- **Vendor: Microsoft**
- **Exam Code: MD-101**
- **Exam Name: Managing Modern Desktops**
- **New Updated Questions from Braindump2go (Updated in Oct./2020)**

QUESTION 179
You use Microsoft Intune to manage client computers. The computers run one of the following operating systems:
- Windows 8.1
- Windows 10 Pro
- Windows 10 Enterprise
- Windows 10 Enterprise LTSC

You plan to manage Windows updates on the computers by using update rings.
Which operating systems support update rings?

A. Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC only
B. Windows 8.1, Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Enterprise LTSC
C. Windows 10 Enterprise and Windows 10 Enterprise LTSC only
D. Windows 10 Pro and Windows 10 Enterprise only

Answer: D
Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure

QUESTION 180
You have a computer named Computer1 that runs Windows 8.1.
You plan to perform an in-place upgrade of Computer1 to Windows 10 by using an answer file.
You need to identify which tool to use to create the answer file.
What should you identify?

A. System Configuration (Msconfig.exe)
B. Windows Configuration Designer
C. Windows System Image Manager (Windows SIM)
D. Windows Deployment Services (WDS)

Answer: C
Explanation:
https://thesleepyadmins.com/2019/05/31/create-windows-10-answer-file/

QUESTION 181
Your network contains an Active Directory domain. The domain contains 10 computers that run Windows 8.1 and use local user profiles.
You deploy 10 new computers that run Windows 10 and join the computers to the domain.
You need to migrate the user profiles from the Windows 8.1 computers to the Windows 10 computers.
What should you do?

A. From the Windows 8.1 computer of each user, run imagex.exe/capture, and then from the

Windows 10 computer of each user, run imagex.exe/apply.

B. Configure roaming user profiles for the users. Instruct the users to first sign in to and out of their Windows 8.1 computer and then to sign in to their Windows 10 computer.

C. From the Windows 8.1 computer of each user, run scanstate.exe, and then from the Windows 10 computer of each user, run loadstate.exe.

D. Configure Folder Redirection for the users. Instruct the users to first sign in to and out of their Windows 8.1 computer, and then to sign in to their Windows 10 computer.

Answer: C
Explanation:
The ScanState command is used with the User State Migration Tool (USMT) 10.0 to scan the source computer, collect the files and settings, and create a store.
Reference:
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-scanstate-syntax
https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-loadstate-syntax

QUESTION 182
You have an Azure Active Directory (Azure AD) tenant named contoso.com.
You create a terms of use (ToU) named Terms1 in contoso.com.
You are creating a conditional access policy named Policy1 to assign a cloud app named App1 to the users in contoso.com.
You need to configure Policy1 to require the users to accept Terms1.
What should you configure in Policy1?

A. Grant in the Access controls section
B. Conditions in the Assignments section
C. Cloud apps or actions in the Assignments section
D. Session in the Access controls section

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-tou

QUESTION 183
Your network contains an on-premises Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD).
You have the Windows 10 devices shown in the following table.

Name	Active Directory	Endpoint Configuration Manager agent	Microsoft Intune	Azure AD
Device1	Joined	Not installed	Enrolled	Registered
Device2	Not joined	Installed	Enrolled	Registered
Device3	Not joined	Not installed	Enrolled	Joined
Device4	Joined	Installed	Not enrolled	Registered
Device5	Not joined	Installed	Not enrolled	Joined
Device6	Joined	Installed	Enrolled	Joined

You need to ensure that you can use co-management to manage all the Windows 10 devices.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Join Device 1, Device2, and Device4 to Azure AD.
B. Unjoin Device3, Device5, and Device6 from Azure AD, and then register the devices in Azure AD.
C. Enroll Device4 and Device5 in Intune.
D. Join Device2, Device3, and Device5 to the domain.

E. Install the Endpoint Configuration Manager agent on Device1 and Device3.

Answer: CE
Explanation:
Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune.
Co-management requires Configuration Manager version 1710 or later and enrollment in Microsoft Intune.
Windows 10 devices must be hybrid Azure AD joined.
Reference:
https://docs.microsoft.com/en-us/mem/configmgr/comanage/overview

QUESTION 184
Hotspot Question
You have an Azure Active Directory (Azure AD) tenant named adatum.com that contains the users shown in the following table.

Name	Role
User1	*None*
User2	Global administrator
User3	Cloud device administrator
User4	Intune administrator

You configure the following device settings for the tenant:
- Users may join devices to Azure AD: User1
- Additional local administrators on Azure AD joined devices: None

You install Windows 10 on a computer named Computer1.
You need to identify which users can join Computer1 to adatum.com, and which users will be added to the Administrators group after joining adatum.com.
Which users should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Users who can join Computer1 to adatum.com:
- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User3, and User 4 only
- User1, User2, User3, and User4

Users who will be added to the Administrators group after joining adatum.com:
- User1 only
- User2 only
- User1 and User2 only
- User3 and User4 only
- User2, User3, and User4 only

Answer:

Answer Area

Users who can join Computer1 to adatum.com:

- User1 only
- User1 and User2 only
- User1, User2, and User3 only
- User1, User3, and User 4 only
- User1, User2, User3, and User4

Users who will be added to the Administrators group after joining adatum.com:

- User1 only
- User2 only
- User1 and User2 only
- User3 and User4 only
- User2, User3, and User4 only

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/devices/assign-local-admin

QUESTION 185
Hotspot Question
You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	Group
Device1	Windows 10	Group1, Group2
Device2	Android	Group2
Device3	iOS	Group2, Group3

You create device configuration profiles in Intune as shown in the following table.

Name	Platform	Minimum password length
Profile1	Windows 10 and later	4
Profile2	Android	5
Profile3	iOS	6
Profile4	Android	7
Profile5	iOS	8

You assign the device configuration profiles to groups as shown in the following table.

Group	Profile
Group1	Profile3
Group2	Profile1, Profile2, Profile4
Group3	Profile3, Profile5

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Device1 must have a minimum password length of seven characters.	○	○
Device2 must have a minimum password length of seven characters.	○	○
Device3 must have a minimum password length of six characters.	○	○

Answer:

Answer Area

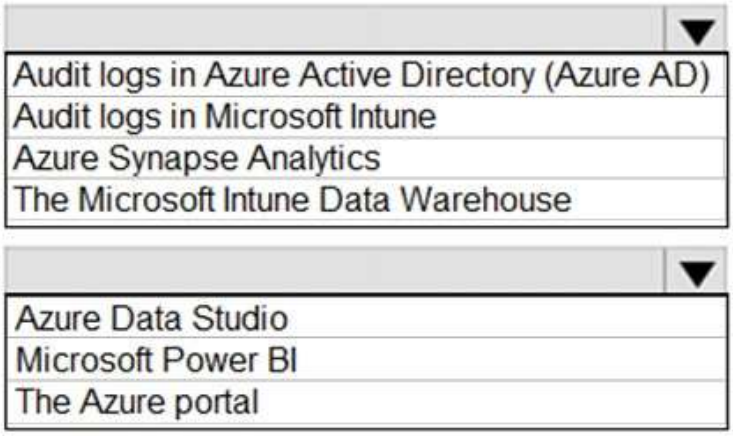
Statements	Yes	No
Device1 must have a minimum password length of seven characters.	○	●
Device2 must have a minimum password length of seven characters.	●	○
Device3 must have a minimum password length of six characters.	○	●

Explanation:
If a compliance policy evaluates against the same setting in another compliance policy, then the most restrictive compliance policy setting applies.
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-troubleshoot

QUESTION 186
Hotspot Question
You use Microsoft Endpoint Manager to manage Windows 10 devices.
You are designing a reporting solution that will provide reports on the following:
- Compliance policy trends
- Trends in device and user enrolment
- App and operating system version breakdowns of mobile devices

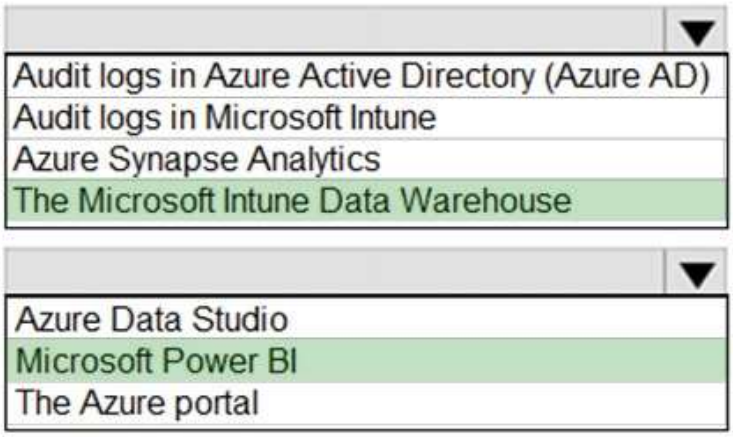
You need to recommend a data source and a data visualization tool for the design.
What should you recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area

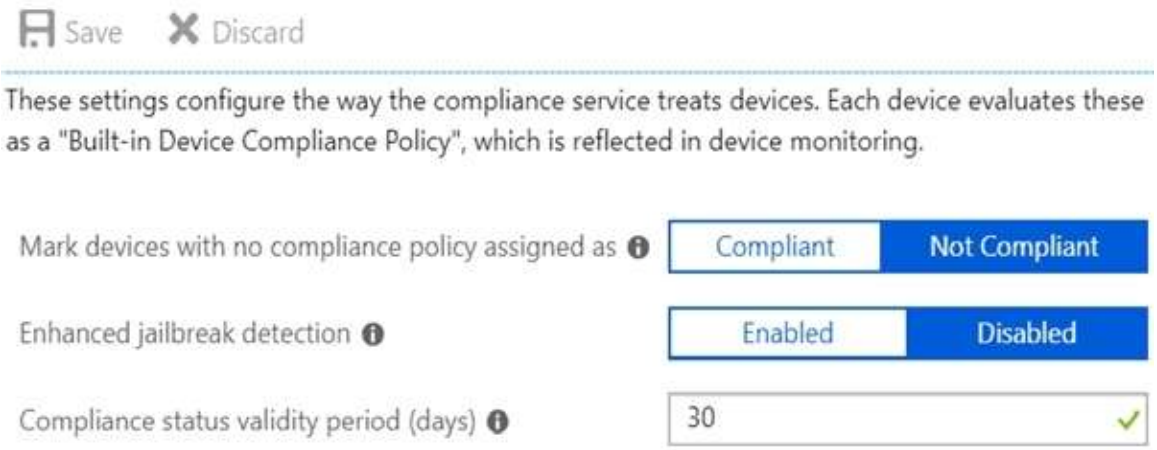


Explanation:
https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports
https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

QUESTION 187
Hotspot Question
In Microsoft Intune, you have the device compliance policies shown in the following table.

Name	Type	Encryption	Windows Defender antimalware	Mark device as not compliant	Assigned to
Policy1	Windows 8	Require	*Not applicable*	5 days	Group1
Policy2	Windows 10	Not configured	Require	7 days	Group2
Policy3	Windows 10	Required	Require	10 days	Group2

The Intune compliance policy settings are configured as shown in the following exhibit.



On June 1, you enroll Windows 10 devices in Intune as shown in the following table.

Name	Use BitLocker Drive Encryption (BitLocker)	Windows Defender	Member of
Device1	No	Enabled	Group1
Device2	No	Enabled	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On June 4, Device1 is marked as compliant.	○	○
On June 6, Device1 is marked as compliant.	○	○
On June 9, Device2 is marked as compliant.	○	○

Answer:

Answer Area

Statements	Yes	No
On June 4, Device1 is marked as compliant.	○	○
On June 6, Device1 is marked as compliant.	○	○
On June 9, Device2 is marked as compliant.	○	○

Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

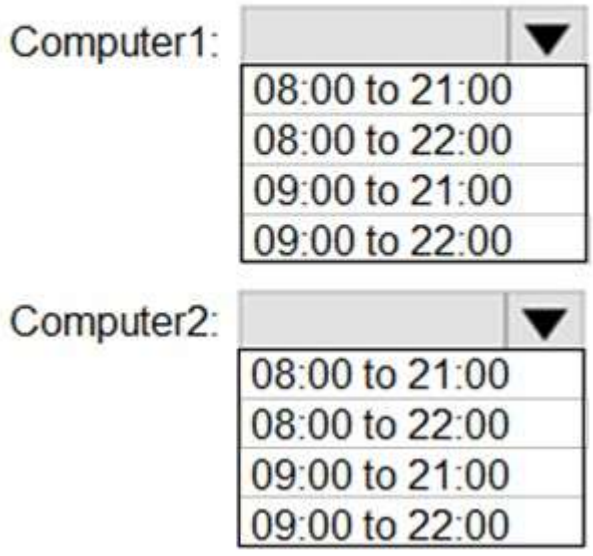
QUESTION 188
Hotspot Question
Your network contains an Active Directory domain named contoso.com that syncs to Azure Active Directory (Azure AD). The domain contains computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of
Computer1	Group1
Computer2	Group2

All the computers are enrolled in Microsoft Intune.
You configure the following Maintenance Scheduler settings in the Default Domain Policy:
- Turn off auto-restart for updates during active hours: Enabled
- Active hours start: 08:00
- Active hours end: 22:00

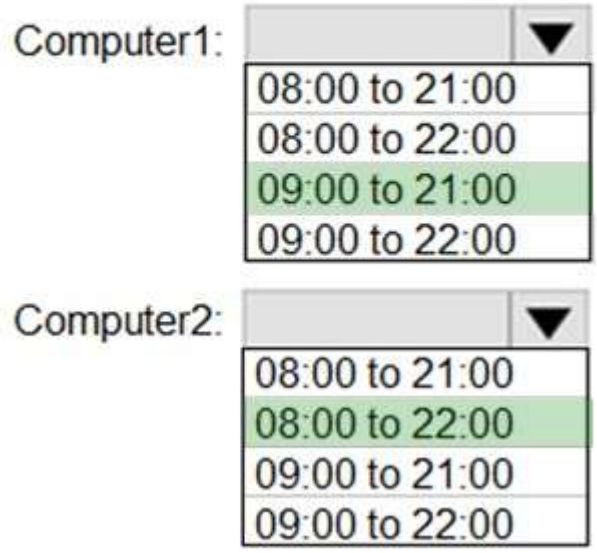
In Intune, you create a device configuration profile named Profile1 that has the following OMA-URI settings:
./Device/Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP set to value 1
./Device/Vendor/MSFT/Policy/Config/Update/ActiveHoursStart set to value 9
./Device/Vendor/MSFT/Policy/Config/Update/ActiveHoursEnd set to value 21
You assign Profile to Group1.
How are the active hours configured on Computer1 and Computer2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area

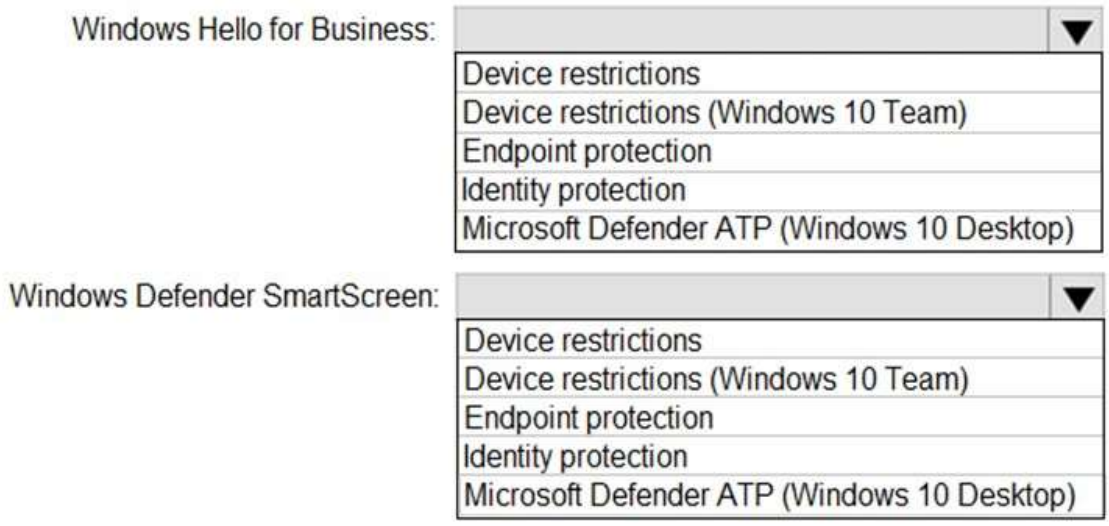


Explanation:
https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-controlpolicyconflict

QUESTION 189
Hotspot Question
You have a Microsoft 365 subscription.
You have 25 Microsoft Surface Hub devices that you plan to manage by using Microsoft Endpoint Manager.
You need to configure the devices to meet the following requirements:
- Enable Windows Hello for Business.
- Configure Microsoft Defender SmartScreen to block users from running unverified files.

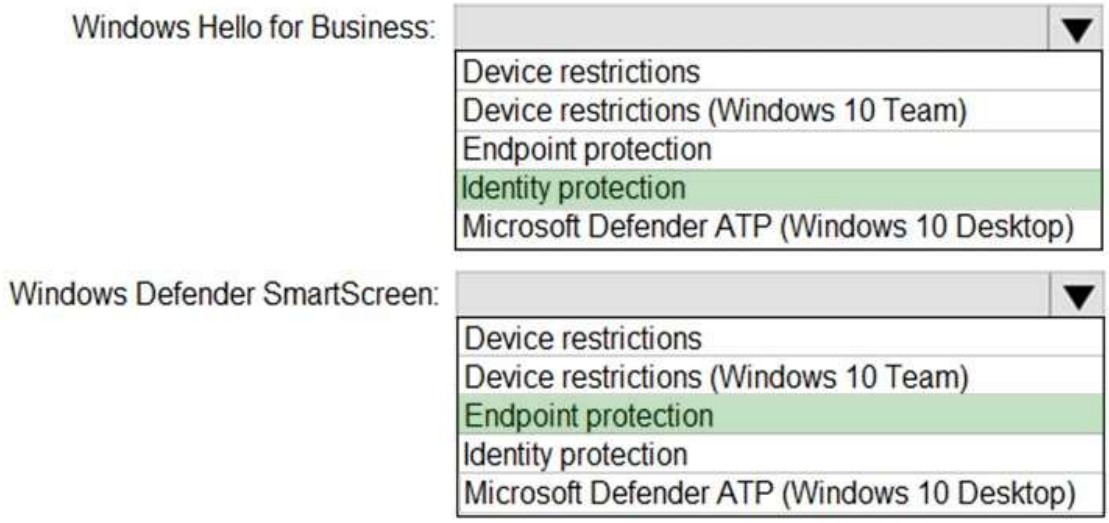
Which profile types should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/identity-protection-windows-settings?toc=/intune/configuration/toc.json&bc=/intune/configuration/breadcrumb/toc.json
https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10?toc=/intune/configuration/toc.json&bc=/intune/configuration/breadcrumb/toc.json

QUESTION 190
Hotspot Question
You have a Microsoft 365 subscription.
You plan to enroll devices in Microsoft Endpoint Manager that have the platforms and versions shown in the following table.

Platform	Version
Android	8, 9
iOS	11, 12

You need to configure device enrollment to meet the following requirements:
- Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager.
- Ensure that devices are added to Microsoft Azure Active Directory (Azure AD) groups based on a selection made by users during the enrollment.

Which device enrollment setting should you configure for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- Enrollment restrictions
- Windows enrollment

Answer:

Answer Area

Ensure that only devices that have approved platforms and versions can enroll in Endpoint Manager:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- Device categories
- **Enrollment restrictions**
- Windows enrollment

Ensure that devices are added to Azure AD groups based on a selection made by users during enrollment:

- Android enrollment
- Apple enrollment
- Corporate device identifiers
- **Device categories**
- Enrollment restrictions
- Windows enrollment

Explanation:
https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set
https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping

QUESTION 191
Hotspot Question
Your company has 1,000 Windows 10 devices that are enrolled in Windows Analytics.
You need to view the following information:
- The number of devices that are vulnerable to Spectre and Meltdown vulnerabilities
- The number of devices that have Windows Defender real-time protection turned off

Which Windows Analytics solutions should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Note: Windows Analytics is now known as Desktop Analytics and Windows Defender is now known as Microsoft Defender Antivirus

QUESTION 192
Hotspot Question
A company named A.Datum Corporation uses Microsoft Endpoint Configuration Manager, Microsoft Intune, and Desktop Analytics.
A.Datum purchases a company named Contoso, Ltd. Contoso has devices that run the following operating systems:
- Windows 8.1
- Windows 10
- Android
- iOS

A.Datum plans to use Desktop Analytics to monitor the Contoso devices.
You need to identify which devices can be monitored by using Desktop Analytics and how to add the devices to

Desktop Analytics.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Devices that can be monitored by using Desktop Analytics:
- Windows 10 only
- Windows 10, Android, and iOS only
- Windows 8.1 and Windows 10 only
- Windows 8.1, Windows 10, Android, and iOS

To add a device to Desktop Analytics, you must:
- Enroll the device in Microsoft Intune.
- Install the Endpoint Configuration Manager agent.
- Install the Microsoft Monitoring Agent.

Answer:

Answer Area

Devices that can be monitored by using Desktop Analytics:
- Windows 10 only
- Windows 10, Android, and iOS only
- **Windows 8.1 and Windows 10 only**
- Windows 8.1, Windows 10, Android, and iOS

To add a device to Desktop Analytics, you must:
- Enroll the device in Microsoft Intune.
- **Install the Endpoint Configuration Manager agent.**
- Install the Microsoft Monitoring Agent.

Explanation:
https://docs.microsoft.com/en-us/mem/configmgr/desktop-analytics/overview