Windows LAPS in Azure AD

By: Shehan Perera | MVP - Enterprise Mobility
https://linktr.ee/shehanjp

LAPS Capabilities with Azure AD

- Enabling Windows LAPS with Azure AD
- Local administrator password management
- Recovering local administrator password
- Enumerating all Windows LAPS enabled devices
- Authorization of local administrator password recovery
- Auditing local administrator password update and recovery
- Conditional Access policies for local administrator password recovery

Supported Operating Systems

Win 11 22H2 - April 11 2023 Update
Win 11 21H2 - April 11 2023 Update
Win 10 20H2, 21H2 and 22H2 - April 11 2023 Update
Win Server 2022 - April 11 2023 Update
Win Server 2019 - April 11 2023 Update

Supported Join Types

Hybrid AAD Join ✅
AAD Join ✅
AAD Registered ❌

Licensing Requirements

LAPS is available to all customers with Azure AD Free or higher licenses. Other related features like administrative units, custom roles, Conditional Access, and Intune have other licensing requirements.

Roles are needed to recover LAPS passwords

Global Administrator, Cloud Device Administrator, and Intune Administrator
or a custom RBAC with
- To read LAPS metadata:
microsoft.directory/deviceLocalCredentials/standard/read
- To read LAPS passwords:
microsoft.directory/deviceLocalCredentials/password/read

shehanperera.com
https://www.linkedin.com/in/shehanperera85/
https://github.com/shehanperera85
https://twitter.com/Shehanperera85

Windows LAPS vs. legacy Microsoft LAPS

- **A** key difference is that Windows LAPS is an entirely separate implementation that's native to Windows
- **W**indows LAPS doesn't require you to install legacy Microsoft LAPS. You can fully deploy and use all Windows LAPS features without installing or referring to legacy Microsoft LAPS.
- You can use Windows LAPS to back up passwords to Azure Active Directory, encrypt passwords in Windows Server Active Directory, and store your password history

Event Logs

To view the Windows LAPS event log channel, in Windows Server Event Viewer, go to Applications and Services > Logs > Microsoft > Windows > LAPS > Operational

Windows LAPS in legacy Microsoft LAPS emulation mode

You can set up Windows Local Administrator Password Solution (Windows LAPS) to honor legacy Microsoft LAPS Group Policy settings but with some restrictions and limitations. The feature is called legacy Microsoft LAPS emulation mode. You might use emulation mode if you migrate an existing deployment of legacy Microsoft LAPS to Windows LAPS.

Graph API

Get deviceLocalCredentialInfo (/beta feature)
Permissions: device.LocalCredentials.Read.All

Conditional Access Policies

Conditional Access policies can be scoped to the built-in roles like Cloud Device Administrator, Intune Administrator, and Global Administrator to protect access to recover local administrator passwords.