Filename: microsoft-ms101-1-4-1-set-device-enrollment-limit-for-users
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Mobile Device Management (MDM)
EpisodeName: Set Device Enrollment Limit for Users
Description: Adam and Wes discuss the steps necessary to help you successfully set a device enrollment limit for users.

Set Device Enrollment Limit for Users

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

==========

Set device enrollment limit for users:

As an Intune administrator, you can create and manage enrollment restrictions that define what devices can enroll into management with Intune, including the:

```
• number of devices
• operating systems and versions
```

You can create multiple restrictions and apply them to different user groups.

You can set the priority order for your different restrictions.

The specific enrollment restrictions that you can create include:

```
• Maximum number of enrolled devices

• Device platforms that can enroll:

    Android device administrator
    Android Enterprise work profile
    iOS
    macOS
    Windows
    Windows Mobile

• Platform operating system version for iOS, Android device administrator,
```

Android Enterprise work profile, Windows, and Windows Mobile. (Only Windows 10 versions can be used. Leave this blank if Windows 8.1 is allowed.)

```
• Restrict personally owned devices (iOS, Android device administrator, Android
Enterprise work profile, macOS, Windows, and Windows Mobile only).
```

Default restrictions:

Default restrictions are automatically provided for both device type and device limit enrollment restrictions. You can change the options for the defaults. Default restrictions apply to all user and userless enrollments. You can override these defaults by creating new restrictions with higher priorities.

Create a device type restriction:

Under Versions, choose the minimum and maximum versions that you want the allowable platforms to support.

Version restrictions only apply to devices enrolled with the Company Portal. Supported version formats include:

```
• Android device administrator and Android Enterprise work profile support
```

major.minor.rev.build.

```
• iOS supports major.minor.rev. Operating system versions do not apply to Apple
```

devices that enroll with the Device Enrollment Program, Apple School Manager, or the Apple Configurator app.

```
• Windows supports major.minor.rev.build for Windows 10 only.
```

NOTE: Windows 10 does not provide the build number during enrollment so for instance if you enter in 10.0.17134.100 and the device is 10.0.17134.174 it will be blocked during enrollment.

Create a device limit restriction:

Device limit restrictions do not apply for the following Windows enrollment types:

```
• Co-managed enrollments
• GPO enrollments
• Azure Active Directory joined enrollments
• Bulk Azure Active Directory joined enrollments
• Autopilot enrollments
• Device Enrollment Manager enrollments
```

Device limit restrictions are not enforced for these enrollment types because they are considered shared device scenarios. You can set hard limits for these enrollment types in Azure Active Directory.

Blocking personal Android devices:

If you block personally owned Android device administrator devices from enrollment, personally owned Android Enterprise work profile devices can still enroll.

By default, your Android Enterprise work profile devices settings are the same as your settings for your Android device administrator devices. After you change your Android Enterprise work profile or your Android device administrator settings, that's no longer the case.

If you block personal Android Enterprise work profile enrollment, only corporate-owned Android devices can enroll with Android Enterprise work profiles.

Blocking personal Windows devices:

If you block personally owned Windows devices from enrollment, Intune checks to make sure that each new Windows enrollment request has been authorized as a corporate enrollment. Unauthorized enrollments will be blocked.

The following methods qualify as being authorized as a Windows corporate enrollment:

```
• The enrolling user is using a device enrollment manager account.

• The device enrolls through Windows Autopilot.

• The device is registered with Windows Autopilot but is not an MDM enrollment
```

only option from Windows Settings.

```
• The device’s IMEI number is listed in Device enrollment > Corporate device
```

identifiers. (Not supported for Windows Phone 8.1.)

```
• The device enrolls through a bulk provisioning package.

• The device enrolls through GPO, or automatic enrollment from SCCM for
```

co-management.

The following enrollments are marked as corporate by Intune. But since they do not offer the Intune administrator per-device control, they will be blocked:

```
• Automatic MDM enrollment with Azure Active Directory join during Windows
```

setup^.

```
• Automatic MDM enrollment with Azure Active Directory join from Windows
```

Settings^.

The following personal enrollment methods will also be blocked:

```
• Automatic MDM enrollment with Add Work Account from Windows Settings^.

• MDM enrollment only option from Windows Settings.
```

^ These will not be blocked if registered with Autopilot.

```
*    Reference:
```