

## Question #1 of 118

Question ID: 1257275

Dreamsuites Incorporated has purchased a Microsoft Office 365 E3 subscription. They recently had a problem with two phishing emails that breached security. The emails impersonated two of the HR team members.

What steps would you take to help prevent a recurrence of this type of issue? (Choose all that apply.)

- ✓ **A)** Create an anti-spam policy, and configure the **Phishing Email** setting.
- X **B)** Create an ATP anti-phishing policy and configure the **Turn On Phishing Protection Tips** action setting.
- X **C)** Create an ATP anti-phishing policy and configure the **Add users to protect** setting.
- X **D)** Create an anti-phishing policy and choose the HR team in the **Applied To** setting.
- ✓ **E)** Purchase an Office 365 ATP protection plan.

### Explanation

You will need to purchase an Office 365 ATP protection plan. The ability to add users to protect from impersonation is only offered in an ATP anti-phishing policy. Alternatively, Dreamsuites could also upgrade to an E5 subscription, which includes ATP.

You will need to create an ATP anti-phishing policy and configure the **Add users to protect** setting.

You would not create an anti-phishing policy and choose the HR team in the **Applied To** setting. A basic anti-phishing policy (as compared to an ATP anti-phishing policy) is extremely limited and does not include the impersonation protections needed by the scenario. In addition, we don't know if all of the impersonated individuals are part of the HR team.

You would not create an anti-spam policy, and configure the **Phishing Email** setting to meet the goal of this scenario, although it may be part of a greater security plan. This is a setting that determines what to do with messages classified as phishing attempts. For this scenario, we would address that issue as part of the ATP anti-phishing policy settings.

An E5 subscription would allow you to protect up to 60 users from impersonation. Note that even though the feature is available with the subscription (or ATP plan purchase), an ATP anti-phishing policy must be in place.

You would not create an ATP anti-phishing policy and configure the **Turn On Phishing Protection Tips** action setting to meet the goal of this scenario, although it may be a part of a greater security plan. This setting adds anti-phishing safety tips to suspect emails.

### **Objective:**

Implement Microsoft 365 security and threat management

### **Sub-Objective:**

Implement threat management

### **References:**

[Microsoft 365 > Protect against threats > Protect against threats in Office 365](#)

[Microsoft 365 > Anti-phishing protection in Office 365](#)

## Question #2 of 118

Question ID: 1257315

Your company has a Microsoft 365 tenant. The company sells travel cruise packages to the Caribbean. This company must process driver license numbers, credit card numbers, and social security numbers. Users use a cloud-based app to update customer accounts.

There are files stored in Microsoft SharePoint Online contains either a driver license numbers, credit card number, or social security number

What should you use?

- X **A)** Cloud App Security (CAS) access policy
- X **B)** Cloud App Security (CAS) session policy
- ✓ **C)** Security & Compliance data loss prevention (DLP) policy
- X **D)** Cloud App Security (CAS) activity policy

#### Explanation

A DLP policy covers locations such as Exchange email, SharePoint sites, OneDrive accounts, or Team chat and channel messages. A DLP policy could be configured to find and protect sensitive information across Exchange email or OneDrive to prevent disclosure of personally identifiable information (PII) such as health records, credit card numbers, social security numbers, or financial data.

New DLP policy

✓ Choose the information to protect





✓ Name your policy

● Choose locations

● Policy settings

● Review your settings

### Choose locations

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	 Exchange email	All <a href="#">Choose distribution groups</a>	None <a href="#">Exclude distribution groups</a>
<input checked="" type="checkbox"/>	 SharePoint sites	All <a href="#">Choose sites</a>	None <a href="#">Exclude sites</a>
<input checked="" type="checkbox"/>	 OneDrive accounts	All <a href="#">Choose accounts</a>	None <a href="#">Exclude accounts</a>
<input checked="" type="checkbox"/>	 Teams chat and channel messages	All <a href="#">Choose accounts</a>	None <a href="#">Exclude accounts</a>

[Back](#)[Next](#)[Cancel](#)

You should not use a Cloud App Security (CAS) activity policy. An activity policy allows for custom alerts when specific user activity is detected. You can choose specific apps and locations as filters. This policy will not notify you when Personal Identifiable Information (PII) is stored in SharePoint Online.

## Create activity policy

Policy template \*

No template

Policy name \*

Nutex Non-US Activity

Description

Create a alert whenever Office 365 is accessed outside of the US>

Policy severity \*

Low

Category \*

Threat detection

Create filters for the policy

Act on:

- ☒ Single activity  
Every activity that matches the filters
- ☐ Repeated activity:  
Repeated activity by a single user

ACTIVITIES MATCHING ALL OF THE FOLLOWING

✕ App equals 4 selected

✕ Location does not equal United States

+

Edit and

Alerts

☒ Create an alert for each matching event with the policy's severity Use your organization's default settings

Daily alert limit 5

☒ Send alert as email ⓘ

secadmin@nutex.com ✕

You should not use a Cloud App Security (CAS) access policy. An access policy would allow for real-time control when the users login to selected cloud apps. An access policy can block access to app. Blocking access is not the goal of this scenario.

You should not use a Cloud App Security (CAS) session policy. A session policy controls and monitors access of a user session. It only applies to browser based apps. A session policy does not notify you if PII is stored in SharePoint Online.

### Objective:

Manage Microsoft 365 governance and compliance

### Sub-Objective:

Configure Data Loss Prevention (DLP)

### References:

[Office 365 > Overview of data loss prevention](#)

## Question #3 of 118

Question ID: 1257354

Dreamsuites has Exchange Online in Office 365. The legal department suspects there were ethics violations within the Dreamsuites finance department. The Dreamsuites legal department has mandated that all users within the finance department should be subject to a hold during the investigation. You must ensure

that the whole mailbox is on hold, rather than only items that contain specific keywords.

You have been supplied with a list of Dreamsuites lawyers who will execute searches against the finance mailboxes. You need to add the list of lawyers to an admin role so that they can search the finance mailboxes.

Which admin role should you assign to the lawyers to meet the business requirements?

- ✓ **A)** Discovery Management
- X **B)** Recipient Management
- X **C)** Compliance Management
- X **D)** Records Management

#### Explanation

The selected members of the Dreamsuites legal team should be added to the Discovery Management role group. This role group will allow members to execute discovery searches of mailboxes and more importantly to create, configure, and manage litigation holds of end user mailboxes.

The Legal Hold management role, which provides the ability to management litigation holds, is assigned to the Discovery Management role group.

The Compliance Management role group will allow members to configure DLP policies, manage Information Rights, and retention settings. This does not meet the business requirement of providing members of the Dreamsuites legal team with the ability to create, configure, and manage litigation holds.

The Records Management role group will allow members to configure transport rules and even retention policy tags. This does not meet the business requirement.

The Recipient Management role group will allow members to create and configure user settings within the Exchange 2016 environment. This role group allows the user to create new mailboxes, distribution groups, track messages, and even move mailboxes. This does not meet the business requirement.

#### **Objective:**

Manage Microsoft 365 governance and compliance

#### **Sub-Objective:**

Manage eDiscovery

#### **References:**

[Exchange > Permissions in Exchange Online](#)

[TechNet > Exchange > Exchange Server 2013 > Messaging policy and compliance > Data loss prevention](#)

[TechNet > Office Products > Exchange Server 2016 > Assign eDiscovery permissions in Exchange 2016](#)

---

## **Question #4 of 118**

Question ID: 1257282

Verigon Corporation would like to take advantage of the security features offered by their Windows 10 Enterprise licenses. They are especially concerned about protecting valuable files from ransomware, and would welcome the benefit of always-on virus scanning.

What options will you configure to address their concerns? (Choose all that apply.)

- X **A)** The **Audit Mode** option of Windows Defender.
- ✓ **B)** The **Real-time protection** option of Windows Defender Antivirus.
- X **C)** The **Tamper Protection** option of Windows Defender Antivirus
- X **D)** The **Automatic sample submission** option of Windows Defender Antivirus.
- ✓ **E)** The **Controlled Folder Access** option of Windows Defender Exploit Guard.

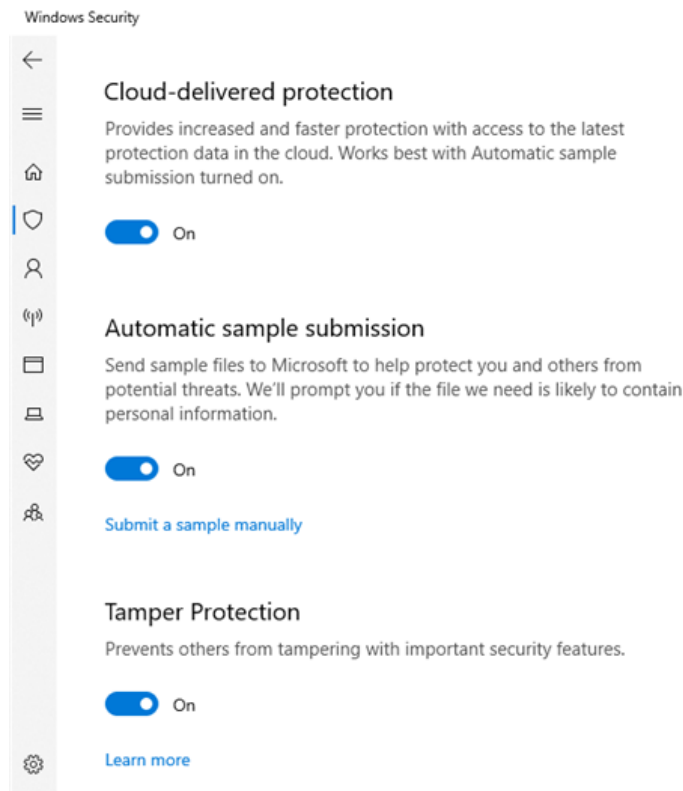
#### Explanation

You will want to enable the **Real-time protection** option of Windows Defender Antivirus. This will provide the "always on" virus scanning desired by Verigon.

You will want to choose the **Controlled Folder Access** option of Windows Defender Exploit Guard. This will allow Verigon to protect specific files and folders from changes caused by malware or ransomware.

You would not choose the **Cloud-delivered protection** option of Windows Defender Antivirus. It does not meet the specific needs of the scenario. This option uses information from Microsoft's cloud offerings to enhance protections.

You would not choose the **Automatic sample submission** option of Windows Defender Antivirus. This causes files to be sent to Microsoft for analysis if potential malware is detected. It does not meet the specific needs of the scenario of protecting files from malware or ransomware. You can use the **Cloud-delivered protection** option of Windows Defender Antivirus along with the **Automatic sample submission** option. The **Cloud-delivered protection** option of Windows Defender Antivirus uses information from Microsoft's cloud offerings to enhance protections. When this option is enabled Windows Defender Antivirus can use additional intelligence to verify the intent of a suspicious file. Metadata of the file is sent to the cloud protection service by Microsoft to determine if the file is safe or malicious instantly



You would not choose the **Audit Mode** option of Windows Defender. It does not meet the specific needs of the scenario of protecting files from malware or ransomware. Audit Mode allows you to test how features might work without affecting the normal use of the machine. The results are still tracked in the Event log.

You would not choose the **Tamper Protection** of Windows Defender Antivirus. This option prevents others from changing or tampering security features.

#### Objective:

Implement Microsoft 365 security and threat management

#### Sub-Objective:

Implement Windows Defender Advanced Threat Protection (ATP)

#### References:

[Microsoft 365 > Step 5: Deploy Windows 10 Enterprise security features](#)

[Docs > Security > Threat Protection > Enable and configure antivirus always-on protection and monitoring](#)

[Docs > Threat Protection > Enable controlled folder access](#)

TXGlobal Corporation wants to encourage users to clean up their Exchange Online mailboxes by giving them many options to mark items for deletion. They would like all existing and future users to be able to tag emails with a two-week delete tag.

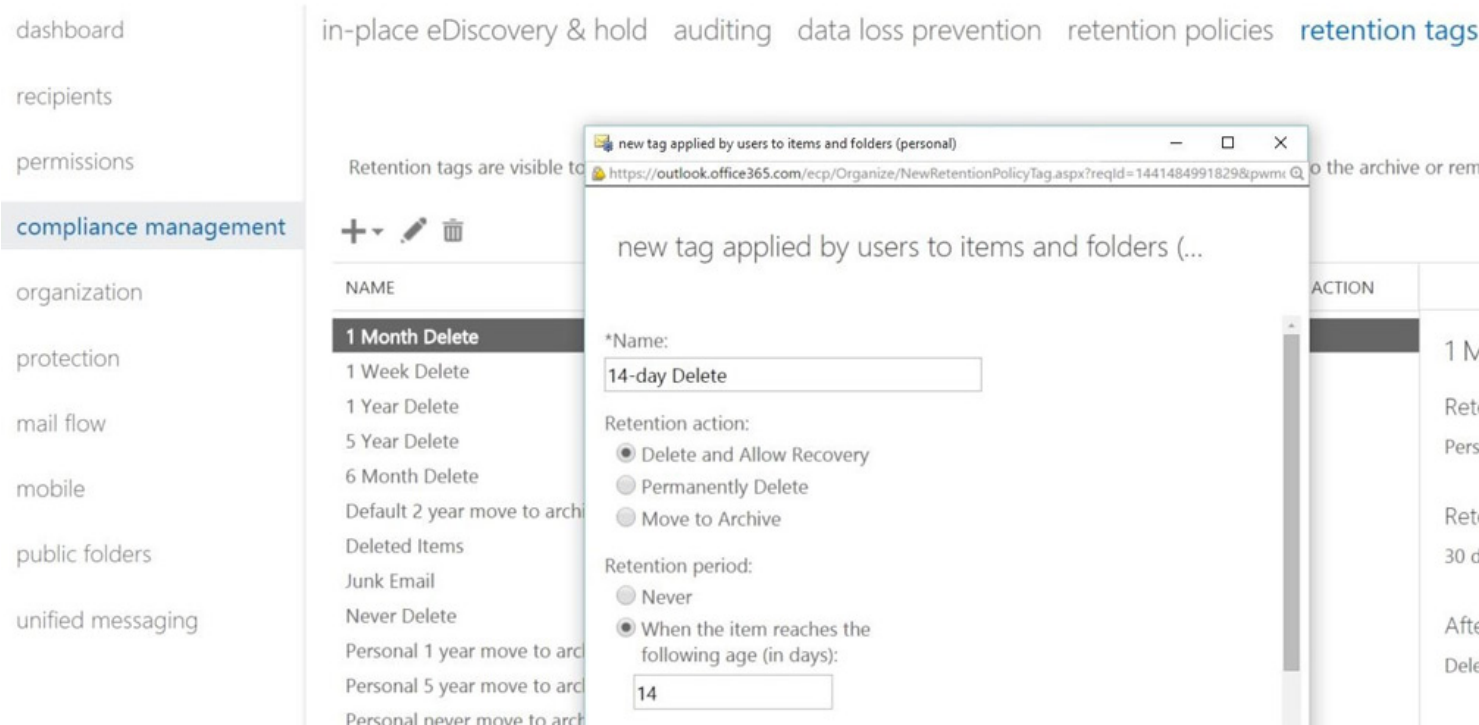
What steps will need to be taken to add this tag as an option for the users? Select the appropriate steps from the left and drag them to the right. The steps must be in the correct order. Some steps may not be necessary.

{UCMS id=5716023640588288 type=Activity}

Explanation

You will need to edit the Default MRM Policy. This policy applies by default to all new and existing users in Exchange Online. You will want to add a new Personal Tag with a retention age of 14 days and a **Delete and Allow Recovery** retention action. After you do so, it will be available for all users to apply in addition to the existing default tags of 1-week, 1-month, 6-month, 1-year, 5-year, and "Never" deletion options.

Exchange admin center



You do not want to delete the Default MRM Policy. This policy already contains many deletion tag options, and the scenario states that you want to expand these options.

You do not want to edit the Default Policy Tag (DPT). This tag's action is about archiving, not deleting.

You do not want to remove the **Never Delete** tag, as this tag allows the users to mark an item so that it is never automatically deleted. The scenario states that you want to offer users another option to tag items for deletion. It does not say that you want to limit the users' ability to prevent deletions.

You do not want to create a new retention policy because if you did so, it would have to be manually applied to the users. You must use the default retention policy so that it is automatically applied to everyone, including future users. You cannot set another policy as the default retention policy.

You would not apply the newly created retention policy to all users because creating a new policy is not part of the solution. Even if a new policy were created, it would have to be manually applied to future users.

Objective:

Manage Microsoft 365 governance and compliance

Sub-Objective:

Configure Data Loss Prevention (DLP)

References:

## Question #6 of 118

Question ID: 1257297

Nutex has successfully implemented a DLP policy to encrypt messages sent to a specific domain outside the organization. This policy has a rule that allows the user to override as needed. There is an additional DLP policy containing a rule that will notify users when any attachments contain sensitive information. You recently added a rule to this policy to block attachments over a size limit. You want to monitor DLP policy activity.

What would be the most effective way to see information as to which specific rules from your policies are affecting emails?

- ☐ A) Create a custom use policy tips configuration.
- ☒ B) In the Office 365 Security and Compliance Center, view the DLP policy matches report.
- ☐ C) In the Office 365 Security and Compliance Center, view the DLP false positives and overrides report.
- ☐ D) Use the default use policy tips option.
- ☐ E) In the Office 365 Security and Compliance Center, view the DLP incident report.

### Explanation

You would, in the Office 365 Security and Compliance Center, view the DLP policy matches report. This report most closely meets the scenario requirements. This report would show a line item for every rule that a specific email matched with. It is more detailed than the DLP incident report. It can be filtered by date, location (which is what Office 365 app it applied to, not a geographic concept), policy, or action.

You would not, in the Office 365 Security and Compliance Center, view the DLP incident report. While this provides useful information, it is not the best answer for this scenario. This report shows matches at an item level, but we would like to know the specific rule(s) that are being applied.

You would not the default use policy tips option to meet the requirements of this scenario. These are optional informative notices that are sent to a user when an email meets a policy condition.

You would not create a customized use policy configuration to meet the requirements of this scenario. These are optional informative notices that are sent to a user when an email meets a policy condition.

You would not, in the Office 365 Security and Compliance Center, view the DLP false positives and overrides report. False positives are reported by users. This report does not match specific rules to emails.

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Configure Data Loss Prevention (DLP)

### **References:**

[Microsoft 365 > DLP > Overview of data loss prevention](#)

[Microsoft 365 > DLP > View the reports for data loss prevention](#)

---

## Question #7 of 118

Question ID: 1257284

The Nutex Corporation has 500 Windows 10 devices in an Active Directory domain named **nutex.com**. These devices use Windows Defender Advanced Threat Protection (ATP) to collect and send data.

Nutex has purchased another company and will move 200 Windows 10 devices to the new company. The new company will be in a separate forest. The new company will collect and send different data with Windows Defender ATP.

What should you do first?

- X **A)** Onboard the 200 Windows 10 devices using System Center Configuration Manager
- X **B)** Onboard the 200 Windows 10 devices using Mobile Device Management tools
- ✓ **C)** Offboard the 200 Windows 10 devices using a Group Policy
- X **D)** Offboard the 200 Windows 10 devices using Active Directory Domains and Trust
- X **E)** Offboard the 200 Windows 10 devices using Server Manager

#### Explanation

You should offboard the 200 Windows devices from the **nutex.com** domain. You can offboard Windows 10 devices with any of the following methods:

- Using a local script
- Using Group Policy
- Using System Center Configuration Manager
- Using Mobile Device Management tools

Offboarding the Windows 10 devices will remove the Windows Defender ATP settings that were configured by the Nutex Corporation. The Windows 10 devices will stop collecting and sending Windows Defender ATP data. Once the Windows 10 devices are offboarded, then you can onboard the Windows 10 devices to the new company with the appropriate Windows Defender ATP settings.

When you create a Group Policy to offboard Windows 10 devices, the package used for the offboarding in the Group Policy will expire 30 days after the date it was downloaded. Once you have downloaded the offboarding package from the Microsoft Defender Security Center, you can configure the package to execute as a scheduled task under Group Policy preferences. From Group Policy Management Editor, go to **Computer configuration> Preferences>Control panel settings**. Right-click **Scheduled tasks**, then click **New task**. Under the **General** tab, choose the local SYSTEM user account (BUILTIN\SYSTEM) under **Security** options, select **Run whether user is logged on or not**, and check the **Run with highest privileges** check-box.

You cannot use Server Manager or Active Domains and Trust to offboard a Windows 10 device. Server Manager or Active Domains and Trust do not remove the Windows Defender ATP settings.

You must offboard a Windows 10 device from the source location before onboarding the Windows 10 device at another location. You can use a local script, Group Policy, System Center Configuration Manager, or Mobile Device Management Tools to onboard a Windows 10 device once it has been offboarded.

#### **Objective:**

Implement Microsoft 365 security and threat management

#### **Sub-Objective:**

Implement Windows Defender Advanced Threat Protection (ATP)

#### **References:**

[Offboard Windows 10 devices of Windows Defender Advanced Threat Protection](#)

[Removing Windows Defender ATP Tracking from Your Devices](#)

[Docs > Threat Protection > Onboard Windows 10 machines using Group Policy](#)

---

## **Question #8 of 118**

Question ID: 1257270

Verigon Corporation has successfully implemented Cloud App Security. They are satisfied with the level of alerting and detail that has been configured. However, upon examination, some of the alerts for the XYZ application that keep appearing are of little value.

As the security administrator, what should you configure on the alerts page in the CAS portal? (Choose all that apply.)

- ✓ **A)** Set a filter to the XYZ app.
- ✓ **B)** Dismiss each individual alert that is of little value.
- X **C)** Set a filter by severity.

X **D)** Resolve each individual alert that is of little value.

X **E)** Create a bulk selection.

#### Explanation

You would set the filter to the XYZ app to narrow the list to just the XYP app alerts. Filtering saves time so that you concentrate on the alerts that need your attention.

You will need to dismiss each alert that is of little value. You will have to decide if the alert is of value or not.

You would not configure a filter by severity as the scenario does not tell us if the alerts share a common severity level. CAS defines the severity level and assigns a score.

You would not create a bulk selection. This option allows you to select all alerts at once so you can perform a bulk action. However, the scenario does not tell us of a unique commonality of these alerts that we could filter on. (If all XYZ alerts of Low severity were of no value, for example, we could filter on that, then do a bulk selection and dismissal. In this scenario, we do not know if all alerts of the same severity are all of no value.)

You would not resolve each alert that is of little value, as these alerts will not be acted upon.

#### **Objective:**

Implement Microsoft 365 security and threat management

#### **Sub-Objective:**

Implement Cloud App Security (CAS)

#### **References:**

[Docs > Microsoft Cloud App Security > Manage Alerts](#)

---

## **Question #9 of 118**

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 #10 of 118**

Question ID: 1353630

The Nutex Corporation has an Active Directory domain named **nutex.com**. Nutex has activated Rights Management in Office 365. The Global Admin would like to empower user Spencer Lee (**spencer.lee@nutex.com**) as the new Rights Management administrator.

Select the appropriate steps from the left and drag them to the right. The steps must be in the correct order. Not all the steps may be used, and all required steps may not be listed.

{UCMS id=5707958497312768 type=Activity}

Explanation

First, you should import the Azure Active Directory Rights Management (AADRM) module by running `Import-Module aadrm` at the PowerShell prompt. Next you must connect to the AADRM service using the `Connect-AadrmService` cmdlet. You will be prompted to enter your credentials.

After entering the Global Admin credentials, you can add Spencer Lee as a Rights Management administrator. To add a user, enter the `Add-AadrmRoleBasedAdministrator` cmdlet with the `-emailaddress` parameter. You can also grant administrative rights to a group or user that has a specified GUID. In this scenario, you should run `Add-AadrmRoleBasedAdministrator -EmailAddress spencer.lee@nutex.com`.

You do not need to run the `Get-AadrmRoleBasedAdministrator -Role GlobalAdministrator` cmdlet. That cmdlet would get information about holders of the Global Administrator role, which is not part of the scenario.

You would not type `Add-AadrmRoleBasedAdministrator -SecurityGroupDisplayName GlobalAdministrators`. That command would add the role to a security group, which is not part of the scenario.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[TechNet >Online Services > Azure Rights Management > Administering Azure Rights Management by Using Windows PowerShell](#)

[Microsoft Azure > Azure > Azure PowerShell > Azure Cmdlet Reference > Azure Service Management Cmdlets > Azure Rights Management Cmdlets > Connect-AadrmService](#)

[Microsoft Azure > Azure > Azure PowerShell > Azure Cmdlet Reference > Azure Service Management Cmdlets > Azure Rights Management Cmdlets > Add-AadrmRoleBasedAdministrator](#)

---

**Question #11 of 118**

Question ID: 1257285

Your company has a Microsoft 365 subscription. If a virus or spyware is detected in a message, the message should be quarantined. A notification should be sent to the recipients if their messages are quarantined.

What should you do?

- X **A)** Create an anti-malware policy from the Office 365 Security & Compliance Center
- ✓ **B)** Create an anti-malware policy from the Exchange admin center
- X **C)** Create a safe attachments policy from the Office 365 Security & Compliance Center
- X **D)** Create a safe attachments policy from the Exchange admin center

#### Explanation

You should create an anti-malware policy from the Exchange admin center. An anti-malware policy can be used to create a malware filter rule that detects malware, quarantines the malware, and notifies the recipients if their messages are quarantined. You should open the Exchange admin center, not the Office 365 Security & Compliance Center to create an anti-malware policy. You should go to **Protection > Malware filter**, and then click **New**. You can give the policy a name and check one of the following settings to all recipients if their message are quarantined:

- **No** – prevents message and attachments from being delivered
- **Yes and use default notification text** – All message attachments are replaced with a text file that contains default message text.
- **Yes and use custom notification text** – All message attachments are replaced with a text file that contains a custom message text of your choosing.

A safe attachment policy is created in the Office 365 Security & Compliance Center. A safe attachment policy can block, replace, and monitor messages that have detected malware. While a safe attachment policy can block or redirect a message to quarantine, but does not notify the recipients if their messages are quarantined.

#### **Objective:**

Implement Microsoft 365 security and threat management

#### **Sub-Objective:**

Implement Windows Defender Advanced Threat Protection (ATP)

#### **References:**

[Microsoft 365 > Anti-malware protection > Configure anti-malware policies](#)

[Microsoft 365 > Advanced Threat Protection > Set up Office 365 ATP Safe Attachments policies](#)

---

## **Question #12 of 118**

Question ID: 1257353

You are the compliance officer for Verigon Office 365 tenant. You have been asked to examine the Office 365 audit logs so that you can determine which mailboxes have been configured to immutably preserve all mailbox items indefinitely.

Which security and compliance report would you access to meet the objective?

- X **A)** Mailbox access by non-owners
- ✓ **B)** Mailbox litigation hold
- X **C)** Mailbox content search and hold
- X **D)** Role group changes

#### Explanation

The mailbox litigation hold log report will show all mailboxes that have been configured with a litigation hold. The litigation hold is typically used when situations arise that require all content within a mailbox to be immutably preserved.

The mailbox access by non-owners log will show any users that have opened a mailbox for which the user was not an owner.

The role group changes log shows information that is stored in the administrator audit log. This will show information regarding any changes to a role group, along with detailed information regarding who changed them and what specifically was changed.

The mailbox content search and hold option will look for changes to an existing in-place eDiscovery and hold. This option allows you to see compliance changes regarding an in-place hold, but it would not show what mailboxes have been configured to immutably preserve all mailbox items indefinitely.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage eDiscovery

**References:**

[TechNet > Exchange auditing reports > Learn more about running a per-mailbox litigation hold report](#)

[Office Products > Office 365 for administrators > Office 365 Security and Compliance > Hold in Office 365](#)

[Office Products > Support > Reports in the Office 365 Security & Compliance Center](#)

[TechNet > Exchange auditing reports > Run a per-mailbox litigation hole report](#)

**Question #13 of 118**

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

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

2



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 #14 of 118**

Question ID: 1353636

You are a member of the Compliance Management role groups in the admin Exchange Center for Verigon Corporation. Verigon wants to audit Exchange Online admin activity as a security measure. Verigon has an Office 365 E3 license. The HR department needs to be able to search the logs for admin activity.

What is the first step in meeting this requirement?

- ☐ A) Enable auditing for all mailboxes using the Powershell `Set-Mailbox -auditenabled $true` cmdlet and parameters.
- ☒ B) Run the Powershell cmdlet `Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true`
- ☐ C) Assign the HR department to the Compliance Management role group.
- ☐ D) Assign the **View-Only Audit Logs role** to the Compliance Management role group.
- ☐ E) In Exchange Online Powershell, run the **Search-UnifiedAuditLog** cmdlet.
- ☐ F) In the Security and Compliance Center, go to **Search and Investigation**, then choose **Audit Log Search**

**Explanation**

You would first need to run the Powershell command `Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true`. This command enables auditing. Alternatively, you could also choose **Start recording user and admin activity** from the **Audit Log Search** page in the Security and Compliance Center.

You would not enable auditing for all mailboxes using the Powershell `Set-Mailbox -auditenabled $true` command as a first step. Auditing admin activity in Exchange Online is already a default audit and is not related to mailbox auditing.

You would not, in the Security and Compliance Center, go to **Search and Investigation**, then choose **Audit Log Search** as a first step. You cannot search the logs until they have been created by enabling auditing.

You would not, in Exchange Online Powershell, run the **Search-UnifiedAuditLog** cmdlet. You cannot search the audit logs until they have been created by enabling auditing.

There is no need to assign the **View-Only Audit Logs** role to the Compliance Management role group. This role is already assigned by default.

As a first step, you would not assign the HR department to the Compliance Management role group. You will need to give the ability to view and search the logs to the HR department after auditing has been enabled. Still, you can more granularly achieve that requirement by giving the **View-Only Audit logs** role to the department or group.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage auditing

**References:**

[Microsoft Support > Auditing in Office 365 \(for Admins\)](#)

## Question #15 of 118

Question ID: 1257290

You are the Office 365 administrator for the DreamSuites Corporation. The compliance department has tasked you to set up all business users within the IT department who do not handle the day-to-day administration of the service. These users must have the minimum set of permissions required to view the service dashboard and open new support tickets.

What Office 365 admin role should be assigned to the designated business users?

- ☐ A) Password administrator
- ☐ B) Global administrator
- ☒ C) Service administrator
- ☐ D) Compliance administrator

### Explanation

The Service administrator can view the service dashboard and open new support tickets within your Office 365 tenant. This role would meet the requirement to use least privilege required to view the service dashboard and open new support tickets.

The Compliance administrator can view and manage compliance and security policies within your Office 365 tenant. This role provides access to the Office 365, Security & Compliance Center, Exchange Online, and Azure AD Admin Centers. This role would not meet the requirement to use least privilege access to view the service dashboard and open new support tickets.

The Global administrator can view and manage all administrative functions within your Office 365 tenant. This role can assign additional users to the Global administrator role. This role would have the ability to view the service dashboard and open new support tickets along with all other administrative functions, so it would not meet the requirement to use least privilege.

The Password administrator can view the service dashboard, open new support tickets, and reset passwords within your Office 365 tenant. This role would not meet the requirement to use least privilege access to view the service dashboard and open new support tickets.

### **Objective:**

Implement Microsoft 365 security and threat management

### **Sub-Objective:**

Manage security reports and alerts

### **References:**

[Microsoft Office > About Office 365 admin roles](#)

---

## Question #16 of 118

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.
- ☐ B) Add the devices to an Azure AD security group
- ☒ C) Add the users to an Azure AD security group.
- ☐ D) Create IOs and Windows 10 device profiles.
- ☐ E) Enroll all devices in Intune.

✓ **F)** In Intune, configure an App Protection Policy and the Data Protection settings.

#### 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 #17 of 118**

Question ID: 1257332

Your company has a Microsoft 365 subscription. You are tasked with configuring permissions for Security & Compliance for specific users.

Ginger needs to perform the following tasks:

- Create and manage Security & Compliance alerts.
- Read audit logs.

Mary Ann needs to perform the following tasks:

- View cases in eDiscovery
- Access case data in Advanced eDiscovery

Thurston needs to perform the following tasks:

- Export audit reports to a third party application
- Edit settings for compliance feature
- Place content in mailboxes on hold

The solution must use the principle of least privilege. To which role group should you assign each user?

{UCMS id=5734032630349824 type=Activity}

#### Explanation

You should assign users to role groups as follows:

Users	Security Operator role group	Reviewer role group	Organization Management role group	eDiscovery Manager role group
Ginger	Ginger	Mary Ann	Thurston	
Mary Ann				
Thurston				

You should assign Ginger to the Security Operator role group. This role group can view reports such as audit logs and view the settings of security features. This role can also manage security alerts.

You should assign Mary Ann to the Reviewer role group. This role group can allow members to view and access case data in Advanced eDiscovery.

You should assign Thurston to the Organization Management role group. This role group has the Audit Logs role assigned which allows a member to view the organization's audit reports, and then export the reports. This role group also has the Compliance Administrator role which can view and edit settings and reports for compliance features. This role group includes the Hold role which can place content in mailboxes, sites, and public folders on hold.

The eDiscovery Manager role group can view all eDiscovery cases in the organization and members of this role group can perform searches and place holds on mailboxes. While this group can allow members to view and access case data in Advanced eDiscovery, it also provides more permissions than necessary.

### Objective:

Manage Microsoft 365 governance and compliance

### Sub-Objective:

Implement Azure Information Protection (AIP)

### References:

[Microsoft 365 > Security > Permissions in the Office 365 Security & Compliance Center](#)

[Azure > Active Directory > Administrator role permissions in Azure Active Directory](#)

## Question #18 of 118

Question ID: 1353623

The Nutex Corporation has an Office 365 subscription and uses Microsoft Exchange Online. You created the following retention tags with this script:

```
New-RetentionPolicyTag -Name "NutexTag1" -Type SyncIssue -AgeLimitForRetention 120 -RetentionAction DeleteAndAllowRecovery -
RetentionEnabled $True
```

```
New-RetentionPolicyTag "Finance" -Type Drafts -RetentionEnabled $True -AgeLimitForRetention 365 -RetentionAction
PermanentlyDelete
```

You need to replace the existing tags in a retention policy named **NutexRetPolicy** with the above retention tags.

What would you type at the PowerShell prompt? Use the space below to write the appropriate command.

### Explanation

Acceptable answer(s) for field 1:

- Set-RetentionPolicy -Identity "NutexRetPolicy" -RetentionPolicyTagLinks "Finance", "NutexTag1",
- Set-RetentionPolicy -Identity "NutexRetPolicy" -RetentionPolicyTagLinks "Finance","NutexTag1",
- Set-RetentionPolicy -Identity "NutexRetPolicy" -RetentionPolicyTagLinks "NutexTag1", "Finance"
- Set-RetentionPolicy -Identity "NutexRetPolicy" -RetentionPolicyTagLinks "NutexTag1","Finance"
- Set-RetentionPolicy -Identity 'NutexRetPolicy' -RetentionPolicyTagLinks 'Finance', 'NutexTag1',
- Set-RetentionPolicy -Identity 'NutexRetPolicy' -RetentionPolicyTagLinks 'Finance','NutexTag1',
- Set-RetentionPolicy -Identity 'NutexRetPolicy' -RetentionPolicyTagLinks 'NutexTag1', 'Finance'
- Set-RetentionPolicy -Identity 'NutexRetPolicy' -RetentionPolicyTagLinks 'NutexTag1','Finance'

You should enter code that resembles the following (tag parameters may be in a different order):

Set-RetentionPolicy -Identity " NutexRetPolicy" -RetentionPolicyTagLinks "NutexTag1", "Finance"

The **Set-RetentionPolicy** cmdlet is used to modify an existing retention policy. You can use this cmdlet to replace retention tags in a retention policy. If a retention policy already has retention tags linked to it, you can use the **-RetentionPolicyTagLinks** parameter of the **Set-RetentionPolicy** cmdlet to replace the existing tags.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Configure Data Loss Prevention (DLP)

**References:**

[TechNet > Office Products > Exchange > Exchange Online > Security and compliance > Messaging records management procedures > Add retention tags to or remove retention tags from a retention policy](#)

---

## Question #19 of 118

Question ID: 1257338

Dreamsuites Corporation wants to retain some Office 365 company data for both compliance and efficiency reasons. They extensively use most Office 365 services.

What services areas can Dreamsuites protect with an information retention policy? (Choose all that apply.)

- ☐ A) Skype for Business peer-to-peer file transfers.
- ☒ B) Teams chats.
- ☒ C) OneDrive accounts
- ☒ D) Exchange Public Folders.
- ☒ E) Exchange Email messages

Explanation

Exchange Email messages can be protected with a retention policy.

OneDrive accounts, like SharePoint sites, can be protected. The retention policy is applied at the site collection level. A Preservation Hold library is created.

Exchange Public Folders can be protected with a retention policy. This policy is off by default.

Teams chats can be protected with a retention policy. Individual users can be excluded or included. Channel messages for specific teams can also be protected.

Skype for Business peer-to-peer file transfers are not protected by retention policies.

Retaining content means that it can't be permanently deleted before the end of a retention period. Deleting content means deleting it automatically at the end of a retention period. You could also choose to retain the data without protection, meaning that it could be manually deleted after the end of the retention period.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage data governance

**References:**

[Microsoft 365 > Overview of retention policies](#)

[Office 365 > Data Retention, Deletion, and Destruction in Office 365](#)

---

## Question #20 of 118

Question ID: 1257269

You want to build a Cloud App Security (CAS) solution for Verigon Corporation to help secure their Office 365 usage. Verigon has a CAS subscription and an Azure AD Premium P1 subscription. You need to provide a complete solution for maximum Office 365 visibility and machine-based investigation. They currently have a mix of Windows 7 and 8.1 Enterprise operating systems on all devices.

What steps and technologies will fit your plan? (Choose all that apply.)

- ✓ **A)** Configure Conditional Access App Control.
- ✗ **B)** Purchase an Azure AD Premium P2 subscription.
- ✓ **C)** Use Connected Apps
- ✓ **D)** Upgrade devices to Windows 10 Enterprise.
- ✗ **E)** Configure an App Discovery Policy.
- ✓ **F)** Purchase a Windows Defender ATP subscription.

### Explanation

You will need to upgrade devices to Windows 10 Enterprise to integrate with Microsoft Defender ATP.

You will need to purchase a Windows Defender ATP subscription. This will allow Cloud App Security to monitor Windows 10 devices both inside and outside the company. The scenario calls for a complete solution, and ATP would be part of that solution.

You will want to use Connected Apps to monitor and audit Office 365 access as needed by the scenario.

You will want to configure Conditional Access App Control. You create these policies in the Azure AD portal which then routes the session to Cloud App Security. As of this writing, full restrictions are only available for Exchange Online and SharePoint Online.

You do not need to purchase an Azure AD Premium P2 subscription. Any premium-level subscription will work with Conditional Access App control.

You do not need to configure an App Discovery Policy to meet the current needs of the scenario, although this would be a good idea assuming the Verigon may use some non-365 applications in the future. An App Discovery policy alerts you when new applications are discovered within the organization. This scenario is focused on Office 365.

### **Objective:**

Implement Microsoft 365 security and threat management

### **Sub-Objective:**

Implement Cloud App Security (CAS)

### **References:**

[Docs > Microsoft Cloud App Security > Microsoft Cloud App Security overview](#)

[Minimizing Cloud Vulnerabilities with Microsoft Cloud App Security](#)

---

## Question #21 of 118

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)** Bitlocker
- ✗ **B)** System Insights
- ✓ **C)** Credential Guard
- ✓ **D)** Configuration Score

- ✓ **E)** Encrypted Hard Drive
- ✓ **F)** Windows Hello
- X **G)** Deduplication

#### 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 #22 of 118**

Question ID: 1353641

You need to have a user named Lynn to import several PST files into mailboxes using the Security & Compliance admin center. You want to assign Lynn the minimum level of privileges.

What should you configure? Choose the appropriate steps and place them in the correct order.

{UCMS id=4901355677286400 type=Activity}

#### Explanation

You should choose the following:

1. Assign the Mailbox Import Export and Mail Recipients roles to Lynn
2. Instruct Lynn to copy the SAS URL for network upload
3. Instruct Lynn to use the Azure AzCopy tool to upload the PST files
4. Instruct Lynn to create a PST import mapping file
5. Instruct Lynn to create a PST import job in Office 365
6. Instruct Lynn to filter data and start the PST import job

You should first assign the Mailbox Import Export and Mail Recipients roles to Lynn. A global administrator can import PST files, but you want to Lynn to have the minimum level of privileges to import PST files. The Mailbox Import Export and Mail Recipients roles have the ability to import PST files.

Lynn will need the use latest version of Azure AzCopy which is the tool that must be used to upload PST files to Office 365. You cannot use the SFTP tool or another tool to upload the PST files.

You should go to <https://protection.office.com> to open the Security & Compliance Center. Click **Import** under **Data Governance**. On the Import page, click **New import job**. On the Import data page, you will have to first **Copy the SAS URL for network upload**. This URL will be used as a destination parameter of the Azure AzCopy tool. Then you must choose **Download Azure AzCopy**.

You then you must use AzCopy.exe to upload your PST files to Office 365. The following example uploads PST files from the share named **\\Server1\PSTs** to the destination URL, and outputs all messages to c:\Users\Admin\Desktop\AzCopy1.log:

```
AzCopy.exe /Source:"\\Server1\PSTs" /Dest:"https://3c3e5952a2764023ad14984.blob.core.windows.net/ingestiondata?sv=2012-02-12&se=9999-12-31T23%3A59%3A59Z&sr=c&si=IngestionSasForAzCopy201601121920498117&sig=Vt5S4hVz1zMcBkuH8bH711atBffdr0S72T1V1mNd0Rg%3D" /V:"c:\Users\Admin\Desktop\AzCopy1.log" /Y
```

You should then create a comma separated value (CSV) file that maps which user mailboxes the PST files will be imported to.

After the CSV file has been created, you need to create a PST Import job.

After the import job has been created, Office 365 begins an analysis of the data to ensure that the data is ready to import. You can choose to trim the data by setting filters or import all of the data.

#### Objective:

Manage Microsoft 365 governance and compliance

#### Sub-Objective:

Manage eDiscovery

#### References:

[Office 365 > Import Data > Use network upload to import your organization PST files to Office 365](#)

---

## Question #23 of 118

Question ID: 1257292

The manager of the sales department wants to know if certain kinds of activity or activity performed by members of the sales department on the Sharepoint site. Specifically, she wants to know when a user deletes files in SharePoint. You need to be able to view the notification in the Security & Compliance center.

What should you do?

- ☐ A) Create an alert activity from the Security & Compliance center
- ☒ B) Create an alert policy from the Security & Compliance center
- ☐ C) Create a data loss prevention (DLP) policy from the Security & Compliance center
- ☐ D) Create an alert from the SharePoint site
- ☐ E) Attach a task to the Security log in Event Viewer

#### Explanation

You should create an alert policy from the Security & Compliance center. When you create an alert policy you can be notified when a specific action is performed by a user, such as deleting a file in a SharePoint site.

You should not create an alert activity from the Security & Compliance center in this scenario. Although you can create an alert activity and be alerted when a file is deleted, the alert policy provides additional functionality, such as alerts when a user performs an activity, as well as displaying alerts on the **View alerts** page in the Security & Compliance center. In this scenario, you need to be able to view the notification in the Security & Compliance center, which you can see on the **View alerts** page in the Security & Compliance center.

You should not create an alert from the SharePoint site. You will not be able to be able to view the notification of the alert in the Security & Compliance center.

You should not attach a task to the Security log in Event Viewer. You can attach a task to the Security log in Event Viewer so if a specific event is logged, you can run a program. However, a file that is deleted from a SharePoint site may not be specifically logged. Meaning that any file that is deleted could be logged, not just from the directory that SharePoint site occupies. The sales manager wanted to be notified when a user deleted a file from the SharePoint site. The sales manager did not want to be notified when other files were deleted.

A DLP policy can prevent accidental sharing of sensitive information. If you wanted to prevent users from sharing information such as human resource records or documents with credit card numbers with people outside your organization, you could prevent an email that contains the file from being sent, or block access to the document. You can use a DLP policy to identify the documents sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams such as documents that have credit card numbers. A DLP policy does not protect against deletion.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Manage security reports and alerts

**References:**

[Microsoft 365 > Create activity alerts in the Office 365](#)

---

**Question #24 of 118**

Question ID: 1257336

Moving to Office 365 has been successful for Dreamsuites Incorporated. For local data, Dreamsuites used third-party software to enhance their business continuity and disaster recovery requirements for Exchange and Sharepoint. Management needs information on the backup and protection offered by Office 365.

What features are available? (Choose all that apply.)

- ✓ **A)** SharePoint Online document versioning.
- ✓ **B)** A Recycle Bin for SharePoint Online sites.
- X **C)** The ability to recover Exchange Online deleted items that are 90 days old.
- X **D)** The ability to restore Exchange Online mailboxes to a point in time.
- ✓ **E)** Automatic SharePoint online backup every 12 hours.
- ✓ **F)** Maintaining email for legal reasons.

Explanation

Office 365 includes a Recycle Bin for SharePoint Online sites. Deleted data is kept for 93 days.

Office 365 includes automatic SharePoint online backup every 12 hours. If data was permanently accidentally deleted, you may be able to ask Microsoft for a backup.

Office 365 includes SharePoint Online document versioning. You can always restore an older version of a document.

Office 365 includes the option of maintaining email for legal reasons. This option is now known as Litigation Hold.

An additional feature is the ability to archive mailboxes forever.

Office 365 includes the ability to recover Exchange Online deleted items. The items are kept for 14 days by default, but this can be extended up to 30 days, not 90 days.

At this time, Office 365 does not include the ability to restore Exchange Online mailboxes to a point in time.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage data governance

**References:**

[Exchange > Policy and Compliance > Place all mailboxes on hold](#)

[Exchange > Exchange Online > Backing up email in Exchange Online](#)

[Restore items in the Recycle Bin of a SharePoint site](#)

[SharePoint Online Backup Strategies for a Cloudy Day](#)

---

**Question #25 of 118**

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

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 #26 of 118

Question ID: 1257335

Verigon Corporation's legal department has decreed that all Exchange Online email messages should be kept for seven years and then deleted. They may want to extend this protection to some SharePoint Online content in the future. Verigon has a Microsoft 365 E3 license.

What steps would be part of this Data Loss Prevention (DLP) plan? (Choose all that apply.)

- ☐ A) Create a retention label for Exchange Online that can be applied by users.
- ☒ B) Create an information retention policy.
- ☐ C) Create a retention label to retain data that is applied automatically based on a condition.
- ☐ D) Upgrade to a Microsoft 365 E5 license.
- ☐ E) Purchase a SharePoint Online plan 2.
- ☐ F) Create a retention label to delete data that is applied automatically based on a condition.

### Explanation

You will want to create an information retention policy. In this policy, you can choose to retain data for some time, or after a specific age. You can then further decide to delete the data after retention. This concept could be indirectly achieved with automatically applied retention labels and custom conditions, but this method directly addresses the issue. The implementation uses retention tags vs. retention labels.

There is no need to upgrade to a Microsoft 365 E5 license. The retention policy required here is available with the existing license.

There is no need to purchase a SharePoint Online plan 2. The retention policy required here is available with the existing Microsoft 365 E3 license.

You would not create a retention label to retain data that is applied automatically based on a condition. A retention label would require an upgrade to Microsoft 365 E5 to have the label apply automatically. A retention policy can be used to meet the requirement.

You would not create a retention label to delete data that is applied automatically based on a condition. A retention label would require an upgrade to Microsoft 365 E5 to have the condition apply automatically. A retention policy meets the requirement with no additional costs.

You would not create a retention label for Exchange Online that can be applied by users. This concept should not require any user intervention. The requirement applies to all documents and, therefore, all users.

If you were to choose the retention label path (outside of this scenario), note that a single email or document can only have a single label applied. However, the label could be used in many different retention policies. Note that a Litigation Hold or In-Place Hold could also have accomplished the goal as far as the email requirement part of the scenario. Microsoft is deprecating In-Place holds.

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Manage data governance

### **References:**

[Microsoft 265 > DLP > Overview of data loss prevention](#)

[Microsoft 365 > Manage information governance > Overview of retention labels](#)

---

## Question #27 of 118

Question ID: 1257333

Your company has a Microsoft 365 subscription and implements Azure Information Protection.

Recently, the former Marketing manager sent an email to a partner that contained words that were considered unprofessional. You need to identify message that contain words that are considered unprofessional and prevent these messages from being sent.

What must you configure?

- X **A)** configure a mail flow trace from the Exchange admin center (EAC)
- X **B)** configure a content search in the Security & Compliance Center
- X **C)** configure a mail flow trace from the Security and Compliance center
- ✓ **D)** a mail flow rule from the Exchange admin center (EAC)

#### Explanation

Mail flow rules, also known as transport rules, are used to identify messages that flow through your Exchange Online organization based on criteria, and once the messages are identified, have actions taken on those messages. You can use mail flow rules on messages that meet the following criteria:

- To route email based on words such as "Confidential" or "Secret", phrases, or patterns
- To set a spam confidence level (SCL) in messages
- To block messages with specific attachments
- To enable message encryption and decryption in Office 365

You should not run a content search in the Security & Compliance Center. A content search in the Security & Compliance Center allows you to find instant messages, email, and documents in Office 365 services such as mailboxes, public folders, SharePoint Online, OneDrive for Business, Skype for Business, and Microsoft Teams. A content search will not take actions on these messages.

You should not configure a mail flow trace from the Exchange admin center (EAC) or the Security and Compliance center. A mail flow trace can be used to find messages that match specific criteria, but will not take actions on these messages.

#### **Objective:**

Manage Microsoft 365 governance and compliance

#### **Sub-Objective:**

Implement Azure Information Protection (AIP)

#### **References:**

[Exchange > Security and compliance > Mail flow rules \(transport rules\) in Exchange Online](#)

---

## **Question #28 of 118**

Question ID: 1353627

An IT employee at Nutex Corporation is attempting to activate Rights Management for their new Office 365 environment. When they log in to the Office 365 Admin center, the **Rights Management** link is not listed under **Service Settings**. Running the **Enable-Aadrm** PowerShell cmdlet returns an error:

"The attempt to connect to the Windows Azure AD Rights Management (AADRM) service failed".

What are some of the possible reasons for this failure? (Choose all that apply.)

- X **A)** The company has purchased a standalone subscription to Azure Rights Management.
- ✓ **B)** The company's Office 365 subscription does not include Rights Management.
- X **C)** The company is using the free 30-day trial of Office 365.
- ✓ **D)** The user has not been added to the Rights Management role
- X **E)** The workstation does not have Internet connectivity.

#### Explanation

There are two possible reasons for the failure in this scenario:

- The company's Office 365 subscription does not include Azure Rights Management.
- The user has not been added to the Rights Management role.

To activate Azure Rights Management (Azure RMS), the subscription must include Rights Management, or you must purchase a standalone subscription to Azure RMS.

The user must be assigned the Rights Management role using the PowerShell cmdlet **Add-AdmRoleBasedAdministrator**. If the user is not specifically assigned that role, she can log in as a Global Administrator.

Internet connectivity is not an issue here. Internet connectivity is required to activate RMS, but the scenario proves that the machine has connectivity because the user has logged in to Office 365.

The use of the free trial is not relevant to the problem here. The trial version is fully functional and includes Rights Management, but a subscription should be purchased soon.

The standalone version of Azure Rights Management is activated in the same way as Rights Management. Activation would not be the problem in this scenario.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[TechNet > Online Services > Azure Rights Management > Getting Started with Rights Management > Requirements for Azure Rights Management](#)

[TechNet > Comparison of Rights Management Services \(RMS\) Offerings](#)

[TechNet > Office Products > Exchange Online > Security and compliance for Exchange Online > Information Rights Management > Configure IRM to use Azure Rights Management](#)

---

**Question #29 of 118**

Question ID: 1353615

Verigon Corporation has created new beta versions of its three bestselling medical diagnostics tools. Any communication about these versions is for internal use only. You have been asked to modify an existing DLP policy labeled "Compliance" to warn users whenever they attempt to send an email containing these names to anyone outside the organization.

What is the best first step in making this happen?

- X **A)** In the Office 365 Security and Compliance center, choose **Classificatio**s > **Sensitive info types** and choose **Create**. Under **Add an Element**, choose to **Add a Dictionary**.
- X **B)** In the Office 365 Security and Compliance center, choose **Classification** > **Sensitive info types** and choose **Create**. Then choose **Configure the Supporting Elements**.
- X **C)** Create a CSV text file containing a header, and the beta names of the tools.
- X **D)** Use Powershell to customize the **U.S. Health Insurance Act DLP** template. Add the beta names of the tools to the XML file.
- ✓ **E)** In the Office 365 Security and Compliance center, choose **Classification** > **Sensitive info types** and choose **Create**. Configure a **Matching Element**.

Explanation

You will need to, in the Office 365 Security and Compliance center, choose **Classification** > **Sensitive info types** and choose **Create**. Configure a **Matching Element**. Here you can list the beta names of the products to match against.

## Editing Requirements for matching

You must add a matching element, which is the sensitive info that this type will look for in content. To increase the accuracy of detection, you can optionally add multiple supporting elements. When the matching element is detected, at least one supporting element you add must be found within your specified proximity of the matching element for this type to be matched.

### Matching element

^ Detect content containing

Regular expression

"asclepius","hygeia","chiron"

### Supporting elements

You don't have any supporting elements.

+ Add supporting elements

You would not want to use Powershell to customize the **U.S. Health Insurance Act DLP** template. It would not be a good practice to modify a template for a temporary situation. In addition, the scenario does not tell us that Verigon is US-based. However, if there ever is a need to customize one of these built-in "sensitive information types", it currently must be done using the Powershell **New-DlpSensitiveInformationTypeRulePackage** cmdlet.

As the first step, you would not in the Office 365 Security and Compliance center, choose **Classification > Sensitive info types**, and choose **Create**. Then choose **Configure the Supporting Elements**. While a Matching Element pattern is a requirement, supporting elements are optional. A supporting element can be used for a more granular accuracy by requiring the supporting element to be found within the proximity of the matching element.

You would not, in the Office 365 Security and Compliance center, choose **Classification > Sensitive info types** and choose **Create**. Under Add an Element, choose to Add a Dictionary. This would be the best solution if there were hundreds of matching beta names, but this is impractical for three words.

You would not create a CSV text file containing a header, and the beta names of the tools. We are not using a dictionary in this scenario. However, if a dictionary was required, this would be the first step.

Whenever you create a new sensitive information type, you will be offered the chance to test it before actual use.

#### Objective:

Manage Microsoft 365 governance and compliance

#### Sub-Objective:

Configure Data Loss Prevention (DLP)

#### References:

[Microsoft 365 > DLP > Overview of data loss prevention](#)

[Microsoft 365 > Sensitive information types > Create a custom sensitive information type in the Security & Compliance Center](#)

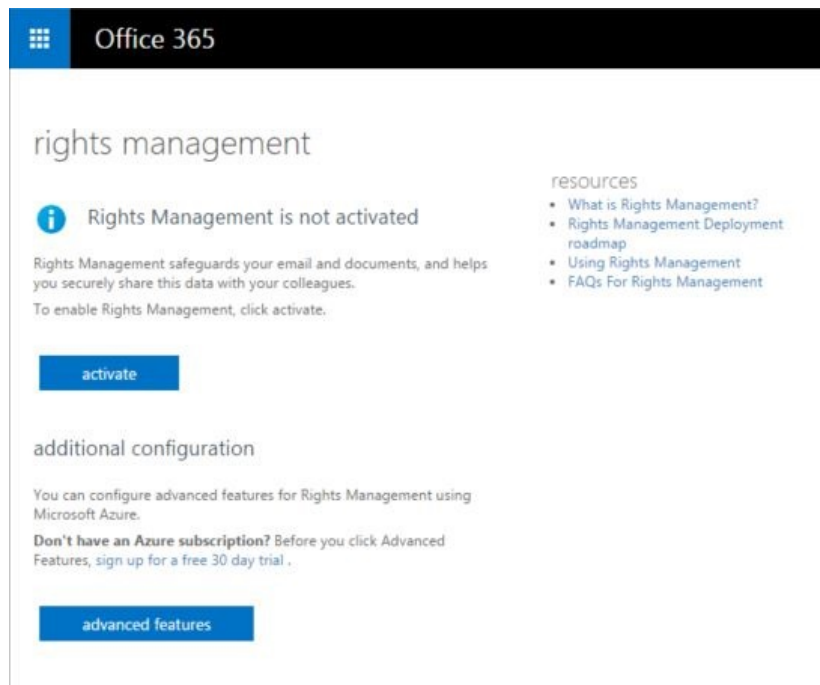
The TxGlobal Corporation is now using Office 365 with an Office 365 Enterprise E3 license. They do not have any on-premises Exchange servers. The legal department needs the ability to create some documents and emails using Office 365 that only management can read, both at work and at home. For legal reasons, management should not be able to copy or modify these documents or emails.

What steps should you perform to meet these requirements? (Choose all that apply.)

- X **A)** Create a folder named **Legal Documents**, then deny the NTFS **modify** permission for the **Managers** group for the folder.
- ✓ **B)** In the Office 365 Admin Center, choose **Activate** under the **Rights Management** management page.
- X **C)** Log in to the Office 365 Admin Center as a Service Admin.
- ✓ **D)** Log in to the Office 365 Admin center as a Global Admin.
- X **E)** In the Office 365 Admin Center, choose **Activate** under the **Rights Management** management page, and then choose **Advanced Features** to configure **Azure Rights Management**.
- X **F)** Install the RMS role on the file servers that will contain the documents.

#### Explanation

To set up Rights Management in Office 365, you must first log in to the Office 365 Admin center as a Global Admin. Next, you should activate the service by choosing "**Activate**" on the **Rights Management** management page:



This step activates the service, but additional steps will still be needed to integrate rights management with Exchange Online.

Alternatively, you could import the Windows PowerShell module **Aadrm** and then use the **Connect-AadrmService** and cmdlets to activate Rights Management. The following script shows the Office 365 administrator, Jimmy Johnson, enabling Rights Management:

```
$credential = Get-Credential -Credential jimmy_johnson@txglobal.com
Import-Module Aadrm
Connect-AadrmService -Credential $credential
Enable-Aadrm
```

Azure Rights Management (Azure RMS) is not included with all subscriptions, but in this scenario you have an Enterprise E3 license.

You should not deny the NTFS **modify** permission at the folder level for the **Managers** group because this would also deny the **read** permission. It would be better to specifically allow the **read** permission only. Even so, this action would affect only this particular folder, and the scope of file locations is not mentioned in this scenario. Note that the **read** permission still allows copying, which can only be prevented with RMS.

You do not need to choose **Advanced Features** in this scenario because you do not need configure Azure Rights Management. Activation is all that is needed.

You should not log in as a Service Admin. By default, you must be a Global Admin to activate Azure Rights Management. A Global admin could then choose to create an RMS administrator using the PowerShell cmdlet **Add-AdmRoleBasedAdministrator**.

You should not install the RMS role on any local servers. There are no on-premises Exchange servers in this scenario. If a company does have local Exchange servers, Microsoft offers a downloadable **Rights Management Connector** that will integrate local Exchange services with Azure RMS.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[TechNet > Online Services > Azure Rights Management > Getting Started with Rights Management > What is Azure Rights Management?](#)

[TechNet > Online Services > Azure Rights Management > Getting Started with Rights Management > Activating Azure Rights Management](#)

---

**Question #31 of 118**

Question ID: 1257266

Nutex Corporation has purchased an Azure AD premium license as a first step in their plan to use cloud applications wherever possible. As a security administrator, you suggest using Cloud App Security to monitor unusual activity, risky sign-ins, and other possible security breaches.

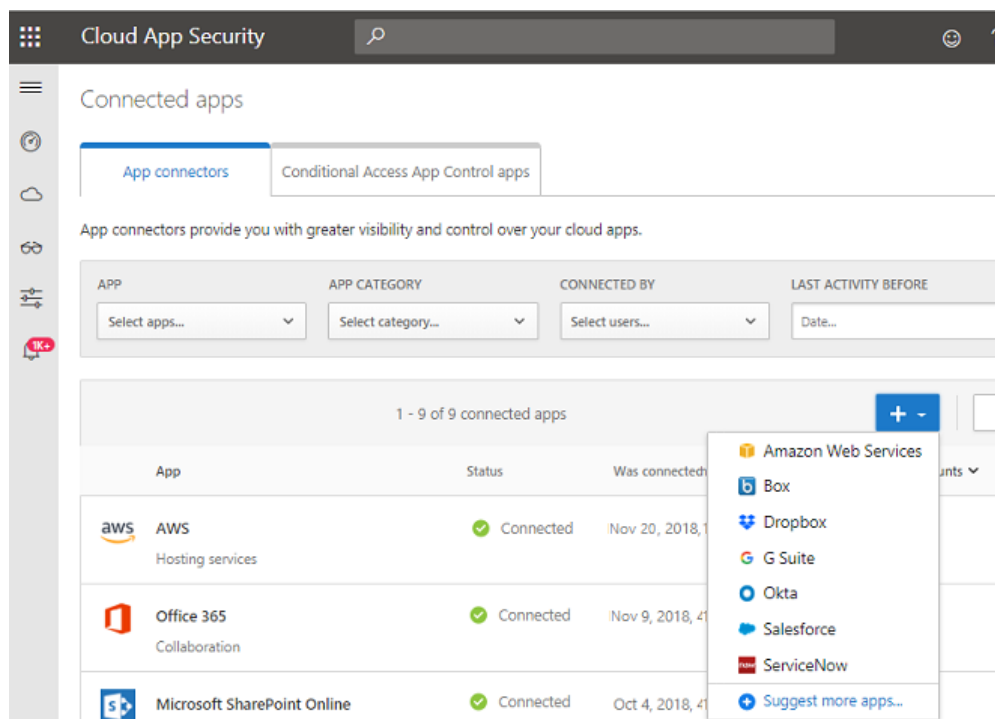
You want to protect the apps via conditional access. What steps are required parts of your configuration efforts? (Choose all that apply.)

- ☐ **A)** Purchase an Office 365 Business license.
- ☐ **B)** Purchase on Office 365 Business Premium license.
- ☒ **C)** Purchase a Cloud App Security license.
- ☒ **D)** Setup Cloud Discovery.
- ☒ **E)** Setup App Connectors in the Cloud App Security portal.

Explanation

You must purchase a Cloud App Security license to use this solution.

You will need to setup App Connectors in the Cloud App Security portal. The connectors do not have to be to Microsoft applications. Cloud App Security setup requires login as a Global Administrator or Security Administrator in Azure AD or Office 365.



You will need to setup Cloud Discovery. This feature compares the company's app usage to a catalog of applications to rank and score them based on risk factors.

You do not need to purchase an Office 365 Business license to use Cloud App Security. The application works with non-Microsoft applications as well as Office 365. Of course, Office 365 apps will need to be licensed if used, although not specifically stated in the scenario.

You do not need to purchase an Office 365 Business Premium license to use Cloud App Security. The application works with non-Microsoft applications as well as Office 365. Of course, Office 365 apps will need to be licensed if used, although not specifically mentioned in the scenario.

There are alternative cloud app security options, including Office 365 Cloud App security, and Azure AD Cloud App discovery, but they are too limited to meet the needs of this scenario.

#### Objective:

Implement Microsoft 365 security and threat management

#### Sub-Objective:

Implement Cloud App Security (CAS)

#### References:

[Docs > Microsoft Cloud App Security > Microsoft Cloud App Security overview](#)

[Docs > Microsoft Cloud App Security > Quickstart: Get started with Microsoft Cloud App Security](#)

### Question #32 of 118

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?

- X A) Feature Updates
- X B) Windows Insider Program
- ✓ C) Long-Term Servicing Channel

- X **D)** Semi-Annual Channel
- X **E)** Deployment Rings

#### 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 #33 of 118

Question ID: 1257271

Verigon Corporation uses several network appliances. They are testing a new firewall appliance before a final purchasing decision. The vendor documentation indicates that this device is supported by Cloud App Security. You would like to use the features of Cloud App Security (CAS) to analyze the traffic monitored by the device.

What should you configure?

- X **A)** Create a log collector on Ubuntu in Azure.
- ✓ **B)** In the CAS portal, from the **Settings** page, create a **Snapshot Report**.
- X **C)** In the CAS portal, add a log collector to the **Automatic Log Upload** tab.
- X **D)** In the CAS portal, create a Custom Log Parser.
- X **E)** Create a log collector using Docker on Windows.

#### Explanation

In the CAS Portal, from the **Settings** page, you will create a **Snapshot Report**. This is a manually, one-time upload of the log files from the appliance. The scenario implies that this is a test and not necessarily a permanent solution.

You would not add a log collector to the **Automatic Log Upload** tab, although this will probably be a follow-up solution after the testing phase. The scenario implies that this is a test and not necessarily a permanent solution. Microsoft recommends that even if you intend to do automatic uploads, you should first upload a log manually to see if it parses successfully.

You do not need to create a custom log parser. This would only be necessary if the device was not supported by Cloud App Security. If this were necessary, the logs would have to be edited in a text editor, and the columns mapped to specific fields in CAS before uploading.

You do not, at this time, need to create a log collector using Docker on Windows. Creating a log collector would only become necessary if it is later decided to implement Automatic Log Upload.

You do not, at this time, need to create a log collector on Ubuntu in Azure. Creating a log collector would only become necessary if it is later decided to implement Automatic Log Upload.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Implement Cloud App Security (CAS)

**References:**

[Docs > Microsoft Cloud App Security](#)

[Docs > Microsoft Cloud App Security > Create snapshot Cloud Discovery reports](#)

---

**Question #34 of 118**

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.
- ✓ **B)** Upgrade to a Premium Azure AD license
- X **C)** Enroll devices to any approved third-party MDM solution.
- ✓ **D)** Enroll the devices in Intune.
- ✓ **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.

Co-management Configuration Wizard

X

 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.

Properties
✕

Enablement
Workloads
Staging
Reporting

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.

[Learn more](#)

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

OK
Cancel
Apply

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](#)

## Question #35 of 118

Question ID: 1353633

You deploy Microsoft Azure Information Protection. You need to ensure that user named Jill Jackson can read and inspect the data that is being protected by the Azure Rights Management Service (Azure RMS), including documents and emails.

What should you configure in a PowerShell script? Choose the appropriate steps from the right and place them in the correct order

{UCMS id=5102870912303104 type=Activity}

### Explanation

You configure the following PowerShell script:

```
Install-Module -Name AIPService
Enable-AipServiceSuperUserFeature
Add-AipServiceSuperUser -EmailAddress Jill.Jackson@nutex.com
```

You will first need to install the AIPService module. This module is required to install Azure Information Protection.

Next, you will need to enable the super user of the AIPService module. The **Enable-AipServiceSuperUserFeature** cmdlet enables the super user for Azure Information Protection. The super user feature is not enabled by default. The super user feature ensures that assigned people can always read and inspect the data that is being protected by the Azure Rights Management Service (Azure RMS), including documents and emails. For example, if a user quits the company, the super user can still access files that the departed employee had protected. You may also need to bulk decrypt files for legal or compliance reasons.

Once the feature is enabled on the module, you will need to add a user or users to the super user group. You can use the **Add-AipServiceSuperUser** cmdlet to accomplish this. You could use the following to assign roles to user accounts:

```
$userName="<sign-in name of the account>"

$roleName="<role name>"

$role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}

if ($role -eq $null) {

$roleTemplate = Get-AzureADDirectoryRoleTemplate | Where {$_.displayName -eq $roleName}

Enable-AzureADDirectoryRole -RoleTemplateId $roleTemplate.ObjectId

$role = Get-AzureADDirectoryRole | Where {$_.displayName -eq $roleName}

}

Add-AzureADDirectoryRoleMember -ObjectId $role.ObjectId -RefObjectId (Get-AzureADUser | Where {$_.UserPrincipalName -eq $userName}).ObjectId
```

You cannot use the eDiscovery Manager role or the Security Reader role to view document and emails protected by Azure RMS. The eDiscovery Manager role searches content with Security & Compliance Center and performs various search-related actions, such as previewing and exporting search results. The Security Reader role can view recommendations, alerts, security policy, and security states in Security Center. Neither of these roles will allow someone to read and inspect the data by Azure Rights Management Service (Azure RMS).

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Implement Azure Information Protection (AIP)

## References:

[Docs > Azure Information Protection > Configuring super users for Azure Information Protection and discovery services or data recovery](#)

### Question #36 of 118

Question ID: 1353618

The Nutex Corporation has an Office 365 deployment. You have determined that the current retention policies are no longer applicable. You need to apply the new retention policy **NewPolicy** to all mailboxes that currently have the old policy applied, named **OldPolicy**. You plan to use the following script.

```
1 $OldPolicy={ A "OldPolicy"}.distinguishedName
2
3 B -Filter { C -eq $OldPolicy} -Resultsize Unlimited | D -RetentionPolicy "NewPolicy"
4
```

Drag the missing cmdlets, parameters, and values from the right to appropriate corresponding letter on the left. You may only use the items once.

{UCMS id=5677724746121216 type=Activity}

#### Explanation

You should choose the following options to complete the script:

```
1 $OldPolicy={Get-RetentionPolicy "OldPolicy"}.distinguishedName
2
3 Get-Mailbox -Filter {RetentionPolicy -eq $OldPolicy} -Resultsize Unlimited | Set-Mailbox -RetentionPolicy "NewPolicy"
4
```

You will need to run the **Get-RetentionPolicy** cmdlet to retrieve the distinguished name of the previous retention policy, which was named **OldPolicy**. This information is saved to a variable called **\$OldPolicy**. You should then run the **Get-Mailbox** cmdlet with the **-Filter** parameter to retrieve the retention policy that is saved to the **\$OldPolicy** variable. Next, you will use the **Set-Mailbox** cmdlet with the **RetentionPolicy** parameter to apply another policy named **NewPolicy** to all mailboxes that have the old policy named **OldPolicy**.

You should not use the **RetentionPolicyTag** parameter or the **New-RetentionPolicyTag** cmdlet in this scenario. The **RetentionPolicyTag** parameter specifies a tag within a retention policy, not the retention policy itself. The **New-RetentionPolicyTag** cmdlet creates a new retention policy tag that can be applied to a retention policy.

You should not use the **TransportRule** parameter or the **New-TransportRule** cmdlet in this scenario. The **New-TransportRule** cmdlet creates a new transport rule in the organization. A transport rule allows you to create a rule condition, such as adding a disclaimer to a message automatically. You do not need to specify a condition, but a retention policy.

#### Objective:

Manage Microsoft 365 governance and compliance

#### Sub-Objective:

Configure Data Loss Prevention (DLP)

## References:

[TechNet > Office Products > Exchange > Exchange Online > Security and compliance for Exchange Online > Messaging records management > Apply a retention policy to mailboxes](#)

### Question #37 of 118

Question ID: 1257331

You have a Microsoft Azure Active Directory (Azure AD) tenant named **nutex.com**.

Nutex has several users that need specific permissions in Microsoft Store. Those users and permissions are as follows:

- Moe needs to sign up for Microsoft Store for Business and Education, purchase subscription-based software, and purchase apps.
- Larry needs to purchase apps.

- Curley needs to modify the company profile settings
- Betty needs to be able to sign agreements and view the account for Microsoft Store
- Veronica needs to sign agreements, view the account for Microsoft Store, and edit that account.

Map the user to the appropriate role. The solution must use the principle of least privilege.

{UCMS id=5674502471024640 type=Activity}

Explanation

You should choose the following:

User	Global Administrator	Billing Administrator	Signatory	Billing account contributor	Billing account owner
Moe	Moe	Larry	Betty	Veronica	
Larry	Curley				
Curley					
Betty					
Veronica					

You can have the following global user accounts and permissions in Microsoft Store:

Permissions	Global Administrator	Billing Administrator
Purchase apps	X	X
Distribute apps	X	X
Purchase subscription-based software	X	X
Sign up for Microsoft Store for Business and Education	X	
Modify company profile settings	X	

Besides global user accounts, you can set roles at the billing account level so that you can manage tasks for Microsoft Store. The following lists the billing account roles and permissions:

Role					
	Buy from				
	Microsoft Store	Assign roles	Edit account	Sign agreements	View account
Billing account owner	X	X	X	X	X
Billing account contributor			X	X	X
Billing account reader					X
Signatory				X	X

Moe should be a member of the Global Administrator role because he needs to sign up for Microsoft Store for Business and Education, purchase subscription-based software, and purchase apps.

Larry should be a member of the Billing Administrator role because he only needs to purchase apps.

Curley should be a member of the Global Administrator role because he needs to modify the company profile settings.

Betty should be a member of the Signatory role because she needs to be able to sign agreements and view the account for Microsoft Store.

Veronica should be a member of the Billing account role because she needs to be able to sign agreements and view the account for Microsoft Store.

Objective:

Manage Microsoft 365 governance and compliance

Sub-Objective:

Implement Azure Information Protection (AIP)

References:

### Question #38 of 118

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?

- ☐ A) A device-based, Azure AD joined policy.
- ☐ B) A device-based, device platform policy.
- ☐ C) An app-based policy.
- ☒ D) A device-based, device compliance policy.
- ☐ E) A device-based, device enrollment 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 #39 of 118

Question ID: 1257319

Nutex Corporation has successfully implemented Azure Implementation Protection with an Azure Premium P1 license to encrypt corporate data. The HR department has requested that any documents from the Finance team containing U.S. Social Security Numbers are automatically encrypted.

What steps must you take to implement this using AIP?

(Choose all that apply.)

- ☒ A) Create an AIP label and configure permissions for the Finance team.
- ☒ B) Select to apply the label automatically.
- ☐ C) Create a retention label.

- ✓ **D)** Configure a condition for the label.
- ✗ **E)** Select to recommend the label to the user.
- ✓ **F)** Upgrade the AIP license to Premium P2.

### Explanation

You will want to create an AIP label and configure permissions for the Finance team (assuming that the Finance team is a group.) As soon as you choose the Protect option for the label, you will be presented with the options to choose what users or groups can apply this label. You also configure what control they have over such documents.

**Label: General** □ ×

Azure Information Protection

Save Discard Delete this label

**Specify how this label is displayed in the Information Protection client on user devices**

Enabled  
☐ Off ☒ On

Label display name \*  
Contains SSN ✓

Description \*  
This label is for Nutex documents containing a US Social Security Number ✓

Color  
☒ Select from list ☐ Custom  
Blue ✓

**Set permissions for documents and emails containing this label**

☐ Not configured ☒ Protect ☐ Remove Protection

Protection  
Azure (cloud key) >

**Set visual marking (such as header or footer)**

Documents with this label have a header  
☒ Off ☐ On

Documents with this label have a footer  
☒ Off ☐ On

Documents with this label have a watermark  
☒ Off ☐ On

**Configure conditions for automatically applying this label** ⓘ

If any of these conditions are met, this label is applied

Condition name	Occurrences
USA Social Security Number (SSN)	1

+ Add a new condition

Select how this label is applied: automatically or recommended to user  
☒ Automatic ☐ Recommended

Add policy tip describing to users the reason for applying this label  
This file was automatically labeled as Contains SSN ✓

You will need to configure a condition for the label. For this scenario, we can choose one of the built-in conditions, one of which is the US SSN condition.

You will need to select to apply the label automatically as required by the scenario.

You will need to upgrade the AIP license to Premium P2. Labeling and automatic classification is only available with the AIP P2 license.

Note that when you save a condition, it is now published automatically, unlike previous versions. Microsoft is "unifying" labels in Office 365, and AIP labels can be migrated to Office 365. AIP labels are similar to "Sensitivity Labels", but AIP labels are created in Azure AD.

You do not need to create a retention label for this scenario. A retention label is created to determine how long content must be kept before it can be deleted.

That is not a topic of this scenario.

You should not select to recommend the label to the user. The scenario states that the files should be encrypted automatically, so we cannot choose this option. The choices are mutually exclusive.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[Docs > Azure Information Protection > How to create a new label for Azure Information Protection](#)

[Docs > Azure Information Protection > How to migrate Azure Information Protection labels to unified sensitivity labels](#)

---

**Question #40 of 118**

Question ID: 1257267

Nutex Corporation is implementing Cloud App Security (CAS) to protect and monitor user usage of multiple cloud applications. You have been asked to create a CAS policy to alert you whenever US employees access Office365 from outside the United States.

What CAS policy should you configure?

- X **A)** A session policy
- X **B)** An access policy
- X **C)** An app discovery
- X **D)** A Cloud Discovery anomaly detection policy
- ✓ **E)** An activity policy

Explanation

An activity policy allows for custom alerts when specific user activity is detected. You can choose specific apps and locations as filters. This best meets the needs of the scenario.

## Create activity policy

Policy template \*

No template

Policy name \*

Nutex Non-US Activity

Description

Create a alert whenever Office 365 is accessed outside of the US>

Policy severity \*

Low

Category \*

Threat detection

Create filters for the policy

Act on:

- ☒ Single activity  
Every activity that matches the filters
- ☐ Repeated activity:  
Repeated activity by a single user

ACTIVITIES MATCHING ALL OF THE FOLLOWING Edit and

✕ App equals 4 selected

✕ Location does not equal United States

+

Alerts

☒ Create an alert for each matching event with the policy's severity [Use your organization's default settings](#)

Daily alert limit 5

☒ Send alert as email ⓘ

secadmin@nutex.com ✕

A session policy controls and monitors access of a user session. It only applies to browser based apps. The scenario does not tell us how Office 365 apps are being accessed. It is not the best solution for the scenario.

An app discovery policy detects new applications. This is not a goal in this scenario.

An access policy would allow for real-time control when the users login to selected cloud apps. An access policy can block access to app. Blocking access is not the goal of this scenario.

A Cloud Discovery anomaly detection policy looks for unusual increases in cloud application usage compared to normal usage patterns. This is not a goal in this scenario.

Microsoft provides a variety of Cloud App Security policy templates that are a useful starting point when creating your own.

Note that before creating the policies, you must have apps deployed using Conditional Access App Control.

### Objective:

Implement Microsoft 365 security and threat management

### Sub-Objective:

Implement Cloud App Security (CAS)

### References:

[Docs > Microsoft Cloud App Security > Access policies](#)

## Question #41 of 118

Question ID: 1257322

Dreamsuites has implemented Azure Information Protection (AIP) to protect and classify sensitive documents. They have purchased the AIP Premium 2 license. The Madrid office has over 100 Windows 8.1 laptops and Windows Server 2016 on all servers. They use both SCCM and Intune to deploy some applications. Dreamsuites would like users in the Madrid office to have Office content automatically labeled with some sensitive labels that have been created.

What steps will you take in the Madrid office? (Choose all that apply.)

- ☐ A) Upgrade the Madrid laptops to Windows 10.
- ☒ B) Download the AIP unified labeling client MSI from the Microsoft Download Center.
- ☒ C) Use SCCM to deploy the unified labeling client MSI to the Madrid laptops.
- ☐ D) Download **AzInfoProtection.exe** from the Microsoft Download Center.
- ☐ E) Deploy the unified labeling client MSI to the Madrid laptops using Intune.

### Explanation

You will need to download the AIP unified labeling client MSI from the Microsoft Download Center.

You will use SCCM to deploy the unified labeling client MSI to the Madrid laptops.

You do not need to upgrade the Madrid laptops to Windows 10. The client is compatible with Windows 7 SP1 and higher.

You do not need to download AzInfoProtection.exe from the Microsoft Download Center. This file is an executable that you would use for a manual install of the client, and would not be a practical choice here.

You will not deploy the unified labeling client MSI to the Madrid laptops using Intune. Intune requires Windows 10.

There are currently three client options, the "classic client", the Unified Labeling Client, and the built-in Office labeling client. The built-in client is limited in features but offers the best performance as no add-in is required. The classic client and the Unified Labeling client almost identical similar feature sets, but Microsoft is recommending the Unified Labeling client for the future.

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Implement Azure Information Protection (AIP)

### **References:**

[Docs > The client side of Azure Information Protection](#)

[Docs > Admin Guide: Install the Azure Information Protection client for users](#)

[Docs > Azure Information Protection client: Installation and configuration for clients](#)

---

## Question #42 of 118

Question ID: 1353613

As a security administrator for Verigon Corporation you need to monitor a recent increase in suspicious Office 365 activity. You want to be notified if users open malicious URLs.

What is the first step in configuring this option?

- ☐ A) In Cloud App Security, create an **Advanced Alert**.
- ☒ B) In **Security and Compliance Center > Search > Audit log search**, choose **Turn on Auditing**

- X C) In **Security and Compliance Center** Search the **Audit Log**.
- X D) In **Security and Compliance Center**, assign the **View-Only Audit logs** role to yourself.
- X E) In **Security and Compliance Center**, Create an Activity Policy for "**A potentially malicious URL click was detected**"
- X F) In **Security and Compliance Center**, Create an Activity Policy for "**Email messages containing phish URLs removed after delivery**"

#### Explanation

Your first step must be, in **Security and Compliance Center > Search > Audit log search**, choose **Turn on Auditing**. An alternative method would be to select any one the default alert policies, and choose "**Turn On Now**" in the pop-up dialog box.

Your first step would not be to create an Activity Policy for "**Email messages containing phish URLs removed after delivery**". Auditing must be turned on first, and this policy does not address the issue in the scenario.

Your first step would not be to search the **Audit Log**. Auditing must be turned on first, and, while this would reveal the issues, it is not a notification method.

You do not need to assign the **View-Only Audit logs** role to yourself, as searching the logs is not the desired solution.

[Home](#) > Audit log search

#### Audit log search

! To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report. [Turn on auditing](#)

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, and more.

Search  Results

Your first step would not be to create an Activity Policy for "**A potentially malicious URL click was detected**". However, once auditing is enabled, you would want to enable the existing default policy with this name. You can also create your new policy if desired.

You would not, in Cloud App Security, create an **Advanced Alert**. Advanced alerts cover cloud applications beyond the scope of Office 365. You can access this console by choosing "**Manage Advanced Alerts**" from the **Security and Compliance Center**

Note that, as of this writing, turning on auditing is the required first step. However, Microsoft has plans to turn it on by default in the future. Alert policies can also be turned on using the **New-ProtectionAlert** cmdlet in Security and Compliance Center Powershell.

#### Objective:

Implement Microsoft 365 security and threat management

#### Sub-Objective:

Manage security reports and alerts

#### References:

[Microsoft 365 > Create activity alerts in the Office 365](#)

[Microsoft 365 > Alerts in the Office 365 Security & Compliance Center](#)

### Question #43 of 118

Question ID: 1257278

Nutex Incorporated has asked you to implement Advanced Threat Analytics (ATA) as their security administrator. You have successfully configured ATA and have been running for a month.

How will you know when any suspicious activity has been detected? (Choose all that apply.)

- X A) In the ATA console, download the "**Passwords Exposed in Cleartext**" report.
- ✓ B) In the ATA console, run the built-in summary report.
- X C) In the ATA console, run the "**Passwords Exposed in Cleartext**" report.
- ✓ D) Receive an email notification.

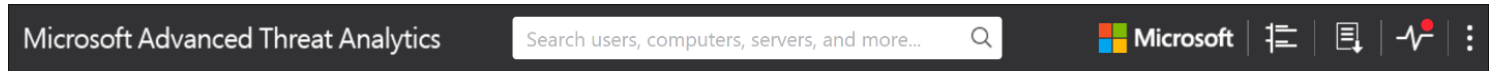
- ✓ **E)** In the ATA health center toolbar, look for a red dot.
- ✓ **F)** In the ATA console, observe the ***Suspicious Activities*** timeline.

#### Explanation

In the ATA console, you can observe the Suspicious Activities timeline. It's the first thing you will see when you go to the console.

In the ATA console, you could run the built-in summary report. This would include suspicious activities, as well as other health issues, such as problems with the ATA Gateway.

In the ATA health center toolbar, you can look for a red dot. Clicking on the dot will allow you to review the alert, and then close, or suppress the alert.



You can receive an email notification when suspicious activity occurs, assuming you have configured a valid email address.

In the ATA console, you would not run the "***Passwords Exposed in Cleartext***" report. This report would not alert you to all suspicious activities, just this particular type. And only if such activity has occurred.

In the ATA console, you would not download the "***Passwords Exposed in Cleartext***" report to meet the specific goals of this scenario. This report would not alert you to all suspicious activities, just this particular type. And only if such activity has occurred.

#### **Objective:**

Implement Microsoft 365 security and threat management

#### **Sub-Objective:**

Implement threat management

#### **References:**

[Docs > Advanced Threat Analytics > Working with ATA system health and events](#)

[Docs> Advanced Threat Analytics > ATA Reports](#)

## **Question #44 of 118**

Question ID: 1353637

You are the Exchange Online administrator for your company. You are investigating issues where Office 365 Exchange Online tenant settings have been changed without your consent.

What tool or PowerShell command can be used to view changes that have been executed against the Exchange Online environment?

- X **A) Search-MailboxAuditLog**
- X **B) Microsoft Online Services Sign-in Assistant**
- ✓ **C) Search-AdminAuditLog**
- X **D) Write-AdminAuditLog**

#### Explanation

The **Search-AdminAuditLog** cmdlet is used to parse through the administrator audit log and will allow you to search for specific cmdlets that have been run against your Exchange Online organization. Any **Set** cmdlets, for instance, that were run against your tenant will be searchable in the administrator's audit log. The following example finds all administrator audit log entries that contain either the **New-InboundConnector** or the **New-OutboundConnector** cmdlets:

```
Search-AdminAuditLog -Cmdlets New-InboundConnector, New-OutboundConnector
```

The Microsoft Online Services Sign-in Assistant installs the components required to provide the ability to connect into the Office 365 environment. Typically, the Azure Active Directory module for PowerShell will also need to be installed to make a remote PowerShell connection from an administrative workstation. This will not provide the ability to view changes that have been executed against the Exchange Online environment.

The **Search-MailboxAuditLog** cmdlet allows you to search a specific mailbox for actions that have been taken against it. For example, you may want to search a specific mailbox to see what actions a delegate has taken, like deletions of folders or mail items.

The **Write-AdminAuditLog** cmdlet is used to inject a comment into the administrator audit log. This cmdlet will allow you to add a specific comment into the administrator audit log. For example, you may want to add into the log stream that you ran a specific PowerShell script. This comment will be visible to any administrator that searches the administrator audit log.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage auditing

**References:**

[TechNet > Office Products > Exchange > Exchange Online Protection > PowerShell in Exchange Online Protection > Exchange Online Protection cmdlets > Search-AdminAuditLog](#)

---

## Question #45 of 118

Question ID: 1257277

Dreamsuites Incorporated uses Microsoft 365 extensively, so they have purchased an Enterprise E5 subscription. A recent increase in phishing and spoofing attempts has caused security issues, including sporadic impersonation attempts. You would like to increase phishing protection for all users, and prevent spoofing emails from appearing in user mailboxes.

What would be some additional steps you could take in this direction? (Choose all that apply.)

- ☐ A) Use the Message Trace Tool to find email messages.
- ☐ B) Create an ATP Safe Attachments Policy.
- ☒ C) Configure the "**Action to Apply when somebody spoofs your Domain**" to the **Quarantine** setting.
- ☒ D) Configure the "**Who the Policy Applies To**" setting to the **Dreamsuites.com** domain as part of a custom ATP anti-phishing policy.
- ☐ E) Configure the "**Define Protected Users**" setting in a custom ATP anti-phishing policy.

### Explanation

You will need to configure the "**Who the Policy Applies To**" setting to the **Dreamsuites.com** domain as part of a custom ATP anti-phishing policy. Other options would be to apply to a specific group or user.

You will want to configure the "**Action to Apply when somebody spoofs your Domain**" to the **Quarantine** setting. The default option sends the email to the users' Junk Mail folder.

Note that, of this writing, Microsoft makes a distinction between an "anti-phishing policy" and an "ATP anti-phishing policy".

You would not use the Message Trace Tool to find email messages to meet the needs of this scenario. The Message Trace tool is used to find emails that have been dropped after being flagged as spam. It will not increase phishing protection.

You would not configure the "**Define Protected Users**" setting in a custom ATP anti-phishing policy. This setting would let you specify up to 60 users from being impersonated, but the scenario does not list specific users. Note that protected users are not the only users protected from phishing attempts. In this scenario, everyone is protected.

You would not create an ATP Safe Attachments Policy to meet the needs of this scenario. A Safe Attachments policy is used to help prevent malware included in an unsafe email attachment.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Implement threat management

**References:**

[Microsoft 365 > Anti-phishing > Set up Office 365 ATP anti-phishing and anti-phishing policies](#)

[Office 365 > Office 365 Advanced Threat Protection Service Description](#)

---

**Question #46 of 118**

Question ID: 1353631

Several Nutex Corporation employees have recently left the company. These former employees used Rights Management to protect and lock down some important company documents, preventing current employees from accessing them.

You need to empower several staff members with the ability to recover protected documents and remove the protection if needed in case this situation occurs again. You choose three staff members, Tracy Walker (*tracy.walker@nutex.com*), Jane Li (*jane.li@nutex.com*), and Dennis King (*dennis.king@nutex.com*).

Select the steps on the left and place them into correct order on the right. Not all steps may be required.

{UCMS id=5631692494602240 type=Activity}

Explanation

You should first run the **Enable-AadrmSuperUserFeature** cmdlet. The feature is disabled by default, as this is a powerful role. The SuperUser can read any RMS protected document, and remove or edit the protection.

After enabling the SuperUser role, you need to run the **Add-AadrmSuperUser** cmdlet. You need to add each user individually because this cmdlet does not accept groups as a parameter.

You should not run the **Add-AadrmRoleBasedAdministrator** cmdlet because this would add more privileges to the employees than needed for the scenario.

You should not make a security group, as the **Add-AadrmSuperUser** cmdlet does not accept groups as a parameter, so this group would not be needed.

The **Enable-AadrmSuperUserFeature** cmdlet does not accept a parameter for a group or a user. This cmdlet simply enables the super user feature for Rights Management. It does not assign an individual to the super user role.

You do not need to run the **Enable-Aadrm** cmdlet because Rights Management is already running.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[Configuring Super Users for Rights Management and Discovery Services or Data Recovery Microsoft Azure > Azure PowerShell > Azure Cmdlet Reference > Azure Service Management Cmdlets > Azure Rights Management Cmdlets > Add-AadrmSuperUser](#)

---

**Question #47 of 118**

Question ID: 1353624

The Nutex Corporation has an Office 365 implementation. The company wants to increase the retention age of Deleted Items tag. You need to change number of days for the Deleted Items tag to 100 days.

What should you type at the PowerShell prompt?

Explanation

Acceptable answer(s) for field 1:

- Set-RetentionPolicyTag "Deleted Items" -AgeLimitForRetention 100
- Set-RetentionPolicyTag 'Deleted Items' -AgeLimitForRetention 100
- Set-RetentionPolicyTag -AgeLimitForRetention 100 -Identity "Deleted Items"
- Set-RetentionPolicyTag -Identity Deleted Items -AgeLimitForRetention 100

You should enter the following:

```
Set-RetentionPolicyTag "Deleted Items" -AgeLimitForRetention 100
```

The **Set-RetentionPolicyTag** cmdlet allows you to change the properties of a retention tag. The **-AgeLimitForRetention** parameter sets a time limit on the tag in a value measured in days.

#### Objective:

Manage Microsoft 365 governance and compliance

#### Sub-Objective:

Configure Data Loss Prevention (DLP)

#### References:

[Manage Retention Policy by using PowerShell](#)

[TechNet Library > Office Products > Exchange > Exchange Online Powershell > Cmdlets > Policy and compliance cmdlets in Exchange Online > Set-RetentionPolicyTag](#)

---

## Question #48 of 118

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

#### 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:

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 (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 #49 of 118

Question ID: 1353634

Nutex Corporation wants to be able to recover Office 365 data accidentally or maliciously deleted by users.

What can be recovered? (Choose all that apply.)

- ✓ **A)** OneDrive data from an earlier date.
- X **B)** Data deleted in Outlook using Security & Compliance
- ✓ **C)** A deleted user's OneDrive
- ✓ **D)** Data deleted 90 days ago from a SharePoint Online site Recycle Bin
- ✓ **E)** Outlook data purged by a user.

#### Explanation

You can restore data deleted from a SharePoint site Recycle Bin by signing in as a SharePoint admin and choosing **Restore**. Deleted items for SharePoint Online are retained in recycle bins for 93 days.

You can restore a deleted user's OneDrive. This action is accomplished via Powershell, using the `Get-SP0DeleteSite` (to find the URL), the `Restore-SP0DeletedSite` (to reactivate the site), and the `Set-SP0User` (to assign an admin to the OneDrive) cmdlets.

You can restore OneDrive data from an earlier date. In a browser open the OneDrive site, choose Settings, click **Restore your Onedrive**, and choose the desired date.

You can restore Data deleted in Outlook either directly from the Deleted Items folder, or, if necessary, by choosing **Recover Deleted Items** from the menu on the Deleted Items folder.

Data can also be restored from the OneDrive Recycle Bin.

You cannot restore data deleted in Outlook using Security & Compliance. You can restore Outlook data purged by a user using the Exchange Admin Center, and choosing **Compliance Management** from the left menu. Under **In-Place eDiscovery and Hold**, you would perform a search of a user's mailbox for deleted items.

#### **Objective:**

Manage Microsoft 365 governance and compliance

#### **Sub-Objective:**

Manage data governance

#### **References:**

[Microsoft > Restore items in the Recycle Bin of a SharePoint site](#)

[Microsoft > Restore deleted items from the site collection recycle bin](#)

[Microsoft > Restore deleted files or folders in OneDrive](#)

[OneDrive for Business > Restore a deleted OneDrive](#)

[Office 365 Enterprise > Manage Office 365 > Recover deleted items in a user mailbox - Admin Help](#)

## **Question #50 of 118**

Question ID: 1257308

Nutex Corp is concerned about mailbox size limits. The company has decided to implement a corporate policy wherein all items in the default Outlook folders should be automatically deleted after one year. The company does not want this to affect user-created folders.

As part of implementing this policy, what should you create?

- ✓ **A)** A retention policy tag
- X **B)** A retention hold
- X **C)** A default policy tag
- X **D)** A personal tag

#### Explanation

You should create a retention policy tag. This tag only applies to the default folders, such as Deleted Items and the Inbox. It does not apply to user-created folders. After the tag is created, it must then be linked to a retention policy.

You should not make a default policy tag. A default policy tag would apply to anything in the entire mailbox that was not already tagged, which could affect user-created folders. In this scenario, the items in the default Outlook folders, not in the user-created folders, should be automatically archived after one year.

You should not create a personal tag because these are intended for the users as needed. A personal tag lets users apply their own retention settings to their folders and messages.

You would not create a retention hold. A retention hold is like a "pause" button for retention. It stops any retention actions until the hold is lifted. For example, this could be useful for someone who is on unplanned leave to prevent a retention policy from affecting a mailbox while the person is out.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Configure Data Loss Prevention (DLP)

**References:**

[TechNet > Office Products > Exchange Online > Security and compliance > Messaging records management > Retention tags and retention policies](#)

[TechNet > Office Products > Exchange Online > Security and compliance > Messaging records management > Retention tags and retention policies > Default Retention Policy in Exchange Online and Exchange Server](#)

---

**Question #51 of 118**

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)** The Reports section of the Microsoft 365 Security Center
- X **B)** Remote Monitoring Solution Accelerator
- X **C)** Windows Analytics Upgrade Readiness
- X **D)** Windows Analytics Update Compliance
- ✓ **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 #52 of 118**

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 #53 of 118**

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 Standalone via the Azure portal.
- X **B)** Choose Hybrid Mobile Device Management

- X **C)** Choose Office 365 MDM Coexistence via the Office 365 admin portal.
- X **D)** Choose MDM Management for Office 365 via the Office 365 admin portal.
- X **E)** Choose Intune Co-Management via the ConfigMgr console.

#### 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 #54 of 118**

Question ID: 1257279

Verigon Corporation has a Microsoft 365 E3 license and has also purchased a Windows 10 Enterprise E5 volume license. They want to use Microsoft Defender ATP to protect their Windows 10 and Windows 7.1 SP1 Pro laptops.

As their security administrator, what steps will you take as part of the solution? (Choose all that apply.)

- ✓ **A)** Configure Security Intelligence updates on the laptops.
- X **B)** Upgrade the Windows 7.1 laptops to Windows 10.
- X **C)** Upgrade the Microsoft 365 E3 license to an E5 lisence.
- ✓ **D)** Onboard the Windows 10 laptops.
- X **E)** Configure Group Policy to disable the Microsoft Defender ELAM driver on all laptops.
- ✓ **F)** Install the Microsoft Monitoring Agent on the Windows 7.1 laptops.

#### Explanation

You must onboard the Windows 10 laptops. You have various methods to choose from, including Group Policy, a local script, SCCM, and more.

You must configure Security Intelligence updates on the laptops.

You need to install the Microsoft Monitoring Agent on the Windows 7.1 laptops. As of this writing, compatibility with earlier Windows versions is still in Preview, so **Preview Features** would also need to be enabled in this scenario.

Another significant step not listed here will be to access the Microsoft Defender Security Center to run the setup wizard to create the cloud instance of Microsoft Defender ATP. Note that Microsoft Defender ATP was formerly known as Windows Defender ATP. You may find some inconsistencies in Microsoft documentation.

You do not need to upgrade the Windows 7.1 laptops to Windows 10. As of this writing, Microsoft Defender ATP can protect Windows 7.1 SP1 laptops in Preview mode.

You do not want to configure Group Policy to disable the Windows Defender ELAM driver on all laptops. The Early Launch Antimalware (ELAM) must be enabled, even if you are using another product for antimalware. The driver will load and enable automatically when a machine is successfully onboarded. However, if you do choose another antimalware product, the driver must be configured in passive mode.

You do not need to upgrade the Microsoft 365 E3 license to an E5 license. A Windows 10 E5 Enterprise license includes Microsoft Defender ATP licensing.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Implement Windows Defender Advanced Threat Protection (ATP)

**References:**

[Docs > Threat Protection > Minimum requirements for Microsoft Defender ATP](#)

[Docs > Threat protection > Manage Windows Defender Antivirus updates and apply baselines](#)

---

**Question #55 of 118**

Question ID: 1257313

The manager of the sales department wants to know if sales department employees are sharing SharePoint documents that contain customer credit card numbers with people outside the organization.

What should you do?

- ☐ A) Attach a task to the Security log in Event Viewer
- ☐ B) Create an alert from the SharePoint site
- ☒ C) Create a data loss prevention (DLP) policy from the Security & Compliance center
- ☐ D) Create an alert policy from the Security & Compliance center
- ☐ E) Create an alert activity from the Security & Compliance center

Explanation

You should create a data loss prevention (DLP) policy from the Security & Compliance center. A DLP policy can prevent accidental sharing of sensitive information. In this scenario, you want to prevent users from sharing information such as human resource records or documents with credit card numbers with people outside your organization. You could prevent an email that contains the file from being sent or block access to the document with a DLP policy. You can use a DLP policy to identify the documents sensitive information across many locations, such as Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams, such as documents that have credit card numbers.

You should not create an alert policy from the Security & Compliance center. When you create an alert policy, you can be notified when a specific action is performed by a user, such as deleting a file from a SharePoint site. In this scenario, you need to know when a document that contains PII is being shared outside the organization.

You should not create an alert activity from the Security & Compliance center in this scenario. Although you can create an alert activity and be alerted when a file is deleted, the alert policy provides additional functionality, such as alerts when a user performs an activity. You can display alerts on the **View alerts** page in the Security & Compliance center. In this scenario, you need to know when a document that contains PII is being shared outside the organization. An alert activity cannot do that.

You should not create an alert from the SharePoint site. You cannot use an alert from the SharePoint site to prevent a document from being shared.

You should not attach a task to the Security log in Event Viewer. You can attach a task to the Security log in Event Viewer so if a specific event is logged, you can run a program. However, you will not be notified if a document is shared outside the organization in the Security log.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Configure Data Loss Prevention (DLP)

**References:**

[Microsoft 365 > Create activity alerts in the Office 365](#)

---

**Question #56 of 118**

Question ID: 1353614

For legal reasons, Verigon Corporation needs to keep all content in their Sharepoint site for at least seven years from date of creation.


What data-loss prevention concept should you implement to meet this requirement?


- ☐ **A)** Create a retention policy to retain the content for seven years based on when it was created. Choose to delete the content after that time.
- ☐ **B)** Create a retention policy and place a Preservation Lock on the policy.
- ☐ **C)** Create a retention policy to retain the content for seven years from creation.
- ☐ **D)** Create a retention policy to retain the content for seven years based on when it was modified.
- ☒ **E)** Create a retention policy to delete the content that is older than seven years.
- ☐ **F)** Create a retention policy and configure the advanced retention settings.


Explanation


You will create a retention policy to retain the content for seven years from creation. You would not configure the delete option. This solution meets the goals of the scenario. The net effect would be that a copy of the content would be maintained in a secure location (known as **Preservation Hold** in SharePoint), even if deleted "locally" by the user, for at least seven years. If you had chosen the deletion option also, then all copies would be deleted at the end of seven years.

Create a policy to retain what you want and get rid of what you don't.

 **Name your policy**


 **Settings**


 **Choose locations**

 **Review your settings**

## Decide if you want to retain content, delete it, or both

Do you want to retain content? 


☒ Yes, I want to retain it 

For this long...  years 

Retain the content based on  


Do you want us to delete it after this time? 

☐ Yes ☒ No

☐ No, just delete content that's older than 

years 

Need more options?

☐ Use advanced retention settings 

[Back](#) [Next](#) [Cancel](#)

You would not create a retention policy to delete the content for seven years based on when it was created and choose to delete the content after that time. The scenario does not indicate that the content must be deleted after seven years only that is retained for "at least" seven years. However, if the scenario had indicated "only" seven years, then this would be the proper solution.

You would not create a retention policy and place a Preservation Lock on the policy, as the scenario does not state the need for it. A Preservation Lock permanently and irrevocably sets a policy in effect. It can only be made more restrictive, never less, so this option must be used with caution. It is commonly used for financial institutions to comply with SEC regulation.

You would not create a retention policy to retain the content for seven years based on when it was modified. The scenario states that the age should be based on the creation date.

You would not create a retention policy to delete the content that is older than seven years. The scenario wants to retain the data for "at least" seven years, not "only" seven years. A "deletion only" policy would not prevent a user from deleting content.

You do not need to create a retention policy and configure the advanced retention settings. These settings allow you to trigger a policy based on content, such as specific words or information.

### Objective:

Manage Microsoft 365 governance and compliance

### Sub-Objective:

Configure Data Loss Prevention (DLP)

### References:

[Microsoft 365 > Retain data > Overview of retention policies](#)

Nutex Corporation has successfully implemented Microsoft Defender ATP. After a few weeks of usage, you want to make some changes based on the results. Many of the alerts are caused by a known internal tool used and developed by Nutex. You do not want to be alerted on this harmless tool.

What will you configure in the Microsoft Defender ATP portal?

- X **A)** Select one of the relevant alerts in the Alerts queue and set the **Classification** as a "false positive"
- ✓ **B)** Select one of the relevant alerts in the Alerts queue, and choose "**Create a suppression rule**"
- X **C)** Choose **Settings > Alert notifications> Add Notification Rule**, and configure a new rule.
- X **D)** Choose **Rules > Indicators>** Add an indicator for the selected tool file and choose the **Alert and Block** action.
- X **E)** Choose **Settings > Alert suppression**.

#### Explanation

You need to select one of the relevant alerts in the **Alerts** queue, and choose "**Create a suppression rule**". You would choose the context called "**Suppress alert in my organization**" as the scenario does not give us information that would confine the alerts to a particular machine.

You would not select one of the relevant alerts in the Alerts queue and set the **Classification** as a "false positive". This is useful to make alerts more accurate but does not suppress the alert.

You would not choose **Settings > Alert notifications> Add Notification Rule**, and configure a new rule. We do not need to configure the notification for the alerts, as we do not want to see it at all.

You would not choose **Settings > Alert suppression**. This would show you a list of existing suppression rules.

You would not choose **Rules > Indicators>** Add an indicator for the selected tool file and choose the Alert and Block action. This would block the action of the internal tool file itself, not the alert about the tool.

Note that suppression rules only take effect for new incoming alerts. It will not affect alerts already in the queue, so you will have to handle any existing alerts manually, while these are settings, Microsoft groups them together as "preferences". Preference categories include General, Permissions, APIs, Rules, and Machine Management.

#### **Objective:**

Implement Microsoft 365 security and threat management

#### **Sub-Objective:**

Implement Windows Defender Advanced Threat Protection (ATP)

#### **References:**

[Docs > Security > Threat protection > Configure Microsoft Defender Security Center settings](#)

[Docs > Security > Threat protection > Manage suppression rules](#)

---

## **Question #58 of 118**

Question ID: 1353609

You configure a conditional access policy with the following settings:

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.

- ✓ **A)** Configure a named location on the Conditional Access policy.
- X **B)** Open the Conditional Access policy and choose **Grant access** and **Require device to be marked as compliant**.
- X **C)** Open the **Locations** tab of the Conditional Access policy and choose **Any location** on the **Include** section.
- 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 #59 of 118**

Question ID: 1257273

Your company has several cloud apps that are accessed by hundreds of users and devices. The traffic logs are saved on a file share in the Azure cloud. You need to know the following information from the logs:

- The IP ranges that are accessing a particular app
- The outdated devices that are accessing a particular app
- The failed logins that are coming from allowed IP addresses

What action should you perform in Microsoft Cloud App Security?

- X **A)** Click **Investigate** and then click **Connected apps**
- X **B)** Click **Investigate** and then click **Files**
- ✓ **C)** Click **Investigate** and then click **Activity log**
- X **D)** Click **Policies** and then click **Activity policy**

**Explanation**

You should click **Investigate** and then click **Activity log**. You can use this option to filter by a particular app. On each app, you can find the following information:

- Users and devices accessing your cloud environment.
- The IP ranges that are accessing the app.
- The admin activity on the app.
- The locations from which admins are connecting.
- Any outdated devices connecting to your cloud environment.
- Any failed logins coming from expected IP addresses.

All other choices are incorrect.

You should not click **Investigate** and then click **Connected apps**. This dashboard view allows you to see the following information:

- Types of devices that your users are using to connect to the app.
- Types of files that are being saving in the cloud?
- The activity occurring in the app right now?
- The connected third-party apps to your environment.
- The authorized level of access for the third-party apps to your environment.

You should not click **Investigate** and then click **Files**. This option allows you to see the following:

- The number of files that are shared publicly so that anyone can access them without a link
- The partners that you are sharing files with (outbound sharing)
- The sensitive names of the files
- If a file is being shared with someone's personal account.

You should not click **Policies** and then click **Activity policy**. This action allows you to detect when files are accessed from that are not based on your organization's common locations. You can use this to identify malicious access or a potential data leak.

**Objective:**

Implement Microsoft 365 security and threat management

Sub-Objective:

Implement Cloud App Security (CAS)

References:

[Docs > Mobile Cloud App Security > Investigate](#)

Question #60 of 118

Question ID: 1353622

The Exchange Online staff at TXGlobal Corporation would like to implement a default archive behavior for all users in the sales department wherein all untagged mailbox items would be automatically moved after one year. Staff members have created a new Default Policy Tag (DPT) labeled "Default 1 year move to Archive" with the correct one-year archive settings. Upon attempting to add this tag to the Default MRM Policy, this error shown is displayed.

Default MRM Policy

'Name'  
Default MRM Policy

Retention tags  
+ -

NAME	TYPE	RETENTION PERIOD	RETENTION ACTION
5 Year Delete	Personal		Delete
6 Month Delete	Personal		Delete
Default 1 year move to Archive			Archive
Default 2 year move to archive	Default		Archive
Junk Email	Junk Email		Delete

error

Unable to execute the task, reason: RetentionPolicy 'Default MRM Policy' has a conflicting MessageClass '\*' for linked default RetentionPolicyTags. Please correct and retry.

[Click here for help...](#)

OK

What would be the next step taken so that TXGlobal staff members can achieve their goal?

- ✓ A) Create another retention policy, and add the tag there.
- X B) Edit the existing "Default 2 year move to Archive" tag, change the settings to one year and rename as appropriate.
- X C) Change the tag type for the "Default 2 year move to Archive" tag to Personal.
- X D) Remove the existing "Default 2 year move to Archive" tag
- X E) Change the tag type for the "Default 1 year move to Archive" tag to Personal.

Explanation

TXGlobal staff members should create another retention policy and add the tag there. Then they can apply the policy to the mailboxes for members of the Sales department only. The error is displayed because there can only be one Default Policy Tag (DPT) per retention policy. The Default MRM policy applies to every mailbox that does not have another retention policy assigned to it. Changes here would affect everyone, not just the Sales department.

## Exchange admin center

dashboard

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

mailboxes groups resources contacts shared migration



DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS	
Jane		@microsoft.com	enable   Disable
Julia		@microsoft.com	Archive
Jun		@microsoft.com	Enable   Disable
Kari		@microsoft.com	
Katie		@microsoft.com	Address Book P
MO		@microsoft.com	Update...
Moll		@microsoft.com	
Pave		@microsoft.com	Retention Policy
Rob		@microsoft.com	Update...
Robi		@microsoft.com	
Sara		@microsoft.com	Role Assignmen
Tony		@microsoft.com	Update...
Zrink		@microsoft.com	Sharing Policy

To apply the new retention policy to the Sales department only, you could use the EAC, navigate to **Recipients**, then **Mailboxes**, and use the [Ctrl] and [Shift] keys to select multiple mailboxes. Then, in the details pane, you would choose **More Options**, **Retention Policy**, and **Update**. Under Bulk Retention Policy, you should pick the new policy and click **Save**. Alternatively, you could use the **Get-Mailbox** cmdlet to find all of the users from the Sales Department, and pipe the output to the **Set-Mailbox** cmdlet with the **-RetentionPolicy** parameter. For example, the following applies the retention policy **RetentionPolicy-Sales** to all mailboxes in the Sales OU:

```
Get-Mailbox -OrganizationalUnit "Sales" -ResultSize Unlimited | Set-Mailbox -RetentionPolicy "RetentionPolicy-Sales"
```

You should not remove the existing Default 2 year move to Archive tag. While this would allow the new DPT to be added, and would eliminate the error, it changes the Default MRM Policy behavior, which goes beyond the scope of the Sales department.

You should not edit the existing Default 2 year move to Archive tag, change the settings to one year and rename as appropriate. This would change the Default MRM Policy behavior, which goes beyond the scope of the Sales department.

You should not change the tag type for the Default 1 year move to Archive tag to Personal. Not only would this modify the Default MRM Policy affecting everyone who does not have a retention policy applied; it would require the user to manually apply the tag.

You should not change the tag type for the Default 2 year move to Archive tag to Personal. Not only would this modify the Default MRM Policy affecting everyone who does not have a retention policy applied, it would require the user to manually apply the tag.

### Objective:

Manage Microsoft 365 governance and compliance

### Sub-Objective:

Configure Data Loss Prevention (DLP)

### References:

[TechNet > Office Products > Exchange Online > Security and compliance > Messaging records management > Retention tags and retention policies](#)

## Question #61 of 118

Question ID: 1353620

The Nutex Corporation has an Office 365 deployment. You have determined that the current retention policies are no longer applicable. You remove the mailbox retention policies on all Office 365 mailboxes by running the following script:

```
$UserMailboxes = Get-Mailbox -Filter {(RecipientTypeDetails -eq 'UserMailbox')}}
$UserMailboxes | Set-Mailbox RetentionPolicy $Null
```

You create the following script to apply the **RetentionPolicy-Nutex** to all mailboxes:

```
Get-Mailbox -ResultSize unlimited | Set-Mailbox -RetentionPolicy "RetentionPolicy-Corp"
```

Another employee must run the script. What management role group must this employee belong to in order to run the script? (Choose all that apply.)

- ☒ **A) Organization Management**
- ☐ **B) Server Management**
- ☐ **C) Discovery Management**
- ☒ **D) Records Management**
- ☒ **E) Recipient Management**
- ☐ **F) Compliance Management**

#### Explanation

The employee can belong to either the following management role groups:

- Organization Management
- Recipient Management
- Records Management

In this scenario, you removed the mailbox retention policies on all mailboxes by using the **Get-Mailbox** cmdlet to filter on the recipient type of **UserMailbox** to retrieve all mailboxes. You use the **Set-Mailbox** cmdlet with the **-RetentionPolicy \$Null** parameter to remove all retention policies.

Once the retention policies are removed, someone else who is a member of one of the above role groups can apply a new retention policy. These role groups can do the following:

- **Organization Management** - Members of this role group have administrative access to the entire Exchange 2013 organization and can perform any task against any Exchange 2013 object except mailbox searches and management of unscoped top-level management roles.
- **Recipient Management** - Members of this role group have administrative access to create or modify Exchange 2013 recipients within the Exchange 2013 organization.
- **Records Management** - Members of this role group can configure retention policy tags, message classifications, transport rules, and other compliance features.

The following cannot apply a retention policy:

- **Compliance Management** - Members of this role group can configure and manage Exchange compliance configuration in accordance with their policies.
- **Discovery Management** - Members of this role group can configure litigation holds on mailboxes and perform searches of mailboxes in the Exchange organization for data that meets specific criteria.

#### **Objective:**

Manage Microsoft 365 governance and compliance

#### **Sub-Objective:**

Configure Data Loss Prevention (DLP)

#### **References:**

[TechNet > Office Products > Exchange > Exchange Server 2013 > Permissions > Features permissions > Messaging policy and compliance permissions](#)

[TechNet > Office Products > Exchange > Exchange Server 2013 > Permissions > Understanding Role Based Access Control > Understanding management role groups](#)

[Manage Retention Policy by using PowerShell](#)

---

## Question #62 of 118

Question ID: 1257351

Dreamsuites Corporation makes frequent use of the Exchange Online Litigation Hold feature. The legal department has submitted a request to keep mailbox items from selected users. As the security admin, you place an infinite hold on those users' mailboxes. What happens when a user both deletes AND purges an item from their mailbox?

- X A) The item is no longer recoverable.
- X B) The item is deleted when the retention period of the related deletion policy expires.
- X C) The item is moved to the Recoverable Items folder
- X D) The item is moved to the Deletions subfolder and removed when the mailbox is processed by the Managed Folder Assistant (MFA).
- ✓ E) The item is moved to the Purges subfolder.

### Explanation

The item is moved to the Purges subfolder when the user purges the item. With an indefinite hold, the item will never be removed from the Purges subfolder. If this were an eDiscovery hold, the item would have been moved to a DiscoveryHolds subfolder.

The item is not moved to the Recoverable Items folder.

The item is not moved to the Deletions subfolder and removed when the mailbox is processed by the Managed Folder Assistant (MFA). This folder contains items that have been permanently deleted (but not purged) by the user.

The item is not deleted when the retention period of the related deletion policy expires. When a retention period expires, the item moves to the Purges subfolder.

The item is indefinitely recoverable with an infinite litigation hold, which is the intent of the feature.

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Manage eDiscovery

### **References:**

[Microsoft 365 > Create a Litigation Hold](#)

[Exchange > In-Place Hold and Litigation Hold](#)

## Question #63 of 118

Question ID: 1257294

To ensure HIPAA compliance, Nutex Corporation needs to insure the protection of personally identifiable information (PII) and prevention of medical terms in both Exchange Email and Teams chat messages.

What will be the easiest DLP (Data Loss Prevention) method?

- X A) In the Office 365 Security and Compliance portal, choose **Data Loss Prevention**, and the **U.S. Personally Identifiable Data** template.
- X B) In the Office 365 Security and Compliance portal, choose **Data Loss Prevention**, then **Create a Policy >Custom Policy**
- X C) In the Office 365 Security and Compliance portal, choose **Data Loss Prevention**, then the **General Data Protection Regulation Policy**.
- ✓ D) In the Office 365 Security and Compliance portal, choose **Data Loss Prevention** and the **U.S. Health Insurance Act** template. Choose specific locations for the new policy.

- X E) In the Office 365 Security and Compliance portal, choose **Data Loss Prevention** and the **U.S. Personally Identifiable Data** template. Choose specific locations for the new policy.

### Explanation

You should choose **Data Loss Prevention** and the **U.S. Health Insurance Act** template. Choose specific locations for the new policy. This policy covers the needs of the scenario. You will only need to modify the policy by choosing the "locations". Microsoft uses the term "locations" for the products to be covered, in this case, Exchange and Teams.

New DLP policy

Choose the information to protect

Name your policy

Choose locations

Policy settings

Review your settings

Financial

Medical and health

Privacy

Custom

Australia Health Records Act (HRIP Act)

Canada Health Information Act (HIA)

Canada Personal Health Information Act (PHIA) - Manitoba

Canada Personal Health Act (PHIPA) - Ontario

**U.S. Health Insurance Act (HIPAA)**

**Description**  
Helps detect the presence of information subject to United States Health Insurance Portability and Accountability Act (HIPAA).

**Protects this information:**  
PII Identifiers  
Medical Terms

Start with a template or create a custom policy

Choose an industry regulation to see the DLP policy templates you can use to protect that info or create a custom policy start from scratch. If you need to protect labeled content, you'll be able to choose labels later.

[Learn more about DLP policy templates](#)

Search

Show options for All countries or regions

You would not choose **Data Loss Prevention**, then the **General Data Protection Regulation Policy**. This policy does not cover the HIPAA concerns of the scenario.

You would not choose **Data Loss Prevention** and the **U.S. Personally Identifiable Data** template. While this does cover the PII requirement of the scenario, you would have to modify it to include the medical term prevention required. There is an easier method.

You would not choose **Data Loss Prevention** and the **U.S. Personally Identifiable Data** template. Choose specific locations for the new policy. While this does cover the PII requirement of the scenario, you would have to modify it to include the medical term prevention required. There is an easier method.

You would not choose **Data Loss Prevention**, then **Create a Policy >Custom Policy**. While this could become a solution to the scenario, it is not the easiest method. Microsoft already provides a template just for this purpose.

### Objective:

Manage Microsoft 365 governance and compliance

### Sub-Objective:

Configure Data Loss Prevention (DLP)

### References:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-dlp-policy-from-a-template>

## Question #64 of 118

Question ID: 1257317

Verigon Corporation has an on-premises Exchange environment. They have moved most locations to Exchange Online, but there are still some user mailboxes on local Exchange Servers. Verigon intends to use Azure Information Protection to protect all email attachments. You have successfully configured and licensed AIP for all users. All Verigon servers are running 64-bit Windows Server 2012 R2.

What still needs to be done to ensure data protection for the on-premises mail messages? (Choose all that apply)

- ✓ **A)** Configure directory synchronization between the on-premises AD and Azure Active Directory (Azure AD).
- ✓ **B)** Install an RMS Connector on two computers that will not use the connector.
- X **C)** Upgrade at least two servers to Windows Server 2016.
- X **D)** Install an RMS Connector on one of the Exchange Servers.
- X **E)** Deploy Active Directory Rights Management (AD RMS) on-premises
- ✓ **F)** Confirm or activate Azure Rights Management.

#### Explanation

You must confirm or activate Azure Rights Management. For newer subscriptions, this is activated by default.

You must configure directory synchronization between the on-premises AD and Azure Active Directory (Azure AD).

You must install an RMS Connector on two computers that will not use the connector. The connector allows the on-premises servers to use AIP. Connectors cannot be placed on any computer that needs to use the connector, such as Exchange Servers, SharePoint Servers, or servers configured for file classification.

You do not want to install an RMS Connector on one of the Exchange Servers. You will need two RMS Connectors, but they cannot be placed on any computer that needs to use the connector, such as Exchange Servers, SharePoint Servers, or servers configured for file classification.

You do not want to deploy Active Directory Rights Management (AD RMS) on-premises. This is not compatible with Azure Rights Management.

You do not need to upgrade at least two servers to Windows Server 2016. The RMS connector can be installed on Windows Server 2008 R2 and higher, on both physical and virtual systems.

#### **Objective:**

Manage Microsoft 365 governance and compliance

#### **Sub-Objective:**

Implement Azure Information Protection (AIP)

#### **References:**

[Docs > Azure Information Protection > Deploying the Azure Rights Management connector](#)

[Docs > Azure Information Protection > Installing and configuring the Azure Rights Management connector](#)

---

## **Question #65 of 118**

Question ID: 1353617

Dreamsuites marketing has created five new marketing words and phrases for their multi-million dollar hotel renovation project that is underway. The registration of these words and phrases as trademarks and service marks is in process. Dreamsuites would like to take advantage of the Data Loss Prevention feature of Office365. Dreamsuites has an E3 License. They would like to prevent any emails containing any of these words or phrases from being sent to external recipients until the new marketing and advertising campaign is launched.

What steps must be part of the process to add these words? (Choose all that apply.)

- X **A)** Use the **Set-DlpKeywordDictionary** cmdlet to export the existing dictionary.
- X **B)** Add the keywords and phrases to a comma-separated CSV file.
- ✓ **C)** Connect to Exchange Online Powershell
- X **D)** Login to the Exchange Admin Center, choose **Compliance Management > Data Loss Prevention > New Custom DLP Policy**
- X **E)** Login to the Exchange Admin Center, choose **Compliance Management > Data Loss Prevention > Import DLP Policy**

- ✓ **F)** Use the **New-DlpKeywordDictionary** cmdlet to create a keyword dictionary containing the five words and phrases.

#### Explanation

The first step in adding these words will be to connect to Exchange Online Powershell. Keyword dictionaries cannot be configured from the Exchange Admin Center. You can use the **New-DlpKeywordDictionary** cmdlet to create a dictionary with the desired words and phrases. Because there are only five words in this scenario, they can just be directly added as part of the cmdlet. Note that creating the keyword dictionary is just part of the process that will be needed to complete overall goal of the scenario. A new DLP policy may need to be created. A new sensitive information type rule package may also be needed to protective your sensitive information by creating keyword lists for identifying generic content such as healthcare-related communication.

We would not Login to the Exchange Admin Center, choose **Compliance Management > Data Loss Prevention > New Custom DLP Policy**. We may need to do this later in the process, but it is not a required step in adding words to the dictionary.

Adding the words and phrases as a comma-separated file, to be encoded and uploaded using the **New-DlpKeywordDictionary** cmdlet, is additional work that is unneeded in this scenario. If there were a long list of words beyond the five mentioned in the scenario, this might be a better choice.

We would not use the **Set-DlpKeywordDictionary** cmdlet to export the existing dictionary, because exporting the dictionary does not add words to it. (Note: this cmdlet could, in fact, be used to add terms to an existing dictionary, but that was not offered as a solution.)

We would not login to the Exchange Admin Center, choose **Compliance Management > Data Loss Prevention > Import DLP Policy**. We may need to do this later in the process, but it is not a required step when adding words to the dictionary.

#### **Objective:**

Manage Microsoft 365 governance and compliance

#### **Sub-Objective:**

Configure Data Loss Prevention (DLP)

#### **References:**

[Microsoft Office > Create a keyword dictionary](#)

[Docs > Connect to Exchange Online PowerShell](#)

---

## **Question #66 of 118**

Question ID: 1257356

You create a content search report from the Security & Compliance Center in Office365. The report has the following configuration:

|~Security&Compliance\_ContentExport.png~|

Which of the following files are excluded from the export? (Choose all that apply.)

- ✓ **A)** A file encrypted by another user's Linux OS that is 4 MB
- ✓ **B)** An audio file with a MP3 extension that is 8 MB
- X **C)** A spreadsheet with a XLSX extension that is 15 MB
- X **D)** A word processing document with a RTF extension that is 20 MB
- X **E)** A word processing document with a DOCX extension that is 50 MB
- X **F)** 6 MB file encrypted with Cipher
- ✓ **G)** An audio file with a FLAC extension that is 3 MB
- ✓ **H)** A password protected file that contains license keys that is 6 KB

#### Explanation

The following files will be excluded:

- A file encrypted by another user's Linux OS that is 4 MB

- A password protected file that contains license keys that is 6 KB
- An audio file with a FLAC extension that is 3 MB
- An audio file with a MP3 extension that is 8 MB

The exhibit shows that the items to be EXCLUDED in the report are files that have an unrecognized format, are encrypted , or were not indexed.

The files with FLAC or MP3 extensions were not indexed because of unrecognized formats. MP3, FLAC, or Bitmaps are file types not indexed for search.

A password protected file is not indexed.

A file that is encrypted with non-Microsoft technologies such as the file that is encrypted by another user's Linux OS is not indexed.

Other types of files that are not indexed or returned as partially indexed items when you run a search are as follows:

- Messages have an attached file without a valid handler, such as image files like JPG, PNG, and BMP.
- The file type is supported for indexing but an indexing error occurred for a specific file.
- An email message that has too many files attached
- A file attached that is too large that is attached to an email message

The following files are supported:

- A word processing document with a DOCX extension that is 50 MB
- A word processing document with a RTF extension that is 20 MB
- A spreadsheet with a XLSX extension that is 15 MB
- 6 MB file encrypted with Cipher

The files with DOCX, RTF, and XLSX are formats that are recognized and indexed.

The encrypted file with Cipher is supported because the file is encrypted with a supported Microsoft technology.

#### Objective:

Manage Microsoft 365 governance and compliance

#### Sub-Objective:

Manage eDiscovery

#### References:

[Microsoft 365 > Content Search > Partially indexed items in Content Search in Office 365](#)

[Microsoft 365 > Content Search > Export a Content Search report](#)

## Question #67 of 118

Question ID: 1353625

Verigon Corporation uses Azure Information Protection (AIP) and the Azure Rights Management service to protect Exchange emails and SharePoint files. A key employee has just left the company, and management needs to access their encrypted emails immediately. They would like members of the HR group to have this power going forward as well as access to other protected content.

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

- ☐ **A)** Run the Powershell **Set-IRMConfiguration** cmdlet, with the **-DecryptAttachmentForEncryptOnly** parameter.
- ☐ **B)** Create a new rights definition object using the Powershell **New-AipServiceRightsDefinition** cmdlet.
- ☒ **C)** Run the Powershell **Add-AipServiceSuperUser** cmdlet and add a user.
- ☒ **D)** Run the Powershell **Enable-AipServiceSuperUserFeature** cmdlet.
- ☒ **E)** Run the Powershell **Set-AipServiceSuperUserGroup** cmdlet, and add the HR group.

[Explanation](#)

You will need to run the Powershell **Enable-AipServiceSuperUserFeature** cmdlet. This cmdlet enables a "superuser" that always has the rights management "full control" rights over the data.

You will need to run the Powershell **Add-AipServiceSuperUser** cmdlet and add a user. Although you will be empowering the HR group with a separate cmdlet, you need this to comply with the scenario requirement for immediate decryption. Azure Rights Management caches the group membership for performance reasons.

You will need to run the Powershell **Set-AipServiceSuperUserGroup** cmdlet, and add the HR group. This cmdlet will give members of the group the rights that they need.

You do not need to run the Powershell **Set-IRMConfiguration** cmdlet, with the **-DecryptAttachmentForEncryptOnly** parameter. This parameter is used to specify the rights users have on their email attachments sent with Office 365 message encryption. It is not needed to meet the requirements of the scenario.

You do not need to create a new rights definition object using the Powershell **New-AipServiceRightsDefinition** cmdlet. This cmdlet would let you create a rights definition object to be used in the process of creating or updating an AIP template.

The scenario does not tell us if there is an on-premises Exchange environment. If so, it would also be necessary to configure the Rights Management Connector for the local Exchange server. Do so would automatically enable the superuser account, in that case.

#### Objective:

Manage Microsoft 365 governance and compliance

#### Sub-Objective:

Implement Azure Information Protection (AIP)

#### References:

[Docs > Configuring super users for Azure Information Protection and discovery services or data recovery](#)

[Configuring Azure Information Protection Superuser Access](#)

---

## Question #68 of 118

Question ID: 1257316

Dreamsuites Incorporated has just licensed a Microsoft 365 E3 subscription. They have Azure AD, but all users are now in an on-premises AD forest. They do not currently employ rights management, which they hope to resolve with this subscription. Dreamsuites would like to use Azure Information Protection (AIP) to help prevent sensitive documents stored in the cloud from being transmitted outside of the organization. Word users should be able to classify a document as "Confidential" by applying a label.

What steps will be part of this process? (Choose all that apply.)

- ☒ **A)** Synchronize on-premises users with Azure AD.
- ☒ **B)** Assign User Licenses to all users who will be classifying documents.
- ☐ **C)** Export the Trusted Publishing domains (TPD's) to an XML file.
- ☐ **D)** Deploy the Azure Information Protection scanner to automatically classify and protect the existing files.
- ☒ **E)** Select a tenant key topology.
- ☒ **F)** Configure sensitivity labels.

#### Explanation

You will need to assign User Licenses to all users who will be classifying documents. The easiest way to do this would be to create and groups for this purpose.

You will need to configure sensitivity labels. Note that there are several labeling "clients" to choose from for Windows computers. The latest client is called the Unified Labeling Client. After creating the label, it must be added to a policy. You can create a label that automatically is applied, or have recommendations made to the user when conditions are met.

You will need to synchronize the on-premises users with Azure AD. Another option not listed here would be to create user accounts directly in Azure AD.

You will need to select a tenant key topology. You can choose from a Microsoft-managed key or bring your own.

You will not need to export the Trusted Publishing domains (TPD's) to an XML file. This would apply to a business migrating from the former Rights Management Service (RMS). The scenario states that Dreamsuites does not currently have an RMS solution.

You cannot deploy the Azure Information Protection scanner to automatically classify and protect the existing files. The scanner option is not included in a Microsoft 365 E3 license.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[Docs > Azure Information Protection > Requirements for Azure Information Protection](#)

[Docs > Azure Information Protection > Azure Information Protection deployment roadmap](#)

[Docs > Azure Information Protection > Preparing users and groups for Azure Information Protection](#)

---

**Question #69 of 118**

Question ID: 1257320

Verigon Corporation has recently moved to Exchange Online and Sharepoint Online. The Corporation has configured AIP with an AIP P2 subscription. They want to protect Exchange Online email messages and their SharePoint Online document libraries with Information Rights Management (IRM).

What is a required step?

- ✓ **A) In the classic SharePoint Admin center > *Settings*, choose "*Use the IRM service specified in your configuration*"**
- X **B) Under the IRM settings for each SharePoint Online library, choose *to Set group protection and credentials interval*.**
- X **C) From an administrative Powershell prompt, run the *Set-IRM Configuration* cmdlet.**
- X **D) Under the IRM settings for each SharePoint Online library, choose to *Configure document access rights*.**
- X **E) From an administrative Powershell prompt, run the *Get-IRM Configuration* cmdlet.**

Explanation

To enable IRM for SharePoint Online, a required first step is found in the "classic" version of the SharePoint Admin Center. Under **Settings**, choose "**Use the IRM service specified in your configuration**". This option also enables IRM for OneDrive for Business.

There is no need to run the **Get-IRM Configuration** cmdlet. This cmdlet would tell you the status of IRM enablement for Exchange Online. IRM for Exchange Online is now automatically enabled for new tenants, and checking the status is not a required step.

You may choose to **Configure document access rights** for each library, but this is not a required step for the scenario. These options do not appear until IRM has been enabled in the classic SharePoint Admin center.

You may choose to **Set group protection and credentials interval**, but this is not a required step for the scenario. These options do not appear until IRM has been enabled in the classic SharePoint Admin center.

You do not need to run the **Set-IRM Configuration cmdlet**. This cmdlet would be used to enable IRM for Exchange Online. IRM for Exchange Online is now automatically enabled for new tenants. This cmdlet would not enable IRM for SharePoint Online as required by the scenario.

**Information Rights Management (IRM)**

Set IRM capabilities to SharePoint for your organization (requires Office 365 IRM service)

- ☒ Use the IRM service specified in your configuration
- ☐ Do not use IRM for this tenant

[Refresh IRM Settings](#)

**Objective:**  
Manage Microsoft 365 governance and compliance

**Sub-Objective:**  
Implement Azure Information Protection (AIP)

**References:**

[Microsoft 365 > Set up Information Rights Management \(IRM\) in SharePoint admin center](#)

[Apply Information Rights Management to a list or library](#)

Question #70 of 118

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.)

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

Dashboard > Microsoft Intune > Device compliance - Policies > Create Policy > iOS compliance policy > Device Health

Create Policy

Name

Jailbreak Policy

Description

Enter a description...

Platform

iOS

Settings

Configure

iOS compliance policy

Select a category to configure settings.

Email

1 setting available

Device Health

2 settings available

Device Properties

4 settings available

System Security

10 settings available

Device Health

Jailbroken devices

Block Not configured

Require the device to be at or under the Device Threat Level

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>

---

**Question #71 of 118**

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.

Co-management Configuration Wizard

Staging

Tenant onboarding

Enablement

Workloads

Staging

Summary

Progress


Completion

### Configure roll out collections

Pilot

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.

Compliance policies:	<span>Compliance policies</span>	<span>Browse...</span>
Device Configuration:	<span></span>	<span>Browse...</span>
Endpoint Protection:	<span></span>	<span>Browse...</span>
Resource access policies:	<span></span>	<span>Browse...</span>
Office Click-to-Run apps:	<span>Click-to-Run</span>	<span>Browse...</span>
Windows Update Policies:	<span></span>	<span>Browse...</span>

< Previous Next > Summary Cancel

**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 #72 of 118**

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

**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>

<https://docs.microsoft.com/en-us/azure/active-directory/devices/hybrid-azuread-join-plan>

---

**Question #73 of 118**

Question ID: 1257314

You need to configure a data loss prevention (DLP) policy to protect internal health records from being shared with external users.

A user informs you that he can share health records with Exchange email. The same user cannot share the same health records using OneDrive for Business.

What should you configure?

- X **A)** Configure a priority of a DLP rule
- X **B)** Configure a label as a condition of a DLP rule.
- ✓ **C)** Configure locations for the DLP Policy rule
- X **D)** Configure a condition of a DLP rule

#### Explanation

A DLP policy covers locations such as Exchange email, SharePoint sites, OneDrive accounts, or Team chat and channel messages. A DLP policy could be configured to find and protect sensitive information across Exchange email or OneDrive to prevent disclosure of personally identifiable information (PII) such as health records, credit card numbers, social security numbers, or financial data. In this scenario, OneDrive is covered by an existing DLP policy, but Exchange is not.

New DLP policy

✓ Choose the information to protect

✓ Name your policy

● Choose locations

● Policy settings

● Review your settings

### Choose locations

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	Exchange email	All <a href="#">Choose distribution groups</a>	None <a href="#">Exclude distribution groups</a>
<input checked="" type="checkbox"/>	SharePoint sites	All <a href="#">Choose sites</a>	None <a href="#">Exclude sites</a>
<input checked="" type="checkbox"/>	OneDrive accounts	All <a href="#">Choose accounts</a>	None <a href="#">Exclude accounts</a>
<input checked="" type="checkbox"/>	Teams chat and channel messages	All <a href="#">Choose accounts</a>	None <a href="#">Exclude accounts</a>

Back

Next

Cancel

You should not configure a condition of a DLP rule. A DLP rule requires that you configure conditions. If the condition is met, then an action is performed. When the action is performed, a notification is sent to the user. In this scenario, you want the DLP rule to work in both Exchange email and OneDrive for Business. This requires a location, not a condition.

You should not configure a priority of a DLP rule. A priority is used if you have content that will match multiple rules. Configuring the priority allows rules to be processed in the order of priority. If content matches multiple rules, the rule that is enforced is the one with the highest priority and most restrictive. You do not have to create multiple rules in the scenario.

You should not use a label as a condition of a DLP rule. Retention labels classify data across your organization to enforce retention rules based on classification. Labels do not assign a DLP rule to locations, such as Exchange email, SharePoint sites, OneDrive accounts, or Team chat and channel messages.

#### Objective:

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Configure Data Loss Prevention (DLP)

**References:**

[Office 365 > Overview of data loss prevention](#)

---

**Question #74 of 118**

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

**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 #75 of 118**

Question ID: 1257272

The Nutex Corporation has a Microsoft 365 subscription. From the Cloud App Security page, you run Discovered app filters. You notice that several of the apps have a low preliminary score because the app is missing basic facts, such as its domain and funding year.

What should you configure in Cloud Discovery settings so that missing facts about the app will not affect the score in the future?

- X A) On the **Score Metric** page, slide the metrics under the **Security** section to **High**
- ✓ B) On the **Score Metric** page, slide the metrics under the **General** section to **Ignore**
- X C) Set the app tag for the application to sanctioned
- X D) Create a custom app tag for the application

#### Explanation

You should change the score metrics of the application in Cloud Discovery by sliding the metrics under the General section to Ignore. This can be accomplished on the Score Metric page.

The risk score of any app is a weighted average of the following categories:

- General – This information includes the year in which the app provider was founded, whether the company is privately or publicly held, date on which the domain was registered, and consumer popularity.
- Security – This information includes whether the app uses multi-factor authentication, whether encryption is used, the classification of data, and information about data ownership.
- Compliance -This information includes whether the data adheres to specifications of HIPAA, CSA, and PCI-DSS.
- Legal – Displays which aps have regulations and policies in-place for privacy and data protection.

For every field under each category., you can slide the Importance metric to Ignored, Low, Medium, or Very High. In this scenario, you could change the fields for the General category of Founded, Holding, Domain Registration, and Consumer popularity from the default of Medium to Ignored or Low.

The screenshot shows the 'Cloud App Security' interface. On the left, a sidebar contains a search bar and a list of settings categories: System, Organization details, Mail settings, Export settings, Cloud Discovery, Score metrics (highlighted with a red arrow), Snapshot reports, Continuous reports, Automatic log upload, App tags, Exclude entities, User enrichment, Anonymization, Delete data, and Information Protection. The main panel is titled 'Settings' and 'Score metrics'. It includes a sub-header 'Configure your own preferences and priorities for each app property to customize the calculation of discovered app scores.' Below this, the 'General' category is expanded, showing four fields with sliders and checkboxes:

Field	Importance	N/A values
<b>Founded</b> The year in which the provider was founded.	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As
<b>Holding</b> Displays whether the provider is a publicly or privately held company.	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As
<b>Domain registration</b> The date on which the domain was registered.	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As
<b>Consumer popularity</b> Popularity of this app among SaaS users world-wide. A high score indicates a popular app with high-use rates.	Medium (x2)	<input checked="" type="checkbox"/> Exclude N/As

You can use app tags to set the application as sanctioned by your organization or unsanctioned by your organization. Changing the app tag will not affect the risk score. However, you can override the risk score for apps. To override the risk score, in the Discovered apps table or in the Cloud app catalog, click the three dots to the right of any app and choose Override app score. You can have an app tag for an application that sanctions the app for the organization, but the application may have a low score. You can override the risk score on the application to encourage users in your organization to use the application.

Override score

Current score: 10

Select a new score for Microsoft Exchange Online:

Select score... ▾

App notes ▾

Restore default score

Save

Cancel

You would not slide the metrics under the **Security** section to **High** on the Score Metric page. While this action would prioritize the fields under the **Security** section in the risk score, it does not address the missing information under the **Security** section and would not affect the risk score as much as sliding slide the metrics under the **General** section to **Ignore** on the Score Metric page.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Implement Cloud App Security (CAS)

**References:**

[Docs > Cloud App Security > Working with App risk scores](#)

[Docs > Cloud App Security > Discovered app filters and queries](#)

---

**Question #76 of 118**

Question ID: 1257291

As part of Nutex Corporation's ongoing security certifications, you need to know how Office 365 meets the regulatory and security standards that apply to specific industries and regions

What options in the Office 365 Security and Compliance portal under **Service assurance** can help with this?

- X **A)** Audited controls
- X **B)** Trust documents
- X **C)** Settings
- ✓ **D)** Compliance reports

Explanation

Compliance reports would provide information on the state of which technologies align with standards, guidelines, and regulations of specific industries and regions.

You should not choose Audited Controls. Audited Controls would provide information concerning Office 365 implementation of security standards.

You should not choose Settings. Settings would allow you to change the region or industry filter for the audited controls and compliance reports.

You should not choose Trust Documents. Trust Documents provides FAQs, with papers, and other trust-related documents. These documents may contain useful information, but will not specify whether Office 365 meets the regulatory and security standards that apply to specific industries and regions

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Manage security reports and alerts

## References:

[TechNet Blog > An Overview of Office 365 Service Assurance Resources](#)

[Microsoft 365 > Office 365 Service Assurance—gaining your trust with transparency](#)

---

## Question #77 of 118

Question ID: 1257276

Nutex Corporation has purchased Azure ATP and configured an Azure ATP sensor. You need to create a threat detection policy to track and notify you of user activity on any Nutex domain controller. What steps will you take in the CAS portal? (Choose all that apply.)

- ☐ A) Create a policy filter that selects users from the **Administrators** group.
- ☒ B) Create a new activity policy.
- ☒ C) Create an alert to be sent as email.
- ☐ D) Create a new session policy.
- ☒ E) In the CAS portal, select **Active Directory** in the APP filter.

### Explanation

In the CAS portal, you will want to select Active Directory in the APP filter. You would do this from the Activity Log page. This narrows the search for activities.

You will want to create a new activity policy. Here you define the criteria that you would like to track.

You will want to create an alert to be sent as email. The scenario requests notification. An alternative not listed here would be to have an alert sent as a text message. You could also do both.

You will not create a policy filter that selects users from the **Administrators** group. This is too restrictive. The scenario states "user activity". A better choice would be choose "**From Domain**" or "**From Organization**".

You would not create a new session policy. We are not interesting in session control of browser-based apps.

### **Objective:**

Implement Microsoft 365 security and threat management

### **Sub-Objective:**

Implement threat management

### **References:**

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-activities-filtering-mcas#create-activity-policies-in-cloud-app-security>

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-activities-filtering-mcas>

---

## Question #78 of 118

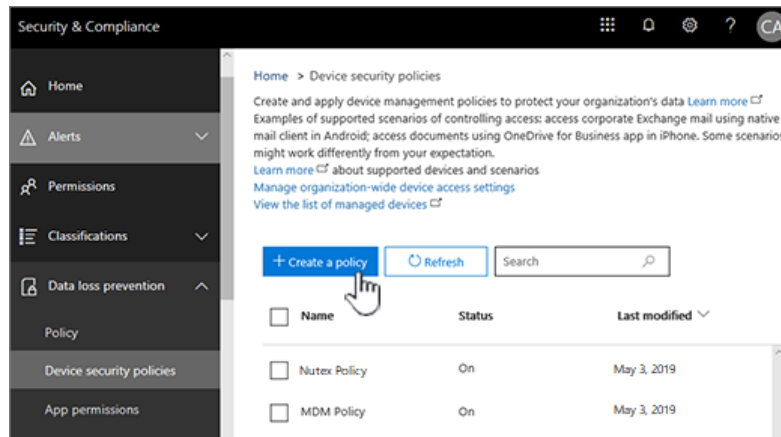
Question ID: 1257240

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?

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

## 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-be91-9ccec25905b0>

## Question #79 of 118

Question ID: 1257357

The Nutex Corporation needs to analyze user's data using Advanced eDiscovery.

The Nutex Corporation has an Office 365 E5 subscription. You are a member of the eDiscovery Manager role group in the Office 365 Security & Compliance Center.

You need Moe, Larry, and Curley to view and access case data in Office 365 Advanced eDiscovery. Your solution to adhere to the principle of least privilege.

What do you need to configure? Place the appropriate steps in the correct order.

{UCMS id=5754094858797056 type=Activity}

## Explanation

You should perform the following steps:

1. Assign Moe, Larry, and Curley to the Reviewer role group

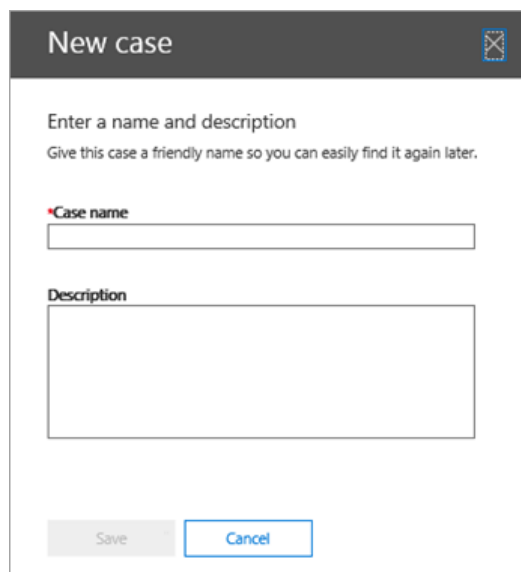
2. Create an eDiscovery case named **Search**
3. Add Moe, Larry, and Curley as members of **Search**

You will first need to assign Moe, Larry, and Curley the required permissions in the Security & Compliance Center so that they can view and access case data in Office 365 Advanced eDiscovery. There are several role groups that can view and access case data; Reviewer, eDiscovery Manager, and eDiscovery Administrator.

- **Reviewer** – This role group allows members to view and access case data in Office 365 Advanced eDiscovery, but not to create cases, add members to a case, create holds, create searches, preview search results, export search results, or prepare results for Advanced eDiscovery.
- **eDiscovery Manager** - This role group allows members to create and manage eDiscovery cases including adding and removing members, placing content locations on hold, creating and editing Content Searches associated with a case, exporting the results of a Content Search, and preparing search results for analysis in Advanced eDiscovery.
- **eDiscovery Administrator** -This role group can view all cases that are listed on the eDiscovery page, manage any case that they have added themselves to, access case data in Advanced eDiscovery for any case, as well as all tasks that an eDiscovery Manager can perform.

You should choose the Reviewer role group because it meets the principal of least privilege.

You should then create an eDiscovery case in the Security & Compliance Center by choosing **eDiscovery > eDiscovery** and then **Create a case**.



New case

Enter a name and description  
Give this case a friendly name so you can easily find it again later.

\*Case name

Description

Save Cancel

You should then assign Moe, Larry, and Curley to the case.

Manage this case

Manage members

+ Add

— Remove

Search

^ Users (1)

Company Admin

Manage role groups

+ Add

— Remove

Search

^ Role Groups (0)

Manage case status

Name \*

New case1

Description

test

Created

2018-03-22 15:15:16

Status

Closing

Delete case

Reopen case

Save

Close

Feedback

After you add members to the eDiscovery case and, the members of the case can access the case in Advanced eDiscovery.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage eDiscovery

**References:**

[Microsoft 365 > Set up users and cases in Office 365 Advanced eDiscovery](#)

**Question #80 of 118**

Question ID: 1353629

Your organization has Azure Activity Directory Rights Management implemented

Several spreadsheets have been encrypted. A group of two auditors need to be able to decrypt the spreadsheets and review the numbers as per regulations set forth by the Security Exchange Commission (SEC). The two auditors are Mark Williamson and Michelle Smith, who are assigned to the following group and department:

Name	Department	Global Group	Email
Mark Williamson	Tax	TaxAudit	<a href="mailto:MarkWilliamson@nutex.com">MarkWilliamson@nutex.com</a>
Michelle Smith	Tax	TaxAudit	<a href="mailto:MichelleSmith@nutex.com">MichelleSmith@nutex.com</a>

You must make these auditors super users to be able decrypt these spreadsheets. You have written the following partially completed script:

```
Import-Module AADRM
$AdminCredentials = Get-Credential Admin@aadrm.nutex.com
Connect-AadrmService -Credential $AdminCredentials
```

What other commands should you add to the script?

- ✓ **A)** Enable-AadrmSuperUserFeature  
Add-AadrmSuperUser -EmailAddress ""  
Add-AadrmSuperUser -EmailAddress ""
- X **B)** Enable-AadrmSuperUserFeature  
Add-AadrmSuperUser -Identity ""
- X **C)** Enable-AadrmSuperUserFeature  
Add-AadrmSuperUser -Identity ""  
Add-AadrmSuperUser -Identity ""
- X **D)** Enable-Aadrm  
Add-AadrmRoleBasedAdministrator -Identity ""
- X **E)** Enable- AadrmSuperUserFeature  
Add-AadrmRoleBasedAdministrator -Identity ""

#### Explanation

You should add the following commands:

```
Import-Module AADRM
$AdminCredentials = Get-Credential Admin@aadrm.nutex.com
Connect-AadrmService -Credential $AdminCredentials
```

```
Enable-AadrmSuperUserFeature
Add-AadrmSuperUser -EmailAddress ""
Add-AadrmSuperUser -EmailAddress ""
```

In this scenario, auditors need to decrypt spreadsheets. Only a **SuperUser** role can decrypt a file. A super user has full control over all rights-protected content that is managed by Rights Management. You can have more than one super user.

To add a super user, first run the **Import-Module AADRM** cmdlet to install the Windows PowerShell module for Azure Rights Management. Next, run the **Connect-AadrmService** cmdlet to connect with the Rights Management service.

You will need to enable the super user feature before you can add a super user. You must run the **Enable-AadrmSuperUserFeature** cmdlet to enable the super user feature. This cmdlet only has to be run once.

To add an individual user as a super user, you will need to run the **Add-AadrmSuperUser** cmdlet. This cmdlet only accepts users, not groups, and you must use the **-EmailAddress** parameters to specify the individual user. You cannot use the **-Identity** parameter with the **Add-AadrmSuperUser** cmdlet. Run the cmdlet once for each super user you wish to add. You cannot add a group as a super user.

You cannot use the **Add-AadrmRoleBasedAdministrator** cmdlet to add a super user. This cmdlet adds a user or group to the list of users and groups that can administer Rights Management.

You do not have to run the **Enable-Aadrm** cmdlet. This cmdlet enables the capabilities of Azure Rights Management for your organization. Rights Management has already been enabled in the organization.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[TechNet > Online Services > Azure Rights Management > Configuring Super Users for Azure Rights Management and Discovery Services or Data Recovery](#)

[Managing Azure Active Directory Rights Management](#)

[Microsoft Azure > Azure > Azure PowerShell > Cmdlet Reference > Azure AD Cmdlets > Azure Service Management Cmdlets > Enable-AadrmSuperUserFeature](#)

---

**Question #81 of 118**

Question ID: 1257268

Nutex Corporation will be using Cloud App Security (CAS) to protect selected cloud apps that work with CAS, such as Dropbox. You are assigned to configure Dropbox as a Connected App.

What steps will you include in your setup? (Drag and drop in order. Some choices may not be needed.)

{UCMS id=5121480670052352 type=Activity}

Explanation

You should choose the following:

1. Sign in to the Cloud App Security Portal
2. Choose **Connected Apps**
3. Choose **App Connectors**
4. Click **+** to choose Dropbox
5. Sign in to Dropbox.
6. Confirm the request allow Cloud App Security to access information.

Sign in to the Cloud App Security Portal, using a Global Administrator or Security Administrator account.

Choose **Connected Apps**. The Connected Apps tab will show a list of applications that offer an API to work with CAS.

Choose **App Connectors**.

Click on the Plus (+) sign, then choose **Dropbox** as the app to connect.

Select **Follow this Link**. Although not listed as choice here, you would first choose **Generate Link** if the select **Follow this Link** option is not available.

Sign in to Dropbox.

A message will appear asking if you want to allow Cloud App Security access to your information. Confirm the request.

A final step not listed as a choice here would be choosing **Test Now** to verify that the app is connected successfully.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Implement Cloud App Security (CAS)

**References:**

[Docs > Microsoft Cloud App Security > Connect apps](#)

[Docs > Microsoft Cloud App Security > Connect Dropbox to Microsoft Cloud App Security](#)

---

## Question #82 of 118

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) Azure AD integration with Intune
- ☐ B) Subscription Activation
- ☒ C) In-place upgrade
- ☐ D) Traditional refresh
- ☐ E) Windows Autopilot

### 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 #83 of 118

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) Office 365 ATP (Threat Protection Service)
- ☒ B) Intune Device configuration profiles.
- ☒ C) Azure AD conditional access policies.
- ☒ D) Intune Device compliance 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](#)

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

---

**Question #84 of 118**

Question ID: 1257286

As part of Nutex Corporation's ongoing security certifications, you have been asked to report on Office 365's compliance with the ISO 27001 standard. You will also need to record and track Nutex's implementations of this and other industry standards.

What options in the Office 365 Security and Compliance portal can help with this? (Choose all that apply.)

- ☐ **A)** Information Governance - Dashboard
- ☒ **B)** Service Assurance -Compliance Manager
- ☒ **C)** Service Assurance - Audit Reports
- ☐ **D)** Service Assurance - Dashboard
- ☐ **E)** Reports - Dashboard

Explanation

The Service Assurance -Compliance Manager and Service Assurance - Audit Reports would help with the scenario.

The Service Assurance -Compliance Manager section would allow you to verify and document Nutex's compliance with a standard.

The Service Assurance - Audit Reports would be useful as this section allows you to perform a risk assessment of Microsoft's cloud services. You can see the results of independent, third-party audits.

The Information Governance - Dashboard option would not be appropriate for the scenario. This toolbox allows you to classify and manage your content.

The Service Assurance - Dashboard does not meet the requirements. It does, however, give you an overview of the Service Assurance offerings.

The Reports - Dashboard does not meet the requirements of the scenario. However, it does offer information and new insights are added regularly.

The screenshot displays the Office 365 Security & Compliance center interface. On the left is a navigation sidebar with icons and labels for various security and compliance tools. The main area is titled 'Service Assurance' and contains introductory text about Microsoft's commitment to security and compliance, as well as information about the Compliance Manager tool. A 'What's new' section highlights updates to Compliance Manager and the addition of search functionality to the Service Trust Portal. An 'Add users' section provides instructions on how to grant the 'Service Assurance User' role to other users in the organization.

Note you must be a member of the **Service Assurance** user role in order to see the Dashboard option in the Office 365 Security and Compliance center. You will have to choose your Region and Industry Settings on first-time use. The portal offerings and labels are always updating, so become familiar with the most current options.

#### Objective:

Implement Microsoft 365 security and threat management

#### Sub-Objective:

Manage security reports and alerts

#### References:

[Microsoft 365 > Office 365 Service Assurance—gaining your trust with transparency](#)

[TechNet Blog > An Overview of Office 365 Service Assurance Resources](#)

### Question #85 of 118

Question ID: 1257348

Your company has a Microsoft 365 subscription. You need to know if someone has changed the SharePoint sharing policy.

What should you do?

{UCMS id=5693469110566912 type=Activity}

#### Explanation

You should do the following:

1. Open the Microsoft Edge browser by pressing CTRL+SHIFT+P

2. Open Security & Compliance Center
3. Export the results of an audit log search

You can know if someone has changed a sharing policy by searching the audit log. You can configure this by opening an in-private browser session with the Microsoft Edge browser by pressing CTRL+SHIFT+P or with the Chrome browser by CTRL+SHIFT+N. Using a private browsing session instead of a regular session prevents the credentials that you are currently logged on with from being used.

You should then sign in to Office 365 with your account and open the Security & Compliance Center. You should then configure an Audit log search. You can export the results to a comma-separated value (CSV) file to use a third party tool to search or filter the results. You can find results for the **SharingPolicyChanged** operation, which logs any changes to the settings of the sharing policy.

You should not create a DKIM policy. This is a Domain Keys Identified Mail signatures policy. A DKIM policy allows recipients of mail to know that messages actually came from your users.

You should not open the SharePoint Admin center and modify the mail sharing settings to know if someone modified these settings. You need to discover whether someone had changed the mail sharing settings. This can be done via an audit log search.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage auditing

**References:**

[Office 365 > Search the audit log in the Security & Compliance Center](#)

---

## Question #86 of 118

Question ID: 1257307

The Virtuart Corporation does not want to add to their Exchange Online Default MRM Policy, which is the only policy that exists at the moment. Virtuart has not modified the Default MRM Policy. The policy currently meets the company's needs, but the management leaders plans to offer an intern program to about fifty interns this summer. They will create mailboxes for the interns. They plan to create an additional policy called "InternPolicy".

What reasons would create a need for a custom retention policy? (Choose all that apply.)

- ☒ **A)** They want to assign multiple retention policy tags (RPTs) to the default Inbox.
- ☒ **B)** They want interns to be able to tag email in non-default folders with a "1-year" delete tag.
- ☒ **C)** They want the policy to be automatically applied to new interns as they are assigned mailboxes.
- ☒ **D)** They want interns' emails to remain in the mailboxes unless manually deleted.
- ☒ **E)** They do not want interns to be able to recover deleted email.

Explanation

They would want to create a new retention policy if they want the intern's email to stay until manually deleted. The Default MRM Policy includes many retention tags that will delete email after a certain time period if an intern applies them, so they don't want to use that policy.

## new tag applied automatically to entire mailbox (default)

\*Name:

Intern Tag

Retention action:

- ☐ Delete and Allow Recovery
- ☒ Permanently Delete
- ☐ Move to Archive

Retention period:

- ☒ Never
- ☐ When the item reaches the following age (in days):

Comment:

They would want to create a new retention policy if they do not want interns to be able to recover deleted emails. This policy would include a Default Policy Tag (DPT) with a "Permanently Delete" action. They could not use the Default MRM Policy as this would affect all users, not just the interns. Note: that one retention policy can be applied to each mailbox.

They would not create a new policy to automatically apply to new interns as they are assigned mailboxes because this is not a feature. The policy will have to be manually assigned

They would not create a new policy to assign multiple retention policy tags (RPTs) to the default Inbox, as you can't link more than one RPT for a particular default folder to the same retention policy.

They would not create a new policy just because they want interns to be able to tag email in non-default folders with a "1-year" delete tag. The Default MRM Policy already includes this capability.

Even though there are labeled "retention policies" by Microsoft, it may be helpful to realize that the policies are, in a sense, actually "deletion" policies, because email never leaves the mailbox unless acted upon by a person or a policy.

### Objective:

Manage Microsoft 365 governance and compliance

### Sub-Objective:

Configure Data Loss Prevention (DLP)

### References:

[TechNet > Office Products > Exchange Online > Security and Compliance > Messaging records management > Retention tags and retention policies](#)

## Question #87 of 118

Question ID: 1257274

A Threat Management solution is needed at Verigon Corporation. Verigon has an Azure AD subscription, and many users are Office 365 users. Verigon also has on-premises Active Directory as part of a hybrid solution as they slowly move to the cloud.

What single product would you suggest to offer as a threat management solution?

- ✓ **A)** Windows Azure Threat Protection (Azure ATP)
- X **B)** Microsoft Defender ATP
- X **C)** Azure Security Center
- X **D)** Office 365 ATP
- X **E)** Advanced Threat Analytics (ATA)

#### Explanation

You will want to use Azure ATP. Windows Azure Threat Protection (Azure ATP) is a cloud-based solution. It uses on-premises ATP "sensors" instead of the gateways used by ATA. This will allow Verigon the functionality of ATA, but offloaded to the cloud. It is the solution for hybrid IT.

You would not choose Advanced Threat Analytics (ATA). ATA is a solution for on-premises networks. It protects Active Directory, looking for identity anomalies, and uses data gathered by on-premises ATA gateways. However, it cannot collect information from Azure AD.

You would not choose Microsoft Defender ATP if you could only choose one solution. Microsoft Defender ATP is unified endpoint detect-and-response (EDR) security platform. It detects attacks against Windows 10 desktops and Windows servers. Formerly known as Windows Defender ATP, it has been rebranded as it now also works with the MacOS. Do not confuse Microsoft Defender ATP, a post-breach investigation tool, with the antivirus tool Windows Defender.

You would not choose Azure Security Center if you could only choose one solution. Azure Security Center is a cloud workload protection product. It helps make sure workloads are secure and can monitor both on-premises and cloud workloads. It is a "single pane of glass" console.

You would not choose Office 365 ATP if you could only choose one solution. Office365 ATP looks for malware, unsafe attachments and other threats for Office 365 email, Sharepoint, OneDrive and Teams. This would not offer any on-premises protection.

In actual practice, you would likely combine several products for a comprehensive solution. Adding Microsoft Defender to Azure ATP is a common choice, for example. Note that while ATA is still available as of this writing, Microsoft is moving towards Azure ATP as a replacement, and offers documentation on how to "move" from ATA to Azure ATP. Azure ATP components and requirements would be a good focus for exam study.

#### **Objective:**

Implement Microsoft 365 security and threat management

#### **Sub-Objective:**

Implement threat management

#### **References:**

[Microsoft Advanced Threat Analytics vs. Advanced Threat Protection: What's the difference?](#)

[Azure advanced threat protection Azure ATP vs ATA](#)

[Docs > Integrate with Windows Defender ATP > Integrate Azure ATP with Windows Defender ATP](#)

---

## **Question #88 of 118**

Question ID: 1257318

Dreamsuites has purchased a Microsoft 365 E5 subscription and configured Microsoft Intune for mobile access management. They have not implemented EFS, but now want to use a Microsoft solution to protect and encrypt company Office app data on iOS and Windows 10 devices. Not all devices are company-owned. Dreamsuites also wants to be able to wipe all corporate Office app data from these personal devices if necessary. What steps will you implement as part of the solution? (Choose all that apply.)

- ✓ **A)** Create or verify an EFS Data Recovery Agent (DRA) certificate.
- ✓ **B)** Create a Windows Information Protection policy using the Azure portal for Intune.
- X **C)** Enroll all Windows 10 devices in Microsoft Intune.
- X **D)** Purchase a license for Azure Information Protection (AIP) Premium P1.
- X **E)** Create a Windows Information Protection policy using System Center Configuration Manager.

#### Explanation

You will need to create a Windows Information Protection policy using the Azure portal for Intune. You will not be enrolling devices, but you want to wipe them, so it will be important to configure the policy as a MAM policy, not MDM.

You will want to create or verify an EFS Data Recovery Agent (DRA) certificate. This will allow you to recover/decrypt any WIP protected file if necessary. The recovery process only applies to Windows 10 desktop devices.

As part of creating your WIP policy, you must add the apps you want to protect to the policy. Microsoft refers to apps that understand the difference between corporate and personal data (such as the Office apps) as **enlightened apps**.

You do not need to purchase a license for Azure Information Protection (AIP) Premium P1. While this is already included as part of the E5 subscription, AIP is not the product to meet the scenario requirements. While AIP can offer encryption protection, it does not allow the wiping of corporate data from devices.

You do not want to create a Windows Information Protection policy using System Center Configuration Manager in this scenario. This would be acceptable for the encryption requirement, but a WIP policy via Intune is required to wipe devices.

You do not need to enroll all Windows 10 devices in Microsoft Intune. WIP policies can be deployed without requiring device enrollment.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[Docs > Information protection > Protect your enterprise data using Windows Information Protection \(WIP\)](#)

[Docs > Information protection > Create a Windows Information Protection \(WIP\) policy using the Azure portal for Microsoft Intune](#)

[Docs > Information protection > Create and deploy a Windows Information Protection \(WIP\) policy using System Center Configuration Manager](#)

---

## Question #89 of 118

Question ID: 1257281

Dreamsuites Incorporated has chosen Microsoft Defender ATP to protect its Windows 10 machines. They have also purchased an Intune subscription, but not all Windows 10 clients will be enrolled in the service. You need an efficient way to "onboard" the Windows 10 machines in a large-scale deployment across many regions. What would you suggest as the single best "onboarding client" solution?

- ☐ A) Use the local script provided by Microsoft.
- ☐ B) Create a Group Policy to distribute the software at the domain level.
- ☒ C) Use ConfigMgr (SCCM) to deliver the **WindowsDefenderATPOnboardingScript.cmd** package.
- ☐ D) Use Intune to deliver the **WindowsDefenderAtp.onboarding** file.
- ☐ E) Create a Powershell script to run **Start-Process "C:\test-WDATP-test\invoice.exe** on all machines.

Explanation

You would use ConfigMgr (SCCM) to deliver the **WindowsDefenderATPOnboardingScript.cmd** package. The latest versions have built-in support for managing Microsoft Defender ATP and is a good choice for large deployments with little administrative overhead.

You would not use the local script provided by Microsoft. This can work for a minimal deployment, but this is not efficient for large deployments.

You would not use Intune to deliver the **WindowsDefenderAtp.onboarding** file if you are looking for a single solution, as not all machines are enrolled in Intune. If they were, then this would be a good solution.

You would not create a Group Policy to distribute the software at the domain level. There is no reporting with this method. While Group Policy method does work, ConfigMgr is the more comprehensive choice.

You would not create a Powershell script to run **Start-Process "C:\test-WDATP-test\invoice.exe** on all machines. This is only an excerpt of the complete command line to run a test on an onboarded device.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Implement Windows Defender Advanced Threat Protection (ATP)

**References:**

[Docs > Security > Threat Protection > Onboarding tools and methods for Windows 10 machines](#)

[Docs > Configuration Manager > Microsoft Defender Advanced Threat Protection](#)

[Peter van der Woude > Offboard Windows 10 devices of Windows Defender Advanced Threat Protection](#)

---

**Question #90 of 118**

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](#)

## Question #91 of 118

Question ID: 1353616

You work for a pharmaceutical company called Nutex that utilizes the cloud-based Office 365 collaboration service. You have a requirement from the legal department to provide general DLP detection and rule match information. The information should be aggregated per day and sent to a specific distribution list each Friday morning.

Only high-level information should be distributed, because the legal department will initiate an exhaustive inquiry if required.

What cmdlet should be used to provide the minimum required information?

- ☐ A) **Get-DlpDetailReport**
- ☒ B) **Get-DlpDetectionsReport**
- ☐ C) **Start-HistoricalSearch**
- ☐ D) **Get-HistoricalSearch**

### Explanation

The **Get-DlpDetectionsReport** cmdlet will return a summarized list of all DLP rule matches found within the OneDrive for Business and SharePoint Online workloads within an Office 365 tenant. You can use the following example to find all DLP activities for July 2017:

```
Get-DlpDetectionsReport -StartDate 07/01/2017 -EndDate 07/31/2017
```

The **Get-DlpDetectionsReport** cmdlet will ensure the minimum set of data is provided to the legal department.

The **Get-DlpDetailReport** cmdlet will return a detailed list of all DLP rule matches found within the OneDrive for Business and SharePoint Online workloads within an Office 365 tenant. This cmdlet would provide more detail than required by the report.

The **Get-HistoricalSearch** cmdlet will return details concerning all historical searches executed over the last ten days within an Office 365 tenant. This cmdlet will not provide general DLP detection and rule match information that is aggregated per day.

The **Start-HistoricalSearch** cmdlet will execute a brand new historical search within an Office 365 tenant. This cmdlet will not provide general DLP detection and rule match information that is aggregated per day.

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Configure Data Loss Prevention (DLP)

### **References:**

[TechNet > Exchange Online cmdlets > Get-DlpDetectionReport](#)

---

## Question #92 of 118

Question ID: 1353638

The Nutex Corporation plans to use a third-party security information and event management (SIEM) application to access your auditing data. This application will search for information in the Office 365 audit log.

You have been assigned the Audit Logs role in Exchange Online. What must you type at the PowerShell prompt to turn on audit log search?

Please type the correct response in the textbox provided above.

### Explanation

Acceptable answer(s) for field 1:

- Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled \$true

You should type the following:

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
```

After typing the above command, it can take up to 60 minutes for the audit log search to take effect. The **Set-AdminAuditLogConfig** cmdlet allows you to configure global changes in Exchange Online. The -UnifiedAuditLogIngestionEnabled parameter is used to turn the audit log search on or off.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage auditing

**References:**

[Microsoft 365 > Turn Office 365 audit log search on or off](#)

---

## Question #93 of 118

Question ID: 1257244

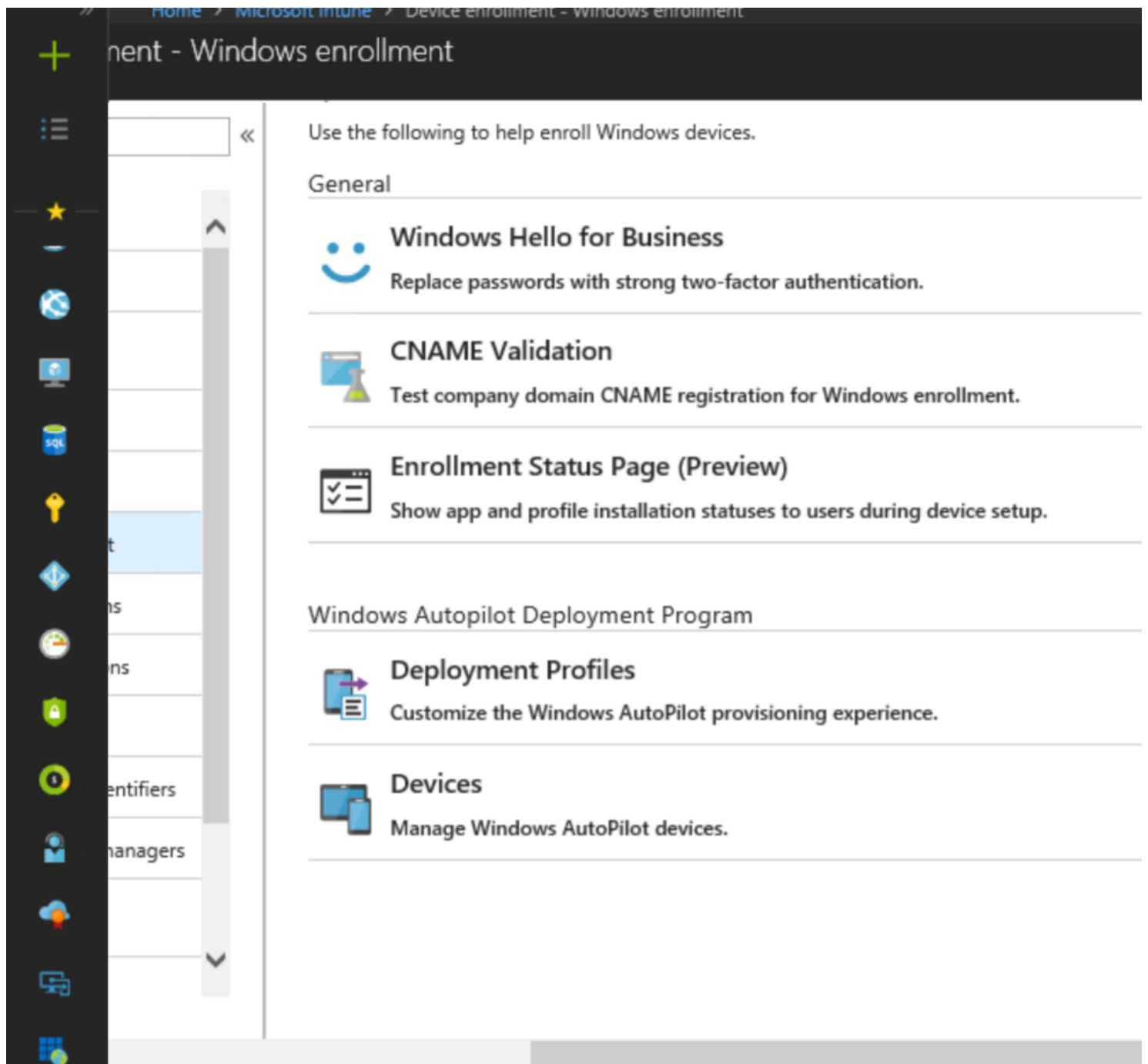
The Nutex Corporation plans to deploy Windows Hello for Business for SSO to Microsoft 365 services. All devices used by users run Windows 10 Enterprise and will be hybrid Azure AD joined.

What is a prerequisite of the deployment?

- ☐ A) Devices that allows biometric authentication
- ☐ B) Upgrade all domain controllers to Windows Server 2016
- ☒ C) Microsoft Intune enrollment
- ☐ 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 to 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 #94 of 118

Question ID: 1353632

The Nutex Corporation recently entered into a joint partnership with Metroil to introduce a new product line called DreamSuites. Part of the preparation to launch DreamSuites requires the use of rights management templates to protect all messaging communication regarding this new product line. You need to perform the following actions:

- Configure the Rights Management Service online key-sharing location as the Office 365 administrator for Nutex
- Disable IRM templates in OWA and Outlook
- Enable IRM for Office 365 Message Encryption

You create the following script:

```
Untitled1.ps1* X
1
2 # configure the RMS Online key sharing location for a customer in Tokyo
3 [A] -RMSOnlineKeySharingLocation "https://sp-rms.ap.aadrm.com/TenantManagement/ServicePartner.svc"
4
5 #Disables IRM templates in OWA and Outlook
6 Set-IRMConfiguration [B] [C]
7
8 #Enables IRM for Office 365 Message Encryption:
9 Set-IRMConfiguration [D] [E]
```

Choose the appropriate cmdlets, parameters, or values from the left and drag them to corresponding letter on the right.

{UCMS id=5705770748346368 type=Activity}

### Explanation

You should choose the following to complete the script:

```
Untitled1.ps1* X
1
2 # configure the RMS Online key sharing location for a customer in Tokyo
3 Set-IRMConfiguration -RMSOnlineKeySharingLocation "https://sp-rms.ap.aadrm.com/TenantManagement/ServicePartner.svc"
4
5 #Disables IRM templates in OWA and Outlook
6 Set-IRMConfiguration -ClientAccessServerEnabled $false
7
8 #Enables IRM for Office 365 Message Encryption:
9 Set-IRMConfiguration -InternalLicensingEnabled $true
```

```
Set-IRMConfiguration -RMSOnlineKeySharingLocation "https://sp-rms.ap.aadrm.com/TenantManagement/ServicePartner.svc"
```

```
Set-IRMConfiguration -ClientAccessServerEnabled $false
```

```
Set-IRMConfiguration -InternalLicensingEnabled $true
```

You can use the **Set-IRMConfiguration** cmdlet to enable, disable, or configure Information Rights Management (IRM) features. The -**ClientAccessServerEnabled** parameter specifies whether to disable IRM in OWA and Outlook. IRM is enabled in both by default. The -**InternalLicensingEnabled** parameter enables IRM features for messages sent to internal recipients. By default, licensing is disabled for internal messages for on-premises deployments.

The **-RMSOnlineKeySharingLocation** parameter sets the RMS Online URL to obtain the trusted publishing domain (TPD). There are different URLs for different locations, such as North America, Asia, Europe, South America, and Office 365 for Government.

You should not use the **Import-RMSTrustedPublishingDomain** cmdlet. This cmdlet imports a trusted publishing domain (TPD) from an on-premises server or from an on-premises server running Active Directory Rights Management Services (AD RMS).

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[Set up Microsoft Azure Rights Management for Office 365 Message Encryption](#)

[Configure IRM to use Azure Rights Management](#)

[Set-IRMConfiguration](#)

---

**Question #95 of 118**

Question ID: 1257347

Your company has a Microsoft 365 subscription. You need to track password resets. Specifically, you need to view the time when the password reset occurred, and the name of the user and the IP address of the user who performed the reset.

What should you do? Choose the appropriate steps from the left and place them in the correct order.

{UCMS id=6196163427434496 type=Activity}

Explanation

You should do the following:

1. Go the <https://protection.office.com> URL
2. Perform search of the audit log
3. Filter the results
4. Export the results to Excel

To view the time when the password reset occurred, and the name of the user and the IP address of the user performed the reset, you will need to open the Security & Compliance Center. The <https://protection.office.com> URL will open the Security & Compliance Center. It is recommended to use a private browsing session instead of a regular session when opening the Security & Compliance Center. This action prevents the credentials that you are currently logged on with from being used.

You should then sign in to Office 365 with your account and open the Security & Compliance Center. You should then configure an Audit log search. You can export the results to a comma-separated value (CSV) file to use a third party tool or use Excel to search or filter the results.

You should not use the SharePoint Admin Center or the Microsoft 365 Admin Center. Neither of these have a unified audit log like the Security & Compliance Center. You can view the usage report from the SharePoint Admin Center or the Microsoft 365 Admin Center. The usage report will not show you password resets. It can show you information about email activity, mailbox usage, office activation, email app usage, information about active users, as well as other information. These activity reports are available for the last 7 days, 30 days, 90 days, and 180 days.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage auditing

**References:**

[Office 365 > Search the audit log in the Security & Compliance Center](#)

---

## Question #96 of 118

Question ID: 1257344

Verigon Corporation would like to take advantage of the Unified Audit Logs available for Office 365. Historically, they would check their Sharepoint and Exchange Online logs from their individual admin portals. Now that they can see all the logs in a centralized place, they want to monitor admin activity in SharePoint Online, and user activity in Exchange Online, such as creating mailbox items. What steps will need to be taken to meet this requirement? (Choose all that apply.)

- ☒ **A)** Run the Powershell Set-Mailbox -AuditEnabled \$True cmdlet and parameter for all mailboxes.
- ☐ **B)** Run the Powershell Get-AdminAuditLogConfig cmdlet.
- ☒ **C)** Run the Powershell cmdlet and parameter Set-AdminAuditLogConfig-UnifiedAuditLogIngestionEnabled \$true
- ☐ **D)** Export the audit logs and run the Power Query Editor.
- ☐ **E)** Run the Powershell Write-AdminAuditLog cmdlet.

### Explanation

You will need to run the Powershell cmdlet and parameter Set-AdminAuditLogConfig-UnifiedAuditLogIngestionEnabled \$true. This step enables unified audit logging. Auditing can also be enabled under **Security and Compliance Center > Search > Audit log search > Turn on auditing**

You will need to run the Powershell Set-Mailbox -AuditEnabled \$True cmdlet and parameter for all mailboxes. This enables mailbox logging. Most admin activity for Office 365 is already enabled by default, but mailbox activity logging needs this additional step.

You do not need to run the Powershell Get-AdminAuditLogConfig cmdlet, but you might choose to. This will tell you if auditing is enabled or not.

You do not need to run the Powershell Write-AdminAuditLog cmdlet. This cmdlet lets you add manual comments to the audit log.

You do not need to export the audit logs and run the Power Query Editor. You can view and search the logs without exporting them.

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Manage auditing

### **References:**

[Microsoft Support > Auditing in Office 365 \(for Admins\)](#)

[Office 365 Audit Logging and Monitoring](#)

[Docs > Set-AdminAuditLogConfig](#)

[Microsoft 365 > Turn Office 365 audit log search on or off](#)

## Question #97 of 118

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 a MAM User scope in the automatic enrollment settings
- ☐ **B)** Configure multi-factor authentication (MFA)
- ☒ **C)** Set the mobile device management (MDM) authority
- ☐ **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 #98 of 118

Question ID: 1257296

Nutex Corporation uses Office 365 extensively. The legal department has advised extra protection for messages that contain Social Security Numbers or U.S. Passport Numbers. You have created a DLP policy with an advanced setting rule called "Sensitive Nutex Data". You have customized the policy to only apply to content that contains the specified sensitive information types. If so, the rule will encrypt the content and send the user a notification.

You do not want these actions for messages sent to internal users. How will you arrange this?

- X **A)** Add a "User Override" to the "Sensitive Nutex Data" rule.
- X **B)** Add an exception to the "Sensitive Nutex Data" rule using the "***Except if content contains sensitive information***" exception.
- X **C)** Modify the "Sensitive Nutex Data" rule by adding a "***Recipient Domain is***" condition.
- X **D)** Add an exception to the "Sensitive Nutex Data" rule using the "***Except if document property is***" exception.
- ✓ **E)** Add an exception to the "Sensitive Nutex Data" rule using the "***Except if recipient domain is***" exception.

#### Explanation

You will need to add an exception to the "Sensitive Nutex Data" rule using the "***Except if recipient domain is***" exception. This exception will cause all sensitive messages to be encrypted and "notified" unless they are intended for an internal company user.

Sensitive Nutex Data

Name	Conditions	Exceptions	Actions	User notifications
<div><div>Name *</div><div>Sensitive Nutex Data</div><div>Description</div><div>Encrypt messages with sensitive data and send a notification to the sender.</div></div>				
<div>^ Conditions</div> <div>We'll apply this policy to content that matches these conditions.</div> <div>+ Add a condition ▾</div>				
<div>^ Exceptions</div> <div>We won't apply this rule to content that matches any of these exceptions.</div> <div>Except if recipient domain is</div> <div>Detects when content is sent in an email message to the recipient domains you specify.</div> <div>Nutex.com</div> <div>Enter additional domains names (such as contoso.com) and then click 'Add'. Separate multiple domains with a comma.</div>				

You do not want to add an exception to the "Sensitive Nutex Data" rule using the "**Except if content contains sensitive information**" exception. The rule was created to apply to sensitive information, so we don't want to exclude that.

You do not want to modify the "Sensitive Nutex Data" rule by adding a "**Recipient Domain is**" condition. This condition would cause actions to be taken only for internal recipients, which is opposite of our intention.

You do not want to add a "User Override" to the "Sensitive Nutex Data" rule. User overrides would allow the user to bypass the actions of these rules, which is not the goal of the scenario.

You do not want to add an exception to the "Sensitive Nutex Data" rule using the "**Except if document property is**" exception. This exception would exempt messages that had been previously classified and labeled using the File Classification System. Our focus is on the message destination.

Another option, not offered here, would be, instead of creating an "advanced" setting, to just modify the content configuration to only detect "content shared outside of the organization".

**Objective:**  
Manage Microsoft 365 governance and compliance

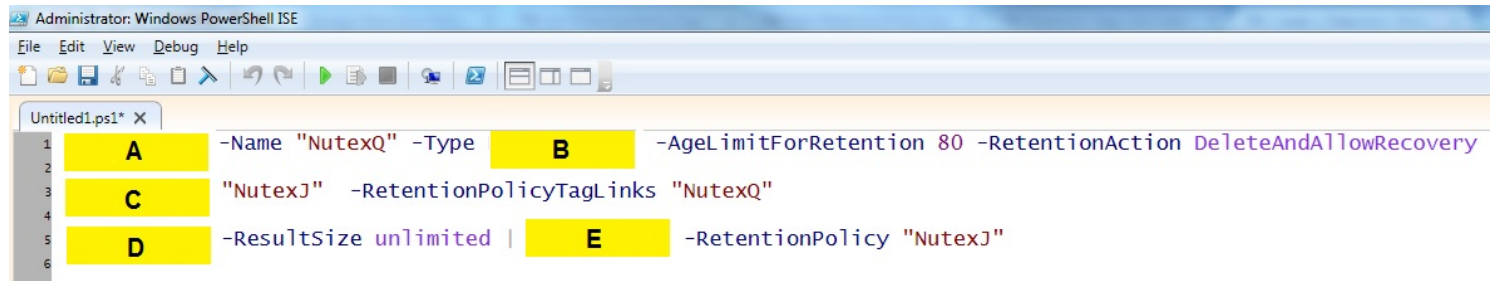
**Sub-Objective:**  
Configure Data Loss Prevention (DLP)

**References:**  
[Microsoft 365 > DLP > Overview of data loss prevention](#)

## Question #99 of 118

Question ID: 1353619

The Nutex Corporation has an Office 365 implementation. The company wants to change the retention age of the **DeletedItems** folder for all mailboxes. You disable the current retention policy tag applied to the **DeletedItems** folders. You need to change the retention limit for the **DeletedItems** folders to 80 days for all mailboxes. You create the following script:



How should you complete the relevant script? Drag the missing cmdlets, parameters, or values from the right to appropriate corresponding letter on the left. You may only use the items once.

{UCMS id=5665980560703488 type=Activity}

### Explanation

You should choose the following options to complete the script:



In this scenario, you must first create a retention tag, then create a retention policy and apply the retention policy to the mailbox users.

Running the following at the PowerShell prompt will disable the current retention tag:

```
Set-RetentionPolicyTag Deleted Items -RetentionEnabled $false
```

You can then use the **New-RetentionPolicyTag** cmdlet to create a new retention tag. The **-Type** parameter specifies the type of retention tag to be used. The value of **DeletedItems** indicates this tag is for the **DeletedItems** folder. If you specify **All** as the value for the **-Type** parameter, then you will create a default policy tag (DPT) instead of a retention policy tag (RDT). The **-RetentionAction** parameter specifies the action of the tag, and the value of **DeleteAndAllowRecovery** for the **-RetentionAction** parameter specifies that the tag's action will be to delete a message, but allow recovery from the **RecoverableItems** folder.

The following creates a retention tag named **NutexDelete** for the **DeletedItems** folder in the mailbox that sets the retention age for 80 days:

```
New-RetentionPolicyTag -Name "NutexDelete" -Type DeletedItems -AgeLimitForRetention 80 -RetentionAction DeleteAndAllowRecovery
```

The **New-RetentionPolicy** cmdlet creates a new retention policy that you can link with the retention tag. The following script creates a retention policy named **NutexRetentionPolicy** and links it with the retention tag **NutexDelete**:

```
New-RetentionPolicy -Name "NutexRetentionPolicy" -RetentionPolicyTagLinks "NutexDelete"
```

Once you have created the retention tag and linked it to a retention policy, you can apply the retention policy to the mailbox users. First, you should use the **Get-Mailbox** cmdlet with the **-ResultSize unlimited** parameter to retrieve all mailbox users, then use the **Set-Mailbox** cmdlet to apply the retention policy. The following script applies the retention policy named **NutexRetentionPolicy** to all mailbox users:

```
Get-Mailbox -ResultSize unlimited | Set-Mailbox -RetentionPolicy " NutexRetentionPolicy"
```

You will not use either the **Get-RetentionPolicy** cmdlet or the **Get-RetentionPolicyTag** cmdlet. The **Get-RetentionPolicy** cmdlet retrieves an existing retention policy. The **Get-RetentionPolicyTag** cmdlet retrieves an existing retention policy tag. In this scenario, you need to create a retention policy tag and

policy.

You should not use either the **Get-TransportRule** or **New-TransportRule** cmdlets. A transport rule is used to add a disclaimer to a message or define conditions for messages.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Configure Data Loss Prevention (DLP)

**References:**

[TechNet > Office Products > Exchange > Exchange Online > Security and compliance for Exchange Online > Messaging records management > Create a Retention Policy](#)

[Manage Retention Policy by using PowerShell](#)

[TechNet > Office Products > Exchange > Exchange Online > Powershell > Policy and compliance cmdlets > New-RetentionPolicyTag](#)

[TechNet > Office Products > Exchange > Exchange Online > Security and compliance for Exchange Online > Messaging records management > Retention tags and retention policies](#)

---

**Question #100 of 118**

Question ID: 1257302

The Dreamsuites team has successfully tested Microsoft Flow to automate some HR processes. Based on their success, the Marketing department has been exploring ways to automate some of their processes, such as automatically adding a press release to their Facebook page when a particular event occurs. Some marketing staff has access to Salesforce revenue information. Dreamsuites wants to ensure that no data from Salesforce is ever included in a Facebook post as part of a Flow.

What should Dreamsuites do?

- ✓ **A)** Create a data loss prevention policy.
- X **B)** Create a Microsoft Flow custom connector for Salesforce.
- X **C)** Deploy a DPM protection group.
- X **D)** Connect Salesforce to Microsoft Cloud App Security.
- X **E)** Create a custom Microsoft Flow environment.

Explanation

Dreamsuites needs to create a data loss prevention (DLP) policy. This policy controls how data can be shared based on connectors. A connector is a set of actions and triggers that let you connect your Flow to a SaaS application, in this case Facebook. The DLP will blocks Salesforce data from being used in Facebook posts.

Dreamsuites does not need to create a Microsoft Flow custom connector for *Salesforce*. They may choose to, but it is not required. Microsoft Flow already includes many connectors for popular **SaaS** applications, including **Salesforce and Facebook**. Some connectors require a Premium subscription plan.

Creating a custom Microsoft Flow environment would be a good idea, as it would allow only Marketing to create or modify their workflows, but it does not meet the goal of restricting the data.

Creating a DPM protection group would create a collection of data sources to share common backup and restore settings. That is outside the scope of this scenario.

Connecting *Salesforce* to Microsoft Cloud App Security would help trigger alerts when there are security issues with user access to *Salesforce*, but it does not protect the data flow as required by this scenario.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Configure Data Loss Prevention (DLP)

**References:**

[Docs > Flow > Data loss prevention \(DLP\) policies](#)

---

**Question #101 of 118**

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
- X **C)** Windows operating system version
- ✓ **D)** Client apps
- ✓ **E)** Locations
- X **F)** Schedule

**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

Home
Microsoft Intune
Conditional access - Policies
New
Conditions
Device platforms

New

Info

Name

Example: 'Device compliance app policy'

Assignments

Users and groups

All users

Cloud apps

1 app included

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Create

Conditions

Info

Sign-in risk

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps (preview)

Not configured

Device state (preview)

Not configured

Done

Device platforms

Configure

Yes

No

Include

Exclude

All platforms (including unsupported)

Select device platforms

Android

iOS

Windows Phone

Windows

macOS

Done

*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.

Device state (preview)

Info

Configure

Yes

No

Include

Exclude

Select the device state condition used to exclude devices from policy.

Device Hybrid Azure AD joined

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 #102 of 118

Question ID: 1257341

Dreamsuites Corporation wants to retain some Office 365 company data for both compliance and efficiency reasons. They extensively use most Office 365 services. You need to plan for the retention of deleted data in an Active Deletion or Passive Deletion scenario.

Which of the following statements are true? (Choose all that apply.)

- ✓ **A)** Session IDs, User GUIDs, PUIDs, or SIDs are retained for at most 30 days in an Active Deletion scenario
- X **B)** End User Identifiable Information (EUII) such as a user name, user principal name, and user-specific IP address is retained for at most 30 days in an Active Deletion scenario.
- ✓ **C)** Customer passwords, certificates, encryption keys, and storage keys are retained for at most 30 days in an Active Deletion scenario
- X **D)** Customer data including all text, audio, video, and image files created using Office 365 and stored in Microsoft data centers in an Active Deletion Scenario is retained for at most for 180 days.

#### Explanation

Session IDs, User GUIDs, PUIDs, or SIDs are retained for at most 30 days in an Active Deletion scenario. Customer passwords, certificates, encryption keys, and storage keys are retained for at most 30 days in an Active Deletion scenario.

There are two scenarios, Active Deletion and Passive Deletion, when customer data is deleted:

- Active Deletion occurs when a user or administrator deletes data or another user when the tenant has an active subscription.

- Passive Deletion occurs after the tenant subscription expires or is terminated.

Customer passwords, certificates, encryption keys, and storage keys are retained for at most 30 days in an Active Deletion scenario and at most in 180 days in a Passive Deletion scenario.

End User Pseudonymous Identifiers (EUPI), which is an identifier created by Microsoft tied to the user of a Microsoft service such as Session IDs, User GUIDs, PUIDs, or SIDs are retained for at most 30 days in an Active Deletion scenario. This information is retained at most for 180 days in a Passive Deletion scenario.

Customer data including all text, audio, video, and image files created using Office 365 and stored in Microsoft data centers in an Active Deletion scenario is retained for at most for 30 days, not 180 days. This information is retained at most for 180 days in a Passive Deletion scenario.

End User Identifiable Information (EUII) such as a user name, user principal name, and user-specific IP address is retained for at most 180 days in an Active Deletion scenario, not 30 days. This information is retained at most for 180 days in a Passive Deletion scenario.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage data governance

**References:**

[Office 365 > Data Retention, Deletion, and Destruction in Office 365](#)

[Microsoft 365 > Overview of retention policies](#)

---

**Question #103 of 118**

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

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 #104 of 118**

Question ID: 1353639

As a security administrator for Nutex Corporation, the legal department has asked for your assistance. They would like to start receiving a monthly spreadsheet showing all Office 365 admin activities performed by a specific administrator to document an HR issue. You offer the logs from each Office 365 service, but they would like consolidated information.

What steps in the Office 365 Security and Compliance Center will you take to create this spreadsheet? (Drag and drop the correct steps in order. Some steps may not be used.)

{UCMS id=5619457633288192 type=Activity}

Explanation

You should choose the following steps in the Office 365 Security and Compliance Center:

1. Go to **Search > Audit log search > and choose Turn on Auditing**.
2. Run an audit log search for the named administrator.
3. View the search results.
4. Export the search results to a CSV file.

The first step: In the Office 365 Security and Compliance Center, go to **Search > Audit log search > and choose Turn on Auditing**. This is not enabled by default. Since the scenario is only interested in the future, this will meet the scenario requirement. If the legal department had requested historical information, it would not be available, as events would not be recorded until now.

Office 365 Security & Compliance

# Audit log search

To use this feature, turn on auditing so we can start recording user and admin activity in your organization. When you turn this on, activity will be recorded to the Office 365 audit log and available to view in a report.

Turn on auditing

Need to find out if a user deleted a document or if an admin reset someone's password? Search the Office 365 audit log to find out what the users and admins in your organization have been doing. You'll be able to find activity related to email, groups, documents, permissions, directory services, and much more. [Learn more about searching the audit log](#)

Search

Clear

Activities

Show results for all activities

Start date

2019-09-30

00:00

End date

2019-11-04

00:00

Users

AJexW@nutex.com

File, folder, or site

Add all or part of a file name, folder name, or URL.

Search

Results

Date

IP address

User

Activity

Item

Detail

Run a search to view results

The second step: In the Office 365 Security and Compliance Center, run an audit log search for the named administrator. You can choose the specific user(s) and/or activities that you want to audit as part of the search. You can choose the time window for the report. In this scenario, you will need to accumulate a month of information before you do the search as data was not being recorded until you enabled auditing.

The third step: In the Office 365 Security and Compliance Center, view the search results.

You do not need to, in the Office 365 Security and Compliance Center, filter the search results by user. This is because you already narrowed the search to the specified user in the second step. However, if you had not named a specific user during the search, you could filter the view at this step to get the same output. You can also filter on other criteria, such as type of activity.

The fourth step: You will need to export the search results to a CSV file, so that they can be imported into a spreadsheet.

You can also perform searches using the Powershell **Search-UnifiedAuditLog** cmdlet.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage eDiscovery

**References:**

[Microsoft 365 > Search the audit log in the Security & Compliance Center](#)

## Question #105 of 118

Question ID: 1353635

Nutex Corporation has an Office 365 E3 license. Nutex regularly examines the audit logs for many of their Office 365 services. Nutex would like to centralize its search for particular admin activity in Exchange Online, SharePoint Online, and Azure AD. Nutex needs to retain a year of audit log information. This information must be searchable and viewable by the CIO.

What are some of the requirements to implement this retention plan? (Choose all that apply.)

- ☐ A) Assign the CIO to the **Compliance Management role** group.
- ☒ B) Assign the CIO to the **Audit Logs role** in Exchange Online.
- ☒ C) Upgrade to an Office E5 license.
- ☒ D) Use Powershell to turn on the audit log search.
- ☐ E) Use Powershell to turn on mailbox auditing.
- ☐ F) In the Site Settings of the SharePoint sites, under **Site Collection Audit Settings**, choose **Configure Audit Settings** and check the desired boxes.

### Explanation

You will need to upgrade to an Office E5 license to retain the logs for a year. An E3 license only offers up to 90 days retention.

You would use Powershell to turn on audit log search using the **Set-AdminAuditLogConfig** cmdlet. You could also achieve this in the Security and Compliance Center by going to **Search > Audit Log Search > Turn on Auditing**

You would want to assign the CIO to the **Audit Logs role** in Exchange Online. This will allow them to search and view the audit logs. Another option not listed here would be to add them to the View-Only Audit Logs role.

You do not need to use Powershell to turn on mailbox auditing. This would be needed if you wanted to audit user activity in a mailbox, but that is not part of the scenario. Office 365 already audits many areas of many services by default, including Admin activity in Exchange Online, SharePoint Online, and Azure AD as required by the scenario.

You do not, in the Site Settings of the SharePoint sites, under **Site Collection Audit Settings**, need to choose **Configure Audit Settings** and check the desired boxes. Office 365 audits many areas of many services by default, including Admin activity in Exchange Online, SharePoint Online, and Azure AD.

You would not assign the CIO to the **Compliance Management role** group. This would allow the searching and viewing requirements of the scenario, but it includes additional auditing permissions that are beyond the scope of what is necessary.

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Manage auditing

### **References:**

[Microsoft 365 > Search the audit log in the Security & Compliance Center](#)

[Microsoft 365 > Turn Office 365 audit log search on or off](#)

## Question #106 of 118

Question ID: 1257340

You work as an Office 365 administrator for a manufacturing company called Metroil. The security team has mandated that the Security & Compliance center should be used to analyze data produced by Office 365 and to automatically evaluate the company's risk of a lawsuit in the case of a data breach using machine learning. The desired result is to automatically find, classify, and set policies on high-value data to keep what is relevant and delete stale data. The legal team also wants to alert on unusual behavior such as a sudden large volume of file deletions.

You review the features in the Office 365 Security & Compliance center. What feature will meet the business request?

|~inline\_70-347Rev201706\_Security&ComplianceCenter.jpg~|

- X **A)** Office 365 Secure Score
- X **B)** Search & Investigation
- X **C)** Threat Management
- ✓ **D)** Data Governance

#### Explanation

The Data Governance section allows the Office 365 administrator to configure the data lifecycle policies, import data from on-premises servers, and apply retention policies. Specifically, the advanced data governance feature will apply machine learning to help determine what data should be kept versus what data is redundant and can be eliminated.

Automatic classification of data, system alerts to surface unusual activity like a high volume of file deletions and the ability to apply compliance controls is all part of the advanced data governance feature within Office 365 Security & Compliance center. This feature requires an Office 365 Enterprise E5 plan or the Advanced Compliance plan.

The Threat Management section allows the Office 365 administrator to identify trends and patterns using Office 365 Analytics to respond to malicious activities. This feature can provide protection by reviewing malicious email attachments, tracking phishing and malware, and quarantining messages.

The Office 365 Secure Score section allows the Office 365 administrator to identify what proactive steps and controls have been taken to reduce the risk of a data breach. The secure score feature will automatically examine which features are being used within the Office 365 tenant and then examine those configurations against a list of best practices. The more best practices are followed, the higher the score achieved by the Office 365 administration staff. For instance, enabling multi-factor authentication for global admins will increase the score.

The Search & Investigation section allows the Office 365 administrator to search data found within email, documents, Skype for Business conversations, and Teams. Additionally, this feature will provide the ability for an Office 365 administrator to search audit logs to track activity around email, groups, documents, permissions, and passwords. Often, the legal department of an organization will use this feature to create eDiscovery cases to preserve desired data.

#### **Objective:**

Manage Microsoft 365 governance and compliance

#### **Sub-Objective:**

Manage data governance

#### **References:**

[TechNet > Blogs > Office 365 Partner Community: Advanced data governance and threat intelligence](#)

[Office 365 Advanced Data Governance Demo](#)

---

## **Question #107 of 118**

Question ID: 1257349

Your company has a Microsoft 365 subscription. You need to investigate whether a user viewed a specific document or purged an item from their mailbox.

Which admin center would you use to find the information with the least administrative effort?

- X **A)** Azure ATP
- X **B)** Stream
- ✓ **C)** Security & Compliance
- X **D)** Kaizala

#### Explanation

You should use Security & Compliance. You can search the audit log in the Security & Compliance center to see if a user viewed a file, created a file, or purged an item from a mailbox. If you enable auditing, you can search for user and admin activity in all of the Office services.

You will need to run the following to turn on audit log search in Office 365 for your organization:

Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled \$true

You can also enable auditing on the **Audit log** search page in the Security & Compliance Center by clicking **Start recording user and admin activity**.

Audit records are retained in the audit log based on the type of subscription that you have. For example, records for an Office 365 E3 subscription are retained for 90 days.

You should not use Azure Advanced Threat Protection (ATP). This tool is used to identify user and device activity that is considered to be suspicious by using technique detection and behavioral analytics. ATP is not designed to find if a user viewed a specific document or purged an item from their mailbox. ATP does not directly read the audit log.

You should not use Stream. Stream does not read the audit log, but is a separate Office 365 service that allows organizational users to upload, view, and share videos securely.

You should not use Kaizala. Kaizala does not read the audit log, but is a separate Office 365 service that provides mobile messaging to users in your organization.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Manage auditing

**References:**

[Office 365 > Search the audit log in the Security & Compliance Center](#)

---

## Question #108 of 118

Question ID: 1257287

Dreamsuites Incorporated has been successfully using Azure AD as part of its cloud-based services. There have been recent failed AD login attempts that were not performed by the legitimate account owner. As a security administrator, you have been asked to add Azure Active Directory Identity Protection as a security measure. What steps will be included to implement this protection offering to address the issue?

Choose the appropriate steps and place them in the correct order.

{UCMS id=5101386095132672 type=Activity}

Explanation

You should choose the following:

- Open the Marketplace in the Azure Portal
- Configure a sign-in risk policy

You will want to configure a sign-in risk policy. This policy detects suspicious actions that come along with the sign-in. The policy analyzes the probability that the sign-in was not performed by the actual account owner. You could then choose to conditionally block access based on risk level, if desired.

The first step will be to open the Marketplace in the Azure Portal. You will need to manually add the Azure AD Identity Protection blade.

For the issue in this scenario, you do not need to configure the Azure Multifactor Authentication Registration Policy. This policy requires users to provide more than a name and password to login.

You do not need to configure a user risk policy to address this specific issue, although it would be an excellent complement. This policy detects the probability that a user's account has been compromised.

You do not need to unblock any users as they will not be blocked until you configure conditional access with a policy.

Note that a new "overview" dashboard, now in "preview", will be replacing the current overview.

You should not open Monitor in the Azure Portal. Monitor allows you to see metrics, analyze logs, and configure actions for alerts, but it will not allow you add a sign-in risk policy.

**Objective:**

Implement Microsoft 365 security and threat management

**Sub-Objective:**

Manage security reports and alerts

**References:**

[Azure > Identity Protection > What is Azure Active Directory Identity Protection?](#)

[Azure > Identity Protection > Azure Active Directory Identity Protection - Security overview](#)

**Question #109 of 118**

Question ID: 1353612

The Nutex Corporation uses Microsoft Azure Advanced Threat Protection (ATP) and Windows Defender ATP. You must maximize the security of all resources. You have been asked to integrate Windows Defender ATP and Azure ATP.

What should you do?

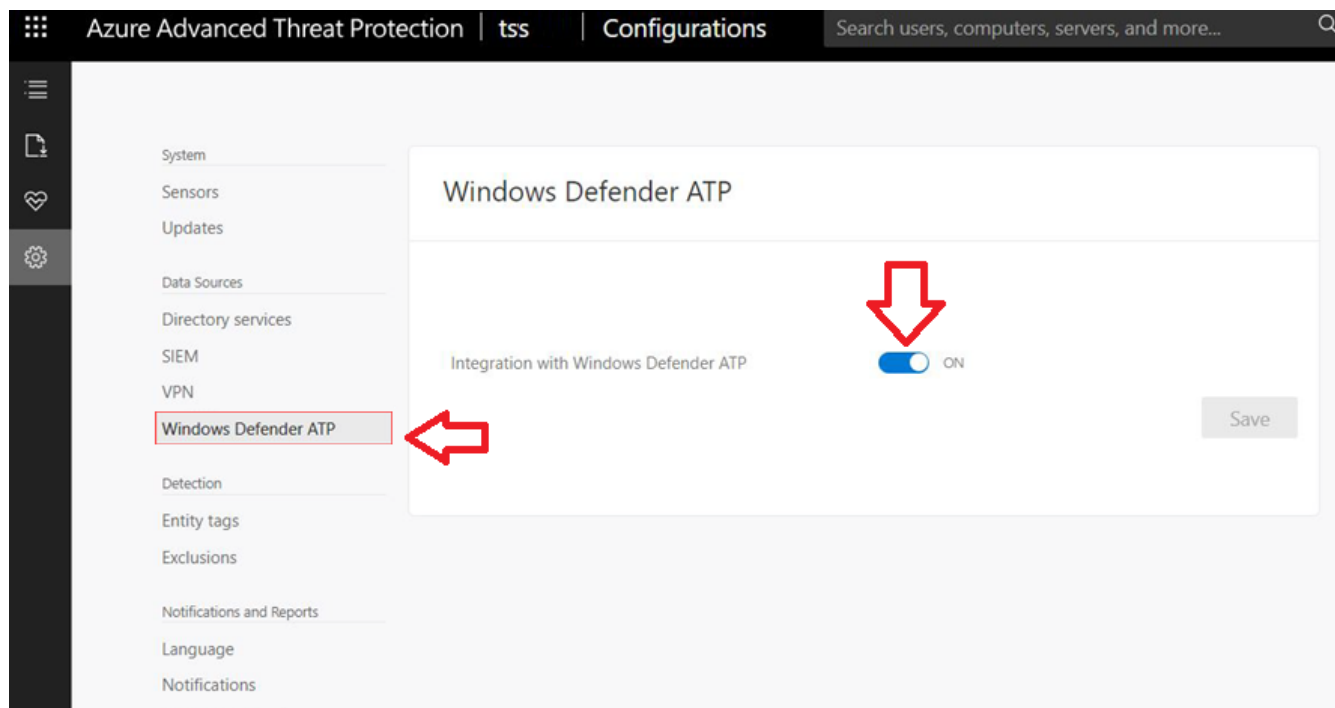
{UCMS id=5036573730013184 type=Activity}

Explanation

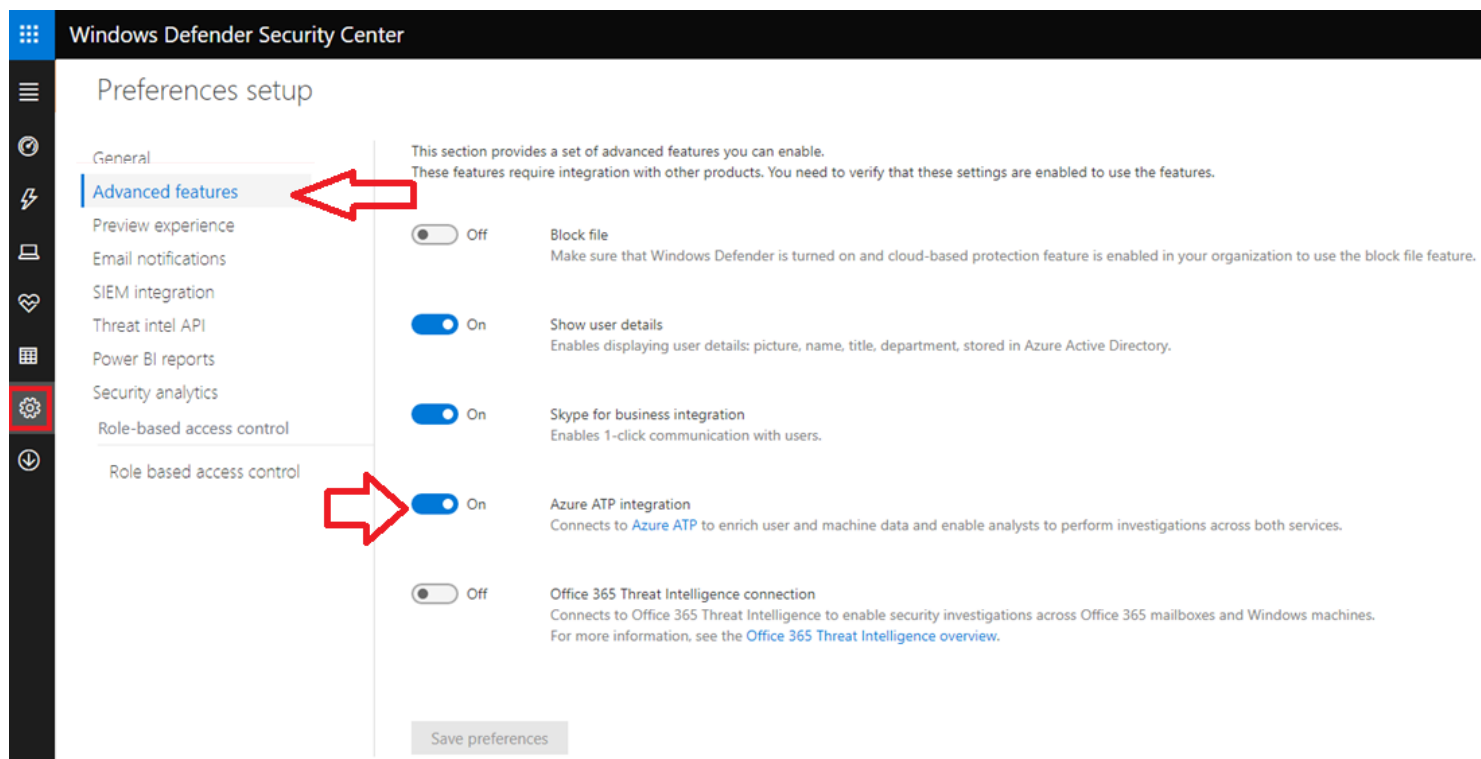
You should perform the following steps:

1. Open Azure ATP.
2. Choose **Configuration**.
3. Select **Windows Defender ATP** and set the integration toggle to ON.
4. Open the Windows Defender ATP Portal.
5. Go to **Settings, Advanced features**
6. Set **Azure ATP integration** to ON.

You should go to the Azure portal and choose **Configuration**. You should pick Windows Defender ATP from the list. On the Windows Defender ATP page, set the Integration with Windows Defender ATP to ON.



After you have configured that option, you should open the Windows Defender ATP Portal. On the Windows Defender Security Center screen, you should choose Advance Features. On the Advanced Features page, turn the **Azure ATP integration** to ON.



You should not go to **General** settings under Windows Defender Security Center. This option will have generic settings and does not contain the options for Azure ATP integration.

You should not go to **Security analytics** settings under Windows Defender Security Center. This option will display analytics of threats such as malware and virus. This option does not contain the options for Azure ATP integration.

#### Objective:

Implement Microsoft 365 security and threat management

#### Sub-Objective:

Implement Windows Defender Advanced Threat Protection (ATP)

#### References:

[Docs > How to Guides > Integrate Azure ATP with Windows Defender ATP](#)

### Question #110 of 118

Question ID: 1353626

Dreamsuites will be implementing Azure Information Protection (AIP) to protect content with Azure Rights Management. Because AIP relies on a tenant key, you will need to choose a key option during setup. Dreamsuites wants a low-cost yet secure solution with ease of management.

What will be the best option to meet their needs?

- ✓ **A)** Choose a "Managed By Microsoft" key.
- X **B)** Create a software-protected key in Azure Key Vault.
- X **C)** Create an on-premises hardware-HSM (hardware security module) protected key and transfer it to the Azure Key Vault
- X **D)** Create an HSM-protected key in Azure Key Vault.
- X **E)** Create an on-premises software-protected key and transfer it to the Azure Key Vault.

#### Explanation

It would be best to choose a "Managed By Microsoft" key. This option has the lowest administrative overhead. It is generated by default and is used exclusively for AIP. In addition, Microsoft is responsible for the backup and recovery of the key.

You would not create an on-premises hardware-HSM (hardware security module) protected key and transfer it to the Azure Key Vault. The scenario does not state if an HSM exists, and this option has high administrative overhead. In addition, this requires Azure Key Vault Premium, which is not a low-cost solution.

You would not create an on-premises software-protected key and transfer it to the Azure Key Vault. Azure Key Vault is not low-cost; it requires a subscription.

Create a software-protected key in Azure Key Vault. Azure Key Vault is not low-cost; it requires a subscription.

You would not want to create an HSM-protected key in Azure Key Vault. This type of key requires Azure Key Vault Premium, which is not a low-cost solution.

If you choose the wrong tenant key topology during initial deployment, you can change the key using the Powershell **Set-AipServiceKeysProperties** cmdlet.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Implement Azure Information Protection (AIP)

**References:**

[Docs > Azure Information Protection > Planning and implementing your Azure Information Protection tenant key](#)

[Docs > What is Azure Key Vault?](#)

[Docs > Azure Information Protection > Bring your own key \(BYOK\) details for Azure Information Protection](#)

---

**Question #111 of 118**

Question ID: 1257289

As part of readying Verigon Corporation for ISO certification, you need security-related information on you Azure AD users. You need to see the effectiveness of your recent rollout of Multi-Factor Authentication (MFA).

What would be a good reporting starting point in the Azure AD Identity Protection Overview?

- ☐ **A) New Risky Users - Medium Risk**
- ☐ **B) Protected Risky Sign-ins**
- ☒ **C) Unprotected Risky Sign-Ins**
- ☐ **D) New Risky Users - High Risk**
- ☐ **E) Identity Secure Score**

Explanation

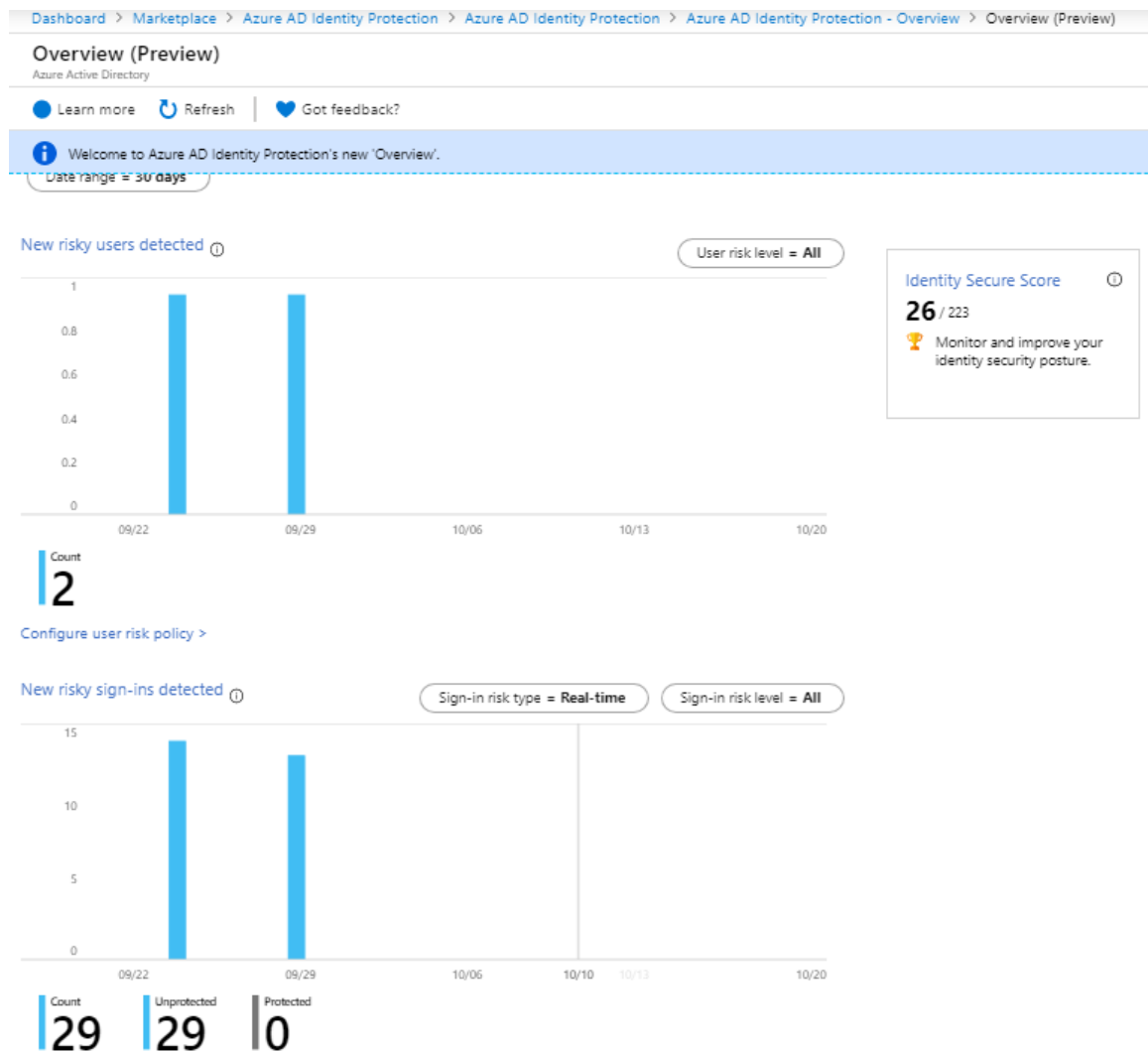
You will want to look at **Unprotected Risky Sign-Ins**. This report will show you logins that were not MFA-challenged. You could choose to make a policy to block such attempts.

**Identity Secure Score** does not give you the required information. It compares your company to industry patterns.

You will not want to look at **Protected Risky Sign-Ins** as these were MFA-challenged.

You would not look at **New Risky Users - Medium Risk** if you are focused on MFA. This report shows a filtered view of users who have logged in with a medium likelihood of compromised identity.

You would not look at **New Risky Users - High Risk** if you are focused on MFA. This report shows a filtered view of users who have logged in with a high likelihood of compromised identity.



Note that a new Overview is replacing the original "overview" dashboard. The level of features depends on the Azure AD premium license version.

#### Objective:

Implement Microsoft 365 security and threat management

#### Sub-Objective:

Manage security reports and alerts

#### References:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/enable>

[Azure > Identity Protection > Azure Active Directory Identity Protection - Security overview](#)

### Question #112 of 118

Question ID: 1353621

TXGlobal Corporation has created a new Personal Retention Tag labeled **AutoArchive** for members of the Legal department that allows them to archive items more frequently than the rest of the company. This tag will be one of several new tags to be added to a new Legal Retention Policy named **Legal**.

How can TXGlobal create the new custom retention policy? (Choose all that apply.)

- X A) In the Exchange Admin Console, navigate to **Organization**, then **Compliance Management**, then **Retention Policies**, and click the Add (+) icon.
- X B) Run Set-RetentionPolicy "Legal" -RetentionPolicyTagLinks "AutoArchive"

- ✓ **C)** In the Exchange Admin Console, navigate to **Compliance Management**, then **Retention Policies**, and click the Add (+) icon.
- X **D)** In the Exchange Admin Console, navigate to **Protection**, then **Compliance Management**, then **Retention Policies**, and click the Add (+) icon.
- ✓ **E)** Run `New-RetentionPolicy "Legal" -RetentionPolicyTagLinks "AutoArchive"`
- X **F)** Run `New-OutlookProtectionRule -Name "Legal" -ApplyRightsProtectionTemplate "AutoArchive"`

#### Explanation

You could use the Exchange Admin Console, navigate to **Compliance Management**, then **Retention Policies**, and click the Add (+) icon. You could link the AutoArchive tag at this point, or edit the policy later and add/remove tags as desired. Note that if a retention policy has a Default Policy Tag (DPT), the tag applies to all items in the mailbox that have not been manually tagged. Users cannot change the DPT; but they can, in a sense, "override" the behavior by assigning a Personal Tag. You cannot navigate to the **Retention Policies** page from either **Organization** or **Protection**.

The screenshot shows the Exchange Admin Center interface. The left navigation pane has 'compliance management' selected. The main content area is titled 'Retention policies' and shows a list of policies. The 'Legal' policy is selected, and a modal window is open for editing it. The modal shows the policy name 'Legal' and a table of retention tags. The table has four columns: NAME, TYPE, RETENTION PERIOD, and RETENTION ACTION. There is one row with the tag 'AutoArchive', type 'Personal', retention period '30 days', and action 'Archive'.

You could run the Powershell command `New-RetentionPolicy "Legal"`. The **New-RetentionPolicy** cmdlet would create a new retention policy named Legal; however, no tags would be linked to it. You would then need to use the EAC to link the tags, or you could run the Powershell command `Set-RetentionPolicy "Legal" -RetentionPolicyTagLinks "AutoArchive"`. This action would use the **Set-RetentionPolicy** cmdlet to change the properties of an existing retention policy named Legal by linking the AutoArchive tag with the **RetentionPolicyTagLinks** parameter to the retention policy.

You would not run the Powershell command `Set-RetentionPolicy "Legal" -RetentionPolicyTagLinks "AutoArchive"`. This cmdlet is used to modify an existing retention policy; you need to create a new one.

You would not run the Powershell command `New-OutlookProtectionRule -Name "Legal" -ApplyRightsProtectionTemplate "AutoArchive"`. This cmdlet creates rules to inspect message content and apply Active Directory Rights Management templates before sending the message.

#### Objective:

Manage Microsoft 365 governance and compliance

#### Sub-Objective:

Configure Data Loss Prevention (DLP)

#### References:

[TechNet > Office Products > Exchange Online > Security and Compliance > Messaging records management > Apply a retention policy to mailboxes](#)

## Question #113 of 118

Question ID: 1257323

Verigon Corporation has just implemented Azure Information Protection. They have created a collection of labels to cover all sensitivity topics. It has been decided that all Verigon documents and emails must have a label.

How will you meet this requirement?

- X **A)** Create a new policy, and enable the setting "***Users must provide justification to set a lower classification level, remove a label, or remove protection***"
- X **B)** Create a new AIP policy, and add the default labels.
- ✓ **C)** Edit the Global policy, and enable the setting "***All documents and emails must have a label***"
- X **D)** Create a new label with a custom condition. Set the "***Set permissions for documents and emails containing this label***" to "***protect***".
- X **E)** Create a new AIP policy, and add all existing labels.

### Explanation

The easiest method will be to edit the Global policy, and enable the setting "All documents and emails must have a label". This requirement will apply to all users automatically, so you will just have to add all labels. Each label has the option to be deployed manually by users or to be applied automatically.

Send audit data to Azure Information Protection analytics

☐ Off ☒ Not configured

All documents and emails must have a label (applied automatically or by users)

☐ Off ☒ On

Users must provide justification to set a lower classification label, remove a label, or remove protection

☒ Off ☐ On

For email messages with attachments, apply a label that matches the highest classification of those attachments

☒ Off ☐ Automatic ☐ Recommended

Display the Information Protection bar in Office apps

☐ Off ☒ On

Add the Do Not Forward button to the Outlook ribbon

☒ Off ☐ On

Make the custom permissions option available for users

☒ Off ☐ On

Provide a custom URL for the Azure Information Protection client "Tell me more" web page (optional; otherwise keep blank)

You would not create a new policy and enable the setting "Users must provide justification to set a lower classification level, remove a label, or remove protection". The scenario requires all content to be labeled, so we don't want users to be able to remove a label.

You would not create a new policy and add the default labels. All labels need to be available for application.

You would not create a new policy and add all existing labels. While you could meet the scenario requirements adding all labels and then adding every user and group, this is not as practical as just modifying the Global policy.

You would not create a new label with a custom condition. The desired labels have been created. We only want to enforce application.

While this scenario is easily resolved by modifying the Global policy, it is recommended to create scoped policies. A scoped policy is tailored to a specific department. You can have scoped policies that override Global policy settings. If there are multiple policies, they are applied in order, with Global policy first.

### Objective:

Manage Microsoft 365 governance and compliance

### Sub-Objective:

Implement Azure Information Protection (AIP)

## References:

[Docs > Azure Information Protection > Configuring the Azure Information Protection policy](#)

[Docs > Azure Information Protection > How to configure the policy settings for Azure Information Protection](#)

---

## Question #114 of 118

Question ID: 1353640

Dreamsuites Incorporated wants to manage the content search permissions and queries against their Office 365 services. Dreamsuites has an Office 365 E3 subscription. They need to allow specific administrators to run restricted content searches.

What is the first step?

- ✓ **A)** Create an eDiscovery case.
- X **B)** Add a custodian.
- X **C)** Configure an In-Place Hold.
- X **D)** After performing a search, click on Prepare for Advanced Ediscovery.
- X **E)** Configure a Litigation Hold.

### Explanation

You would need to create an eDiscovery case. An eDiscovery case allows you to organize your discovery work granularly and add an extra layer of permissions. Users are authorized by adding them to the Discovery Management role group.

You would not configure a Litigation Hold. This action does not offer the level of permissions granularity required by Dreamsuites. A Litigation Hold keeps all mailbox data. Litigation Hold is not supported for public folders.

You would not configure an In-Place Hold. An In-Place hold is more flexible than a Litigation Hold, in that you can specify what to hold, but does not offer the permissions control of an eDiscovery case.

You would not click on **Prepare for Advanced Ediscovery**. Advanced Ediscovery offers additional functionality but is not available with an E3 license.

You would not add a custodian. A custodian is a user whose data sources will be preserved and held for future searches. This option is only available in Advanced Ediscovery, which requires an E5 license. (or an Advanced Compliance add-on to the E3 subscription.)

### **Objective:**

Manage Microsoft 365 governance and compliance

### **Sub-Objective:**

Manage eDiscovery

### **References:**

[Microsoft 365 > eDiscovery cases in the Security & Compliance Center](#)

[Microsoft 365 > Overview of the Advanced eDiscovery solution in Microsoft 365](#)

[Microsoft 365 > Manage legal investigations > Set up users and cases in Office 365 Advanced eDiscovery](#)

---

## Question #115 of 118

Question ID: 1257293

Your company has 6,000 Windows 10 devices. These devices are protected by Microsoft Defender Advanced Threat Protection (ATP). The devices are generating a large volume of alerts. The security team is overwhelmed try to address these alerts. The security team needs to manage these alerts and take remediation action to resolve breaches.

Which component of the Microsoft Defender ATP should the security team utilize?

- X **A)** Advance hunting
- ✓ **B)** Automated Investigations
- X **C)** Endpoint detection and response
- X **D)** Threat Analytics

#### Explanation

Automated investigations use playbooks which are inspection algorithms and process used by analysts. These playbooks are used to examine alerts and take remediation actions against breaches. The playbooks allow you to reduce the volume of alerts thus freeing up the time of the security team personnel. The Automated investigations show the status, detection, source and date of each investigation that has been initiated.

Microsoft Defender ATP endpoint detection and response allows security analysts to prioritize alerts so that they can see a big picture of a breach so they can investigate, and take action to remediate the threats. Microsoft Defender ATP endpoint detection and response allows you to prioritize alerts, but not to reduce the volume of alerts that need to be investigated individually. Automated investigations help the security team to achieve that.

You should not choose threat analytics. Threat analytics are reports published by Microsoft as soon as threats and outbreaks are found. Threat analytics allow you to access the impact of threats. Threat analytics will not allow you to manage alerts.

You should not choose advanced hunting. Advance hunting uses a search and query tool to hunt for possible threats. You can configure detection rules based on queries and alerts. Advance hunting will not allow you to reduce the volume of alerts.

#### **Objective:**

Implement Microsoft 365 security and threat management

#### **Sub-Objective:**

Manage security reports and alerts

#### **References:**

[Docs > Security > Overview of Automated investigations](#)

[Docs > Security > Investigate Microsoft Defender Advanced Threat Protection alerts](#)

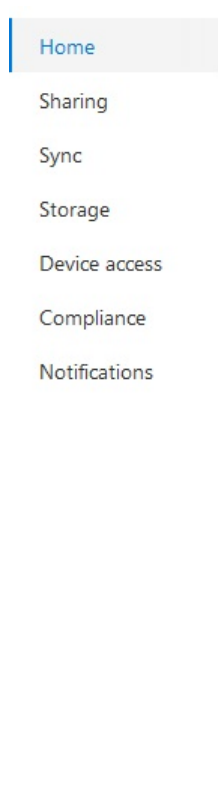
---

## **Question #116 of 118**

Question ID: 1257339

You are currently working as an Office 365 administrator for the Dream Suites organization. The legal department has requested that an alert notification be sent through email when users delete specific files within OneDrive for Business.

You open the OneDrive admin center:



## OneDrive admin center



### Welcome to the OneDrive admin center

This is the new place to manage all your organization's OneDrive settings. We'll be adding reports and many other features soon, and would love to hear your suggestions on what to add or change.

[Send feedback](#)

Which menu within the OneDrive admin center would you select?

- ✓ **A)** Compliance
- X **B)** Sharing
- X **C)** Device Access
- X **D)** Sync

#### Explanation

The **Compliance** menu item allows the admin to configure auditing, data loss prevention policies, retention, eDiscovery, and alert notifications. The alert notifications can be generated when users perform specific activities within OneDrive:

Home

Sharing

Sync

Storage

Device access

Compliance

Notifications

# Compliance

If your organization has legal, regulatory, or technical standards that you Security and Compliance Center to perform the following tasks.

## Auditing

View user activities related to OneDrive, such as who recently accessed, deleted, or shared  
[Search the audit log](#)

## Data loss prevention (DLP)

Protect your organization's sensitive information so it doesn't get into the wrong hands. Y  
[Create a DLP policy](#)  
[View DLP policy match reports](#)

## Retention

Preserve OneDrive files as long as you need.  
[Create a preservation policy](#)

## eDiscovery

Identify, hold, search, and export content that can be used as evidence in legal cases.  
[Create an eDiscovery case](#)

## Alerts

Get notified when users perform specific activities in OneDrive.  
[Create an alert](#)

The **Sharing** menu item allows the OneDrive administrator to set specific controls of how SharePoint content is shared with external users. Options available include turning on or off the ability to globally share content with external users, who users can share content with, limiting sharing by domain, or even allowing external users to share items they do not own.

The **Sync** menu item allows the OneDrive administrator to configure how files in OneDrive and SharePoint are synchronized. The administrator can show the sync button on the OneDrive website, allow sync activity only from PCs joined to corporate-owned Active Directory domains, and to define what file types can be synced.

The **Device Access** menu item allows the administrator to configure access to OneDrive content based on network location, approved apps, and mobile application management policies for Android and iOS within the OneDrive and SharePoint mobile apps.

**Objective:**  
Manage Microsoft 365 governance and compliance

**Sub-Objective:**  
Manage data governance

**References:**  
[Microsoft Support > Create activity alerts in the Office 365 Security & Compliance Center](#)

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?

- ✓ **A)** Create a compliance policy and add an action for non-compliant devices.
- X **B)** Create a compliance policy and add a scope tag.
- X **C)** Create a conditional access policy and add a device state condition.
- X **D)** Create a conditional access policy and add a location condition.
- X **E)** Create a compliance policy, and sync all 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 #118 of 118**

Question ID: 1257301

Nutex has Office 365. The legal department suspects there were customer privacy violations within the Nutex product development department. The legal department has ensured that all users in the product development department are subject to a hold during the investigation. Any messages destined to leave the Nutex messaging environment that contain customers' sensitive information should be blocked and not delivered. The legal department has specifically stated that credit card numbers should not be sent outside the organization.

What step should you take to meet the compliance request?

- ✓ **A)** Create a data loss prevention policy
- X **B)** Export the administrator audit log
- X **C)** Create an in-place hold
- X **D)** Export the Mailbox audit log

#### Explanation

A data loss prevention policy (DLP) should be used. A DLP policy will evaluate each piece of information that is sent through the transport pipeline and decide whether the message should be sent or blocked. When creating a DLP policy, you can choose an action that should be taken when evaluated messages match the configured criteria, such as sending an alert or actually blocking the message.

In this situation, you should create a DLP rule that blocks messages when credit card numbers are found in messages that are scheduled to be delivered outside the Nutex messaging environment.

An in-place hold would not meet the required business objectives. An in-place hold will allow you to create a hold that utilizes filter-based criteria. This allows a hold to be created by using keywords or start and end dates deemed important.

The mailbox auditing feature would not meet the required business objectives. Mailbox auditing is used to log what user accounts access a specific mailbox and the actions or changes they make.

The administrator audit log will show what changes have been made within the Exchange organization. For instance, if an administrator makes a change to the certificate on a Mailbox server with the Client Access service, all the commands executed will be logged for review in the administrator audit log.

**Objective:**

Manage Microsoft 365 governance and compliance

**Sub-Objective:**

Configure Data Loss Prevention (DLP)

**References:**

[TechNet > Exchange > Exchange Online > Messaging policy and compliance > Data loss prevention](#)