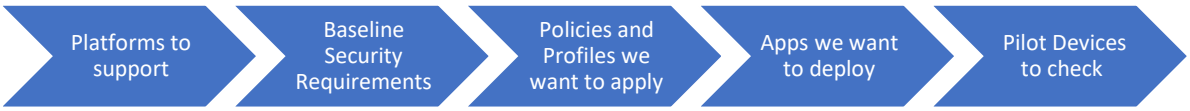
INTUNE Deployment Plan

Pre-Flight Checklist



a. Determine Platforms that we will support

- iOS/Android
- Mac/Windows

b. Have baseline security requirements complied that we want to implement

- Min/Max OS versions
- Password Requirements
- Encryption Enabled

c. Determine if there will be separate groups for security policies (*create 365 or security test groups for piloting*)

d. Assess if there are any apps beyond 365 that we want users to have access to

e. Choose pilot devices to enroll into Intune

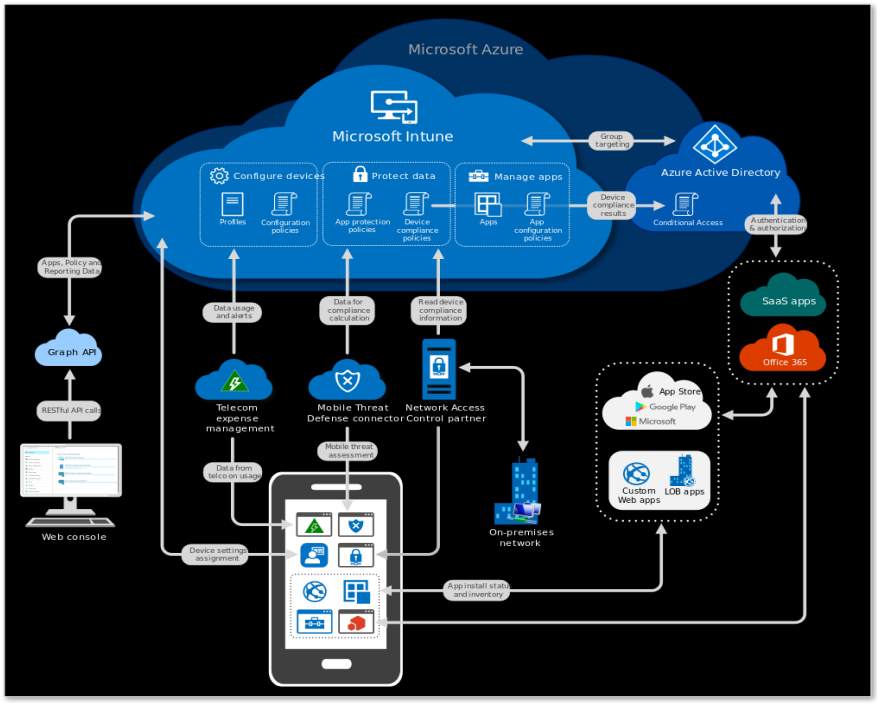
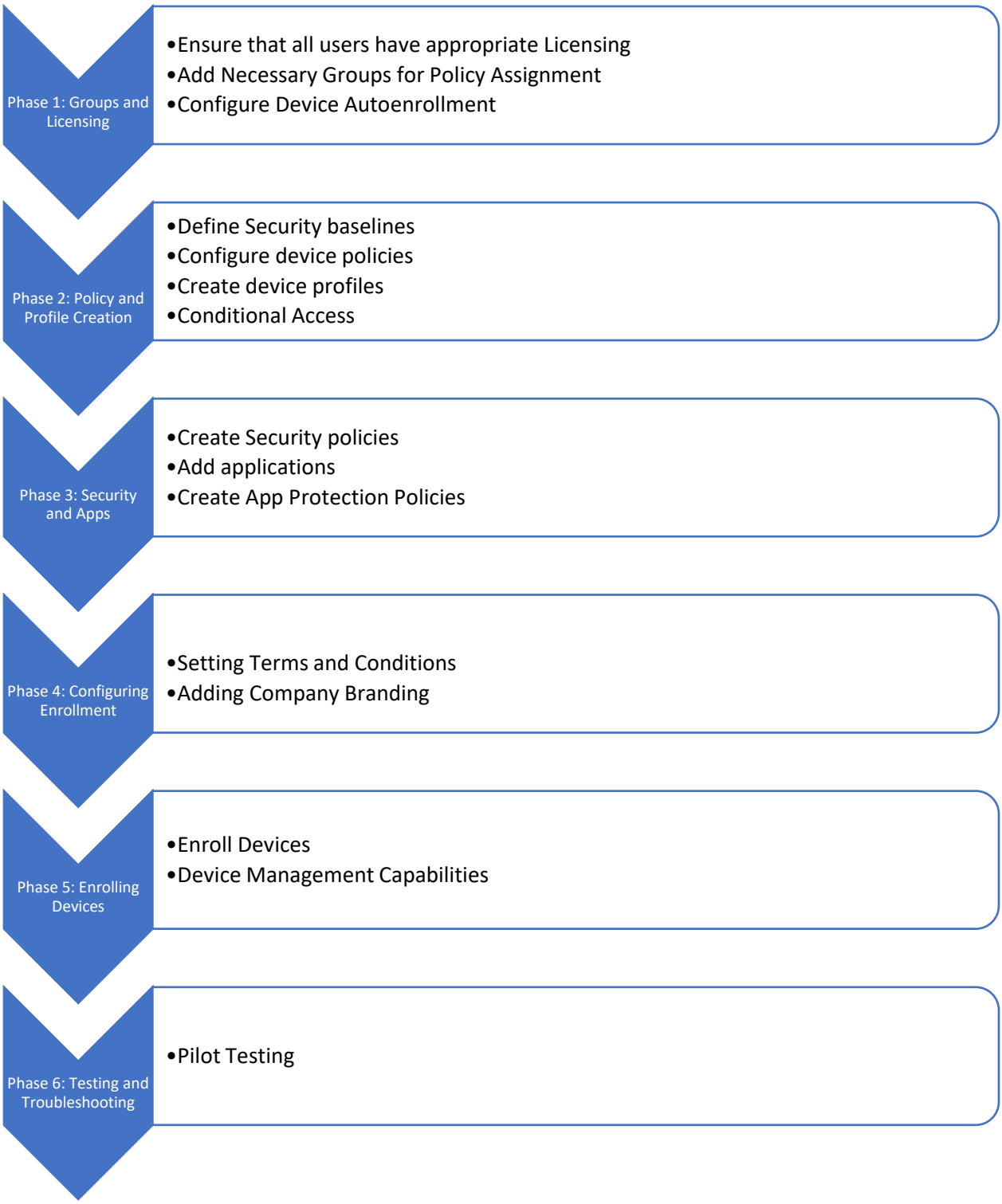


Table of Contents



Phase 1

Licensing Users: Ensure all appropriate users are licensed

Create Groups: Create different groups if we want to separate out different people into different Intune Polices

Device Autoenrollment: Ensure Device Autoenrollment is Turned On, it allows devices that join to Azure AD to automatically be enrolled in Intune and have policies push down to them

Phase 2

Configure Device Policies: Designate which devices are compliant and non-compliant. When we join devices to Intune after configuring these policies, we can check why the devices are not compliant. We will create a device policy for every platform we support in our organization

Create Device Profile: It allows us to have uniform settings for all devices across our organization Ex. We can set up a profile for Bit locker so that users are immediately prompted to configure if they do not have it already

Conditional Access Policies: For granular access control and securing corporate data

Phase 3

Create Security policies: Antivirus with Microsoft Defender, Firewall policies: Inbound and Outbound rules can be configured, Disk encryption (Bitlocker) for Windows and MacOS platform will be configured

Add required applications: When users enroll, they can download from Company Portal App, or apps can be required and automatically installed without end user interaction Ex: M365 Suite, LOBA, Win32 apps

Create App Protection Policies: Create policies to protect Corporate Data

Phase 4

Setting Up Terms and Conditions: As an Intune admin, we can require that users accept our company's terms and conditions before using the Company Portal to enroll devices and access resources like company apps and email.

Add Company Branding: Company Branding allows us to label the end user experience when they are enrolling their device to Intune. This applies to both existing devices that are just now enrolling and OOBE for new devices.

Phase 5

Enroll Devices: Windows: *From Access work or school → Join this device to Azure AD → Enter Credentials → Click join*

Enroll Devices: MacOS: *Install a Company Portal(.pkg file) → Enter Credentials → Download and Install the Management profile*

Enroll Devices: iOS and Android: iOS and Android device enrollment can be completed by downloading the Intune Company Portal app from the App Store or Google Play Store

Device Management Capabilities: See reports on users and devices, explore wipe options, remote wipe if devices are lost, enforce encryption, MFA and Antivirus

Phase 6

Pilot Testing and Remediation: During our Pilot we want to discover

- Common FAQs
- whether we need to tighten or loosen our policies
- End User Experience for Communications to Broad audience
- Common Troubleshooting Techniques for each platform

About Us

NewWave Computing Pvt Ltd is a leading Systems Integrator and IT Infrastructure solution provider focused on empowering organizations with its innovative IT product, solutions & services portfolio, both on-premises and cloud. Having started its operations in 1999, the organization with its mission 'Passion for Success' (clients success) has a proven track record of delivering predictable & sustainable IT solutions and services that drive business outcomes for Organizations.

The Suite Of Solutions That We Bring To Our Customers Would Not Be Possible Without The Backing And Support Of Our Principal Product Partners.