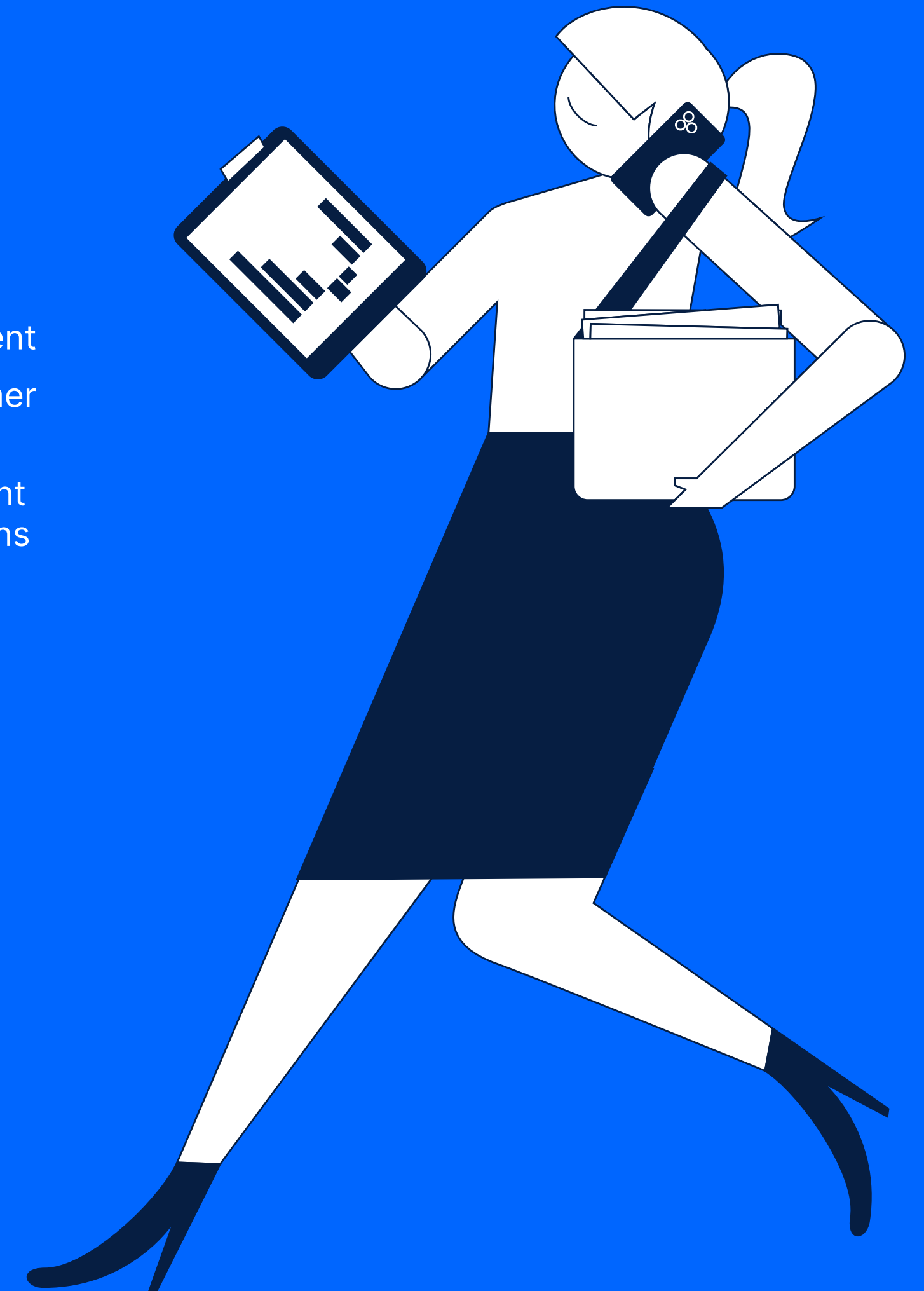
This engagement is designed based on the following assumptions:

- The customer already has a Microsoft 365 Tenant in place
- Ogi will be provided with delegated admin access as a Microsoft Partner for at least the duration of the engagement
- For Hybrid Identity environments Ogi will work with Customer IT Teams to ensure prerequisites are in place
- Any additional licensing required to support the engagement can be provided by Ogi as a Microsoft Direct Cloud Solutions Partner.
- Workshops and non-disruptive implementation work will be carried out during standard business hours

Exclusions

- Upgrade of on-premise solution software/hardware if required as a prerequisite
- Migration of non-Microsoft users onto Microsoft 365 platform
- Migration of any other workflows to support the roll-out of the device and application management solution

Ogi are able to assist with many excluded items through other pre-defined engagements such as those covering Microsoft 365 Migration, Identity Management and Content Management.



Structure

All Ogi Cloud Engagements have a consistent structure designed to deliver customer-value against a set of agreed success criteria. These are measurable and unique to each customer, driven by their priorities, organisational culture, and mission. Our approach is based on Microsoft's Service Adoption Framework and consists of three main stages; Envision, Implement, and Enable.



Envision

In the Envision stage we determine with the customer the required scope of the engagement and establish the necessary involvement from interested parties and stakeholders. This is typically conducted through a workshop session which can be in-person or remote.

It will cover:

- Exploring customer requirements/drivers including security requirements
- Review of existing environment including device types in use and existing device management solutions
- Define scope and user scenarios (e.g. BYOD, fully managed, need for conditional access restrictions)
- Advise our recommended settings for configuration and compliance policies following best-practice
- Review of built in tools from Microsoft 365 – features and limitations
- Review of additional tools provided by Intune/EMS and the various licensing models
- Agree a strategy for delivering and maintaining device management going forward including identifying required licensing/feature options.
- Identify customer champions, to encourage successful service adoption

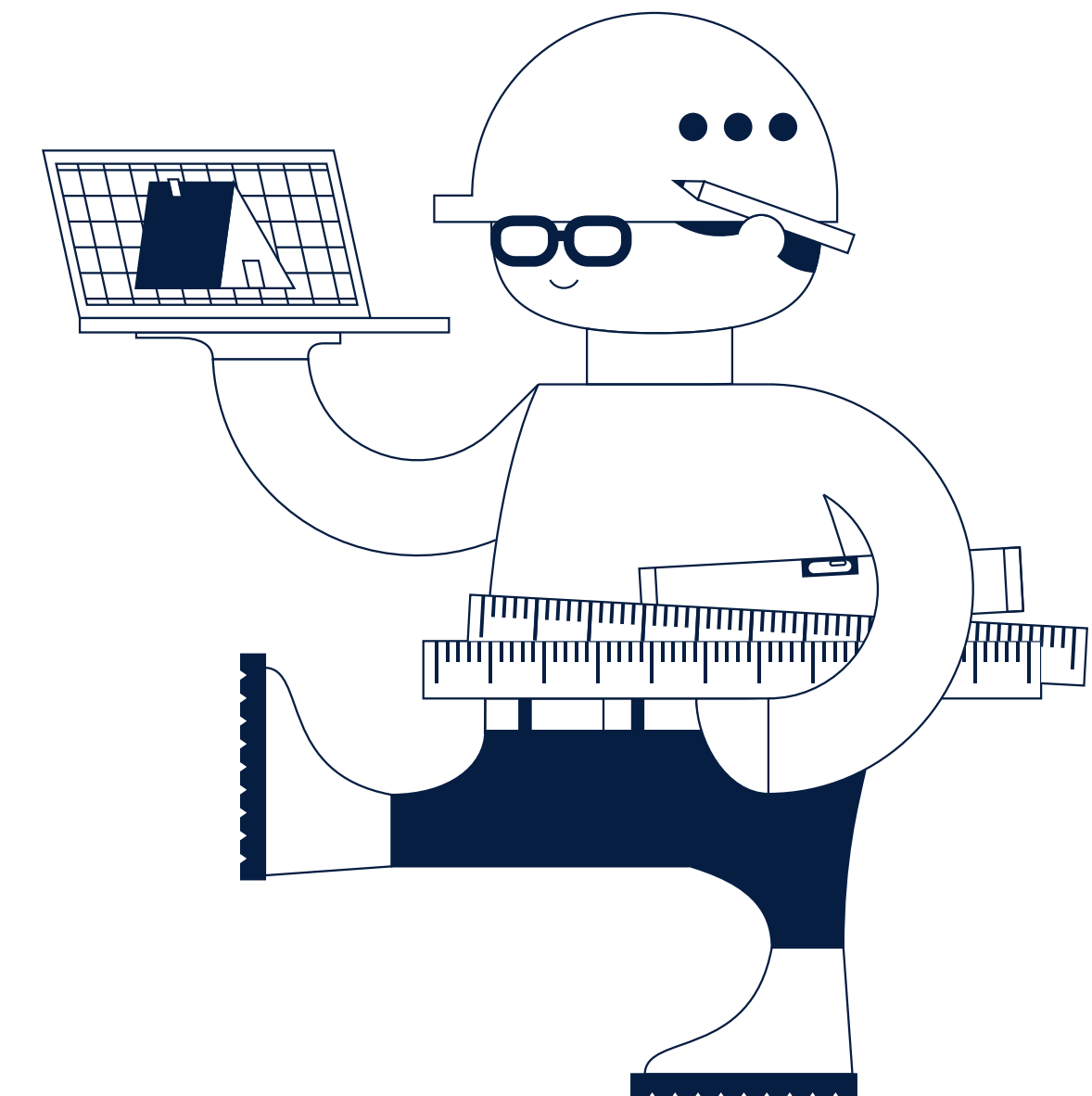
Duration:

Typically half-day session led by Service Adoption Specialist with Senior Cloud Engineer. Implementation plan typically follows on within two weeks.

Key outputs:

Implementation plan covering:

- Agreed policies/best practice changes to be made
- Agreed scope and device scenarios (e.g. BYOD, fully managed)
- Agreed scope for application management and restrictions
- Roll-out timetable
- Agreed end-user training requirements



Implement

This stage typically takes place over 2-4 weeks and is focussed on delivering the Implementation plan agreed in the previous stage. This plan will outline the key objectives to be delivered, with a clear scope and defined success criteria. Due to the possible variety of customer environments the implementation stage can also vary considerably between engagements however most will contain the following elements.

Initiation

- Confirm prerequisites are in place
- Establish licensing
- Setup basic environment

Device enrolment

- Configuration of AutoPilot where appropriate
- Configuration of Android Enterprise where appropriate
- Configuration of iOS Business Manager where appropriate
- Integration with third party solutions where appropriate (e.g. Samsung Knox)
- Enrolment of Pilot group devices or all devices depending on scale/scope

Policy creation

- Create compliance policies for each device type/usage scenario (draw in best practice)
- Created configuration policies for each device type/usage scenario
- Create application protection policies for each user scenario/profile
- Create conditional access policies for each usage scenario/user profile

Note: Ogi follow best-practice models established for each device type based on advice from security centres of excellence, e.g. NCSC, GCA).

Compliance testing/review

This element ensures that devices are enrolling correctly and that policies are being applied as expected. At the completion of this stage there should be 100% compliance.

Duration

Typically 2-4 days of Cloud Engineer time spread across 2-3 weeks with customer-lead and user champions involved in any User Acceptance Testing (UAT).



Enable

This final stage is led by the Service Adoption Specialist. While nominally following on from the Implement stage there is often an element of parallel working to ensure lessons-learned during UAT are captured and integrated into user-facing materials. This stage includes the following key activities/deliverables:

User training

This element is optional and can cover:

Training end-users in use of specific features e.g. self-enrolling devices

Training customer support team in administration of endpoints and use of monitoring and reporting tools

Documentation and handover

Device management policy documents (optional)

Where the customer has a requirement for providing documentation to support compliance standards such as ISO 9001/ISO 27001, we can assist with this by providing appropriate templated policy documents.

User guides

Develop appropriate user guidance for common device/application management tasks as required.

Handover

Typically in the form of a meeting/video conference and consists of brief review of the implementation plan to ensure all success measures have been met and that the customer is satisfied with the outcome. This is also an opportunity to confirm how the solution will be maintained in the future.

Duration

Typically 1-2 days of Service Adoption Specialist/Cloud Engineer time spread across 2-3 weeks with customer-lead and user champions assisting with onboarding and training.

Agenda timeframe

(Accelerated – actual depends on customer involvement)

Week 1

Day 1 Envision session and produce outputs

Day 2 Produce and agree implementation plan

Day 3 Implement initial best-practice/policies
 Implement active directory connector/password write back etc.

Days 4/5 Enable early adopters and test

Week 2

End-user engagement and wider deployment



Let's hold a no obligation discovery call to see how we can help.

029 2002 0535

pro@ogi.wales



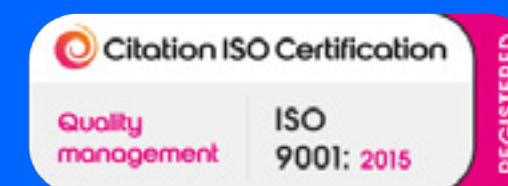
Crown
Commercial
Service
Supplier



Certificate No. 364832021



Certificate No. 345842020



Certificate No. 166022021



Ogi is a trading name of Spectrum Fibre Ltd. Registered in England and Wales No. 1288320. Registered office: Ty Ogi, Hodge House, 114-116 St Mary Street, Cardiff CF10 1DY. Phone: +44(0) 2920 0535