Intune Managing Mac

<https://techcommunity.microsoft.com/t5/microsoft-intune-blog/now-is-the-time-manage-your-mac-endpoints-with-microsoft-intune/ba-p/3974449>

**Enhancing secure productivity**

**User-centric features**

Streamline the process of setting up and working securely with a Mac in the enterprise environment.

* Single sign-on (SSO) reduces password fatigue and simplifies device setup.
* Microsoft Entra ID passwords can be used to log in to Mac (estimated Q1 2024).
* Exclusive to Intune, SSO can also pre-configure user accounts in Office apps (including Outlook, Microsoft Edge, and Safari).
* SSO enables conditional access to company resources, eliminating the need to launch the Intune Company Portal app and making the experience simpler and faster while reducing costs and time.
* Reducing a confusing step and multiple passwords, local primary account creation during provisioning will be automated (estimated Q1 2024).
* Apple-native apps are optimized for Apple processors: Microsoft Teams, Microsoft Edge, Office apps, Microsoft Defender, Company Portal, and the Intune agent.
* [Remote Help for macOS](https://learn.microsoft.com/mem/intune/fundamentals/remote-help-macos) is part of the Microsoft Intune Suite or available separately as an Intune add-on.

**Admin-centric features**

Comprehensive management in a familiar interface.

* [Declarative Device Management (DDM) protocol-capable](https://learn.microsoft.com/mem/intune/protect/software-updates-macos#configure-the-policy).
* [Configure SSO with a simple user interface](https://learn.microsoft.com/mem/intune/configuration/use-enterprise-sso-plug-in-macos-with-intune?tabs=prereq-intune%2Ccreate-profile-intune).
* SSO improves security by using platform hardware to bind secrets.
* Provision users’ apps from Intune—SSO can be expanded to additional apps.
* [Simple interface to support pre-install and post-install, scripting for additional customizability t...](https://learn.microsoft.com/mem/intune/apps/macos-unmanaged-pkg#step-2--program).
* Awaiting final configuration support during Setup Assistant will ensure that the most critical device configuration policies get to the device before the end user lands on the home screen (estimated Q1 2024).
* Customize Setup Assistant screens for ADE Macs.
* [Carry out remote actions like restart, merge, wipe, or erase](https://learn.microsoft.com/mem/intune/remote-actions/device-management#available-device-actions).
* Microsoft Cloud public key infrastructure (PKI) will include certificate lifecycle management for Mac when it launches as part of the Intune Suite (estimated Q1 2024).

th all these new features for Mac (and more to come), in addition to the cross-platform capabilities and tight integration with Microsoft 365, Microsoft Entra, and Microsoft Defender security offerings, the opportunity to retire on-premises solutions and consolidate to a single solution is more compelling than ever.

The goal should be to have a common management strategy, using mostly the same tools and infrastructure components we are familiar with. This way we get synergy effects during day-by-day operations. So, I looked at ways to manage a macOS similar to Windows with [Microsoft Intune](https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune?WT.mc_id=EM-MVP-5003177)

## How well can a macOS device be managed via Intune?

Short answer, very well 😄.

Everything starts with a user account within the enterprise. This user account is typically used for **user logon** and getting access to devices and resources. When we talk about management, we need a way to **enroll the device** into an MDM system, as MDM is the new golden standard for **configuration management** for all platforms. Next, a way to handle additional tasks outside of the MDM protocol like executing scripts via an additional **management agent**to accomplish all the left-over tasks we couldn’t solve with MDM and configuration profiles. And as last puzzle piece, we need a proper way of **distributing software**. For me these 5 areas are the essential parts to look at, to accomplish all typical device management tasks.

1. **User Logon**  
   When we think of user logon it can mean different things. First, I have to say, I want to look at options in a cloud-only approach. I’m not going to consider a domain join; this is not the future of identity management for me. Next, I will differentiate between two scenarios here. Logon to the OS and logon to services like SaaS applications in the browser session. macOS does not provide the native support of a cloud identity provider (IDP) like [Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis?WT.mc_id=EM-MVP-5003177) during OS logon (I’m hoping Apple decides to add this in the future). Meaning right now, you have to have a local account on the device for logon. This account can be the same as the centrally managed account, but again it has no real relationship. Password change of the local account will not change the account managed by the IDP and vice versa. On the other hand, if I’m logged on to the device with a local user and have to authenticate against my cloud resources with my IDP managed identity, my data is still protected very well. To make this scenario even easier we can support the user by configuring and providing the [macOS Microsoft Azure AD single sign-on](https://docs.microsoft.com/en-us/azure/active-directory/develop/apple-sso-plugin?WT.mc_id=EM-MVP-5003177) (how to configure [link](https://docs.microsoft.com/en-us/mem/intune/configuration/use-enterprise-sso-plug-in-ios-ipados-macos?WT.mc_id=EM-MVP-5003177)) experience within the Apple Desktop session for cloud resources.
2. **Device Enrollment**  
   Here it will become interesting. The latest additions to the [Automated Device Enrollment](https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-program-enroll-macos?WT.mc_id=EM-MVP-5003177) (ADE) (formerly known as DEP) supports Apple Setup Assistant with modern authentication. That means during the enrollment process we have cloud IDP support and therefore can force the user to authenticate against Azure AD and do additional MFA for example. Microsoft Intune supports this enrollment experiences for the macOS devices. In addition, we have two options for enrollment with user affinity and an option without user affinity. Enrollment with user affinity is the common enrollment method used, meaning a one-to-one relationship of user to device. With ADE we have the most streamlined experience with minimal user input. In addition, we have the “[user approved enrollment](https://docs.microsoft.com/en-us/mem/intune/enrollment/macos-enroll?WT.mc_id=EM-MVP-5003177)” scenario, driven by the Microsoft Company Portal, and a “[direct enrollment](https://docs.microsoft.com/en-us/mem/intune/enrollment/device-enrollment-direct-enroll-macos?WT.mc_id=EM-MVP-5003177)” scenario for enrollment with no user affinity.
3. **Configuration Management**  
   Once enrolled we can configure the devices with MDM configuration profiles provided by Microsoft Intune. These are typically security configurations as well as configurations for usability or look and feel (wallpaper etc.). For Compliance policy processing we need the [Company Portal](https://docs.microsoft.com/en-us/mem/intune/apps/apps-company-portal-macos?WT.mc_id=EM-MVP-5003177) here as well. The compliance policies are most important for the Conditional Access scenarios.
4. **Management Agent**  
   Special modifications (like configurations which can’t be done via configuration profile) are typically done via shell scripts, as they provide the maximum on flexibility. We can achieve basically everything we want, when it comes to special requirements. We can configure something (e.g., write to the defaults), we can run binaries, we can download something, we can read and report, and so on. All this is supported via the [Microsoft Intune Management Agent](https://docs.microsoft.com/en-us/mem/intune/apps/macos-shell-scripts?WT.mc_id=EM-MVP-5003177) which gets automatically deployed by Intune as soon as we assign shell scripts.
5. **Software** **Distribution**  
   Software distribution with Microsoft Intune can be achieved by utilizing the Company Portal and the distribution of applications wrapped as .intunemac packages so called [line-of-business (LOB) apps](https://docs.microsoft.com/en-us/mem/intune/apps/lob-apps-macos?WT.mc_id=EM-MVP-5003177). The Company Portal is the software center showing the available software to the user for installation. This needs re-packaging and is limited to .pkg apps (even though with some tricks we can get .dmg [support here](https://techcommunity.microsoft.com/t5/intune-customer-success/how-to-deploy-dmg-or-app-format-apps-to-intune-managed-macs/ba-p/1503416) as well). But as this approach is limited and generates too much labor for maintaining packages, I will introduce [Munki](https://www.munki.org/munki/) as an alternative here to support software distribution in an easier way, and with some tweaks, fully backed by cloud infrastructure.

A screenshot of a computer

Description automatically generated