

# MD-101<sup>Q&As</sup>

Managing Modern Desktops

**Pass Microsoft MD-101 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/md-101.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

What is the maximum number of devices that User1 and User2 can enroll in Intune? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

User1 can enroll a maximum of:

<input type="checkbox"/>
5 devices
10 devices
15 devices
1,000 devices
An unlimited number of devices

User2 can enroll a maximum of:

<input type="checkbox"/>
5 devices
10 devices
15 devices
1,000 devices
An unlimited number of devices

Correct Answer:

**Answer Area**

User1 can enroll a maximum of:

<input type="checkbox"/>
5 devices
<input checked="" type="checkbox"/> 10 devices
15 devices
1,000 devices
An unlimited number of devices

User2 can enroll a maximum of:

<input type="checkbox"/>
5 devices
10 devices
<input checked="" type="checkbox"/> 15 devices
1,000 devices
An unlimited number of devices

Box 1: 10 devices User1 is a member of GroupA. GroupA device limit is 10.

Box 2: 15 devices User2 is a member of GroupB. GroupB device limit is 15.

**QUESTION 2**

You need to consider the underlined segment to establish whether it is accurate.

After installing a feature update on a Windows 10 computer, you have 7 days to roll back the update

Select “No adjustment required” if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.

B. 10

C. 90

D. 30

Correct Answer: B

Microsoft has changed the time period associated with operating system rollbacks with Windows 10 version 1607, decreasing it to 10 days.

Previously, Windows

10 had a 30-day rollback period.

References:

<https://redmondmag.com/articles/2016/08/04/microsoft-shortens-windows-10-rollback-period.aspx>

By default settings, Windows 10 allows you to go back to the previous version of Windows in the first 10 days. And after that system Automatically delete this old windows folder, and can\’t go back to the previous build windows 10.

Reference:

<https://howtofixwindows.com/roll-back-windows-10-upgrade-after-10-days-limit/>

---

### QUESTION 3

Your network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD).

You have a Microsoft 365 subscription.

You create a conditional access policy for Microsoft Exchange Online.

You need to configure the policy to prevent access to Exchange Online unless a user is connecting from a device that is hybrid Azure AD-joined.

Which settings should you configure?

A. Locations

B. Device platforms

C. Sign-in risk

D. Device state

Correct Answer: D

The device state condition was used to exclude devices that are hybrid Azure AD joined and/or devices marked as compliant with a Microsoft Intune compliance policy from an organization's Conditional Access policies.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions#device-state>

---

#### QUESTION 4

You have a Microsoft 365 E5 subscription that contains a group named Group1. You create a Conditional Access policy named CAPolicy1 and assign CAPolicy1 to Group1.

You need to configure CAPolicy1 to require the members of Group1 to reauthenticate every eight hours when they connect to Microsoft Exchange Online.

What should you configure?

- A. Session access controls
- B. an assignment that uses a User risk condition
- C. an assignment that uses a Sign-in risk condition
- D. Grant access controls

Correct Answer: A

User sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

The Azure Active Directory (Azure AD) default configuration for user sign-in frequency is a rolling window of 90 days.

Sign-in frequency control

Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.

Browse to Azure Active Directory > Security > Conditional Access.

Select New policy.

Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Choose all required conditions for customer's environment, including the target cloud apps.

Under Access controls > Session.

Select Sign-in frequency.

Choose Periodic reauthentication and enter a value of hours or days or select Every time.

Save your policy.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session->

lifetime

---

**QUESTION 5**

You need to meet the OOBE requirements for Windows AutoPilot.

Which two settings should you configure from the Azure Active Directory blade? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**i Overview**

Getting started

**Manage**

Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

Correct Answer:

**i Overview**

Getting started

**Manage**

Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings

From the scenario:

Ensure that the company name and logo appears during the Out of Box Experience (OOBE) when using Windows AutoPilot.

Company Branding: When you use Windows AutoPilot to deploy new devices, you want the process to be friendly and familiar for the users going through the process. One of the ways that is done is by customizing the logon experience to

include logos and company-specific text.

The basic steps:

1.

Sign into the Azure Portal as a tenant admin.

2.

Navigate to Azure Active Directory "> Company branding.

3.

Click Edit to configure the needed settings.

4.

Fill in all the customizations (Including the company logo and company name) Properties: you can set that value in the Name field of the Azure AD tenant properties:

Reference: <https://blogs.technet.microsoft.com/mniehaus/2017/12/22/windows-autopilot-azure-ad-branding>

[MD-101 Practice Test](#)

[MD-101 Study Guide](#)

[MD-101 Brindumps](#)