wanstor

Microsoft Intune and Windows Autopilot

Service Description

Confidentiality and copyright

EXECUTIVE SUMMARY

Intune and Autopilot are part of the Microsoft Enterprise Mobility + Security (EMS) suite, this suite of products is designed by Microsoft to be an intelligent mobility management and security platform. These products help protect and secure your organization and empower your employees to work in new and flexible ways.

The EMS suite consists of 4 pillars:

- **Identity and access management** - Ensure secure connections between people, devices, apps, and data. Increase your security and productivity with a single, holistic identity solution that gives you flexibility and control.
- **Information protection** - Protect your sensitive data everywhere, even in transit and when shared. See and control how files are used with a comprehensive and integrated information protection solution.
- **Threat protection** - Detect and investigate advanced threats, compromised identities, and malicious actions across your on-premises and cloud environments. Protect your organization with adaptive, built-in intelligence.
- **Cloud security** - cross-cloud protection with Microsoft cloud security solutions.

Microsoft Intune

As most organizations increase usage of cloud services and adopt the approach of allowing personal devices (such as mobile devices), continuous software updates, access to data, protection of resources, and cybersecurity become a concern.

Modern workplace technology has evolved changing the landscape that not only includes corporate networks with legacy apps but new cloud-managed and SaaS apps.

Access to data needs to be secure and seamless not only with corporate-owned devices but with personal devices such as Phones, Tablets, and Laptops.

Therefore, a modern workplace must accomplish the following:

- Support for a diverse mobile environment that is securely and centrally managed.
- Ensure flexible compliance technology for devices and apps meeting company security requirements.
- Ensure all company services are easily available to staff on all devices that meet compliance.
- Create a distribute digital policies that keep organizational data safe on all compliant personal and corporate-owned devices.
- A centralized, mobile solution that enforces these digital policies and helps manage users, groups, apps, and devices.
- Protect and control the way your workforce accesses and shares its data.

Wanstor implements its management infrastructure based on Microsoft's Endpoint manager that provides IT services, apps, protection, and configuration, which combines these services and tools in one location.

Intune deployment process

- **Determine endpoint management objectives**: access apps and email, secure access on devices, and keep organization data inside the organization.
- **Inventory device endpoints**: Organizations have a range of devices, including desktop computers, laptops, tablets, and mobile phones. These devices can be owned by the organization, or owned by users. When planning a device management solution, consider every device that will access your organization's resources, including users' personal devices.
- **Determine endpoint management licensing**: Managing endpoints with Microsoft Endpoint Manager involves using a number of technologies. These technologies require your organization to purchase plans that provide the appropriate licenses involved in managing all endpoint management aspects.
- **Review existing endpoint management policies and infrastructure**: Many organizations have existing policies and device management infrastructure that's only being "maintained".
- **Create an endpoint management rollout plan**: Your endpoint management rollout plan identifies the organizational groups and time frames you want to target, the rollout phases for each group, and the enrolment approaches you will use.
- **Determine endpoint management communication**: good change management relies on clear and helpful communications about the upcoming changes.
- Prepare endpoint management support and service desk
- Sign up for Intune: register Intune on your AAD subscription
- **Configure Intune tenant domain name**: When your organization signs up for Intune. You're given an initial domain name hosted in AAD. If you have not added a custom domain, this needs to be completed.
- **Add users to Intune**: Once added, you can grant permissions and assign licenses to users. (If you have an on-prem AD, set up directory synchronization using AD Connect).
- Add groups to Intune
- **Assign licenses to users**: Microsoft Intune is available for different organization sizes and needs, from a simple-to-use management

experience for schools and small businesses, to more advanced functionality required by enterprise customers.

- Set the MDM authority.

Windows Autopilot

Before a device is enrolled with Intune, you may need to provision the devices. As part of the provisioning process, the user signs in to the device and steps through the process of connecting to your organization.

If you are currently using image-based provisioning to install a specific configuration to a device, you should consider modern provisioning going forward.

Modern provisioning provides the following benefits:

- Decrease overall costly IT workloads by autogenerating the creation of each device image.
- Provide self-service provisioning directly by end-users.
- Provides faster time to productivity to end-users.
- Increases out-of-the-box security.
- Lowers operational expenses.

To provision Windows devices using modern provisioning, Wanstor uses Windows Autopilot.

Windows Autopilot simplifies enrolling devices in Intune reducing the building and maintenance of customized operating system images which is inherently a time-consuming process.

With Microsoft Intune and Autopilot, you can give new devices to your end-users without the need to build, maintain, and apply custom operating system images to the devices.

When you use Intune to manage Autopilot devices, you can manage policies, profiles, apps, and more after they're enrolled.

Autopilot deployment process

- **Configure Azure Active Directory automatic enrolment**: allows your end-users the ability to register devices.
- **Configure Azure Active Directory custom branding**: customizes the devices with company logos and wallpapers.
- **Optional**: To automatically step up from Windows Pro to Windows Enterprise, enable Windows Subscription Activation.
- **Complete device registration**: Devices are added to Windows Autopilot to support most Windows Autopilot scenarios. (POC will enable up to 5% of devices in the company).
- **Dynamic Security Groups**: Create required groups to automatically apply all configurations to autopilot-enabled devices based on group tags.
- **Deployment profile configuration**: Once devices have been added to Windows Autopilot, a profile of settings needs to be applied to each device.
- **Configure Intune connector for Active directory**: for hybrid deployments, this additional step allows devices the ability to join your on-premise active directory domain.
- **Configure domain join configuration profile**: part of the hybrid domain join process.
- **Configure default applications**: O365, Edge, Chrome, and Adobe reader.
- **Enrolment configuration**: The enrolment status page appears during the initial device setup and during the first user sign-in.
- Deployment to the POC devices
- Documentation

Project deliverables

Project planning and discovery - 1 Day

- Ensure prerequisites have been met and are in line with project objectives.
- Complete an initial discovery of the current M365 environment (including workstations), and document what currently exists, including changes required or new tasks needed.
- Review project deliverables and changes based on discovery.
- Schedule project resources and book in days
- If required sign up for Microsoft Intune and configure Intune tenant domain.

Prepare the environment – 1 Day

- Add users to Intune
- Create required security groups for Intune and autopilot
- Add and configure required licenses for users
- Grant admin permissions for Intune (Customer onsite Support staff)
- Confirm MDM authority configuration

Deploy MDM, Autopilot and increase security controls – (MDM 3 Days, Autopilot 2 Days)

- Configure security baselines
- Configure account protection policies
- Configure app protection policies
- Configure configuration profiles
- Configure scripts
- Configure compliance policies (Windows, Android, and Apple)
- Configure conditional access rules (reporting only)

Additional options

Configure conditional access (enforcement mode – 1 hour per device)

By configuring Conditional Access policies, you can maintain control over how and where your company data is accessed, making your business more secure. You can define the exact criteria for who can gain access and block those who don't meet the criteria.

This can be based on factors like the type of device, application accessing the data, and location. Conditional Access enables Zero Trust security, helping you provide this access while maintaining control over "where, when, and who" is connecting to your Office 365 environment; so, you can protect company assets while also enabling employees to be productive from anywhere securely.

Enrol existing devices to Intune and Autopilot

Onboarding tasks for existing devices via Autopilot, or manually, Wanstor will handle the onboarding of existing devices by means of bulk enrolment, using provisioning packages or group policy, and helping our customers onboard BYOD devices using the company portal.

- **Domain joined devices** - (1 Day, 1 hour per 10 devices)
- **Azure AD only join** - (1 hour per 5 devices)

Prerequisites

Intune requirements:

- You can manage devices running operating systems on the following platforms:
  - Apple iOS/iPadOS
  - macOS
  - Android
  - Android Enterprise
  - Surface Hub
  - Windows operating systems (professional and above)
- **Intune network configuration requirements**: To ensure devices receive the updates and content from Intune, they must periodically connect to the Internet.
- **Global Administrator access**: To set up Intune, global admin access is required.
- **Hybrid Join** – For connection to existing on-premises active directory forests, the latest version of Azure AD connect.
- **For existing devices** that are domain-joined, a VPN is required for each device.

Autopilot requirements:

- **Azure Active Directory** Tenant
- Verify AAD Premium Subscription
- **A supported MDM service** such as Microsoft Intune
- **Supported versions of Windows 10** (Pro, Pro for Education, Pro for Workstation, Enterprise, Education).
- **Supported versions of Windows 11** (Pro, Pro Education, Pro for Workstations, Enterprise, and Education)

- **Device Registration**
  - Registration can be with an OEM (OEM can automatically register devices to Autopilot),
  - Reseller, distributor, or partner registration.
  - Automatic registration via the MDM platform
  - Manual registration
- Windows Autopilot depends on a variety of internet-based services. Access to these services must be provided for Autopilot to function properly. **Review networking requirements here.**
- **Company Branding:**
  - Sign-in page background image of size: **1920x1080px** and less than **300KB**.
  - Banner logo image of size: **280x60px** and a max of **10KB**.
  - Square logo image of size: **240x240px** and a max of **50KB**
  - Dark theme square logo with the same requirements as the square logo.
- To provide needed Azure Active Directory (automatic MDM enrolment and company branding features) and MDM functionality, one of the following subscriptions is required:
  - Microsoft 365 **Business Premium** subscription
  - Microsoft 365 **F1** or **F3** subscription
  - Microsoft 365 **Academic A1**, **A3**, or **A5** subscription
  - Microsoft 365 **Enterprise E3** or **E5** subscription, which includes all Windows clients, Microsoft 365, and EMS features (Azure AD and Intune).
  - Enterprise **Mobility** + **Security E3** or **E5** subscription, which includes all needed Azure AD and Intune features.
  - **Intune for Education** subscription, which includes all needed Azure AD and Intune features.
  - **Azure Active Directory Premium P1 or P2 and Microsoft Intune** subscription (or an alternative MDM service).

Hybrid requirements:

- Line-of-sight to on-premise domain controllers when staff setup using Autopilot or VPN pre-login for connectivity.
- Server 2016 for Intune connector for Active directory
- Domain Administrator access to the on-premise domain controllers.
- Intune licensed administrator