

1 - Implement modern device services

Test ID: 178015650

Question #1 of 26

Question ID: 1257252

Nutex Corporation manages a consortium of community colleges. For security, they would like to automate the deployment of apps to college-provided student devices. Nutex has an Intune subscription as well as a premium Azure AD license and an Office 365 E3 subscription. All laptops are Windows 8 or higher, and all mobile devices are the latest version of IOs.

What will you suggest as the best option?

- X **A)** Microsoft Store for Business
- X **B)** Microsoft Store for Business connected with Microsoft Intune.
- X **C)** Microsoft Store for Education
- X **D)** Azure App Service
- ✓ **E)** Microsoft Intune

Explanation

Microsoft Intune is the only solution for this scenario due to the variety of operating systems. Intune will need to be chosen as the Mobile Device Management (MDM) via the Azure portal.

You would not use the Microsoft Store for Business, as Windows 10 is a prerequisite and there are other OSes in the scenario. In addition, some of these apps may be line-of-business apps which are apps that are written-in-house..

You would not use the Microsoft Store for Business connected with Microsoft Intune, as Windows 10 is a prerequisite and there are other OSes in the scenario. In addition, some of these apps may be line-of-business apps.

You would not use the Microsoft Store for Education as Windows 10 is a prerequisite and there are other OSes in the scenario. In addition, some of these apps may be line-of-business apps.

You would not use the Azure App Service. This is a service to build and deploy web apps.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Intune > Add apps to Microsoft Intune](#)

[Docs > Microsoft Store for Business > Prerequisites for Microsoft Store for Business and Education](#)

Question #2 of 26

Question ID: 1257244

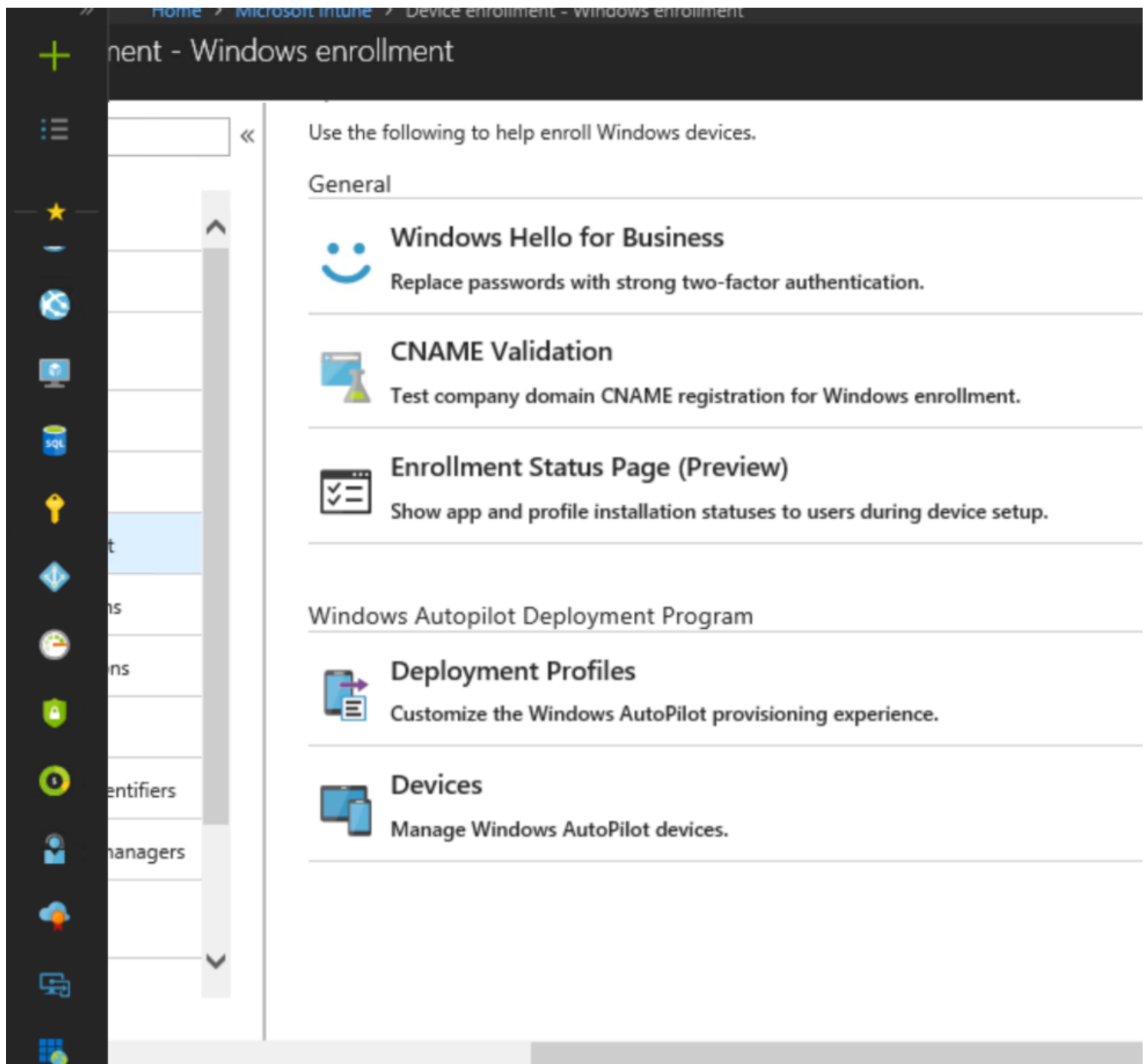
The Nutex Corporation plans to deploy Windows Hello for Business for SSO to Microsoft 365 services. All devices used by users run Windows 10 Enterprise and will be hybrid Azure AD joined.

What is a prerequisite of the deployment?

- ✓ **A)** Microsoft Intune enrollment
- X **B)** Devices that allows biometric authentication
- X **C)** Upgrade all domain controllers to Windows Server 2016
- X **D)** Device that has TPM 2.0 chip

Explanation

To configure Windows Hello for Business Device enrollment, you will need to click **device enrollment** in **Microsoft Intune**. To do this, you need to select **All Services** in the Azure Portal and find Microsoft Intune from the list of services. Choose **Windows Enrollment**, and click **Windows Hello for Business**.



Windows Hello replaces traditional passwords with two-factor authentication. The authentication ties the credential to the device and uses a biometric or a PIN.

The devices do NOT have to have a Trusted Platform Module (TPM) 2.0 chip. Windows Hello provisioning process creates a cryptographic key pair bound to the Trusted Platform Module (TPM) with a device that has a TPM 2.0 chip or with TPM that is in software.

You do not have to enable **Allow biometric authentication** in the Windows Hello for Business configuration. You only need to set this option if you want to allow users to use fingerprint, facial recognition, or other biometrics. You can use a PIN from a TPM instead of a biometric gesture to access keys and obtain a signature to validate user possession of the private key.

You do not have upgrade the domain controllers to Windows Server 2016. This is only needed if you want your environment to use the Windows Hello for Business key rather than a certificate. You can configure your environment to use the Windows Hello for Business certificate rather than key with older domain controllers than Windows Server 2016.

Objective:

Implement modern device services

Sub-Objective:

Implement Mobile Device Management (MDM)

References:

[Docs > Windows Hello for Business > Configure Azure AD joined devices for On-premises Single-Sign On using Windows Hello for Business](#)

[Docs > Identity and access protection > Windows Hello for Business Overview](#)

Question #3 of 26

Question ID: 1257255

Dreamsuites Incorporated has added Intune and Azure AD to their suite of Microsoft offerings. They plan to provide the newest iPads for corporate visitors when visiting the regional factories. They have created a **Visitors** Azure AD group to which the devices are added.

Dreamsuites would like these devices to connect automatically to the local wireless network, which does not broadcast its SSID.

What steps are included in the solution? (Choose all that apply.)

- ☒ **A)** Create an Intune iOS device profile. Under **Wi-Fi** settings, choose **Disable** for **Hidden network**.
- ☒ **B)** Create an Intune iOS device profile. Under **Wi-Fi** settings, choose **Enable** for **Connect Automatically**
- ☒ **C)** Create an Intune iOS device profile. Under **Wi-Fi** settings, choose **Enable** for **Hidden network**.
- ☒ **D)** In Intune, go to **Device Configuration>Profiles>Assignments** and **Include** the **Visitors** group.
- ☒ **E)** Create an Intune iOS device profile. Under **Wi-Fi** settings, configure **SSID**.
- ☒ **F)** Create an Azure AD conditional access policy to create a **Location** condition.

Explanation

You will want to create an Intune iOS device profile. Under **Wi-Fi** settings, choose **Enable** for **Connect Automatically**. This setting is a requirement of the scenario.

You will want to create an Intune iOS device profile. Under **Wi-Fi** settings, configure **SSID**. The scenario states that the SSID is not broadcast, so you need this information in the profile.

You will need to go to **Device Configuration>Profiles>Assignments** and **Include** the **Visitors** group. Profiles are inactive until they are assigned.

You do not need to create an Intune iOS device profile and under **Wi-Fi** settings, choose **Enable** for **Hidden network**. This would allow the network name to appear in the list of available connections, but is not indicated in the scenario, nor is it relevant as the devices will connect automatically.

You do not need to create an Intune iOS device profile and under **Wi-Fi** settings, choose **Disable** for **Hidden network**. This would hide the network name from a list of available connections, but is not indicated in the scenario, nor is it relevant as the devices will connect automatically.

You do not need to create an Azure AD conditional access policy to create a location condition. This condition would determine access to cloud apps based on network location and is not relevant to the scenario requirements.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Intune > Apply features and settings on your devices using device profiles in Microsoft Intune](#)

[Docs > Intune > Create a device profile in Microsoft Intune](#)

[Docs > Intune > Add Wi-Fi settings for iOS devices in Microsoft Intune](#)

Question #4 of 26

Question ID: 1257248

Nutex Corporation has allowed users to bring their own devices (BYOD). As a security advisor, you have chosen to use Intune and Azure AD to enforce device compliance. All non-compliant devices will be denied access after a grace period. You want to notify users of these devices via email.

What will you include in your plan to achieve this?

- X **A)** Create a conditional access policy and add a location condition.
- X **B)** Create a compliance policy, and sync all devices.

- X **C)** Create a compliance policy and add a scope tag.
- X **D)** Create a conditional access policy and add a device state condition.
- ✓ **E)** Create a compliance policy and add an action for non-compliant devices.

Explanation

You will want to create a compliance policy and add an action for non-compliant devices. The action will be an emailed non-compliance notification.

You do not need to create a compliance policy and sync all devices. While users can choose to manually sync, devices are automatically synched via a refresh schedule (typically every 8 hours). This sync does not create a notification.

You do not need to create a conditional access policy and add a location condition. A location condition triggers an action based on location, not device compliance.

You do not need to create a conditional access policy and add a device state condition. A device state condition triggers an action based on compliance, but notification is not a choice of action in such a policy.

You do not need to create a compliance policy and add a scope tag. This can be used to limit the groups that the policy applies to, but in this scenario, we want all devices.

Objective:

Implement modern device services

Sub-Objective:

Manage device compliance

References:

[Docs > Intune > Set rules on devices to allow access to resources in your organization using Intune](#)

[Docs > Intune > Automate email and add actions for noncompliant devices in Intune](#)

Question #5 of 26

Question ID: 1257245

You have a Microsoft 365 tenant. All users are assigned the Enterprise Mobility + Security license. You need to ensure that users join and register their Windows 10 devices in Azure Active Directory. Once registered, the device is managed with Intune.

All the devices are owned by the tenant. None of the employees will be registering their own devices.

What should you configure? Place the appropriate steps in the correct order.

{UCMS id=5764125050273792 type=Activity}

Explanation

You should choose the following steps:

1. Select **Azure Active Directory** from the Azure portal
2. Select **Mobility**
3. Select **Microsoft Intune**
4. Configure **MDM User scope**

To enable Windows 10 automatic enrollment, you will need a Premium subscription and a Microsoft Intune subscription. You will choose **Azure Active Directory** from the Azure portal. From the **Azure Active Directory** page, choose **Mobility (MDM and MAM)**. From the **Mobility (MDM and MAM)** page, choose **Microsoft Intune**.

You should configure the **MDM User scope**. This option allows user's to be managed by Intune. The devices can automatically enroll for management with Intune. Two-factor authentication is not enabled by default, but is highly recommended when registering a device.

You should not configure the **MAM User scope**. When you choose the **MAM User scope**, device uses Windows Information Protection (WIP) Policies (if you configured them) rather than being MDM enrolled. The MAM user scope takes precedence if both MAM user scope for BYOD devices. In this scenario, the devices are corporate-owned and are not BYOD devices.

Objective:

Implement modern device services

Sub-Objective:

Implement Mobile Device Management (MDM)

References:

[Docs > Intune > Enrollment > Set up enrollment for Windows devices](#)

Question #6 of 26

Question ID: 1257254

The IT team at Nutex Corporation tries to keep their Windows 10 Enterprise devices updated as often as possible. However, there is a lack of consistency in models and brands across physical locations. Consequently, there are often device crashes due to driver issues.

Nutex needs to track these issues so they can take corrective action? What solution would you recommend?

- X **A)** Remote Monitoring Solution Accelerator
- X **B)** Windows Analytics Update Compliance
- X **C)** The Reports section of the Microsoft 365 Security Center

- X **D)** Windows Analytics Upgrade Readiness
- ✓ **E)** Windows Analytics Device Health

Explanation

You should suggest the Windows Analytics Device Health solution. Windows Analytics Device Health can identify devices that crash frequently as well as the drivers causing crashes. This uses diagnostic data that is already part of Windows 10 devices.

You would not suggest Windows Analytics Update Compliance. This solution focuses on update management and device capability. While useful, it does not meet the requirement for device crash information.

You would not suggest the Remote Monitoring Solution Accelerator. This solution is useful for monitoring remote machines as part of an IOT solution but does not provide device crash reporting.

You would not suggest the Reports section of the Microsoft 365 Security Center. The device alerts in this section relate to breach activity and potential threats, not physical device information.

You would not suggest Windows Analytics Upgrade Readiness. While useful, it does not meet the requirement for device crash information.

Windows Analytics Device Health requires a Windows 10 Enterprise or Education subscription.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Windows Analytics overview](#)

[Docs > Windows > Monitor the health of devices with Device Health](#)

Question #7 of 26

Question ID: 1353609

You configure a conditional access policy with the following settings:

Locations

Configure ⓘ

Yes No

Include Exclude

☐ Any location

☒ All trusted locations

☐ Selected locations

Select None >

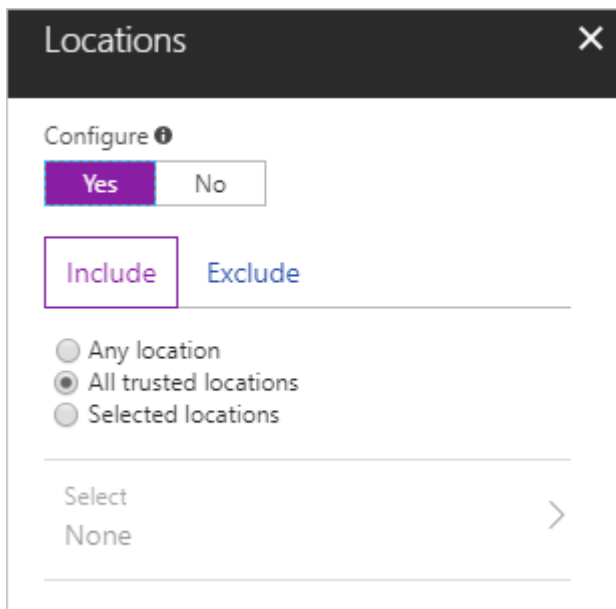
Users report that they cannot sign in to Microsoft Active Directory (Azure AD) on their Windows 10 devices while they are inside the warehouse building adjacent to the main office.

What should you configure so that users can sign in to Microsoft Active Directory (Azure AD) on their Windows 10 devices while they are in the warehouse building? The solution must use the principle of least privilege.

- X **A)** Open the Conditional Access policy and choose **Grant access** and **Require device to be marked as compliant**.
- X **B)** Open the **Locations** tab of the Conditional Access policy and choose **Any location** on the **Include** section.
- ✓ **C)** Configure a named location on the Conditional Access policy.
- X **D)** Open the Conditional Access policy and choose **Grant access** and **Require multi-factor authentication**.

Explanation

You should configure a named location on the Conditional Access policy. You can use a named location to specify a group of IP address ranges for a location, country, or region. With a named location, you can specify IP ranges and specify the location as a trusted location.



The existing Conditional Access policy includes all trusted locations. Trusted locations are typically places that are managed by your IT department, such as the warehouse building that is adjacent to the main office.

You should not choose **Any location** on the **Include** section on the **Locations** tab of the Conditional Access policy. Selecting the **Any location** setting causes the policy to be applied to all IP addresses. While this solution would work, it does not limit the addresses to a location. The users would be able to log in from the warehouse, but could also log in from other areas that may be prohibited.

You should not choose **Grant access** and then choose either **Require device to be marked as compliant** or **Require multi-factor authentication** for the users. While these settings can improve security, they are not restricting the users to a specific location, such as the warehouse.

Objective:

Implement modern device services

Sub-Objective:

Manage device compliance

References:

[Azure > Conditional access > What is the location condition in Azure Active Directory Conditional Access?](#)

Question #8 of 26

Question ID: 1257256

Verigon Corp has partnered with a regional hospital to provide some external services. They have stringent data protection needs due to HIPAA and similar regulations. All Verigon employees use Office 365 applications on their iOS and Windows 10 devices. Verigon is licensed for Intune and Azure AD.

You need to prevent Outlook users from copying and pasting information from their corporate email into other applications. What steps will be included in your solution? (Choose all that apply.)

- ✓ **A)** Create an Azure AD account for all device users.
- X **B)** Add the devices to an Azure AD security group
- ✓ **C)** Add the users to an Azure AD security group.
- X **D)** Create IOs and Windows 10 device profiles.
- ✓ **E)** In Intune, configure an App Protection Policy and the Data Protection settings.
- X **F)** Enroll all devices in Intune.

Explanation

You will need to create an Azure AD account for all device users. App Protection policies are assigned to users.

You will need to add the users to an Azure AD security group because the app protection policies are applied to users.

In Intune, you will need to configure an App Protection Policy and the Data Protection settings. In this scenario you would choose Outlook under **Client Apps > App Protection Policy> Create Policy> Apps**.

Note that this scenario is focused only on App Protection. For many other scenarios, such as device compliance, devices do need to be enrolled in Azure AD.

You do not need to enroll all devices in Intune. Devices do not need to be enrolled in an MDM for this scenario, as App Protection policies apply to users, not the devices. This scenario describes MAM, mobile application management, versus MDM.

You do not need to create IOs and Windows 10 device profiles to meet the goals of the scenario, as the app protection policies do not apply to devices.

You do not need to add the devices to an Azure AD security group, because app protection policies are not applied to devices.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Intune > App protection policies overview](#)

[TechTarget > How to use Intune app protection without MDM enrollment](#)

Question #9 of 26

Question ID: 1257243

Nutex Corporation has chosen Intune as their MDM solution. As part of their security model, it has been decided that only the Sales group members will be allowed to bring two of their own devices (BYOD). What steps in Intune will you take as part of this implementation? (Choose all that apply.)

- ✓ **A)** Add the Sales group under Assignments
- ✓ **B)** Create a device type restriction to allow personally owned IOS devices.
- ✓ **C)** Create a device type restriction to allow personally owned Android devices.
- X **D)** Create a device type restriction to set a version range.
- ✓ **E)** Set the Device Limit Restriction to 2

Explanation

You will want to create a device type restriction to allow personally owned IOS devices. The scenario does not indicate what platforms users have so you will need to allow all platforms.

Dashboard > Microsoft Intune > Device enrollment - Enrollment restrictions > Create restriction

Create restriction

Device limit restriction

✓ Basics

✓ **Device limit**

③ Assignments

④ Review + create

Specify the maximum number of devices a user can enroll.

Device limit

You do not need to create a device type restriction to set a version range. This setting relates to the version of the platform software, which is not relevant here.

You will want to add the Sales group under Assignments. After you create an enrollment restriction, it must be assigned to the group(s) you want it to apply to.

You need to set the Device Limit Restriction to 2. This is a limit on how many devices a user may enroll. Although not required by the scenario, setting this to 1 adds an additional security barrier. By default, a single user can enroll up to 15 devices.

You will want to create a device type restriction to allow personally owned Android devices. The scenario does not indicate what platforms users have so you will need to allow all platforms.

There are other necessary steps not offered here. You would also want to block the appropriate non-Sales groups. If there are overlapping enrollment restrictions for a group, the priority setting would be used as a tiebreaker.

Objective:

Implement modern device services

Sub-Objective:

Implement Mobile Device Management (MDM)

References:

<https://docs.microsoft.com/en-us/intune/enrollment-restrictions-set>

<https://www.systemcenterdudes.com/security-features-microsoft-intune/>

Question #10 of 26

Question ID: 1257264

You need to configure Intune to enroll iOS devices purchased through Apple's Device Enrollment Program (DEP).

When users turn on iOS devices such as iPads, you want to have Setup Assistant automatically run with preconfigured settings and enroll the device into Intune.

What should you do? Place the appropriate steps in the correct order

{UCMS id=5095962252935168 type=Activity}

Explanation

You should do the following:

1. Acquire the Apple MDM Push certificate.
2. Get an Apple DEP token.
3. Create an Apple enrollment profile.
4. Synchronize managed devices.

You need the Apple MDM Push certificate for Intune to manage iOS devices or macOS devices. The Apple MDM Push certificate needs to be added to Intune so your users can enroll devices using the Company Portal app or by using one of Apple's bulk enrollment methods, such as the Device Enrollment Program. You can get the certificate by choosing Device enrollment > Apple Enrollment > Apple MDM Push Certificate in Intune. An Apple MDM Push certificate is a prerequisite for iOS enrollment.

You will need to get an Apple DEP token to enroll iOS devices with DEP. The DEP token (.p7m) file lets Intune sync information about your DEP devices, allows Intune to upload enrollment profiles to Apple, and assign iOS devices to these profiles.

After the token has been installed, you will need to define settings for the group of devices. You can create a device enrollment profile to apply settings to the devices.

Once Intune can manage your devices, you can see your managed devices in Intune in the Azure portal by synchronize Intune with Apple.

You should not add your account as a device enrollment manager. Apple's DEP does not work with device enrollment managers.

Objective:

Implement modern device services

Sub-Objective:

Plan Windows 10 deployment

References:

[Docs > Intune > Automatically enroll iOS devices with Apple's Device Enrollment Program](#)

Question #11 of 26

Question ID: 1257258

You have a Microsoft Azure Active Directory (Azure AD) tenant and have a Microsoft 365 subscription.

You need to ensure that users can manage the configuration settings for the corporate-owned mobile devices issued to them in your organization. What should you configure before you enroll devices?

- ☐ A) Configure multi-factor authentication (MFA)
- ☒ B) Set the mobile device management (MDM) authority
- ☐ C) Configure a MAM User scope in the automatic enrollment settings
- ☐ D) Switch the Intune subscription

Explanation

You will have to set the mobile device management (MDM) authority. Mobile devices must have an MDM authority chose for the device to be managed. You can choose any of the following configurations:

- Intune MDM Authority – Sets Intune as the MDM authority to manage mobile devices
- Configuration MDM Authority – Sets Configuration Manager as the MDM to manage mobile devices with System Center Configuration Manager and Microsoft Intune
- None – No MDM is chosen

Choose MDM Authority



Mobile Device Management Authority

Choose whether Intune or Configuration Manager is your mobile device management authority.

Choose Intune as your MDM authority to manage mobile devices with Microsoft Intune only.

Choose Configuration Manager as your MDM authority to manage mobile devices with System Center Configuration Manager and Microsoft Intune.

Mobile devices cannot be managed if an MDM authority is not chosen.

Learn more about [choosing your MDM Authority](#).

- ☒ Intune MDM Authority
- ☐ Configuration Manager MDM Authority
- ☐ None

You do not have to switch the Intune subscription. You would have to change to a different subscription if you add a Microsoft Intune (either a trial subscription or paid subscription) to Configuration Manager. You would not need to change the Intune subscription for users to manage the configuration settings for all mobile devices.

You should not configure a MAM User scope. When you choose the MAM User scope, Windows 10 device uses Windows Information Protection (WIP) Policies (if you configured them) rather than being MDM enrolled. The MAM user scope takes precedence if both MAM user scope for BYOD devices. In this scenario, the devices are corporate-owned and are not BYOD devices.

You do not have to configure multi-factor authentication (MFA) in this scenario to allow users to manage the configuration settings for the corporate-owned mobile devices issued to them in your organization. MFA allows a user or device to be authenticated by more than a password.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Intune > Set the mobile device management authority](#)

Question #12 of 26

Question ID: 1353610

Dreamsuites Inc employees are all using laptops with the latest version of Windows 10 Enterprise. Dreamsuites has an enterprise Office 365 license. As an administrator, you want to offer users an optional selection of curated online-licensed apps such as **Sway** and **Wunderlist**. However, you want to assign control so that an administrator has complete control over the collection of apps available.

What steps will be involved in your configuration of the Microsoft Store for Business (MSfB)? (Choose all that apply.)

- ☐ **A)** Assign the *Basic Purchaser Role* to the employee responsible for MSfB.
- ☒ **B)** Create Azure AD accounts for all employees.
- ☒ **C)** Edit a group policy to show only the Private Store in the Microsoft Store app.
- ☒ **D)** Have an Azure AD Global Administrator sign up for the MSfB.
- ☐ **E)** Configure an MDM provider.

Explanation

You will need to create Azure AD accounts for all employees.

You must have an Azure AD Global Administrator sign up for the MSfB.

You will want to edit a group policy to show only the Private Store in the Microsoft Store app. This will prevent users from installing any "standard" store apps. You can configure this setting in a Group Policy object (GPO) by going to **User Configuration or Computer Configuration > Administrative Templates > Windows Components**, and then choose **Store**. Each private store app also has a "**Private Store Availability**" setting. The setting is "**only display the private store within the Microsoft Store app**".

Apps can be assigned to users and they will get an email with a link to install. Or they can choose the apps under the **MyLibrary** tab in their Microsoft Store app.

The scenario does not require you to configure an MDM provider. MDM tools can optionally sync with the MSfB to manage apps with offline licenses, which are not indicated here.

The scenario does not require you assign the *Basic Purchaser Role* to the employee responsible for MSfB. This role does not allow for management of items. *Billing Administrator* is a role that can purchase and distribute apps.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Microsoft Store for Business > Distribute apps using your private store](#)

[Docs > Windows > Configuration > Configure access to Microsoft Store](#)

[Docs > Microsoft Store for Business > Sign up and get started](#)

Question #13 of 26

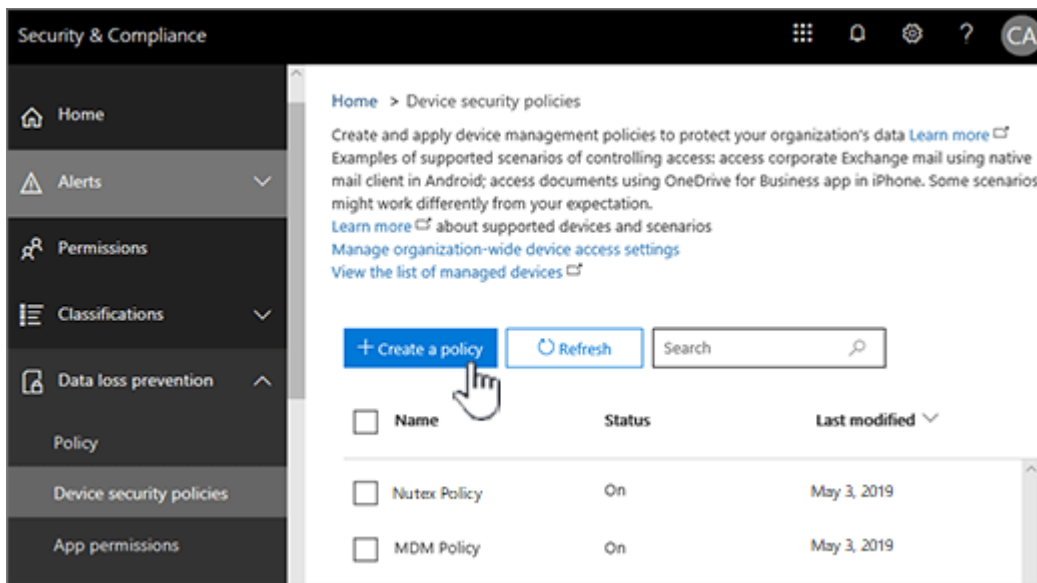
Question ID: 1257240

Nutex Corporation needs a mobile device management solution to gain more control over their devices. As employees are heavy users of several Office 365 services, Nutex has an Office 365 E3 license. Nutex does not have in-house applications. They would like to manage the iOS mobile devices used by the sales department as well as a few Windows phones. What will you suggest as a basic MDM solution to best fit their needs?

- X **A)** Microsoft Intune Hybrid
- ✓ **B)** MDM for Office 365
- X **C)** Windows Autopilot
- X **D)** Microsoft Intune
- X **E)** Configuration Manager (SCCM)

Explanation

MDM for Office 365 would meet all of Nutex Corporation requirements. Their focus is on devices more than applications. Devices can be managed via policies in the *Security and Compliance Center* in Office 365.



You should not suggest Microsoft Intune as it exceeds the needs of the scenario. Intune offers the MDM features of MDM for Office 365, plus control over app behavior, which was not indicated as a need. Intune can also manage PCs. While this solution would work, it is not the best answer for Nutex.

You should not suggest Configuration Manager. Nutex needs a solution that can also manage iOS devices, which cannot be done with SCCM.

You should not suggest Microsoft Intune Hybrid. This bridge between Intune and on-premises management has been deprecated by Microsoft and is no longer supported.

You should not suggest Windows Autopilot. Windows Autopilot is used to simplify the setup of new Windows 10 devices, and is not an MDM solution. (However, Autopilot can be used to automatically enroll devices into MDM services.)

Objective:

Implement modern device services

Sub-Objective:

Implement Mobile Device Management (MDM)

References:

<https://support.office.com/en-us/article/choose-between-mdm-for-office-365-and-microsoft-intune-c93d9ab9-efb2-4349-9b93-30c30562ee22>

<https://docs.microsoft.com/en-us/sccm/mdm/understand/choose-between-standalone-intune-and-hybrid-mobile-device-management>

<https://support.office.com/en-us/article/capabilities-of-built-in-mobile-device-management-for-office-365-a1da44e5-7475-4992-be91-9ccce25905b0>

Question #14 of 26

Question ID: 1257257

Nutex Corp wants to take full advantage of the mobile device security options available with their Intune, Office 365, and Azure AD premium subscriptions.

What are some available components to help them create a multi-layered security model for their enrolled devices? (Choose all that apply.)

- ✓ **A)** Intune Device compliance policies.
- X **B)** Office 365 ATP (Threat Protection Service)
- ✓ **C)** Intune Device configuration profiles.
- ✓ **D)** Azure AD conditional access policies.
- ✓ **E)** Intune App Protection policies.

Explanation

Intune Device configuration profiles can be used to configure device settings for various platforms. These settings can include device restrictions, device features, email, Wi-Fi, and more.

Intune Device compliance policies are used in combination with Azure Ad conditional access policies to check a device for certain settings and then set a compliant flag.

Azure AD conditional access policies apply to Azure AD-joined (and hybrid joined) devices. The policies can be set to include device compliance requirements.

Intune App Protection policies provide an application layer defense that applies to Azure AD accounts. They can be used with or without device enrollment.

Office 365 ATP (Threat Protection Service) is not a mobile device security option. ATP is a cloud-based email filtering service.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Intune > App protection policies overview](#)

[Azure > Active Directory > Conditional Access: Require compliant devices](#)

[Docs > Intune > Set rules on devices to allow access to resources in your organization using Intune](#)

Question #15 of 26

Question ID: 1353611

The Nutex Corporation's client computers run Windows 10 Enterprise. These client computers are domain joined. You need to configure Windows Update for Business to do the following;

- Delay the installation of new Windows builds from being updated for 30 days to test applications
- Receive new builds of Windows before the general public

You do not want to participate in identifying and reporting issues to Microsoft or providing new suggestions on new functionality.

Which Group Policy settings must you enable? (Choose all that apply.)

- ☐ **A)** Under the **Data collection and Preview Builds** Group Policy, configure **Allow Telemetry** to 1
- ☒ **B)** Under Windows Update policy settings, enable **Manage preview builds**
- ☐ **C)** Under the **Data collection and Preview Builds** Group Policy, enable **Configure Connected User Experiences and Telemetry**
- ☒ **D)** Select **Slow** as the readiness level for the updates you want to receive
- ☐ **E)** Select **Fast** as the readiness level for the updates you want to receive
- ☒ **F)** Under Windows Update policy settings, configure **Select when Preview Builds and Feature Updates are received**

Explanation

You should enable **Manage preview builds** under **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update > Windows Update for Business**. This setting enables installation of Insider Preview builds on a Windows 10 device and can stop Insider Preview build updates once the release is public or prevent installation on a device.

You should configure **Select when Preview Builds and Feature Updates are received** under **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update > Windows Update for Business**. This policy allows you configure the Ring (Fast, Slow, Release Preview) from which devices receive Insider Preview builds.

In this scenario, you should select **Slow** instead of **Fast**. The Slow setting allows the device to receive new builds of Windows before they are available to the public, just like the Fast setting. However, unlike the Fast setting, the device does not participate in identifying and reporting issues to Microsoft.

Select when Preview Builds and Feature Updates are received

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on: At least Windows Server or Windows 10

Options:

Select the Windows readiness level for the updates you want to receive:

Fast

After a Preview Build or Feature Update is released, defer receiving it for this many days:

0

Pause Preview Builds or Feature Updates starting:

(format yyyy-mm-dd example: 2016-10-30)

Help:

Enable this policy to specify the level of Preview Build or Feature Updates to receive, and when.

- * Preview Build - Fast: Devices set to this level will be the first to receive new builds of Windows with features not yet available to the general public. Select Fast to participate in identifying and reporting issues to Microsoft, and provide suggestions on new functionality.
- * Preview Build - Slow: Devices set to this level receive new builds of Windows before they are available to the general public, but at a slower cadence than those set to Fast, and with changes and fixes identified in earlier builds.
- * Release Preview: Receive builds of Windows just before Microsoft releases them to the general public.
- * Semi-Annual Channel (Targeted): Receive feature updates when they are released to the general public.
- * Semi-Annual Channel: Feature updates will arrive when they are declared Semi-Annual Channel. This usually occurs about 4 months after Semi-Annual Channel (Targeted), indicating that Microsoft, Independent Software Vendors (ISVs), partners and customer believe that the release is ready for broad deployment.

You should configure the telemetry to level 2 (enhanced) or higher to enable installation of Insider Preview builds. The **Data collection and Preview Builds** Group Policy is under **Computer Configuration > Policies > Administrative Templates > Windows Components**. The Telemetry must be set to 2 (Enhanced) or 3 (Full). Telemetry level 1 (Basic) is not sufficient to enable installation of Insider Preview builds. By default, Windows 10 devices are configured with the **Allow Telemetry** configuration set to 3 (Full) by default.

You do not have to enable **Configure Connected User Experiences and Telemetry** under the **Data collection and Preview Builds** Group Policy. This setting allows you to forward Connected User Experience and Telemetry requests to a proxy server. This action does not apply in this scenario.

Objective:

Implement modern device services

Sub-Objective:

Plan Windows 10 deployment

References:

[Windows Insider > Installing and Managing Preview Builds Using Group Policy](#)

[Microsoft > Manage Insider Preview Builds](#)

Question #16 of 26

Question ID: 1257262

After successfully implementing all laptops to Windows 10, you have been tasked with improving Dreamsuites Corporation's core security. Dreamsuites has an E5 Windows 10 license.

What are some of the options that may be available with Windows 10 Enterprise for these laptops?(Choose all that apply.)

- ✓ **A)** Configuration Score
- ✗ **B)** Deduplication
- ✓ **C)** Encrypted Hard Drive
- ✓ **D)** Credential Guard
- ✓ **E)** Windows Hello
- ✗ **F)** System Insights
- ✓ **G)** Bitlocker

Explanation

Encrypted Hard Drive is a Windows 10 Enterprise option. This option uses Bitlocker encryption but offloads the operation to the latest class of hardware encrypted drives.

Bitlocker is an option on Windows 10 Enterprise as well as earlier versions.

Credential Guard is a Windows 10 Enterprise option. This introduces virtualization-based security to protect signed-in credentials.

Windows Hello for Business is a Windows 10 Enterprise option. Windows Hello is a two-factor credential as an alternative to passwords by including biometrics.

Configuration Score (formerly called Secure Score) is a Windows 10 Enterprise option. It offers a collective security score on devices based on several categories.

Deduplication is a feature of Windows Server, not Windows 10. Deduplication eliminates multiple copies of data and decreases the storage capacity.

System Insights is a feature of Windows Server, not Windows 10. System Insights uses predictive analytics capabilities natively to Windows Server to provide insight into the functioning of your servers.

Objective:

Implement modern device services

Sub-Objective:

Plan Windows 10 deployment

References:

[Docs > Security > Identity and access management](#)

[Docs > Security > Threat protection](#)

[Docs > Security > Information protection](#)

Question #17 of 26

Question ID: 1257261

Dreamsuites Incorporated needs to upgrade all devices in the Boston office. These are currently running the latest version of Windows 8.1. Dreamsuites wants to upgrade the office to the newest Windows 10 Enterprise edition.

As an administrator, you want to use the Upgrade Readiness solution of Windows Analytics to streamline the process. Dreamsuites has an Azure AD subscription.

What steps should you take? (Choose all that apply.)

{UCMS id=5670898188156928 type=Activity}

Explanation

You should choose the following

1. Identify important apps
2. Resolve issues
3. Deploy Windows
4. Monitor Deployment

You will use Upgrade Readiness to identify important apps. This allows you to tag apps to define their level of importance. By default, Upgrade Readiness automatically shows apps that are installed on less than 2% of computers.

You will use Upgrade Readiness to resolve issues. This gives you a chance to resolve existing application and drive upgrade issues before upgrading.

You will use Upgrade Readiness to deploy Windows. You have the option to deploy computers by group, which allows you to create a pilot group for testing.

After deploying Windows, you will use Upgrade Readiness to Monitor the deployment progress. You can see the status of any device that has attempted to upgrade in the past 30 days.

The devices must be configured to send their telemetry data to Azure before you can run the Upgrade Readiness analytics. You can automate this by distributing the Upgrade Readiness deployment script, usually via SCCM or via Powershell in Intune.

You do not need to use Upgrade Readiness to set the Target Version of Windows 10 in this scenario as it states that all of the laptops are Windows 8.1. The Target Version shows how many computers are already running the chosen version of Windows 10. This Azure blade defaults to the latest version.

Objective:

Implement modern device services

Sub-Objective:

Plan Windows 10 deployment

References:

[Docs > Deployment > Upgrade Readiness requirements](#)

[Docs > Deployment > Use Upgrade Readiness to manage Windows upgrades](#)

Question #18 of 26

Question ID: 1257260

Nutex Corporation is ready to upgrade the existing Windows 8.1 Enterprise devices in its Boston office. They want to keep the users' existing custom applications and setting while upgrading to the latest edition of Windows 10 Enterprise. Some devices are protected via Bitlocker. Nutex has an Azure AD and Intune license subscription. What method will best meet their needs?

- ✓ **A) In-place upgrade**
- X **B) Traditional refresh**
- X **C) Windows Autopilot**
- X **D) Azure AD integration with Intune**
- X **E) Subscription Activation**

Explanation

An In-place upgrade will keep all of the applications, data, settings, and drivers. It can be rolled back if needed. Nutex can use SCCM or the Microsoft Deployment Toolkit for deployment.

A traditional refresh would wipe the apps that did not come from the Windows Store, so this would not meet the needs of the scenario.

Windows Autopilot is for pre-configuring new devices, not upgrading existing ones.

Subscription Activation is useful to upgrade users from Windows 10 Pro to Windows 10 Enterprise when the user logs in to Azure AD. It does not meet the needs of the scenario.

Azure AD integration with Intune would allow for the final configuration of the device when it is joined to Azure AD, but this is not an upgrade solution.

Objective:

Implement modern device services

Sub-Objective:

Plan Windows 10 deployment

References:

[Microsoft 365 > Deploy > Step 2: Deploy Windows 10 Enterprise for existing devices as an in-place upgrade](#)

[Docs > Deploy > Windows 10 deployment scenarios](#)

Question #19 of 26

Question ID: 1257263

Your network contains an Active Directory domain named **nutex.com** that is synced to Microsoft Azure Active Directory (Azure AD). Your company has a Microsoft Intune subscription.

You want to concurrently manage Windows 10 devices by using both Configuration Manager and Microsoft Intune.

What should you configure? Place the appropriate steps in the correct order.

{UCMS id=5766517914337280 type=Activity}

Explanation

You should choose the following steps:

1. Configure a hybrid Azure AD join using Azure AD Connect
2. Use Client Settings to configure Configuration Manager clients to automatically register with Azure AD
3. Set up auto-enrollment of devices with Intune
4. Configure a Pilot group collection

You will need to set up a hybrid Azure AD to allow for integration of an on-premises AD with Azure AD. You can use Azure AD Connect to allow sync accounts in your on-premises Active Directory (AD) and the device object in Azure AD.


You will need to allow Configuration Manager clients to automatically register with Azure AD by configuring Client Settings. You should configure the Automatically register new Windows 10 domain joined devices with Azure Active Directory setting to **Yes**.

You should then set up auto-enrollment of devices with Intune. With automatic enrollment, users enroll their Windows 10 devices when a corporate-owned device is joined to Azure Active Directory or when a user adds their work account to their device.

Intune licenses must be assigned to each user. This action can be performed at any time during the process.

After product licenses assigned to users, Configuration Manager client configurations have been configured, and hybrid Azure AD setup has been configured, you are ready to enable co-management of your Windows 10 devices with both Configuration Manager and Intune. You need to choose a small number of clients to assign to a Pilot group, which is used to test your co-management configurations. On the **Enablement** page of the Co-management Configuration Wizard, you can configure the Pilot group. The Pilot group consists of the Configuration Manager clients which are members of the **Intune Auto Enrollment** collection and are automatically enrolled to Intune.

Co-management Configuration Wizard

 Enablement

Tenant onboarding

Enablement

Workloads

Staging

Summary

Progress

Completion

Enable co-management

To enable co-management for devices managed by Configuration Manager, configure automatic enrollment in [Microsoft Intune](#).

[Learn more](#)

Automatic enrollment in Intune

Pilot


Intune Auto Enrollment

Intune Auto Enroll

Browse...

To enable co-management for devices already enrolled in Intune, create an app in Intune to install the Configuration Client. Copy the following command line.

[Learn more](#)

 Please ensure the proper prerequisites are installed.

< Previous

Next >

Summary

Cancel

On the Staging page, configure the pilot collection for each workload.

The screenshot shows the 'Co-management Configuration Wizard' window. The title bar is blue with the text 'Co-management Configuration Wizard' and a close button. On the left is a sidebar with a tree view containing: 'Tenant onboarding', 'Enablement', 'Workloads', 'Staging' (selected and highlighted in blue), 'Summary', 'Progress', and 'Completion'. The main area is titled 'Configure roll out collections'. It features a 'Pilot' section with a warning icon and text: 'When you configure a workload for Pilot Intune, select a device collection to be the pilot group. [Learn more](#). Make sure your pilot devices are already enrolled into Intune.' Below this are six rows, each with a label, a text box, and a 'Browse...' button: 'Compliance policies' (text box contains 'Compliance policies'), 'Device Configuration', 'Endpoint Protection', 'Resource access policies', 'Office Click-to-Run apps' (text box contains 'Click-to-Run'), and 'Windows Update Policies'. At the bottom are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'. A vertical scrollbar is on the right side of the main content area.

Objective:

Implement modern device services

Sub-Objective:

Plan Windows 10 deployment

References:

[Docs > Configuration Manager > Co-management > What is co-management?](#)

[Docs > Configuration Manager > Co-management > Tutorial: Enable co-management for existing Configuration Manager clients](#)

Question #20 of 26

Question ID: 1257253

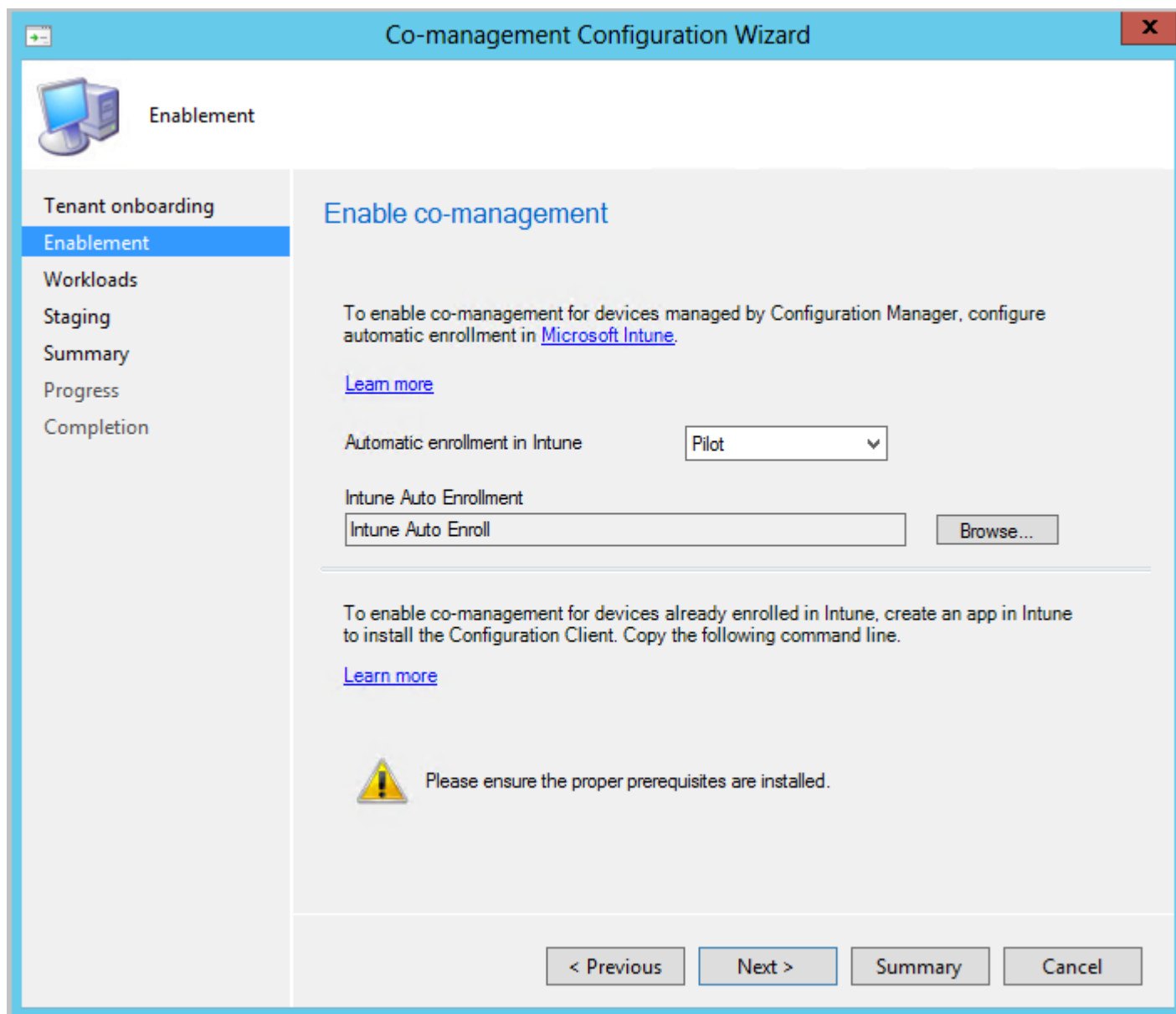
Verigon Corporation plans to move many of their Windows 10 device management tasks to the cloud. They have purchased an Office 365 Apps Azure AD license but use (SCCM) ConfigMgr for most tasks. Verigon has both Windows 7 and Windows 10 devices currently joined to a local AD.

What steps should be included for co-management during the workload transition period? (Choose all that apply.)

- ✓ **A)** Run the *Co-management Configuration Wizard* in ConfigMgr.
- X **B)** Enroll devices to any approved third-party MDM solution.
- ✓ **C)** Enroll the devices in Intune.
- ✓ **D)** Upgrade to a Premium Azure AD license
- ✓ **E)** Setup Hybrid Azure AD

Explanation

You will need to run the *Co-management Configuration Wizard* in ConfigMgr. This will allow you to configure autoenrollment of devices into Intune. This is the opportunity to set up a Pilot test first. You can choose **Pilot** or **All** as values for **Automatic enrollment in Intune** in the wizard. If you choose **Pilot**, then only clients that are members of the **Intune Auto Enrollment** collection are automatically enrolled to Intune. If you choose **All**, then all Windows 10 version 1709 or later clients are enabled for automatic enrollment.



The screenshot shows the 'Co-management Configuration Wizard' window. The title bar is blue with the text 'Co-management Configuration Wizard' and a close button. The left sidebar has a blue header 'Enablement' with a computer icon. Below it are links: 'Tenant onboarding', 'Enablement' (highlighted), 'Workloads', 'Staging', 'Summary', 'Progress', and 'Completion'. The main area is titled 'Enable co-management'. It contains the following text: 'To enable co-management for devices managed by Configuration Manager, configure automatic enrollment in [Microsoft Intune](#).', a link '[Learn more](#)', a dropdown menu 'Automatic enrollment in Intune' with 'Pilot' selected, a text box 'Intune Auto Enrollment' containing 'Intune Auto Enroll' and a 'Browse...' button. Below this is another text block: 'To enable co-management for devices already enrolled in Intune, create an app in Intune to install the Configuration Client. Copy the following command line.', a link '[Learn more](#)', and a warning icon with the text 'Please ensure the proper prerequisites are installed.' At the bottom are four buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

Co-management Configuration Wizard

Enablement

Tenant onboarding

Enablement

Workloads

Staging

Summary

Progress

Completion

Enable co-management

To enable co-management for devices managed by Configuration Manager, configure automatic enrollment in [Microsoft Intune](#).

[Learn more](#)


Automatic enrollment in Intune: Pilot

Intune Auto Enrollment

Intune Auto Enroll Browse...

To enable co-management for devices already enrolled in Intune, create an app in Intune to install the Configuration Client. Copy the following command line.

[Learn more](#)

 Please ensure the proper prerequisites are installed.

< Previous Next > Summary Cancel

You need to enroll the devices in Intune for co-management of workloads. The Workloads page in the Configuration Wizard allows you to select which tool will manage each workload topic. The devices can autoenroll or be configured with a ConfigMgr agent.

The screenshot shows the 'Properties' dialog box with the 'Workloads' tab selected. The dialog has four tabs: 'Enablement', 'Workloads', 'Staging', and 'Reporting'. The 'Workloads' tab contains a text box with the following text: 'the workloads for only clients in the Pilot group (specified later in this wizard). If you are not ready to move workloads to Intune, select Configuration Manager.' Below this text is a link labeled 'Learn more'. The main area of the tab is a table with three columns: 'Configuration Manager', 'Pilot Intune', and 'Intune'. The rows represent different workload categories: 'Compliance policies:', 'Device Configuration:', 'Endpoint Protection:', 'Resource access policies:', 'Client apps:', 'Office Click-to-Run apps:', and 'Windows Update policies:'. Each row has a slider control with a house icon. The 'Configuration Manager' column has sliders for 'Compliance policies:', 'Device Configuration:', and 'Windows Update policies:'. The 'Pilot Intune' column has sliders for 'Endpoint Protection:', 'Resource access policies:', 'Client apps:', and 'Office Click-to-Run apps:'. The 'Intune' column is empty. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

	Configuration Manager	Pilot Intune	Intune
Compliance policies:			
Device Configuration:			
Endpoint Protection:			
Resource access policies:			
Client apps:			
Office Click-to-Run apps:			
Windows Update policies:			

You will need to setup Hybrid Azure AD. The devices will remain joined to the on-premises AD but be registered with Azure AD. This configuration will support the Windows 7 devices and other choices such as local GPOs. Note that Windows 10 devices could be Azure AD joined only.

You will need to upgrade to a Premium Azure AD license. Premium P1 is the minimum level required.

You would not enroll the devices to any approved third-party MDM solution. Microsoft defines that as *coexistence*, not co-management. Co-management requires Intune.

Objective:

Implement modern device services

Sub-Objective:

Plan for devices and apps

References:

[Docs > Configuration Manager > Co-management > How to enable co-management in Configuration Manager](#)

[Docs > Configuration Manager > Co-management > Co-management workloads](#)

[Docs > Configuration Manager > Co-management > What is co-management?](#)

Question #21 of 26

Question ID: 1257242

Dreamsuites Inc has chosen to implement Intune as their MDM solution. They plan to take advantage of the full capabilities of Intune to manage all their Office 365 users, as well as deploying some internal apps. Dreamsuites has a Microsoft 365 E3 subscription. Selecting an MDM authority is a required first step to implement MDM. What should Dreamsuites do?

- ☐ **A)** Choose Intune Co-Management via the ConfigMgr console.
- ☐ **B)** Choose Office 365 MDM Coexistence via the Office 365 admin portal.
- ☒ **C)** Choose Intune Standalone via the Azure portal.
- ☐ **D)** Choose Hybrid Mobile Device Management
- ☐ **E)** Choose MDM Management for Office 365 via the Office 365 admin portal.

Explanation

You would not choose Office 365 MDM Coexistence via the Office 365 admin portal. This solution applies only to customers with a mix of Office 365 and Intune licenses. Dreamsuites wants the full capabilities of Intune, including deployment of some internal apps, which is not possible with MDM for Office 365.

You will choose Intune Standalone via the Azure portal. Dreamsuites wants the full capabilities of Intune, including deployment of some internal apps.

You would not choose MDM Management for Office 365 via the Office 365 admin portal. This option only feature a subset of Intune capabilities. Dreamsuites needs the full Intune suite to be able to deploy internal apps.

You would not choose Intune Co-Management via the ConfigMgr console. This would require integration with SCCM (System Center Configuration Manager), which was not indicated in the scenario.

You would not choose Hybrid Mobile Device Management. Microsoft is ending support for this functionality.

Note that Dreamsuites already has Intune access as part of their Microsoft 365 E3 subscription. This subscription model also includes Windows 10 licenses and basic threat protection. An alternative would be to add an EMS (Enterprise Mobility and Security) option to their Office 365 subscription.

Objective:

Implement modern device services

Sub-Objective:

Implement Mobile Device Management (MDM)

References:

<https://docs.microsoft.com/en-us/intune/mdm-authority-set>

<https://support.microsoft.com/en-us/help/3103996/setting-the-mobile-device-management-authority-in-microsoft-intune>

<https://blogs.technet.microsoft.com/configmgrdogs/2016/01/04/microsoft-intune-co-existence-with-mdm-for-office-365/>

<https://support.office.com/en-us/article/choose-between-mdm-for-office-365-and-microsoft-intune-c93d9ab9-efb2-4349-9b93-30c30562ee22>

Question #22 of 26

Question ID: 1257249

You are a security advisor for Dreamsuites Inc. You have encouraged Dreamsuites to take advantage of the granular options of an Azure AD conditional access policy. Dreamsuites has a premium Azure Ad subscription.

What conditions can Dreamsuites choose from when configuring their policies? (Choose all that apply.)

- ✓ **A)** Device platforms
- ✓ **B)** Device state
- ✓ **C)** Client apps
- X **D)** Windows operating system version
- X **E)** Schedule
- ✓ **F)** Locations

Explanation

Client apps is a condition that can be part of an Azure AD conditional access policy. You can restrict the policy to the type of app it should apply to. By default, the policies will apply to browser-based apps, and apps that use "modern authentication".

Device platforms is a condition that can be part of an Azure AD conditional access policy. You can specify all platforms or specific platforms such as Android, iOS, Windows Phone, Windows, or macOS

The screenshot shows the 'New' policy configuration page in Azure AD. The breadcrumb trail is: Home > Microsoft Intune > Conditional access - Policies > New > Conditions > Device platforms. The page is divided into three main sections: 'Info', 'Conditions', and 'Device platforms'.

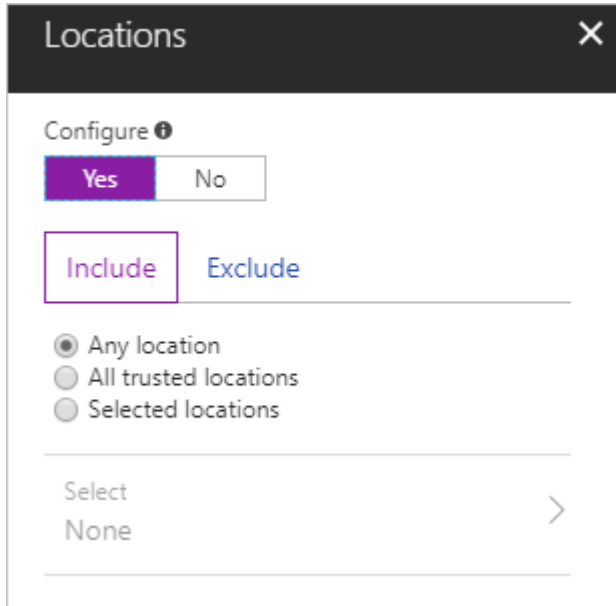
- Info:** Contains a 'Name' field with the example 'Device compliance app policy'. Below it are sections for 'Assignments' (Users and groups: All users; Cloud apps: 1 app included; Conditions: 0 conditions selected) and 'Access controls' (Grant: 0 controls selected). A 'Create' button is at the bottom.
- Conditions:** Lists several conditions, all currently 'Not configured': Sign-in risk, Device platforms (highlighted in blue), Locations, Client apps (preview), and Device state (preview). A 'Done' button is at the bottom.
- Device platforms:** Contains a 'Configure' section with 'Yes' and 'No' buttons. Below is an 'Include' and 'Exclude' section. Under 'Include', there are two radio buttons: 'All platforms (including unsupported)' (selected) and 'Select device platforms'. Under 'Select device platforms', there are checkboxes for Android, iOS, Windows Phone, Windows, and macOS. A 'Done' button is at the bottom.

Device state is a condition that can be part of an Azure AD conditional access policy. This allows you to specifically include or exclude compliant devices from the policy. A compliance policy is a prerequisite for this option.

The screenshot shows the 'Device state (preview)' configuration window. It has a dark header with the title 'Device state (preview)' and a close button. Below the header is an 'Info' section. The main configuration area includes:

- A 'Configure' section with 'Yes' and 'No' buttons.
- An 'Include' and 'Exclude' section.
- A text prompt: 'Select the device state condition used to exclude devices from policy.'
- Two checked checkboxes: 'Device Hybrid Azure AD joined' and 'Device marked as compliant'.

Locations is a condition that can be part of an Azure AD conditional access policy. You can define a condition based on where a device connection was attempted.



Another optional condition not listed here is "*sign-in risk*". This condition uses Azure AD identity sign-in risk detection to assign the policy to sign-in risk levels. You could configure such a condition, for example, to require MFA (multi-factor authentication) sign-in when a user signs in from a new location.

Schedule is not an access policy condition. However, it is a useful option for a compliance policy when triggering an action for non-compliant devices. A schedule could be used to trigger a conditional access policy after a set number of days.

Windows operating system version is not an access policy condition. You can specify device platform, but not version of a particular operating system.

Objective:

Implement modern device services

Sub-Objective:

Manage device compliance

References:

[Azure > AD > Conditional access > What are conditions in Azure Active Directory Conditional Access?](#)

[Docs > Intune > Create a device-based Conditional Access policy](#)

Question #23 of 26

Question ID: 1257247

As a security admin for the Verigon Corporation, you want to have control of mobile devices. Verigon has a premium Azure AD subscription, as well as an Intune subscription. All current devices are enrolled in Intune. Your goal is to block all access for non-compliant devices.

What type of conditional access policy will you define?

- X **A)** A device-based, device enrollment policy.
- ✓ **B)** A device-based, device compliance policy.
- X **C)** A device-based, Azure AD joined policy.
- X **D)** An app-based policy.
- X **E)** A device-based, device platform policy.

Explanation

You will want to create a device-based, device compliance policy. Verigon can make a policy that locks down access but ignores enrolled, compliant devices. Or a policy that only grants access to compliant devices, if that is simpler.

You will not create an app-based policy. An app-based policy is focused on app-based controls, such as requiring a specific client for Exchange Online. Our scenario is focused on device compliance.

You will not create a device-based, Azure AD joined policy. A device could be AD-joined, yet not compliant. Our scenario is focused on device compliance.

You will not create a device-based, device platform policy. This is a condition item, and our condition is compliance, not platform.

You will not create a device-based, device enrollment policy. You do not define enrollment through a conditional access policy.

Note that since you will be blocking access based on compliance, you will also have to first create a compliance policy.

Objective:

Implement modern device services

Sub-Objective:

Manage device compliance

References:

[Docs > Intune > What are common ways to use Conditional Access with Intune?](#)

[Docs > Intune > Learn about Conditional Access and Intune](#)

[Docs > Intune > Create a device-based Conditional Access policy](#)

Question #24 of 26

Question ID: 1257241

Verigon Corporation has just purchased an Azure AD Premium P1 subscription in preparation for their upcoming MDM project. Verigon already has an on-premises AD solution in place, but they plan to use Microsoft Intune as their MDM solution. Verigon has a large number of company-owned Windows 10 devices that they want to protect as quickly as possible. As their MDM administrator, what are some prerequisites that you will meet to prepare for the rollout?

(Choose all that apply.)

- ✓ **A)** Configure the devices for automatic hybrid domain join.
- ✓ **B)** Configure MDM enrollment settings.
- X **C)** Register the Windows 10 device users with Azure AD
- ✓ **D)** Configure automatic device enrollment into Azure AD.
- ✓ **E)** Obtain an MDM subscription.

Explanation

To meet the goal of "as quickly as possible" you will want to configure automatic device enrollment into Azure AD. This requires an Azure AD P1 subscription, which Verigon has purchased.

You would want to obtain an MDM subscription. For Verigon, this will be Intune, but Microsoft does support several third-party MDM applications. You choose these from the Azure AD App Gallery.

You do not need to register the Windows 10 device users with Azure AD. We are focused on device management. A single admin can enroll multiple devices.

You will want to configure the MDM enrollment settings. These may include the scope of devices to use automatic enrollment, and MDM compliance settings.

You will want to configure the devices for automatic hybrid domain join. Verigon already has an on-premises AD environment.

On-premise AD administrators can use Configuration Manager (SCCM) or Group Policy to enable hybrid Azure AD join or device enrollment.

Objective:

Implement modern device services

Sub-Objective:

Implement Mobile Device Management (MDM)

References:

<https://docs.microsoft.com/en-us/windows/client-management/mdm/azure-active-directory-integration-with-mdm>

Question #25 of 26

Question ID: 1257259

Dreamsuites Corporation uses Windows 10 for all laptops. They use Windows Update to keep aware of and updated with the latest features. However, they soon to release a new point-of-sale system that is based on Windows 10. It is important that these new POS devices get only quality updates instead of regular feature updates as Dreamsuites needs stability over many years.

What Windows-As-A-Service (WaaS) plan will best meet their needs?

- ✓ **A) Long-Term Servicing Channel**
- X **B) Deployment Rings**
- X **C) Semi-Annual Channel**
- X **D) Windows Insider Program**
- X **E) Feature Updates**

Explanation

The Long-Term Servicing Channel is made specifically for this purpose. Releases are offered only every 2-3 years, and it has an extended 10-year lifecycle. Note that this servicing model requires installation of a special Long-term Servicing Branch edition (LTSB) of Windows 10. The channel choice cannot be changed without wiping and reloading the OS.

The Semi-Annual Channel would not meet their needs, as it provides updates about every four months.

The Insider Program would not meet their needs. Devices in this program are the first to get new updates, and as such, sometimes have issues. Dreamsuites needs their POS systems to remain stable.

Feature Updates for Windows 10 are twice a year, which does not meet the needs of the scenario. Dreamsuites needs their POS systems to remain stable, so they want to minimize the inclusion of new features. Note that quality updates are still important in this scenario.

Deployment Rings are a suggested method to pilot and test Windows feature updates before widespread rollout. For these POS devices, while testing will be important eventually when new features are installed, this concept is not directly applicable.

Objective:

Implement modern device services

Sub-Objective:

Plan Windows 10 deployment

References:[Docs > Prepare servicing strategy for Windows 10 updates](#)[Docs > Deployment > Overview of Windows as a service](#)[Docs > Deployment > Quick guide to Windows as a service](#)**Question #26 of 26**

Question ID: 1257246

Nutex Corporation has successfully used their Intune subscription to allow the Sales team to bring their own device. Management is now concerned that some of the IOS phones have been "jailbroken" and may be a security hole. As an admin, you are asked to compile a status report using Intune, listing all such devices. What steps will be necessary? (Choose all that apply.)

- ✓ **A)** Create an Intune Device Compliance Policy
- X **B)** Check the setting device compliance status.
- X **C)** Create an Intune Conditional Access Policy.
- X **D)** Assign the Sales group to the built-in compliance policy.
- ✓ **E)** Check the policy compliance status.

Explanation

You do not need to create an Intune Conditional Access Policy. These policies are used to take action based on device compliance. They are not required for status reporting.

You would not check the setting compliance status. Jailbreak status is not a device setting to be checked.

You would not assign the Sales group to the built-in compliance policy. The built-in policies affect all devices, and do not address the jailbroken IOS issue

You will want to check the policy device compliance status. This displays per-policy information.

The screenshot shows the Microsoft Intune console interface. The breadcrumb navigation at the top reads: Dashboard > Microsoft Intune > Device compliance - Policies > Create Policy > iOS compliance policy > Device Health. The interface is divided into three main panels. The left panel, titled 'Create Policy', contains fields for 'Name' (Jailbreak Policy), 'Description' (Enter a description...), and 'Platform' (iOS). The middle panel, titled 'iOS compliance policy', shows a list of categories to configure settings: Email (1 setting available), Device Health (2 settings available), Device Properties (4 settings available), and System Security (10 settings available). The right panel, titled 'Device Health', shows 'Jailbroken devices' with a 'Block' button and a 'Not configured' status. Below this, there is a dropdown menu for 'Require the device to be at or under the Device Threat Level' set to 'Not configured'.

You will want to create an Intune Device Compliance Policy. You would choose to block jailbroken devices under the Device Health settings.

Note that the Nutex policy will need to be assigned to a Sales group. Since the topic of concern for Nutex is jailbreaking, they might also want to enable the built-in "enhanced jailbreak detection" policy. This causes IOS devices to check in with Intune more frequently.

Objective:

Implement modern device services

Sub-Objective:

Manage device compliance

References:

<https://docs.microsoft.com/en-us/intune/create-compliance-policy>

<https://docs.microsoft.com/en-us/intune/device-compliance-get-started>

<https://docs.microsoft.com/en-us/intune/compliance-policy-monitor>