Introduction to Device Management

Device management in AAD



Device management is a foundation of Device based conditional access in AAD. With device-based conditional access, you can ensure that access to resources in your environment is only possible with

Option 02

AAD Joined

managed devices.

Joining a device is an extension of registering. With Azure AD joined, you can implement SSO, Access to Windows store, restriction of apps only to complaint devices and seamless access to on-premise resources. Currently Windows 10 devices are suported

Organizations with an on-premises footprint generally rely on imaging methods to provision devices, and they often use System Center Configuration Manager (SCCM) or group policy (GP) to manage them. Those devices will be domain joined to your on-premises Active Directory and registered with your Azure Active Directory.

Option 01

AAD
Registered

When device is registered, AAD will create an identity that can be used to authenticate the device. Goal is to provide support for Bring Your Own Device (BYOD) scenario. Access is based on a work account that has been entered on the device.

Device management options summary



AAD registered devices

- For personal devices
- To manually register devices with AD

AAD joined devices

- For devices owned by the organization
- Devices that are not domain joined with On-premise AD
- Manually register devices with AAD
- To change the local state of the device

Hybrid AAD joined devices

- For devices owned by the organization
- Devices that are domain joined with On-premise AD
- Automatically register devices with AAD
- To change the local state of the device



Device based conditional access policies



Compliance policies

- Compliance policies define the rules and settings that users and devices must meet to be compliant.
- When combined with conditional access, administrators can block users and devices that don't meet the rules.
- Compliance status is used by conditional access policies to block or allow access to e-mail and other corporate resources.

➤ In simple terms, managed devices are devices that are under some sort of organizational control.

Managed devices

- In Azure AD, the prerequisite for a managed device is that it has been registered with Azure AD.
- Registering a device creates an identity for the device in form of a device object. This object is used by Azure to track status information about a device.

Enterprise state roaming



With Windows 10, Azure Active Directory (Azure AD) users gain the ability to securely synchronize their user settings and application settings data to the cloud. Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

- Separation of consumer and corporate data
- Enhanced security
- Better management and monitoring