

# Q&A from the University of Utah, MacAdmins

## From Enterprise SSO to Platform SSO and Beyond with Microsoft Entra

By Victor H. Vargas

Principal PM Manager | Identity, Network Access + Artificial Intelligence | Customer Experience (CxE)

### PSSO / SSOe / Microsoft Entra – Q&A Summary

| Question   | Answer<br>(Concise & Supportable)   | Support Material  |
|--|---|---|
| <b>When will the Intune Company Portal app support macOS 26 Simplified Setup for Platform SSO (account creation during Setup Assistant)?</b> | There is <b>no public date or committed timeline</b> . Microsoft has not announced when Company Portal will support macOS 26 Simplified Setup for Platform SSO. Today, Platform SSO with Entra ID is supported <b>post-setup</b> , not during | Apple Platform SSO Deployment Guide:<br><a href="https://support.apple.com/guide/deployment/platform-sso-for-macos-dep7bbb05313/web">https://support.apple.com/guide/deployment/platform-sso-for-macos-dep7bbb05313/web</a><br>Microsoft Platform SSO GA blog:<br><a href="https://techcommunity.microsoft.com/blog/microsoft-entra-blog/now-generally-available-platform-sso-for-macos-with-microsoft-entra-id/4437424">https://techcommunity.microsoft.com/blog/microsoft-entra-blog/now-generally-available-platform-sso-for-macos-with-microsoft-entra-id/4437424</a> |

|  |  |  |
|--|--|--|
|  | Setup Assistant.   |  |
| <b>Does Platform SSO automatically configure accounts in the Outlook macOS client?</b> | No. Platform SSO provides <b>authentication and SSO</b> , not <b>application account provisioning</b> . Outlook for macOS still requires the account/profile to be created once (manually, via Internet Accounts, or via MDM). After that, PSSO enables silent sign-in without password prompts. | Microsoft Platform SSO configuration (scope and behavior): <a href="https://learn.microsoft.com/intune/intune-service/configuration/platform-sso-macos">https://learn.microsoft.com/intune/intune-service/configuration/platform-sso-macos</a> |
| <b>By default, does PSSO store the</b>   | Yes. With Platform SSO, the  | Platform SSO technical overview: <a href="https://learn.microsoft.com/entra/identity/devices/macos-pssso">https://learn.microsoft.com/entra/identity/devices/macos-pssso</a>   |

|  |   |  |
|--|---|--|
| <p><b>Workplace Join (WPJ) key in the Secure Enclave?</b></p>  | <p>WPJ key is <b>hardware-bound</b> and protected by the Secure Enclave by default. This differs from the legacy SSOe model, where key storage behavior could vary. Touch ID is <b>not required</b> for Secure Enclave usage.</p> | <p>Platform SSO blog (authentication methods):<br/> <a href="https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/platform-ss0-for-macos/4468070">https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/platform-ss0-for-macos/4468070</a></p>    |
| <p><b>If Secure Enclave is used without biometrics or hardware keys, does PSSO fall back to password authentication?</b></p> | <p>No. Secure Enclave-backed Platform SSO still uses <b>asymmetric, hardware-bound keys</b> for Entra authentication. Biometrics</p>  | <p>Platform SSO authentication methods explained:<br/> <a href="https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/platform-ss0-for-macos/4468070">https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/platform-ss0-for-macos/4468070</a></p> |

|   |   |  |
|---|---|--|
|   | <p>(Touch ID) are a <b>user-unlock convenience</b>, not the security boundary. Phishing resistance is achieved by the key-based flow, not password sync.</p>  |  |
| <p><b>Is the security level the same as password-based PSSO unless biometrics are enforced?</b></p> | <p>No. Password-based PSSO relies on shared secrets and is <b>not phishing resistant</b>. Secure Enclave-based PSSO is phishing resistant even if Touch ID is not enforced, because authentication uses</p> | <p>Microsoft phishing-resistant passwordless guidance: <a href="https://learn.microsoft.com/entra/identity/authentication/how-to-deploy-phishing-resistant-passwordless-authentication">https://learn.microsoft.com/entra/identity/authentication/how-to-deploy-phishing-resistant-passwordless-authentication</a></p> |

|   |   |  |
|---|---|--|
|   | hardware-bound keys.  |  |
| <b>Are there caveats for multi-user macOS environments?</b> | <p>Yes. Platform SSO with Entra ID is fundamentally designed around a <b>primary user and device trust model</b>. Each user must register individually, and some flows (registration, repair) require admin interaction. Entra is not optimized for true shared, anonymous multi-user Macs.</p> | <p>Apple Platform SSO guide (multi-user &amp; shared device notes):<br/> <a href="https://support.apple.com/guide/deployment/platform-sso-for-macos-dep7bbb05313/web">https://support.apple.com/guide/deployment/platform-sso-for-macos-dep7bbb05313/web</a></p> |
| <b>Is there a plist or supported way to</b>                 | <p>Apple does not provide a single, clean plist</p>   | <p>Apple Platform SSO reference:<br/> <a href="https://developer.apple.com/documentation/authentication/services">https://developer.apple.com/documentation/authentication/services</a></p>  |

|  |  |   |
|--|--|---|
| <p><b>reliably identify the currently logged-in PSSO user?</b></p>         | <p>for this. Tools typically rely on <b>app-sso / platform-sso command output</b> or directory attributes. This is an OS limitation, not an Entra or Intune one.</p>   |   |
| <p><b>What do Entra admins need to allow for Platform SSO to work?</b></p> | <p>Users must be allowed to <b>register/join devices</b> in Entra ID, because Platform SSO creates a <b>device object (WPJ)</b>. Conditional Access and device trust rely on this registration. This is expected and</p> | <p>Platform SSO device registration details:<br/> <a href="https://learn.microsoft.com/entra/identity/devices/macospssso">https://learn.microsoft.com/entra/identity/devices/macospssso</a></p> |

|   |   |  |
|---|---|--|
|   | documented behavior.  |  |
| <p><b>Since Microsoft is moving to phishing-resistant passwordless authentication, should we stop syncing macOS and Entra ID passwords?</b></p> | <p>Yes, <b>long-term.</b> Microsoft's recommended end state for macOS is <b>Secure Enclave-backed Platform SSO</b>, not password synchronization. Password sync remains supported only as a <b>migration option</b>, not the security goal.</p> | <p>Microsoft Platform SSO GA blog:<br/> <a href="https://techcommunity.microsoft.com/blog/microsoft-entra-blog/now-generally-available-platform-sso-for-macos-with-microsoft-entra-id/4437424">https://techcommunity.microsoft.com/blog/microsoft-entra-blog/now-generally-available-platform-sso-for-macos-with-microsoft-entra-id/4437424</a><br/> Passwordless strategy:<br/> <a href="https://learn.microsoft.com/entra/identity/authentication/how-to-deploy-phishing-resistant-passwordless-authentication">https://learn.microsoft.com/entra/identity/authentication/how-to-deploy-phishing-resistant-passwordless-authentication</a></p> |
| <p><b>In a fully passwordless Microsoft environment, does Simplified Setup offer benefits beyond eliminating</b></p>                            | <p>Yes. Simplified Setup enforces <b>identity-first onboarding</b>: no unmanaged local account, no</p>  | <p>Apple Platform SSO during Automated Device Enrollment:<br/> <a href="https://support.apple.com/guide/deployment/platform-sso-for-macos-dep7bbb05313/web">https://support.apple.com/guide/deployment/platform-sso-for-macos-dep7bbb05313/web</a></p>   |

|                        |   |  |
|------------------------|---|--|
| <b>an extra login?</b> | skipped registration , immediate device trust, and Zero Trust enforcement <b>before first desktop access.</b> The value is <b>correctness and security,</b> not just convenience. |  |
|------------------------|---|--|