MD-102$^{Q\&As}$

Endpoint Administrator

Pass Microsoft MD-102 Exam with 100% Guarantee

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

https://www.passapply.com/md-102.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have a Microsoft Azure subscription that contains an Azure Log Analytics workspace.

You deploy a new computer named Computer1 that runs Windows 10. Computer1 is in a workgroup.

You need to ensure that you can use Log Analytics to query events from Computer1.

What should you do on Computer1?

A. Join Azure AD.

B. Configure Windows Defender Firewall.

C. Create an event subscription

D. Install the Azure Monitor Agent.

Correct Answer: A

The Windows client installer supports latest Windows machines only that are Microsoft Entra joined or Microsoft Entra hybrid joined. https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client

QUESTION 2

You have a Microsoft 365 subscription that contains 500 computers that run Windows 11. The computers are Azure AD joined and are enrolled in Microsoft Intune.

You plan to manage Microsoft Defender Antivirus on the computers.

You need to prevent users from disabling Microsoft Defender Antivirus.

What should you do?

A. From the Microsoft Intune admin center, create a security baseline.

B. From the Microsoft 365 Defender portal, enable tamper protection.

C. From the Microsoft Intune admin center, create an account protection policy.

D. From the Microsoft Intune admin center, create an endpoint detection and response (EDR) policy.

Correct Answer: B

Manage tamper protection for your organization using Microsoft 365 Defender portal

Tamper protection helps protect certain security settings, such as virus and threat protection, from being disabled or changed. If you\\'re part of your organization\\'s security team, you can turn tamper protection on (or off) tenant wide by using the Microsoft 365 Defender portal (https://security.microsoft.com).

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-tamper-protection-microsoft-365-defender

QUESTION 3

A user named User1 has a computer named Computer1 that runs Windows 10.

User1 connects to a Microsoft Azure virtual machine named VM1 by using Remote Desktop.

User1 creates a VPN connection to a partner organization.

When the VPN connection is established, User1 cannot connect to VM1. When User1 disconnects from the VPN, the user can connect to VM1.

You need to ensure that User1 can connect to VM1 while connected to the VPN.

What should you do?

A. From the proxy settings, add the IP address of VM1 to the bypass list to bypass the proxy.

B. From the properties of VPN1, clear the Use default gateway on remote network check box.

C. From the properties of the Remote Desktop connection to VM1, specify a Remote Desktop Gateway (RD Gateway).

D. From the properties of VPN1, configure a static default gateway address.

Correct Answer: B

QUESTION 4

You install a feature update on a computer that runs Windows 10. How many days do you have to roll back the update?

A. 5

B. 10

C. 14

D. 30

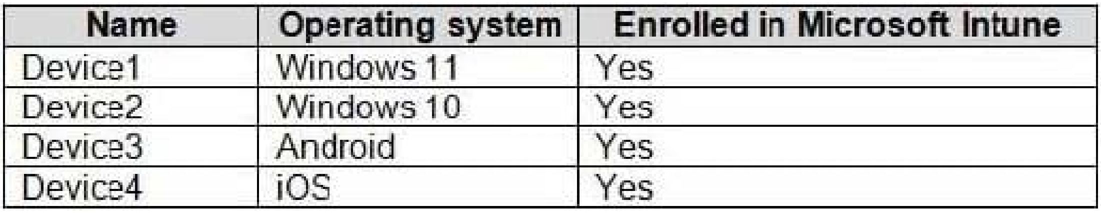
Correct Answer: B

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.

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

QUESTION 5

You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.



Name	Operating system	Enrolled in Microsoft Intune
Device1	Windows 11	Yes
Device2	Windows 10	Yes
Device3	Android	Yes
Device4	iOS	Yes

All devices have Microsoft Edge installed.

From the Microsoft Intune admin center, you create a Microsoft Edge Baseline profile named Edge1.

You need to apply Edge1 to all the supported devices.

To which devices should you apply Edge1?

A. Device1 only

B. Device1 and Device2 only

C. Device1, Device2, and Device3 only

D. Device1, Device2, and Device4 only

E. Device1, Device2, Device3, and Device4

Correct Answer: B

Windows 10 and Windows 11 only.

Reference: https://learn.microsoft.com/en-us/mem/intune/protect/security-baseline-settings-edge

QUESTION 6

You have a Microsoft 365 subscription.

You need to provide a user the ability Security defaults and create Conditional Access policies. The solution must use the principle of least privilege.

Which role should you assign to the user?

A. Global Administrator

B. Conditional Access Administrator

C. Security Administrator

D. Intune Administrator

Correct Answer: B

To enable security defaults (or confirm they\\'re already enabled) Important You must be a Security Administrator, Conditional Access administrator, or Global Administrator to perform this task.

Note: Turn on multi-factor authentication

Multi-factor authentication (MFA) is a very important first step in securing your organization. Microsoft 365 Business Premium includes the option to use security defaults or Conditional Access policies to turn on MFA for your admins and user

accounts. For most organizations, security defaults offer a good level of sign-in security. But if your organization must meet more stringent requirements, you can use Conditional Access policies instead.

This article provides information about:

Security defaults (suitable for most businesses)

Conditional Access (for businesses with more stringent security requirements)

Reference:

https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-turn-on-mfa?

QUESTION 7

You have a computer named Computer1 that runs Windows 10.

You need to prevent standard users from changing the wireless network settings on Computer1. The solution must allow administrators to modify the wireless network settings.

What should you use?

A. Windows Configuration Designer

B. MSConfig

C. Local Group Policy Editor

D. an MMC console that has the Group Policy Object Editor snap-in

Correct Answer: C

QUESTION 8

You have a Microsoft 365 subscription that uses Microsoft Intune Suite.

You use Microsoft Intune to manage Windows 11 devices.

You need to implement passwordless authentication that requires users to use number matching.

Which authentication method should you use?

A. Microsoft Authenticator

B. voice calls

C. FIDO2 security keys

D. text messages

Correct Answer: A

How number matching works in multifactor authentication (MFA) push notifications for Authenticator - Authentication methods policy This topic covers how number matching in Microsoft Authenticator push notifications improves user sign-in security. Number matching is a key security upgrade to traditional second factor notifications in Authenticator. Beginning May 8, 2023, number matching is enabled for all Authenticator push notifications. As relevant services deploy, users worldwide who are enabled for Authenticator push notifications will begin to see number matching in their

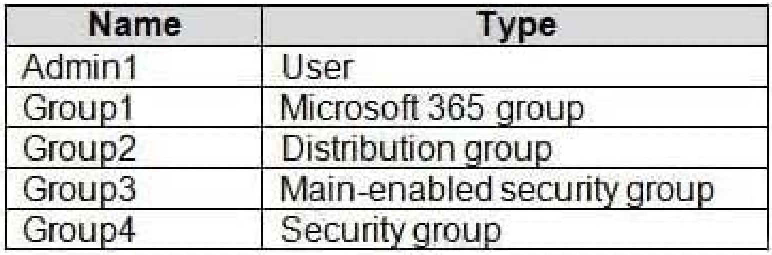
approval requests. Users can be enabled for Authenticator push notifications either in the Authentication methods policy or the legacy multifactor authentication policy if Notifications through mobile app is enabled.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match

QUESTION 9

You have a Microsoft 365 tenant that contains the objects shown in the following table.



Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Main-enabled security group
Group4	Security group

You are creating a compliance policy named Compliance1.

Which objects can you specify in Compliance1 as additional recipients of noncompliance notifications?

A. Group3 and Group4 only

B. Group3, Group4, and Admin1 only

C. Group1, Group2, and Group3 only

D. Group1, Group2, Group3, and Group4 only

E. Group1, Group2, Group3, Group4, and Admin1

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups

QUESTION 10

You have a Microsoft 365 E5 subscription that contains 150 hybrid Azure AD joined Windows devices. All the devices are enrolled in Microsoft Intune. You need to configure Delivery Optimization on the devices to meet the following requirements:

1.

Allow downloads from the internet and from other computers on the local network.

2.

Limit the percentage of used bandwidth to 50. What should you use?

A. a configuration profile

B. a Windows Update for Business Group Policy setting

C. a Microsoft Peer-to-Peer Networking Services Group Policy setting

D. an Update ring for Windows 10 and later profile

Correct Answer: A

Delivery Optimisation through Configuration Profile in Intune

QUESTION 11

You have a Microsoft 365 subscription that includes Microsoft Intune.

You have 500 corporate-owned Android devices enrolled as fully managed devices.

You need to prepare an app named App1 for deployment to the devices.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Intune Company Portal, download App1.

B. Sync App1 with Intune.

C. From the Managed Google Play Store, approve App1.

D. Create an OEMConfig profile.

Correct Answer: BC

C: Add a Managed Google Play store app in the Managed Google Play console (Alternative)

If you prefer to synchronize a Managed Google Play app with Intune rather than adding it directly using Intune, use the following steps.

1.

Go to the Managed Google Play store. Sign in with the same account you used to configure the connection between Intune and Android Enterprise.

2.

Search the store and select the app you want to assign by using Intune.

3.

On the page that displays the app, click Approve.

In the following example, the Microsoft Excel app has been chosen.

A window for the app opens asking you to give permissions for the app to perform various operations.

4.

Select Approve to accept the app permissions and continue.

5.

Select an option for handling new app permission requests, and then select Save.

(B) The app is approved, and it is displayed in your IT admin console. Next, you can Sync a Managed Google Play app with Intune.

Reference:

https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work

QUESTION 12

You have an on-premises server named Server1 that hosts a Microsoft Deployment Toolkit (MDT) deployment share named MDT1.

You need to ensure that MDT1 supports multicast deployments.

What should you install on Server1?

A. Multipath I/O (MPIO)

B. Multipoint Connector

C. Windows Deployment Services (WDS)

D. Windows Server Update Services (WSUS)

Correct Answer: C

Multicast requires that Windows Deployment Services (WDS) is running on Windows Server 2008 or later.

Reference: https://learn.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/deploy-a-windows-10-image-using-mdt

QUESTION 13

You use Microsoft Intune and Intune Data Warehouse.

You need to create a device inventory report that includes the data stored in the data warehouse.

What should you use to create the report?

A. the Company Portal app

B. Endpoint analytics

C. the Azure portal app

D. Microsoft Power BI

Correct Answer: D

Super easy start with reporting and the Intune Data Warehouse

Method 1: Load data using OData URL

The first method is loading data by using the OData URL.

Method 2: Load data and reports using Power BI file (pbix)

The second method is loading data and prebuilt reports using a downloaded Power BI file (pbix). That file contains the connection information for the tenant and contains a set of prebuilt reports based on the Intune Data Warehouse data

model.

Reference:

https://www.petervanderwoude.nl/post/super-easy-start-with-reporting-and-the-intune-data-warehouse/

QUESTION 14

You have a computer named Computer1 that runs Windows 11.

A user named User1 plans to use Remote Desktop to connect to Computer1.

You need to ensure that the device of User1 is authenticated before the Remote Desktop connection is established and the sign in page appears.

What should you do on Computer1?

A. Turn on Reputation-based protection

B. Enable Network Level Authentication (NLA)

C. Turn on Network Discovery

D. Configure the Remote Desktop Configuration service

Correct Answer: B

What is Network Level Authentication?

Network level authentication is used for authenticating Remote Desktop services, such as Windows RDP, and Remote Desktop Connection (RDP Client). You might also hear it called front authentication.

What is Network Level Authentication (NLA) used for?

Before you can start a remote desktop session, the user will need to authenticate themselves - ie, prove that they are who they say they are. Using network level authentication means that a false connection can\\'t be made, which would use

up CPU and cause a strain on the resources of the network. This offers a level of security against some cyberattacks such as Denial of Service attacks, where multiple requests are made all at once towards a network, overwhelming its ability

to cope. To combat this, you can turn on network level authentication to authenticate the user\\'s credentials before starting a remote access session. If the user\\'s credentials aren\\'t authenticated, then the connection is simply denied.

Reference:

https://www.atera.com/blog/what-is-network-level-authenticatio

QUESTION 15

You are creating a device configuration profile in Microsoft Intune. You need to configure specific OMA-URI settings in the profile. Which profile type template should you use?

A. Device restrictions (Windows 10 Team)

B. Identity protection

C. Custom

D. Device restrictions

Correct Answer: C

Windows client custom profiles use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. These settings are typically used by mobile device manufacturers to control features on the device.

Reference: https://docs.microsoft.com/en-us/mem/intune/configuration/custom-settings-windows-10