Filename: microsoft-ms101-1-2-1-configure-mdm-integration-with-azure-ad-overview
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Mobile Device Management (MDM)
EpisodeName: Configure MDM Integration with Azure AD - Overview
Description: Adam and Wes discuss the steps necessary to help you successfully configure Mobile Device Management (MDM) integration with Azure AD.

Configure MDM Integration with Azure AD - Overview

Implement Modern Device Services (30-35%)

Implement Mobile Device Management (MDM)
• Plan for MDM
• Configure MDM integration with Azure AD
• Set an MDM authority
• Set device enrollment limit for users

==========

Configure MDM integration with Azure AD - Overview:

Things to know BEFORE you go... (in other words PLANNING TO SUCCEED)

```
1. Active MDM Subscription with a supported provider

    a. Intune (Default)
    b. Third-Party via the Azure AD app gallery


2. Configure MDM settings

    a. URL for Terms of Use - used for manual device enrollment; defaults to Intune

    b. URL for MDM Discovery - used for device enrollment; defaults to Intune

    c. URL for MDM Compliance - used when a device is not compliant

    d. User Scope - list of users enabled for automatic MDM enrolment


3. Automatic Device Enrollment - Need a Premium Azure AD P1 or P2 plan


4. Configure devices for automatic hybrid domain join with Azure AD and
```

enrollment with Intune - Need more info?

How To: Plan your hybrid Azure Active Directory join implementation:
https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan

Azure AD Connect - used to synchronize users, groups and computer objects in your on-premise AD with Azure AD.

Registration URL's that MUST BE AVAILABLE for hybrid Azure AD join to work:

```
1. https://enterpriseregistration.windows.net
2. https://login.microsoftonline.com
3. https://device.login.microsoftonline.com
```

Setting up MDM Integration using Group Policy - 2 to know:

```
a. Computer Configuration --> Administrative Templates -->
```

Windows Components --> Device Registration: Register domain joined computers as devices

This setting lets you configure how domain joined computers become registered as devices.

When you enable this setting, domain joined computers automatically and silently get registered as devices with Azure Active Directory.

```
b. Computer Configuration --> Administrative Templates -->
```

Windows Components --> MDM: Enable automatic MDM enrollment using default Azure AD credentials

Specifies whether to automatically enroll the device to the Mobile Device Management (MDM) service configured in Azure Active Directory (Azure AD). If the enrollment is successful, the device will be remotely managed by the MDM service.

```
    Important: The device must be registered in Azure AD for enrollment
    to succeed.

    If you do not configure this policy setting, automatic MDM enrollment
    will not be initiated.

    If you enable this policy setting, a task is created to initiate
    enrollment of the device to MDM service specified in the Azure AD.

    If you disable this policy setting, MDM will be unenrolled.
```