# MS-500 Domain 1 Implement and mange identity and access

**Test ID: 200489925**

## Question #1 of 36

Question ID: 1427384

You are an enterprise administrator for the Nutex Company. They are a cloud-first organization that hosts their devices in Azure AD and uses Microsoft Endpoint Manager to deploy configured applications and settings. The company is very strict about implementing least-privilege security principles.

The company recently decided to give department managers more autonomy and allow them to manage the access policies for their departmental applications without IT involvement.

Which step would achieve this objective?

- ✗ **A)** Create a Microsoft 365 group for the department managers using Microsoft Endpoint Manager and assign them the Application Administrator role.
- ✗ **B)** Create administrative units in Azure for the designated departmental resources and assign the department managers the Authentication Administrators role.
- ✓ **C)** Use Identity Governance to create a catalog along with an access package, and make the department managers catalog owners.
- ✗ **D)** Create a security group for the department managers using Microsoft Endpoint Manager and give them the Privileged Role Administrator role.

Explanation

Identity Governance has a feature called Entitlement Management that allows you to create catalog containers for resources that permits non-IT personnel to govern user access to applications. With Entitlement Management, department managers can be granted the ability to delegate access to Azure AD enterprise applications, such as custom-integrated applications and SaaS applications, to the users in their departments.

Creating a security group for the department managers and assigning them the Privileged Role Administrator role would give them overreaching admin powers. Since this role can manage role assignments for any user in Azure AD, the assignment of this role to department managers would allow them to manage users in other departments, which was not called for in the scenario.

Creating a Microsoft 365 group for the department managers and assigning them the Application Administrator role would give them overreaching admin powers. If you assign the Application Administrator role to a user, that user can then impersonate an application’s identity, whether that application was assigned to the department or not.

Administrative units are used to delegate administrators over Azure AD objects such as users and groups, not over applications. Creating an administrative unit would not allow department managers to manage the access policies for their departmental applications.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Privileged Identity Management (PIM)

**References:**

Microsoft Docs > Azure > Active Directory > Identity Governance > What is Azure AD entitlement management?

Microsoft Docs > Learn > Browse > Plan and implement entitlement management

---

## Question #2 of 36

Question ID: 1342934

You are the Microsoft 365 Security Administrator for the Nutex Corporation. They have recently moved to Microsoft 365 and plan to leverage most of the security capabilities available with the subscription. Nutex currently hosts a wide range of apps in their in-house datacenter.

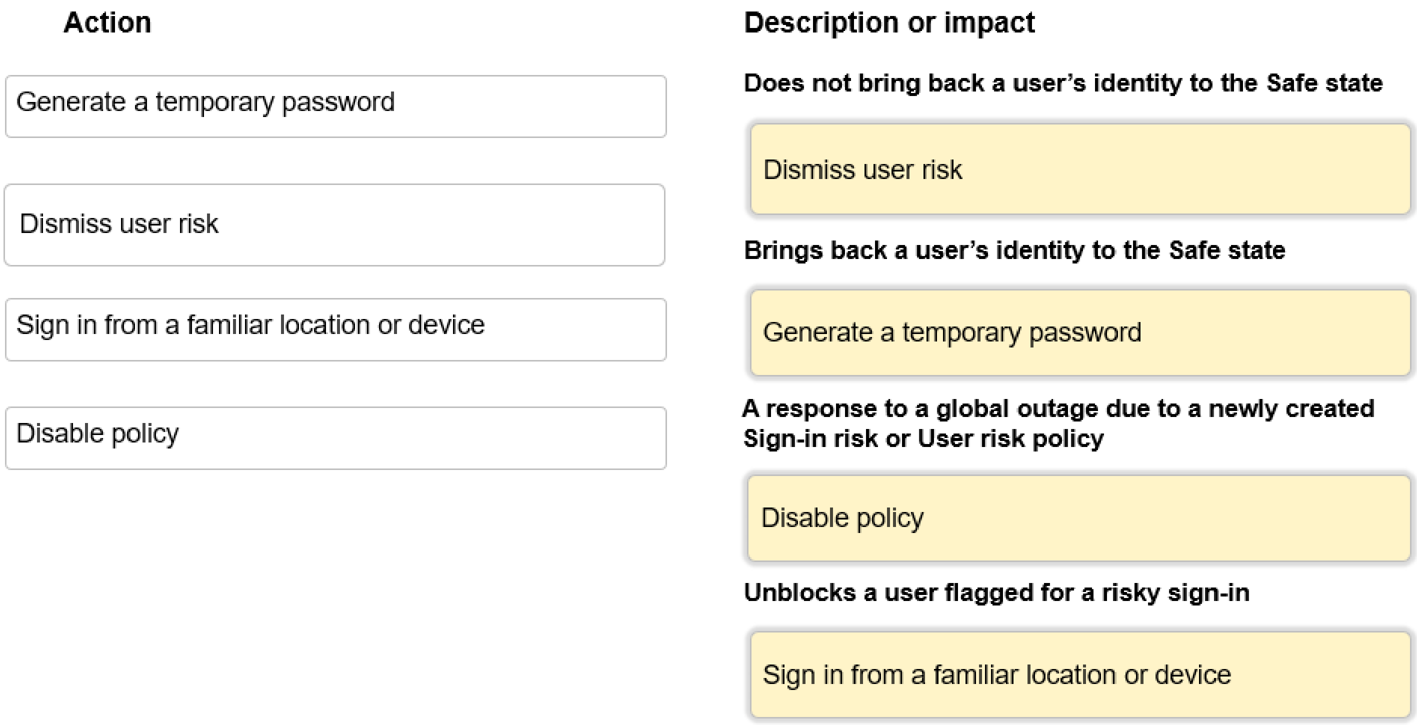
You have added all the required policies, including Sign-in and User risk policies. Your team now needs to start monitoring users and logins that have been impacted by these policies, investigate these activities, and remediate them.

Match the investigative and remediation actions available with the Identity protection reports for risky sign-ins and risky users (on the left) with their description or impact (on the right).

{UCMS id=4726791504658432 type=Activity}

Explanation

You would map as follows:



**Action**

Generate a temporary password

Dismiss user risk

Sign in from a familiar location or device

Disable policy

**Description or impact**

**Does not bring back a user’s identity to the Safe state**

Dismiss user risk

**Brings back a user’s identity to the Safe state**

Generate a temporary password

**A response to a global outage due to a newly created Sign-in risk or User risk policy**

Disable policy

**Unblocks a user flagged for a risky sign-in**

Sign in from a familiar location or device

Generate a temporary password is one of the manual password reset options available to remediate a user’s entry in the Risky Users report. You can see this report on the Azure portal > Identity protection > Risky Users page. This option generates a temporary password and brings a user’s identity back into the Safe state.The new password is sent to the user and during the next sign-in, the user enters this password and is immediately prompted to change it.

Dismiss user risk is a remediation action that closes all events related to the affected user. However, because this method does not impact the existing password, the user’s identity is not brought back to the Safe state.

Signing in from an unfamiliar location or device is one of the common reasons for blocked suspicious sign-in attempts. If the user is unable to sign in from a known location, you must investigate and unblock the user using other options such as Exclude from policy.

Misconfigured Sign-in or User risk policies can cause a global outage for users. Some of the possible causes are incorrect network locations and blocking access as a response to risk events. In such cases, you must temporarily disable policies for all users and unblock them. Change the policies and enforce them as quickly as possible.

**Objective:**

Implement and manage identity and access

**Sub-Objective:**

Implement Azure AD Identity Protection

**References:**

Microsoft Docs > Azure > Active Directory > Identity protection > Remediate risks and unblock users > RemediationMicrosoft Docs > Azure > Active Directory > Identity protection > Remediate risks and unblock users > Unblocking users

## Question #3 of 36

Question ID: 1355544

The Nutex Corporation has seen a spike in international business travel for its employees and more contract employees working remotely, especially in sales and operations. You are the Azure Security Administrator at Nutex. With employees signing in to Microsoft 365 from remote locations, you are concerned about the risks associated with users' identities being compromised.

You plan to implement a User risk policy for your Microsoft 365 deployment.

Which of the following statements about User risk policies are TRUE? (Select all that apply.)

✓ **A)** Leaked login credentials to the web is one of the factors that triggers and executes a User risk policy.

✓ **B)** Before saving a User risk policy, you can view the number of users who will be impacted by the policy.

✗ **C)** The User risk policy always blocks access to users whose identities have been compromised.

✓ **D)** Microsoft recommends that you set the risk level of User risk policies to High.

Explanation

The following statements are true:

- Leaked login credentials to the web is one of the factors that triggers and executes a User risk policy.
- Before saving a User risk policy, you can view the number of users who will be impacted by the policy.
- Microsoft recommends that you set the risk level of User risk policies to High.
- The User risk policy can either block or grant access to users whose identities have been compromised.

Leaked login credentials to the web is one of the factors that triggers and executes a User risk policy. A user risk is calculated based on the probability that the users' identities are compromised. Some of the factors that Microsoft uses to calculate this score are by finding leaked credentials on the Internet and by using Azure AD threat intelligence to analyse users' activities with known attack patterns.

Before saving a User risk policy, you can view the number of users who will be impacted by the policy. This is applicable to both Sign-in and User risk policies. However, this number is only an estimate.

Microsoft recommends that you set the risk level of User risk policies to High. They also recommend that you set the risk level of Sign-in risk policies to Medium or Low. When risk levels are set to High, the policy is triggered less frequently and this can allow attackers from getting in undetected. Setting this to Medium validates users more frequently. Setting it to Low provides the best security posture for your deployment. However, you can always change the risk level of User risk policies to Medium or Low, if you see severe impact when users' identities are compromised.

The User risk policy does not always block access to users whose identities have been compromised. A User risk policy can be configured to block access, allow access, or allow access with a self-service password reset when risky sign-ins are detected. To add a User risk policy, go to Azure Active Directory > Security > Identity Protection > Overview, click User risk policy, specify the inputs, and enforce the policy.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Identity Protection

**References:**

Microsoft Docs > Azure > Active Directory > Identity Protection policies > User risk policy

Microsoft Docs > Azure > Active DIrectory > Identity protection > How To: Configure and enable risk policies > Enable policiesMicrosoft Docs > Azure > Active Directory > Identity protection > How To: Configure and enable risk policies > Choosing acceptable risk levels

Modern Workplace Blog > Azure AD Identity Protection deep dive

---

## Question #4 of 36

Question ID: 1342925

You are the Security Administrator for Nutex Corporation's Microsoft 365 Enterprise deployment. Over the past few months, you have implemented several security measures to secure access to Microsoft 365 services. Nutex is planning to acquire two software development companies with multiple apps and services. You need to implement a robust RBAC model to let administrators and users access the apps and services for Nutex and the companies it will acquire.

Which of the following statements about RBAC with Microsoft 365 are TRUE? (Select all that apply.)

✗ **A)** To allow an administrative role to reset users' passwords, you must always assign the Global Admin role.

✗ **B)** Microsoft recommends not to have more than one user with the Global Admin role per deployment/tenant.

✗ **C)** All Microsoft 365 admin roles can reset the passwords for Microsoft 365 users.

✓ **D)** Authorized Microsoft partners can assign Full administration and Limited administration roles to Microsoft 365 users.

✓ **E)** Microsoft 365 roles can be granted access at four levels of scope: management group, subscription, resource group, and resource.

Explanation

The following statements are true:

- Authorized Microsoft partners can assign Full administration and Limited administration roles to Microsoft 365 users.
- Microsoft 365 roles can be granted access at four levels of scope: management group, subscription, resource group, and resource.

An authorized Microsoft partner who sets up and/or is managing Microsoft 365 services for a customer can assign the Full administration (equivalent to the Global Admin) and Limited administration (equivalent to the Helpdesk Admin) roles to users in their customer's deployment. The customer's admin must add the partner as a delegated admin to their account, then the partner must send the customer's admin an email to grant permissions of a delegated admin for the customer's account.

A role assignment consists of three elements: security principal, role definition, and scope. A security principal is an object (a user, group, service principal, or managed identity) that must be granted access; a role definition is a collection of access permissions that are needed; scope is the set of resources that the access applies to. There are four levels of scope, which are management group, subscription, resource group, and resource, and these are structured in a parent-child relationship. You can assign roles at any of these levels of scope.

All Microsoft 365 admin roles cannot reset the passwords for Microsoft 365 users. Only administrators with the Global Admin, Helpdesk Admin, or User Admin role can reset users' passwords.

The Global Admin role must be assigned to users who need administrative access to most Microsoft 365 services. Microsoft recommends not to have more than two to four users with this role. The user who signed up for Microsoft 365 services is automatically the first Global Admin for the tenant/deployment.

Microsoft recommends that you have somewhere between 2 to 4 users with the Global Admin role for a deployment/tenant. On a Microsoft 365 tenant, only another Global Admin can reset a Global Admin's password. So, having 2 Global Admins can avoid an account lockout. Because Global Admins have almost unlimited access to features and most of the data, Microsoft recommends that you do not have more than 4 Global Admins.

You must never assign the Global Admin role to a user to reset users' passwords. Global Admins have unlimited privileges. You must always assign roles based on the least-privilege principle. In this case, create a custom role with only Reset password permission or, at the most, assign the role of Helpdesk Admin.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**

Implement role-based access control (RBAC)

**References:**

Microsoft Docs > Microsoft 365 > Microsoft 365 admin center help > About admin roles > Commonly used Microsoft 365 admin center rolesMicrosoft Docs > Microsoft 365 > Microsoft 365 admin center help > About admin roles > Delegated administration for Microsoft PartnersMicrosoft Docs > Microsoft 365 > Microsoft 365 admin center help > About admin roles > Security guidelines for assigning roles

Microsoft Docs > Azure > Role-based access control > What is Azure role-based access control (Azure RBAC)? > What can I do with Azure RBAC?

---

## Question #5 of 36

Question ID: 1365722

In the past three weeks, several users assumed an Azure AD role. To meet industry compliance regulations, you must determine if a particular user activated a role assignment. Which actions must you perform in the Azure portal?

Choose the appropriate steps and place them in the correct order.

{UCMS id=5526807529914368 type=Activity}

Explanation

You should choose the following:

1. Open **Azure AD Privileged Identity Management**.
2. Select **Azure AD roles**.
3. Select **Resource audit**.
4. Set the filter for the past 21 days.

The audit history of Privileged Identity Management (PIM) keeps 30 days of data on all role assignments and activations of privileged roles. If you need more than 30 days of audit history, you would use the Azure Active Directory security and activity reports.

You would select **Azure AD roles** in **Azure AD Privileged Identity Management**, choose **Resource audit**, and set the date range filter for the past 3 weeks.

You would not choose **Alerts**. This option shows alerts when there is suspicious or unsafe activity. The alerts show up in the Privileged Identity Management dashboard when they are triggered.

You would not choose **Role Settings**. This option allows you to customize roles, such as adding authentication and duration.

**Objective:**

Implement and manage identity and access

**Sub-Objective:**

Implement Azure AD Privileged Identity Management (PIM)

**References:**

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > View audit history for Azure AD roles in Privileged Identity Management

---

## Question #6 of 36

Question ID: 1342927

You are the Security Administrator for Nutex Corporation's Microsoft 365 Enterprise deployment. You manage a team of newly hired Microsoft 365 administrators. You need to assign RBAC activity monitoring to one of the newly hired administrators.

You need to give a brief overview about how to monitor RBAC activities for Microsoft 365 services.

Which of the following statements about activity logs for RBAC changes are TRUE? (Select all that apply.)

✗ **A)** You can view the activity logs for a maximum of seven days using Azure PowerShell.

✓ **B)** Activity logs do not contain activities for read (GET) operations.

✗ **C)** The activities related to creating or updating custom role definitions are not logged in the activity logs.

✗ **D)** By using the Azure CLI, you can view activity logs for seven days from the start date you specify.

✓ **E)** You can view the activity logs for RBAC changes only for the past 90 days.

Explanation

The following statements are true:

- You can view the activity logs for RBAC changes only for the past 90 days.
- Activity logs do not contain activities to read (GET) operations.

It is always good to monitor the RBAC change-related activities for Microsoft 365 apps and services periodically for auditing and troubleshooting purposes. Azure logs changes to role assignments or role definitions in the Microsoft 365 subscriptions in the Azure Activity Log. You can view the activity logs to see the Azure RBAC changes for the past 90 days.

Activity logs contain details about activities for all write operations (PUT, POST, DELETE), but do not include activities for read operations (GET).

Activities related to creating or updating custom role definitions are logged in the activity logs. The following activities are logged in the activity logs: Create role assignment, Delete role assignment, Create or update custom role definition, and Delete custom role definition.

You can view the activity logs for more than seven days using Azure PowerShell. Use the **Get-AzLog** cmdlet to retrieve the Azure activity logs for up to 90 days. By specifying the StartTime and EndTime of the activity logs, you can retrieve up to 1,000 events in the past 90 days.

By using the Azure CLI, you can view activity logs for a few hours to a few days from the start date you specify. Use the `-offset` parameter to decide the forward-time (hours or days to when the logs must be retrieved). You can specify a value of 1 hour to up to 90 days. The default value for offset is 6 hours.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement role-based access control (RBAC)

**References:**

Microsoft Docs > Azure > Role-based access control > View activity logs for Azure RBAC changes

Microsoft Docs > Azure > Azure PowerShell > Reference > Monitor > Get-AzLog

Microsoft Docs > Azure > Azure CLI > Reference > Monitoring > az monitor activity-log > az monitor activity-log list

Microsoft Docs > Azure > Resource Manager > Management > View activity logs to monitor actions on resources

## Question #7 of 36

Question ID: 1342923

You have recently joined the Nutex Corporation as the Authentication Administrator for their hybrid Microsoft 365 Enterprise deployment. Nutex has recently moved its apps and services to the Azure cloud. They have also hired contractors to meet the upcoming demands for manpower services. Nutex will be managing more than 5,000 employees soon.

One of your primary goals is to implement the self-service password recovery (SSPR) feature in Azure.

Which of the following statements about SSPR are TRUE? (Select all that apply.)

✓ **A)** To enable SSPR, you need the privileges of a Global Admin on Azure AD.

✗ **B)** With SSPR, password reset notifications can only be sent to user accounts, not administrator accounts.

✗ **C)** In a hybrid identity model, when the Writeback passwords to your on-premises directory option is set to No, only users who use federated and password hash sync authentication can reset their passwords, not users who use pass-through authentication.

✗ **D)** SSPR only supports mobile phone notification, mobile phone code, and email as authentication methods to reset passwords.

✓ **E)** By default, SSPR is enabled for administrator accounts on Azure AD.

Explanation

The following statements are true:

- To enable SSPR, you need the privileges of a Global Admin on Azure AD.
- By default, SSPR is enabled for administrative accounts on Azure AD.

The privileges of a Global Admin are one of the prerequisites needed to set up self-service password reset (SSPR) on an Azure AD tenant. One other prerequisite is that the Azure AD tenant must have a working tenant with at least an Azure AD Free or trial license enabled.

By default, administrator accounts are enabled for SSPR with a two-gate password reset policy. This policy can be different from the one for user accounts and cannot be changed. If you have implemented SSPR, you must always test the password reset functionality using a user account.

With SSPR, password reset notifications can be sent to both user and administrator accounts. You would do this by setting both the Notify users on password resets and Notify all admins when other admins reset their password options to Yes. For administrator accounts, the notifications are an additional layer of awareness when the passwords of other privileged accounts on the tenant are reset using SSPR.

In a hybrid identity model, when the Writeback passwords to your on-premises directory option is set to No, users who use federated, password hash sync, or pass-through authentication cannot reset their passwords. Password writeback synchronizes the password changes in Azure AD back to the on-premises AD DS environment. To enable password writeback completely, the account specified in Azure AD Connect must have the appropriate permissions and options set in the AD DS environment, password writeback must be enabled in Azure AD Connect, and the Writeback passwords to your on-premises directory option must be enabled by using the Password reset > On-premises integration page in the Azure portal.

The following additional authentication methods can be enabled before a user resets the password through SSPR: mobile app notification, mobile app code, email, mobile phone, office phone, and security questions. When a user is enabled for SSPR, the user must register at least one authentication method. Microsoft recommends that you choose two or more authentication methods to make password resets easier and more flexible for users. You can enable these methods on the Password reset > Authentication methods page on the Azure portal.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement conditional access

**References:**

Microsoft Docs > Azure > Active Directory > Authentication > Plan an Azure Active Directory self-service password reset deployment > Prerequisites

Microsoft Docs > Azure > Active Directory > Authentication > Tutorial: Enable users to unlock their account or reset passwords using Azure Active Directory self-service password reset > Configure notifications and customizations

Microsoft Docs > Azure > Active Directory > Authentication > Password policies and account restrictions in Azure Active Directory > Administrator reset policy differences

Microsoft Docs > Azure > Active Directory > Authentication > How it works: Azure AD self-service password reset > Authentication methods

---

## Question #8 of 36

Question ID: 1427381

You are serving as an IT intern for the Nutex Company. The company hosts its AD structure in Azure. Senior management wants you to identify stale access assignments. To meet the requirement, you must perform an internal audit that includes an access review of all groups.

Which Azure service should you utilize?

✓ **A)** Identity Governance

✗ **B)** Azure AD Conditional Access

✗ **C)** Managed Identities

✗ **D)** External Identities

Explanation

Identity Governance is an Azure service that can be used to create and manage access reviews for both groups and applications. Access reviews allow you to manage group memberships, access to your organization’s applications, and role assignments. Access reviews allow you ensure that only the right people have continued access.

You should not choose Managed Identities because it does not provide access reviews. Managed Identities can be used by applications that need to connect to resources that support Azure Active Directory authentication, thus eliminating the need for software developers to manage credentials for them.

You should not choose Azure AD Conditional Access because it does not provide access reviews. Azure AD Conditional Access is used to configure and modify access policies to control how and when a specific user has access.

You should not choose External Identities because it does not provide access reviews. External Identities gives you the ability to secure and manage external users such as vendors, partners, and customers to enhance collaboration.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement role-based access control (RBAC)

**References:**

Microsoft Docs > Azure > Active Directory > Identity Governance > Create an access review of groups and applications in Azure AD

## Question #9 of 36

Question ID: 1342916

You have recently joined the Nutex Corporation as a Security Administrator for their Microsoft 365 Enterprise deployment. Nutex has recently adopted this deployment. You are tasked with implementing multi-factor authentication (MFA) for all Microsoft 365 users. Currently, only a few business-critical Microsoft 365 users use MFA.

Which of the following statements about MFA for Microsoft 365 are TRUE? (Select all that apply.)

- ✗ **A)** Microsoft 365 users must use the Microsoft Authenticator app for the second layer of authentication.
- ✗ **B)** MFA can be implemented only by enabling the Security defaults on Azure AD.
- ✓ **C)** The legacy per-user MFA must be disabled before implementing MFA, by enabling the Security defaults or by enforcing Conditional Access policies.
- ✗ **D)** To manage MFA, you must be assigned the Office Apps admin role in the Microsoft 365 admin center.
- ✓ **E)** Implementing Conditional Access policies to enforce MFA is the most granular and comprehensive method to use.

Explanation

The following statements are TRUE:

- The legacy per-user MFA must be disabled before implementing MFA, by enabling the Security defaults or by enforcing Conditional Access policies.
- Enforcing Conditional Access policies to implement MFA is the most granular and comprehensive method to use.

You can configure Conditional Access policies to implement MFA for a specific group of users, to use MFA only for a specific group of apps, and to react to sign-in events and perform additional actions before granting access to users. Also, Conditional Access policies can be set to Report-only to try out the MFA implementation before you enforce the policies.

Microsoft 365 users do not have to use the Microsoft Authenticator app for the second layer of authentication. With Microsoft 365 MFA, in addition to a password that users must enter, a second layer of authentication is required, which can be one of the following: a verification code sent as a text message to a phone, a phone call with a verification code, the Microsoft Authenticator smartphone app or similar, or an OAuth hardware token that generates random time-limited verification codes.

MFA is not implemented only by enabling the Security defaults on Azure AD. MFA can be enabled in one of the following ways: enable Security defaults on Azure AD, enforce Conditional Access policies on Azure AD, or by configuring per-user MFA for selected users from the Microsoft 365 admin center. If you implement MFA by enabling Security defaults, Microsoft 365 users must always use the Microsoft Authenticator smartphone app as the second layer of authentication. If you implement MFA by using one of the other methods, users can choose a desired second layer of authentication (text, phone call, or the authenticator apps).

To manage MFA, you do not have to be assigned the role of an Office Apps admin in the Microsoft 365 admin center. You will need the privileges of the Global admin role to manage MFA.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement authentication methods

**References:**

Microsoft Docs > Microsoft 365 > Microsoft 365 admin center help > Secure your organization > Multi-factor authentication for Microsoft 365 > MFA support in Microsoft 365Microsoft Docs > Microsoft 365 > Microsoft 365 admin center help > Secure your organization > Multi-factor authentication for Microsoft 365 > Ways to manage MFA settings

Microsoft Docs > Microsoft 365 > Microsoft 365 admin center help > Secure your organization > Set up multi-factor authentication > Before you begin

Dirteam > Ways to require multi-factor authentication in Azure AD

Microsoft Docs > Azure Active > Directory > Authentication > Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication

---

## Question #10 of 36

Question ID: 1342928

You have recently joined the Nutex Corporation as their Security Administrator. You are part of a team that has evaluated Microsoft 365 and other such solutions. You need to build a roadmap to implement security measures for the solution that Nutex will purchase and the changes and costs to implement the measures. You will need to implement these security measures in the next few months. One security feature available with Microsoft 365 is Privileged Identity Management (PIM).

Which of the following statements about PIM are TRUE? (Select all that apply.)

✓ **A)** With PIM, all eligible users who need to use their privileged role must activate their role.

✗ **B)** After you implement PIM, all Azure resources are automatically protected with PIM.

✓ **C)** PIM is available with the Microsoft 365 Education A5 and Microsoft 365 Enterprise E5 paid licenses.

✓ **D)** Periodic access reviews after implementing PIM can help reduce the attack surface and stay compliant.

✗ **E)** Microsoft recommends that you double the number of users with the Global Admin role before you implement PIM.

Explanation

The following statements are true:

- PIM is available only with the Microsoft 365 Education A5 and Microsoft 365 Enterprise E5 paid licenses.
- Periodic access reviews after implementing PIM can help reduce the attack surface and stay compliant.
- With PIM, all eligible users who need to use their privileged role must activate their role.

Microsoft 365 Privileged Identity Management (PIM) is available with the Microsoft 365 Education A5 and Microsoft 365 Enterprise E5 free and paid licenses. PIM is also available with the Azure AD Premium P2 and Enterprise Mobility + Security (EMS) E5 licenses.

Microsoft recommends that you set up quarterly access reviews for all your Azure AD and Azure roles. Access reviews are conducted to assess whether the privileged users still need the same kind of access or if it can be restricted based on the least privilege principle. Access reviews can help you eliminate unwanted access, which helps to reduce the attack surface. Access reviews are sometimes needed to stay compliant with laws and regulations.

With PIM, all eligible users who need to use their privileged role must activate their role. When users activate their privileged role, they may need to use multi-factor authentication, request approval for activation, and/or provide a business reason for activation. Users retain the permissions of the role for the duration set in the Azure AD role settings options. Go to Azure portal > Azure AD Privileged Identity Management > Azure AD roles > Role settings to configure the role settings.

Microsoft recommends that you reduce, not double, the number of Global Admins (in case you have more than four) and validate whether they can be assigned other less-privileged administrator roles based on their access needs. Use the Discovery and insights (preview) feature with PIM to get a top-level view of the number of users with privileged access. Work from there to assign roles based on the least-privilege principle.

After you implement PIM, all Azure resources are not automatically protected with PIM. After you set up PIM, you need to discover and select the resources that you want protected. You can add an unlimited number of Azure resources. To discover resources, go to Azure portal > Azure AD Privileged Identity Management > Azure resources > Discover resources.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Privileged Identity Management (PIM)

**References:**

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Deploy Azure AD Privileged Identity Management (PIM) > Licensing requirementsMicrosoft Docs > Azure > Active Directory > Privileged Identity Management > Deploy Azure AD Privileged Identity Management (PIM) > Enforce principle of least privilegeMicrosoft Docs > Azure > Active Directory > Privileged Identity Management > Deploy Azure AD Privileged Identity Management (PIM) > Set up recurring access reviews to regularly audit your organization’s privileged identities

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Discover Azure resources to manage in Privileged Identity Management

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Configure Azure AD role settings in Privileged Identity Management

---

## Question #11 of 36

Question ID: 1427379

You have been hired as a security consultant for a startup company called Nutex. Because the company is growing so quickly, management wants you to assign administrator roles to designated users on a temporary basis for 90 days.

Which of the following tools must you use to achieve this objective?

- ✗ **A)** Azure Portal
- ✗ **B)** Exchange Online PowerShell
- ✗ **C)** Microsoft Endpoint Manager
- ✓ **D)** Privileged Identity Management

Explanation

You would use Privileged Identity Management to assign admin roles to users temporarily within a configured time window. Just-in-time (JIT) access is a feature of Privileged Identity Management to provide temporary permissions to a user to accomplish a task. The permissions have an expiration.

While you can create assignable role groups using Azure AD, the role assignments are permanent.

While you can create assignable role groups using Microsoft Endpoint Manager, the role assignments are permanent.

While you can create role groups using Exchange Online PowerShell, the role assignments are permanent.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement role-based access control (RBAC)

**References:**

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > What is Azure AD Privileged Identity Management?

---

## Question #12 of 36

Question ID: 1342922

You have recently joined the Nutex Corporation as the Security Administrator for their Microsoft 365 Enterprise deployment. They plan to use Microsoft 365 services. One of your goals is to implement Azure AD device-based Conditional Access policies for the Microsoft 365 deployment.

Which of the following statements about device-based Conditional Access policies are TRUE? (Select all that apply.)

- ✗ **A)** Configuring the **Mark devices with no compliance policy assigned as** compliance policy setting of **Compliant** can improve the security posture of the Microsoft 365 deployment.
- ✗ **B)** Compliance status validity periods for Microsoft Intune compliance policies can be set to a maximum of 90 days.

✓ **C)** Intune compliance policies can be configured to remotely retire non-compliant mobile devices.

✓ **D)** Intune compliance policies can be configured to use network location-based compliance rules for mobile devices.

✗ **E)** Intune compliance policies that display a **Conflict** status auto-resolve the conflict within 24 hours.

Explanation

The following statements are true:

- Intune compliance policies can be configured to remotely retire non-compliant mobile devices.
- Intune compliance policies can be configured to use network location-based compliance rules for mobile devices.

Microsoft Intune is a mobile device management (MDM) solution available with Microsoft 365 Business Premium subscriptions. Intune can help protect organizational data by requiring that the users and devices that use the Microsoft 365 services meet certain minimum security requirements. The compliance policies feature in Intune defines rules and settings that users and devices must meet and the actions that must be automated if devices are non-compliant. To set actions that must be automated, go to Microsoft Endpoint Manager admin center > Devices > Compliance policies > Policies. Select a policy, and then select Properties. Select Actions for non-compliance > Add. The actions available are: Send email to end users, Remotely lock the non-compliant device (lock the device and force the user to enter a PIN or passcode to unlock the device), Retire the non-compliant device (remove all company data from the device and remove the device from Intune management), and Send push notification to the end-user.

You can configure network locations on devices and have those locations configured in a compliance rule for the device.

Compliance status validity periods for Microsoft Intune compliance policies can be set to more than 90 days. The compliance status validity period is a setting that specifies a period within which the device managed from Intune must successfully send the compliance status for the compliance policies pushed to it. If a device does not report its compliance status before the validity period expires, the device is flagged as non-compliant. The default setting is 30 days, but you can set it anywhere between 1 and 120 days. Setting a lower value can help you be confident that the devices are consistently secure.

Configuring the **Mark devices with no compliance policy assigned as** compliance policy setting of **Compliant** cannot improve the security posture of the Microsoft 365 deployment. Intune compliance policy settings manage how the policies interact with mobile devices. These settings are distinct from the settings you configure in a device compliance policy. Compliance policy settings can be configured from **Microsoft Endpoint Manager admin center > Endpoint security > Device compliance > Compliance policy settings**. The three compliance policy settings are: Mark devices with no compliance policy assigned as <choice> (how Intune treats devices that have not been assigned a device compliance policy), Enhanced jailbreak detection (for iOS/iPadOS devices, which can track the location of jailbroken devices), and Compliance status validity period (days within which devices must report their compliance status). Marking the devices with no compliance policy assigned to **Compliant** flags devices without Intune compliance policies as “compliant”. This would allow risky devices to sign in to your Microsoft 365 deployment. As a best practice, setting this to “Not compliant” flags devices that do not have Intune policies as non-compliant, which will improve the security posture.

Intune compliance policies that display a **Conflict** status do not auto-resolve the conflict within 24 hours. After you deploy Intune compliance policies, you can check if the policies were successfully enforced or there were issues. To see these details, go to **Microsoft Endpoint Manager admin center > Devices > Compliance policies > Policies**. Select a policy and click **Overview**. Policies display one of the following statuses: Succeeded (policy is applied), Error (policy is not applied), or Conflict. Intune cannot clear the conflict and you should review and update the settings periodically. Conflict has two settings: Pending (the device is not checked in to Intune, so the device has not received the policy yet), and Not applicable (the device cannot receive the policy).

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement conditional access

**References:**

Microsoft Docs > Enterprise Mobility + Security > Microsoft Endpoint Manager > Intune > Use compliance policies to set rules for devices you manage with Intune > Compliance policy settings

Microsoft Docs > Enterprise Mobility + Security > Microsoft Endpoint Manager > Intune > Monitor Intune Device compliance policies > View status of device policies

Microsoft Docs > Enterprise Mobility + Security > Microsoft Endpoint Manager > Intune > Configure actions for noncompliant devices in Intune > Available actions for noncompliance

Microsoft Docs > Enterprise Mobility + Security > Microsoft Endpoint Manager > Intune > Use Locations (network fence) in Intune

## Question #13 of 36

Question ID: 1342911

You have recently joined the Nutex Corporation as the Identity Services Administrator for their hybrid Microsoft 365 Enterprise deployment. Nutex has moved some of its apps and services to the Azure cloud. However, some core services, such as identity management of its employees, are still hosted on Nutex’s premises.

You need to plan for identity-related components and identity synchronization services between the on-premises infrastructure and the Azure cloud.

Which of the following statements about Azure AD Connect and Azure AD Connect sync are TRUE? (Select all that apply.)

✓ **A)** Microsoft cautions against changing the out-of-the box synchronization rules available with Azure AD Connect sync.

✗ **B)** Microsoft recommends that you run at least one synchronization cycle every 30 days.

✗ **C)** The DeviceWriteback feature can be enabled or disabled by using the Set-MsolDirSyncFeature PowerShell cmdlet.

✓ **D)** You cannot make configuration changes in Azure AD Connect when the Azure AD Connect sync scheduler is actively running a synchronization cycle.

✓ **E)** If you enable Staging mode for an Azure AD Connect server that has password hash synchronization enabled, password changes are not synchronized from the on-premises AD.

Explanation

The following statements are true:

- You cannot make configuration changes in Azure AD Connect when the Azure AD Connect sync scheduler is actively running a synchronization cycle.
- Microsoft cautions against changing the out-of-the box synchronization rules available with Azure AD Connect sync.
- If you enable Staging mode for an Azure AD Connect server that has password hash synchronization enabled, password changes are not synchronized from the on-premises AD.

The Azure AD Connect sync component's scheduler in Azure AD Connect synchronizes changes occurring in the on-premises directory using a scheduler. The scheduler runs a synchronization cycle to import, sync, and export changes and other maintenance tasks. This cycle is run every 30 minutes. If you need to make changes to the Azure AD Connect configuration, you must stop the active synchronization cycle. Stopping an active cycle is not harmful, and pending changes are processed when the synchronization runs the next time. To stop an active synchronization cycle, use the **Stop-ADSyncSyncCycle** PowerShell cmdlet.

When Azure AD Connect sync runs for the first time after Azure AD Connect is installed. It uses the default synchronization rules, also known as the out-of-the-box rules, and most of the objects are synchronized. Microsoft recommends that you clone an out-of-the-box rule, edit it, and assign a higher priority (lower value) if you want to modify an out-of-the-box rule. The out-of-box sync rules use a thumbprint. If you edit these rules, the thumbprint does not match, which may cause synchronization issues when you upgrade to a newer version of Azure AD Connect. Therefore, Microsoft cautions against changing the rules.

The Azure AD Connect server can be set to be in the Staging mode. Staging mode can help you run full import and synchronization to verify that all changes are applied to the production environment. Servers in the Staging mode do not run any exports; also, features such as password sync and password writeback do not run, even if they are enabled. Exports and password sync and writeback features start to work when you disable Staging mode.

Microsoft recommends that you run at least one synchronization cycle every 7 days, not 30. According to the design principles for Azure AD, a delta sync needs to happen within 7 days from the last delta sync, and a delta sync (following a full sync) needs to happen within 7 days from the last full sync. Every 30 minutes, a synchronization cycle is run. Microsoft cautions that not running a synchronization cycle once every 7 days may cause synchronization issues, and this will always require that you run a full synchronization cycle.

The DeviceWriteback feature cannot be enabled or disabled by using the Set-MsolDirSyncFeature PowerShell cmdlet. The synchronization feature with Azure AD Connect uses two components: an on-premises component named Azure AD Connect sync and the Azure AD Connect sync service in Azure AD. To see the current configuration and settings for the options in the Azure AD Connect sync, use the Get-MsolDirSyncFeatures cmdlet. Many of these options can be edited only from the Azure AD Connect UI. Some of these options, such as EnableSoftMatchOnUpn and SynchronizeUpnForManagedUs, can be edited using PowerShell.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Secure Microsoft 365 hybrid environments

**References:**

Microsoft Docs > Azure > Active Directory > Hybrid identity > Azure AD Connect sync: Scheduler > Stop the schedulerMicrosoft Docs > Azure > Active Directory > Hybrid identity > Azure AD Connect sync: Scheduler > Overview

Microsoft Docs > Azure > Active Directory > Hybrid identity > Azure AD Connect sync: Best practices for changing the default configuration

Microsoft Docs > Azure > Active Directory > Hybrid identity > Azure AD Connect sync: Understanding the default configuration > Out-of-box rules from on-premises to Azure AD

Microsoft Docs > Azure > Active Directory > Hybrid identity > Azure AD Connect sync service features

Microsoft Docs > Azure > Active Directory > Hybrid identity > Azure AD Connect: Staging server and disaster recovery > Staging mode

---

## Question #14 of 36

Question ID: 1427376

You are the Director of Shipping Operations for the Nutex Company. Your user account has limited administrator directory roles.

To better streamline the company’s operations, you are setting up B2B external collaboration with many of Nutex’s suppliers. You are performing a bulk invite and creating a .CSV file that includes the users of each supplier. Two values are required for each guest user listed in the CSV file.

Which options are required to complete this objective? (Choose all that apply.)

- ✓ **A)** The URL to which the invited user is forwarded after accepting the invitation
- ✗ **B)** The Relative Distinguished Name of each invited user
- ✓ **C)** The email address of each user that will receive the invitation
- ✗ **D)** A onetime password that invited users must use at first logon
- ✗ **E)** A newly assigned Nutex email address for each invited user

Explanation

A bulk invite can be performed via the creation and uploading of a .CSV template. Each invited user is represented by a separate line on the spreadsheet. There are two required properties for each user. The first required property is the email address of each invited user, which is the email address at their own parent organization. The second required property is the redemption URL that will appear in the invitation email. The .CSV template must include the version number in the first row. The following is an example of a bulk upload CSV template:

| **version:v1.0** | |
|---|---|
| DebrahSigna@verigon.com | https://app5.azure.com |
| Laura.Dasovich@verigon.com | https://app5.azure.com |
| JeffWarne@verigon.com | https:/NutexApp.azure.com |
| DaveArcher@metroil.com | https:/NutexApp.azure.com |
| ChrisMiller@metroil.com | https:/NutexApp.azure.com |
| BobbyHebert@dreamsuites.com | https://Dapp.azure.com |

A Relative Distinguished Name (RDN) is not required because it is only used for on-premises AD, not Azure AD. The following is an example of a CN=DaveArcher,OU=Marketing,DC=Metroil,DC=COM.

For B2B collaborations, external users are not assigned email addresses of the inviting organization.

A bulk invite does not require the invited user to enter a one-time password when they accept the invitation and click the redeption URL.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Secure Identities

**References:**

Microsoft Docs > Learn > Browse > Implement and manage external identities > Invite external users - individually and in bulk

## Question #15 of 36

Question ID: 1427377

You are rolling out Windows Hello for Business to Windows 10 version 1703 or later computers in the Marketing department as part of a hybrid deployment model. A Group Policy Object has been configured to enable Windows Hello for Business for all users in the department.

You notice that the Windows Hello for Business provisioning experience does not launch after users sign in on certain computers within the Marketing department.

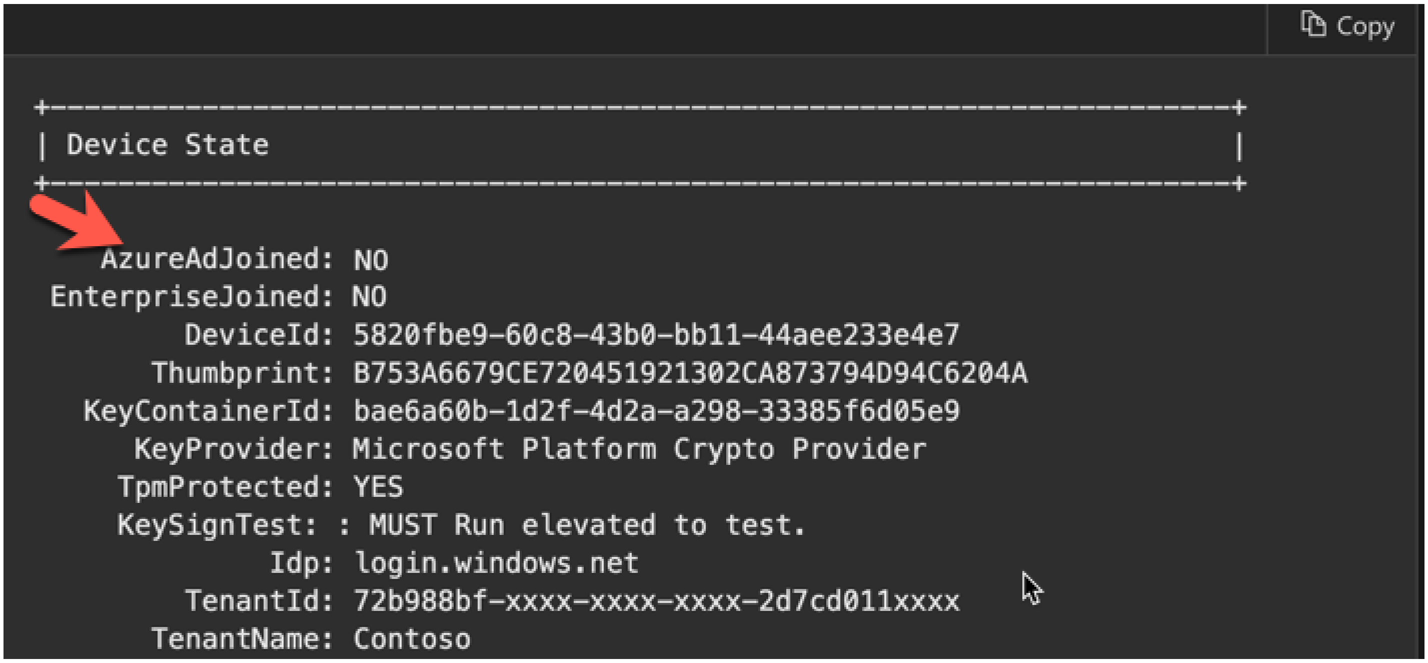
One reason why the Windows Hello for Business provisioning experience does not launch after users sign in is that computers may not be connected Azure AD, and users log in with a cached credential.

What can you run on each computer to verify the Azure AD-joined and domain-joined statuses of a computer?

- ✗ **A) Get-ExecutionPolicy**
- ✓ **B) dsregcmd**
- ✗ **C)** check the status of the Windows Hello for Business Group Policy Object in the Group Policy Management Console
- ✗ **D) Get-Service**

Explanation

The dsregcmd /status can be viewed to see what the AzureAdJoined and DomainJoined statuses are. For example, if the AzureAdJoined value reads "NO", as shown in the screenshot below, that means the computer has not processed the device registration and Windows Hello for Business provisioning has not yet begun. A computer must be domain-joined, or Azure AD-joined in a hybrid Azure Active Directory scenario, for Windows Hello for Business to work. This option will allow you to see the Azure AD-joined and domain-joined statuses of a computer.



```
+---------------------------------------------------------------------+
| Device State                                                        |
+---------------------------------------------------------------------+

    AzureAdJoined: NO
 EnterpriseJoined: NO
         DeviceId: 5820fbe9-60c8-43b0-bb11-44aee233e4e7
       Thumbprint: B753A6679CE720451921302CA873794D94C6204A
   KeyContainerId: bae6a60b-1d2f-4d2a-a298-33385f6d05e9
      KeyProvider: Microsoft Platform Crypto Provider
     TpmProtected: YES
     KeySignTest: : MUST Run elevated to test.
              Idp: login.windows.net
         TenantId: 72b988bf-xxxx-xxxx-xxxx-2d7cd011xxxx
       TenantName: Contoso
```

The Windows Hello for Business Group Policy Object can be used to enable users to enroll and use Windows Hello for Business. This option will not allow you to see the Azure AD and domain-joined statuses of a computer.

The **Get-ExecutionPolicy** cmdlet allows you to see the configured level of security to execute PowerShell scripts. This option will not allow you to see the Azure AD-joined and domain-joined statuses of a computer.

The **Get-Service** cmdlet allows you to see a running list of all services that are installed on the Windows 10 device. This option will not allow you to see the Azure AD and domain-joined statuses of a computer.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement authentication methods

**References:**

Microsoft Docs > Windows > Security > Identity and access protection > Hybrid Windows Hello for Business Provisioning

Microsoft Docs> Windows > Security > Identity and access protection > Planning a Windows Hello for Business Deployment

---

## Question #16 of 36

Question ID: 1342913

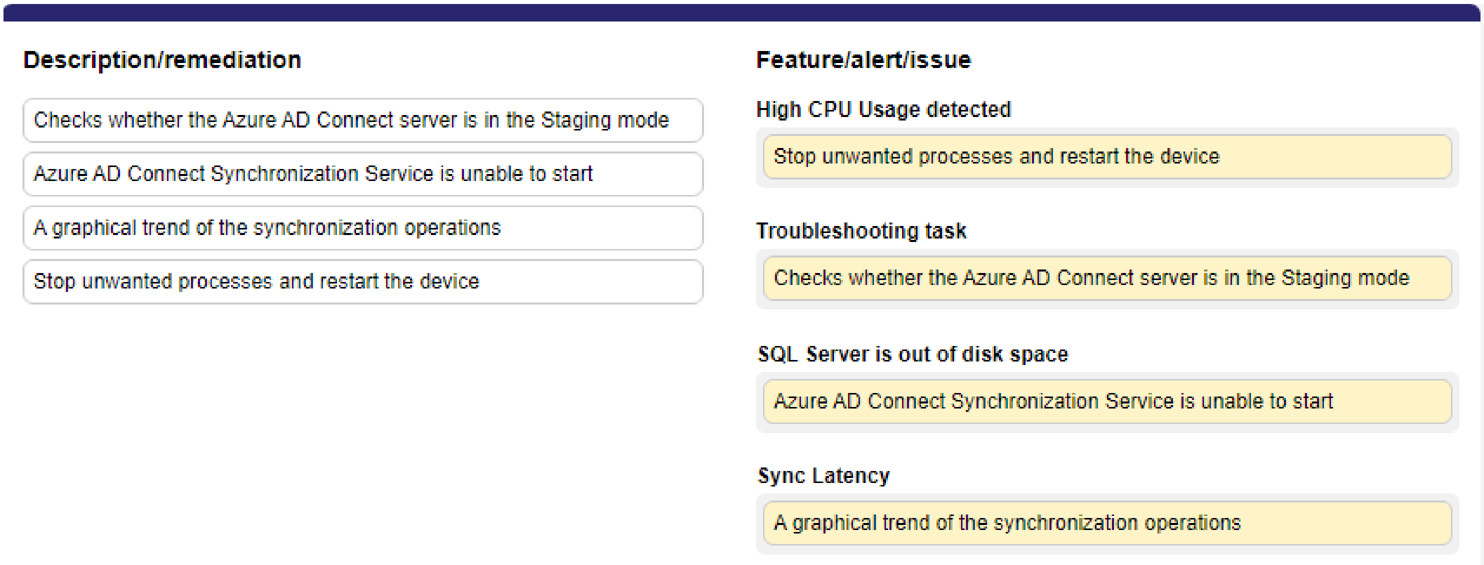
You have recently joined the Nutex Corporation as the Microsoft 365 administrator. Nutex wants to purchase Microsoft 365 licenses. However, the Infrastructure Services team has suggested using a hybrid environment consisting of the on-premises AD FS infrastructure and Microsoft 365 services. To make this happen, you will need to implement Azure AD Connect. You must instruct your team to closely monitor the Azure AD Connect implementation using Azure AD Connect Health alerts and other Azure AD Connect tools and features.

Match the description/remediation (on the left) with their feature/alert/issue associated with Azure AD Connect (on the right).

{UCMS id=5766723782311936 type=Activity}

Explanation

You would map the descriptions/remediations to their feature/alert/issue as follows:



**Description/remediation**

Checks whether the Azure AD Connect server is in the Staging mode

Azure AD Connect Synchronization Service is unable to start

A graphical trend of the synchronization operations

Stop unwanted processes and restart the device

**Feature/alert/issue**

**High CPU Usage detected**

Stop unwanted processes and restart the device

**Troubleshooting task**

Checks whether the Azure AD Connect server is in the Staging mode

**SQL Server is out of disk space**

Azure AD Connect Synchronization Service is unable to start

**Sync Latency**

A graphical trend of the synchronization operations

High CPU usage detected is one of the alerts available with Azure AD Connect Health. This alert is seen when the percentage of CPU consumption on a device crosses a defined threshold. To remediate this, first check whether this is a temporary spike. If you get alerts for this consistently, check the list of processes on the device and stop any that are not needed. If the issue continues to persist, restart the device. If none of these steps work, consider adding more resources to the device.

The troubleshooting task is a wizard available with Azure AD Connect version 1.1.614.0 and later. You can use this to troubleshoot object synchronization issues. During an Azure AD Connect deployment, if you come across an issue where no local passwords are synchronized using password-hash synchronization with Azure AD, you can run the troubleshooting task. This wizard validates that the password hash synchronization feature is enabled for the Azure AD tenant, validates that the Azure AD Connect server is not in Staging mode, and does self-checks on the on-premises Active Directory connectors (corresponds to an existing Active Directory forest).

Azure AD Connect requires an SQL database to store identity data. You can use the default SQL Server Express LocalDB installed with Azure AD Connect or use your own SQL license. SQL Server Express imposes a 10 GB size limit. When this limit is reached, Azure AD Connect Synchronization Service cannot start or synchronize properly. As a temporary fix to recover from this issue, use the Shrink operation and free up enough database space to start the Synchronization Service. This will free up space by removing whitespaces in the database.

Sync Latency can provide a graphical trend of the latency during the Azure AD Connect sync operations (import, export, etc.) for connectors. This can also help you detect anomalies in the latency that may require further investigation. The Azure AD Connect Health Alerts for sync section provides you the list of active alerts.

**Objective:**

Implement and manage identity and access

**Sub-Objective:**

Secure Identities

**References:**

Microsoft Docs > Azure > Active Directory > Hybrid identity > Azure Active Directory Connect Health Alert Catalog > Alerts for Azure AD Connect (Sync)

Microsoft Docs > Azure > Active Directory > Hybrid identity > Troubleshoot password hash synchronization with Azure AD Connect sync > No passwords are synchronized: troubleshoot by using the troubleshooting task

Microsoft Docs > Azure > Active Directory > Hybrid identity > Azure AD Connect: How to recover from LocalDB 10-GB limit

---

## Question #17 of 36

Question ID: 1342924

You have recently joined the Nutex Corporation as the Security Administrator for their Microsoft 365 Enterprise deployment. One of your primary goals is to implement an effective access strategy for apps and services on the Microsoft cloud. You want to leverage the Azure AD Conditional Access policies feature to secure access to apps and services. You plan to implement multiple common Conditional Access policies that Microsoft recommends.

Which of the following statements about implementing common Conditional Access policies are TRUE? (Select all that apply.)

- ✗ **A)** Device-based Conditional Access policies can only block access based on device compliance factors such as a PIN to unlock, minimum encryption on device, and operation system versions.
- ✓ **B)** Microsoft recommends that you use Conditional Access report-only mode before you implement a Block Access Conditional Access policy.
- ✓ **C)** For sign-ins originating from trusted network locations defined in a Conditional Access policy, the sign-in risks are lowered.
- ✓ **D)** Conditional Access policies can be configured with Sign-in risk or User risk as a condition.
- ✓ **E)** Microsoft strongly recommends that you enable Conditional Access policies that require MFA for privileged Azure AD accounts.

Explanation

The following statements are TRUE:

- Microsoft strongly recommends that you enable Conditional Access policies that require MFA for privileged Azure AD accounts.
- Conditional Access policies can be configured with Sign-in risk or User risk as a condition.
- For sign-ins originating from trusted network locations defined in a Conditional Access policy, the sign-in risks are lowered.

- Microsoft recommends that you use Conditional Access report-only mode before you implement a Block access Conditional Access policy.

One of the Conditional Access policies for new deployments is the Require MFA for administrators policy. This policy forces users to use MFA to access apps and services. For accounts with administrative rights in Azure AD, enforcing MFA reduces the risk of the accounts being compromised. Microsoft recommends you require MFA on the following administrator roles at a minimum: Authentication, Billing, Conditional Access, Exchange, Global, Helpdesk, Password, Security, SharePoint, and User administrator.

You can create Sign-in and User risk policies from Azure AD Identity Protection. You can also create Conditional Access policies with Sign-in risk or User risk as a condition. Additional conditions that you can add with Conditional Access policies and not Identity Protection policies is controls by device platforms, locations, client apps, and device states. Sign-in risk analyzes sign-ins and calculates a risk score based on the probability that the sign-in was not performed by the actual owner user. User risk calculates the probability that an identity has been compromised, based on the baseline it sets as normal user behavior.

You can add Conditional Access policies that block or allow (as trusted) sign-ins from specific IP address ranges, countries, and regions. You can add network locations with specific IP address ranges or countries/regions on the Azure portal and use them in Conditional Access policies. An example of this is a policy to detect a sign-in risk and require MFA for users accessing a service when they are off the corporate network. Marking a network location as a trusted location lowers the sign-in risk for sign-ins originating from that location.

A Block Access Conditional Access policy is a conservative cloud migration approach that is primarily used when Microsoft 365 apps and services are not used as the production environment. Misconfiguring a Block Access policy can lead to all users being locked out of the Azure portal. You must test and validate a Block Access policy before enabling it. You can use Microsoft tools such as Conditional Access report-only mode and the What If tool in Conditional Access to gauge the impact before implementing Block Access policies.

The device-based Conditional Access policies can both grant or block access based on device compliance factors, such as needing a PIN to unlock, minimum encryption on device, operation system versions, and the device is not rooted or jailbroken. Devices here refer to both computing devices and mobile phones. When you select a condition as Require device to be marked as compliant, the device must be Microsoft Intune compliant. If the device is non-compliant, you must enroll the device in Intune. Intune marks devices as compliant based on factors such as a PIN to unlock, minimum encryption on device, operation system versions, and the device is not rooted or jailbroken.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement conditional access

**References:**

Microsoft Docs > Azure > Active Directory > Conditional Access > Plan a Conditional Access deployment

Microsoft Docs > Azure > Active Directory > Conditional Access: Require MFA for administrators

Microsoft Docs > Azure > Active Directory > Identity Protection policies > Custom Conditional Access policy

Microsoft Docs > Azure > Active Directory > Conditional Access: User risk-based Conditional Access

Microsoft Docs > Enterprise Mobility + Security > Microsoft Endpoint Manager > Intune > Protect > Create a device-based Conditional Access policy

Microsoft Docs > Azure > Active DIrectory > Conditional Access: Block access

---

## Question #18 of 36

Question ID: 1342917

You are the Microsoft 365 Security Administrator at the Nutex Corporation. Your team implemented multi-factor authentication (MFA) for Microsoft 365 users two months ago, and has ensured that all Microsoft 365 users have enrolled in MFA.

You are required to provide a status report to top management, detailing the current status of the MFA implementation. You want to leverage the MFA reports feature available on Azure AD to track the current status.

Which of the following statements about MFA reports and security management are TRUE? (Select all that apply.)

- ✓ **A)** Result codes of the sign-ins can only be viewed in the downloaded (CSV or JSON) copy of the Sign-ins report.
- ✗ **B)** Password spray is a type of risk detection mechanism on Azure AD that indicates that a user's valid credentials have been leaked.
- ✗ **C)** The Sign-ins report does not contain data about the client app that users used to connect to the Azure AD tenant.
- ✓ **D)** The Sign-ins activity report is available for all the editions of Azure AD.
- ✗ **E)** The Sign-ins report is always up-to-date in real-time and available on the Azure portal.

Explanation

The following statements are true:

- The Sign-ins activity report is available for all the editions of Azure AD.
- Result codes of the sign-ins can only be viewed in the downloaded (CSV or JSON) copy of the Sign-ins report.

The Sign-ins activity report is one of the five MFA reports available on Azure AD and contains data about the users' sign-in activities. Some of the information displayed are the names and usernames of the users, their sign-in status, the applications to which they signed in, the location from which the users signed in, and the Conditional Access policies that were enforced on the sign-ins. This report is available for all Azure AD editions, with the following default data retention periods: Azure AD Free (7 days), Azure AD Premium 1 (30 days), and Azure AD Premium 2 (30 days).

Result codes in a Sign-ins report indicate the result of the sign-in activities. For example, FAILED_AUTH_RESULT_TIMEOUT denotes that the user took longer than allowed to complete the MFA sign-in attempt, and FAILED_SMS_OTP_INCORRECT denotes that the one-time passcode (OTP) that the user entered was incorrect and the sign-in was not authenticated (access denied). These result codes are not visible on the Azure portal. You can see these codes only when you download the Sign-ins report in CSV or JSON format.

Password spray is not a type of risk detection mechanism on Azure AD that indicates that a user's valid credentials have been leaked. Password spray is an attack method that is used by hackers to access a large number of usernames using a few commonly used passwords. Azure AD uses the Identity Protection feature to identify risky sign-ins and risky users (user accounts that may have been compromised). Identity Protection leverages Microsoft’s learnings from the customers’ usage of Azure AD, the consumer space with Microsoft accounts, and the security practices used to protect Xbox users. Microsoft analyzes up to 6.5 trillion signals a day to identify and protect its customers from threats. Azure AD threat intelligence uses Microsoft's internal and external threat intelligence sources to identify a known attack pattern. Risks are detected and classified as follows:

- Sign-in from an unusual location based on the user's recent sign-ins
- Sign-in from an anonymous IP address, such as from Tor browser or anonymizer VPNs
- Sign-in with unusual properties for the given user
- Sign-in from a malware linked IP address
- Valid users’ credentials that have been leaked
- Password spray, which indicates that multiple usernames are being attacked using common passwords in a unified brute force manner.

The Sign-ins report does contain data about the client app that users used to connect to the Azure AD tenant, if configured. To see the Sign-in reports for a tenant, go to the **Azure portal**, select **Azure Active Directory**, and click **Sign-ins** under **Monitoring**. You will see all the sign-ins performed by users on the Sign-ins page. Some of the attributes listed are names and usernames of the users, their sign-in status, the applications to which the users signed in, the location from which the users signed in, and the Conditional Access policies that were enforced on the sign-ins. You can add more attributes (as columns) for the sign-ins to see a more detailed view of the sign-ins. One such column is Client app, which lists the client apps that users used to sign in. Examples of client apps include Exchange ActiveSync, POP3, mobile apps, desktop clients, and browser.

The data on the Sign-ins report is not updated in real-time and available on the Azure portal. The Sign-ins report is updated with an expected latency (at any given point in time) of two minutes for 95% of the sign-ins and five minutes for 99% of the sign-ins.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**

Implement authentication methods

**References:**

Microsoft Docs > Azure > Active Directory > Authentication > Use the sign-ins report to review Azure AD Multi-Factor Authentication events

Microsoft Docs > Azure > Active Directory > Reports and monitoring > Sign-in activity reports in the Azure Active Directory portal

Microsoft Docs > Azure > Active Directory > Identity Protection > What is Identity Protection?

Microsoft Docs > Azure > Active Directory > Reports and monitoring > Sign-in activity reports in the Azure Active Directory portal > Filter sign-in activitiesMicrosoft Docs > Azure > Active Directory > Reports and monitoring > Sign-in activity reports in the Azure Active Directory portal > Download sign-in activities

Microsoft Docs > Azure > Active Directory > Authentication > Use the sign-ins report to review Azure AD Multi-Factor Authentication events > Downloaded activity reports result codes

Microsoft Docs > Azure > Active Directory > Reports and monitoring > Azure Active Directory reporting latencies > Activity reports

## Question #19 of 36

Question ID: 1342920

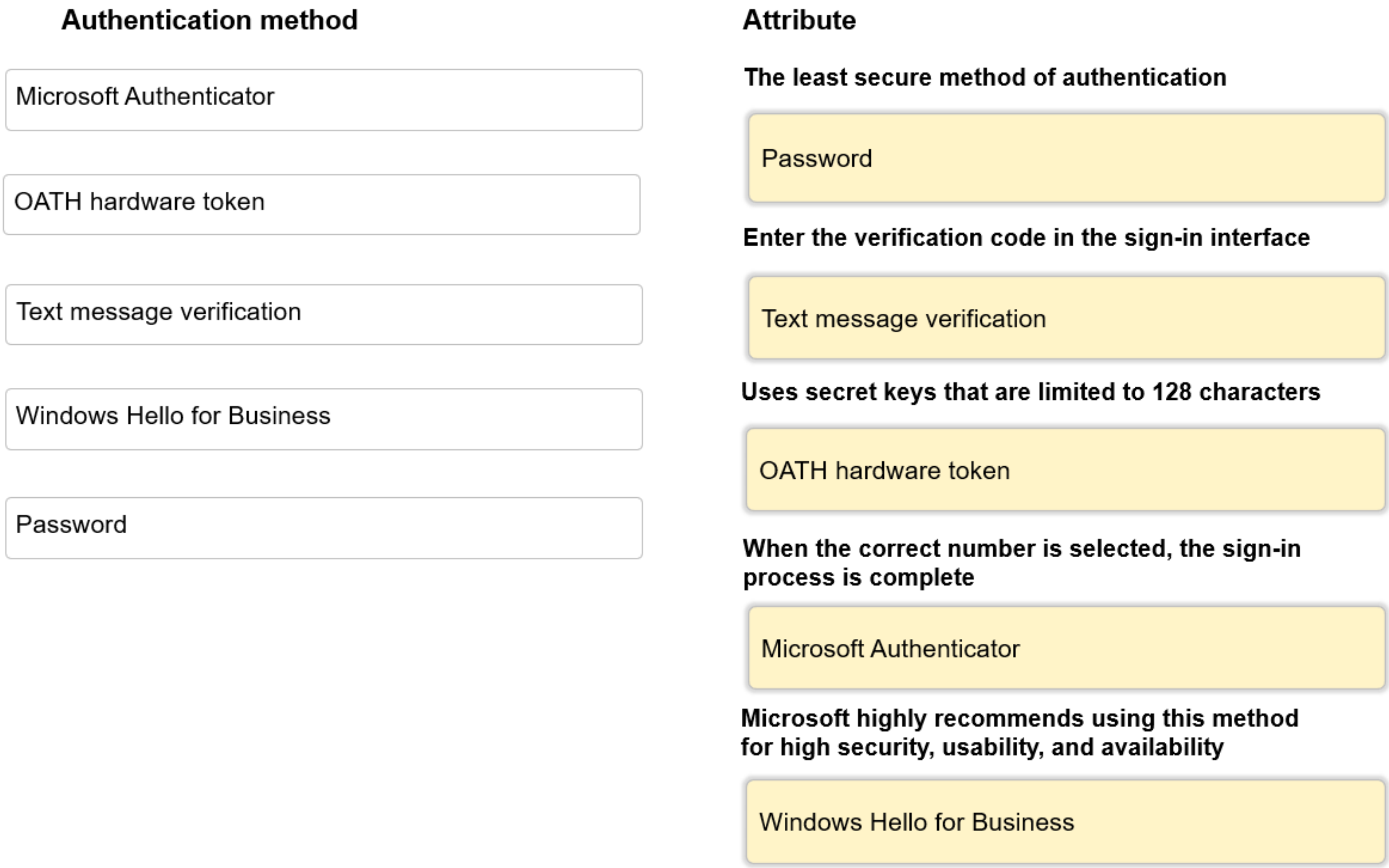
You are the Authentication Administrator for the Nutex Corporation's Microsoft 365 Enterprise deployment. Nutex manages the apps and services in their on-premises infrastructure and have recently moved to the Azure cloud. One of your first goals is to set up viable authentication methods for users who access the Azure cloud.

Match the authentication methods available on the Azure cloud (on the left) with their attribute (on the right).

{UCMS id=5164142286602240 type=Activity}

Explanation

You would map the authentication methods with their attribute as follows:



**Authentication method**

Microsoft Authenticator

OATH hardware token

Text message verification

Windows Hello for Business

Password

**Attribute**

**The least secure method of authentication**

Password

**Enter the verification code in the sign-in interface**

Text message verification

**Uses secret keys that are limited to 128 characters**

OATH hardware token

**When the correct number is selected, the sign-in process is complete**

Microsoft Authenticator

**Microsoft highly recommends using this method for high security, usability, and availability**

Windows Hello for Business

Microsoft Authenticator is a mobile app that provides an additional security level to users with an Azure AD work or school account or a Microsoft account. This app is available for Android, iOS, and Windows Phone platforms. It can be used to authenticate users in a password-less way during sign-in. This app can also be used as an additional verification option during SSPR or Azure MFA events. With the password-less way of signing in, instead of seeing a prompt for a password after entering a username, the user sees a message on their phone or tablet to tap a number in the app. When the correct number is selected, the sign-in process is complete.

With Azure AD, you can use OATH-TOTP SHA-1 tokens for authentication. These tokens refresh authentication codes every 30 to 60 seconds. Azure AD customers/tenants can purchase these OATH hardware tokens from the vendor of their choice. The hardware tokens use a secret key or seed that is pre-programmed in the token and are a maximum of 128 characters in length. You must input the secret key into the Azure portal to be authenticated. You can also import a CSV file with the UPNs, serial numbers, secret keys, time intervals, manufacturer names, and models of the hardware tokens to the Azure portal. Go to Azure portal > **Azure Active Directory > Security > MFA > OATH tokens** and upload the CSV file.

With the Text message verification method, an SMS is sent to the mobile phone number listed for the user containing a verification code. To complete the sign-in process, users must enter the verification code into the sign-in interface.

For Windows 10 devices used to access Microsoft 365 apps and services, Windows Hello for Business replaces passwords with two-factor authentication. Windows Hello for Business uses a new type of user credential tied to a device and uses a biometric feature (facial or fingerprint recognition) or PIN.

Of all the methods of authentication available on Azure AD, a password is the least secure. For SSPR or MFA, choose the methods that meet or exceed your organization's requirements in terms of security, usability, and availability. Microsoft recommends Windows Hello for Business and the Microsoft Authentication app as the best methods for multiple authentication.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement authentication methods

**References:**

Microsoft Docs > Azure > Active Directory > Authentication > Authentication methods in Azure Active Directory - Microsoft Authenticator app > Passwordless sign-in

Microsoft Docs > Azure > Active Directory > Authentication > Authentication methods in Azure Active Directory - OATH tokens > OATH hardware tokens (preview)

Microsoft Docs > Azure > Active Directory > Authentication > Authentication methods in Azure Active Directory - phone options > Text message verification

Microsoft Docs > Windows > Security > Identity and access protection > Windows Hello for Business Overview

Microsoft Docs > Azure > Active Directory > Authentication > What authentication and verification methods are available in Azure Active Directory? > Authentication method strength and security

## Question #20 of 36

Question ID: 1342910

The Nutex Corporation uses an on-premises Active Directory infrastructure that handles the identity management and authentication for the apps and services that they use. Nutex is considering migrating to Azure AD for identity management, authentication, and other security features available in Azure. You have been hired as the Authentication Administrator for Nutex. You must consider the pros and cons of using a pure cloud-based vs a hybrid solution.

Which of the following statements about authentication methods and capabilities available with Azure AD are TRUE? (Select all that apply.)

✓ **A)** You can use Seamless SSO with both password hash and pass-through authentication methods.

✗ **B)** Security key sign-in with FIDO2 security keys is the only password-less authentication method available with Azure AD.

✗ **C)** The Azure AD Smart Lockout feature locks a user's account when the same bad password is entered multiple times.

✓ **D)** For MFA, Microsoft recommends using the Microsoft Authenticator app because it meets the National Institute of Standards and Technology Authenticator Assurance Levels.

✓ **E)** Microsoft recommends that you use password hash synchronization as a backup authentication method for pass-through authentication.

<u>Explanation</u>

The following statements are true:

- For MFA, Microsoft recommends using the Microsoft Authenticator app because it meets the National Institute of Standards and Technology Authenticator Assurance Levels.
- You can use Seamless SSO with both password hash and pass-through authentication methods.
- Microsoft recommends that you use password hash synchronization as a backup authentication method for pass-through authentication.

Multi-factor authentication (MFA) requires that administrators select the multiple authentication methods that they want for users. You can use the following methods for authentication: notification through a mobile app (a push notification is sent to the Microsoft Authenticator app on the user's mobile device), verification code from mobile app (user enters the Initiative for Open Authentication (OATH) verification code that the Microsoft Authenticator app renews every 30 seconds), call to phone (automated voice gives the code during the call), and text message to phone (verification code must be entered at sign-in).

The Microsoft Authenticator app b meets the National Institute of Standards and Technology Authenticator Assurance Levels for MFA.

A hybrid identity solution that consists of Azure AD and an on-premises Active Directory infrastructure can be set up for authentication. You can do this in two ways: cloud-based (authentication happens on Azure AD) and federated (AD FS does the authentication). Cloud-based authentication can either be password hash or pass-through. These methods can be used with the Seamless SSO feature to allow users to use a single sign-on to cloud resources from domain-joined devices in the on-premises network.

For business continuity, Microsoft recommends that you deploy two extra pass-through authentication agents in addition to the first agent on the Azure AD Connect server. As a second layer of continuity, Microsoft recommends using password hash synchronization as a backup authentication method to pass-through authentication. Currently, failover does not happen automatically. You must switch the sign-on method manually, in Azure AD Connect.

Security key sign-in with FIDO2 security keys is not the only password-less authentication method available with Azure AD. Other password-less methods are Windows Hello for Business and phone sign-in with the Microsoft Authenticator app. Eliminating passwords from authentication can reduce the attack surface. It can also improve the user experience during logins. The FIDO (Fast IDentity Online) Alliance promotes open authentication standards and plans for measures to reduce passwords as a form of authentication. FIDO published the latest standard, FIDO2, which is a web authentication (WebAuthn) standard. FIDO2 security keys are an unphishable standards-based password-less authentication method. They can be a USB device, Bluetooth, or near field communication (NFC) security key.

The Azure AD Smart lockout feature does not lock out a user's account when the same bad password is entered multiple times. The smart lockout feature helps lockout attempts from bad actors that try to guess a valid user's password or use brute-force methods to get the password. By default, smart lockout locks the account for one minute after ten failed attempts. After each subsequent failed sign-in attempt, the account is locked out again for one minute at first and becomes more prolonged for each additional attempt. Smart lockout treats multiple attempts with the same bad password as actual user behavior and does not lock out the account.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Secure Microsoft 365 hybrid environments

**References:**

Microsoft Docs > Azure > Active Directory > Authentication > Plan a passwordless authentication deployment in Azure Active Directory > Passwordless authentication methods

Microsoft Docs > Azure > Active Directory > Authentication > Plan an Azure AD Multi-Factor Authentication deployment > Plan authentication methods

Microsoft Docs > Azure > Active Directory > Hybrid identity > Choose the right authentication method for your Azure Active Directory hybrid identity solution > Comparing methods

Microsoft Docs > Azure > Active Directory > Authentication > Protect user accounts from attacks with Azure Active Directory smart lockout

Microsoft Docs > Azure > Active Directory > Identity protection > How To: Configure and enable risk policies > Choosing acceptable risk levels

---

## Question #21 of 36

Question ID: 1365721

You have to assume an Azure AD role. Which actions should you perform in the Azure portal?

Choose the appropriate choices from the left and place them in the correct order.

{UCMS id=5540919819370496 type=Activity}

Explanation

You should choose the following:

1. Open Azure AD Privileged Identity Management.
2. Select **My roles** and choose the appropriate role.
3. Select **Additional verification required**.
4. In the **Reason** box, enter the reason for the activation request.
5. Select **Activate**.

To take on an Azure AD role, you must request activation by selecting **My roles** in Privileged Identity Management. From the list of eligible Azure AD roles, you would choose the appropriate role to activate. Once you have selected the role, you will open the Activate pane. You need to select **Additional verification required** to provide additional security verification via multi-factor authentication. You only need to authenticate once per session. Before you activate the role, you must enter the reason for the activation request in the **Reason** box. Lastly, you would select **Activate**.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Privileged Identity Management (PIM)

**References:**

HYPERLINK "https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role?tabs=new" HYPERLINK "https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-activate-role?tabs=new" Activate my Azure AD roles in PIM - Azure Active Directory | Microsoft DocsMicrosoft Docs > Azure > Active Directory > Privileged Identity Management > Activate my Azure AD roles in PIM

---

## Question #22 of 36

Question ID: 1365719

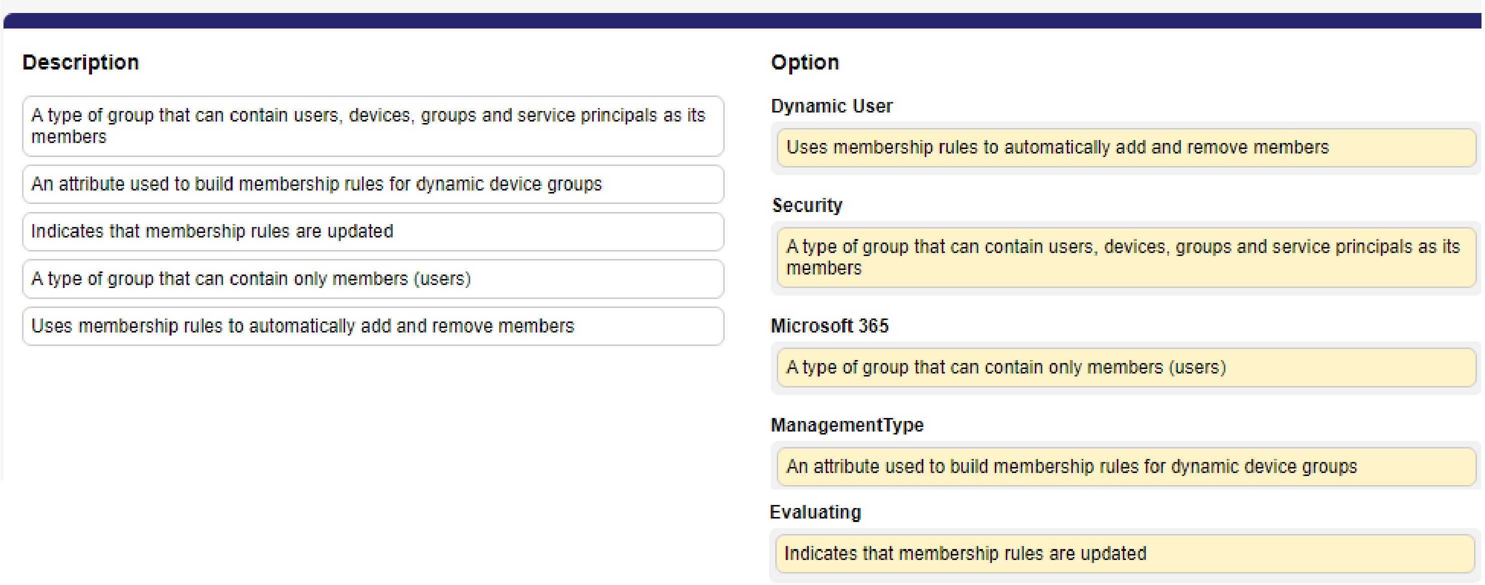
You are the Microsoft 365 administrator at the Nutex Corporation. The company is expanding rapidly and you need to make the necessary arrangements to reduce the effort to manage access to the Microsoft 365 services on the Azure cloud. You need to come up with strategies to group your Microsoft 365 users and the resources they are using.

Match the description of the Groups feature on the Azure cloud (on the left) with the options available (on the right).

{UCMS id=5733302930505728 type=Activity}

Explanation

You would map the descriptions to the options as follows:



**Description**

A type of group that can contain users, devices, groups and service principals as its members

An attribute used to build membership rules for dynamic device groups

Indicates that membership rules are updated

A type of group that can contain only members (users)

Uses membership rules to automatically add and remove members

**Option**

Dynamic User

Uses membership rules to automatically add and remove members

Security

A type of group that can contain users, devices, groups and service principals as its members

Microsoft 365

A type of group that can contain only members (users)

ManagementType

An attribute used to build membership rules for dynamic device groups

Evaluating

Indicates that membership rules are updated

Dynamic user is a type of group membership available with the Azure AD Groups feature. When you create a group with this type of membership, you add dynamic membership rules to automatically add and remove members. When members' attributes change, Azure looks at the dynamic membership rules for the directory. Members who meet the rules are added to the group. Members who no longer meet the requirements of the rule are removed. Other membership types are **assigned** which are manually added by users and **dynamic devices** which are devices that are added by the dynamic membership rules for those devices.

The two types of Azure AD groups you can create are Security and Office 365. Security groups are used to manage members and computer access to shared resources for a group of users. A security group can contain users, devices, groups, and service principals as its members and users and service principals as its owners.

Microsoft 365 groups can help you share member access to a mailbox, calendar, files, or a SharePoint site. A Microsoft 365 group can have only users as its members. Both users and service principals can be owners of a Microsoft 365 group.

You can create dynamic device groups on Azure AD to group devices by their attributes, such as OS, manufacturer, and model. You would use the Rule Builder to create membership rules as expressions, using the attributes and operators supported with Rule Builder. You can construct up to five expressions on Rule Builder. The ManagementType attribute can be used to add devices based on how they are managed within Microsoft services. You can specify the following values for this attribute: MDM or PC. Use MDM for mobile devices and PC for computers managed by the Intune PC agent. For example, `device.managementType -eq "MDM"`.

With dynamic groups, if you make changes to the membership rules, the members must be evaluated against the new rules. When the memberships are re-processed, they can display one of the following statuses: Evaluating (group changes have been received and the updates are being evaluated), Processing (updates are being processed), Update complete (groups have been updated using the new rules), Processing error (update could not be completed because of an error found while evaluating the membership rule), and Update paused (dynamic membership rule updates have been paused by the administrator).

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Secure Identities

**References:**

Microsoft Docs > Azure > Active Directory > Fundamerntals > Create a basic group and add members using Azure Active Directory > Membership typesMicrosoft Docs > Azure > Active Directory > Fundamentals > Create a basic group and add members using Azure Active Directory > Group types

Microsoft Support > Learn about Microsoft 365 Groups

Microsoft Docs > Azure > Active Directory > Dynamic membership rules for groups in Azure Active Directory > Rules for devices

Microsoft Docs > Azure > Active Directory > Create or update a dynamic group in Azure Active Directory > Check processing status for a rule

---

## Question #23 of 36

Question ID: 1342921

You have recently joined the Nutex Corporation as the Security Administrator for their Microsoft 365 Enterprise deployment. They plan to use Microsoft 365 services.

First, you must choose a suitable Microsoft 365 subscription for Nutex. One of your future goals is to implement Azure AD Conditional Access policies for all users, apps, and devices in the Microsoft 365 deployment.

Which of the following statements about Azure AD Conditional Access policies are TRUE? (Select all that apply.)

- ✓ **A)** Conditional Access policies can be evaluated for their impact before enforcing them.
- ✗ **B)** Conditional Access policy features are available with all Microsoft 365 Business subscriptions.
- ✓ **C)** Conditional Access policies can be evaluated to understand why a policy was or was not applied to a user in a specific circumstance.
- ✗ **D)** Conditional Access policies can control user access only by one of the following three conditions: location, device platform, and client apps.
- ✗ **E)** Conditional Access policies enhance security at the cost of decreasing user productivity.

Explanation

The following statements are true:

- Conditional Access policies can be evaluated to understand why a policy was or was not applied to a user in a specific circumstance or if a policy would apply in a known state.
- Conditional Access policies can be evaluated for their impact before enforcing them.

The What If tool available with the Conditional Access feature can help you evaluate and understand why a policy was or was not applied to a user in a specific circumstance or if a policy would apply in a known state. You can access it from Azure portal > Azure Active Directory > Conditional Access > What If. The What If tool can analyze issues with policies based on the following parameters/scopes: User, Cloud apps or actions, IP address, Country/Region, Device platform, Client apps (preview), Device state (preview), and Sign-in risk. You would analyze the results to troubleshoot issues with policies.

Before enforcing Conditional Access policies, you must factor in the number and names of users who will be impacted by the policies. This is important for policies that block legacy authentication, require multi-factor authentication, or implement sign-in risk evaluation. You can use the report-only mode feature available with Conditional Access to evaluate the impact of the policies before enabling them. During sign-in, policies in report-only mode are evaluated but not enforced. You can see the results of the report-only mode in the Conditional Access and report-only tabs of the sign-in log details.

Conditional Access policies enhance security and also can increase user productivity. Policies are run only when the conditions in the policy are met. For example, if users are logging in from locations that are not trusted, they must do MFA to complete the login. Conditional Access policies only interrupt users when one or more conditions in the policies warrant it.

Conditional Access policy features are not available with all Microsoft 365 Business subscriptions. Conditional Access policies are only available with Microsoft 365 Business Premium subscriptions.

Conditional Access policies can control user access by multiple conditions, not just three. Policies can control user access by:

- User risk – the probability that a given identity or account is compromised
- Sign-in risk – the probability that a sign-in is not authorized by the identity owner
- Location – allow sign-ins, allow sign-ins with additional authentication, or block access based on trusted or named locations
- Device platform – control access by OS on the device
- Client apps and Device state, excluding devices that are hybrid Azure AD joined and/or devices marked as compliant with a Microsoft Intune compliance policy.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement conditional access

**References:**

Microsoft Docs > Azure > Active Directory > Conditional Access > Plan a Conditional Access deployment > Benefits

Microsoft Docs > Azure > Active Directory > Conditional Access > Conditional Access: Conditions

Microsoft Docs > Azure > Active Directory > Conditional Access > Troubleshooting Conditional Access using the What If tool

Microsoft Docs > Azure > Active Directory > Conditional Access > What is Conditional Access report-only mode?

---

## Question #24 of 36

Question ID: 1427385

You are the enterprise administrator for the Nutex Company. You are creating a Safe Attachments Policy for your Microsoft 365 environment to help secure user inboxes. You choose Dynamic Delivery as the course of action to address attachments with no known malware signature.

Which of the following happens to emails that meet this criterion as a result of the created policy?

✗ **A)** The email and attachment are delivered together, but the user cannot click on the attachment.

✗ **B)** The email and attachment are forwarded to a designated security administrator for further analysis.

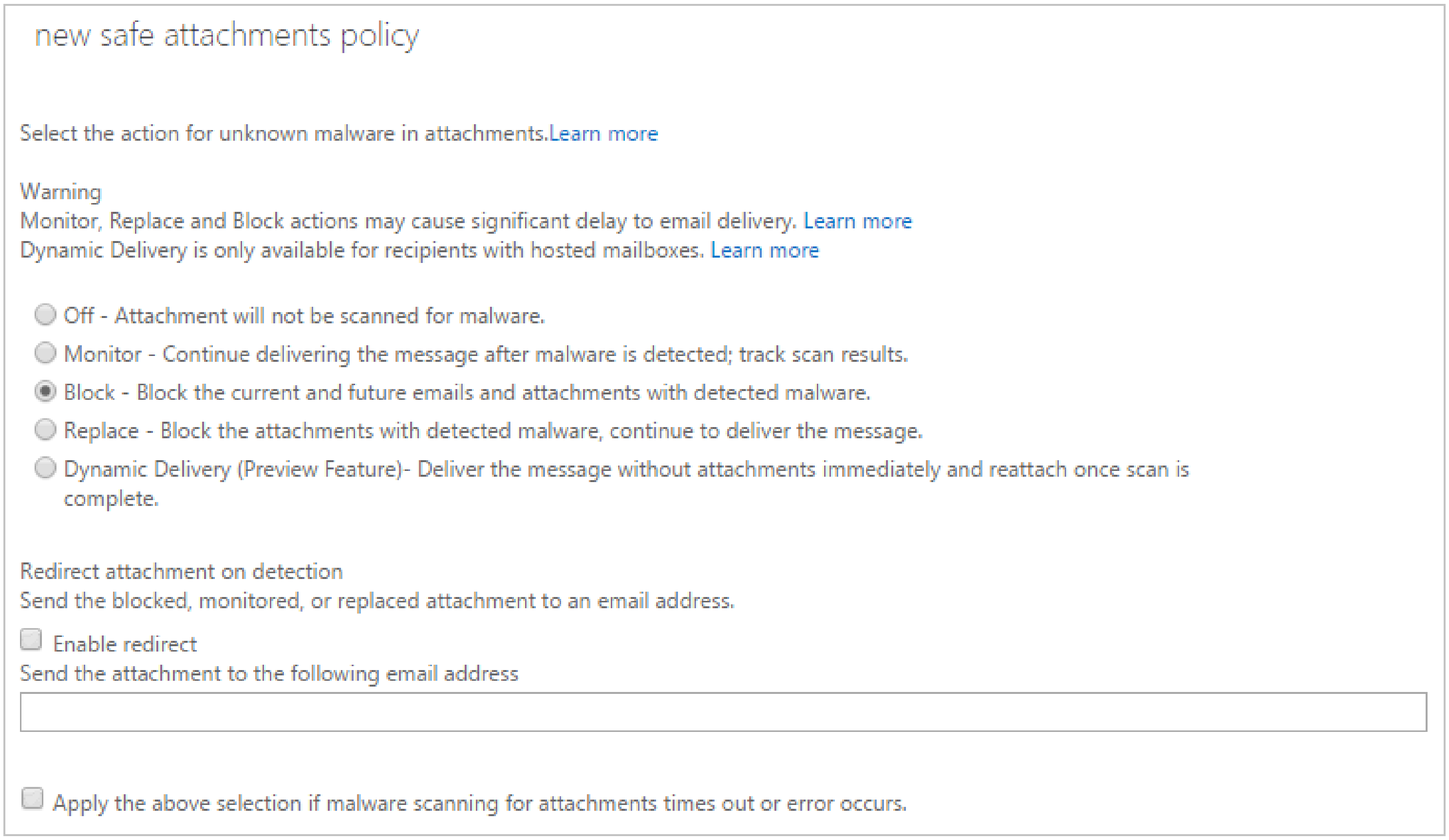
✓ **C)** The email is delivered, and the attachment is stripped and then reattached after being deemed safe following analysis.

✗ **D)** Both the email and the attachment are blocked and deleted along with all future emails from the sender.

Explanation

An Azure Safe Attachments policy that utilizes a Dynamic Delivery action will deliver the message body while stripping the attachment. The attachment is separately quarantined and analyzed for malware detection. If cleared, it is then reattached to the original email.

The following Safe Attachments policy has the Dynamic Delivery action enabled, which will deliver the message without its attachment, then reattach and deliver it when the scan has been successfully completed:



new safe attachments policy

Select the action for unknown malware in attachments.Learn more

Warning
Monitor, Replace and Block actions may cause significant delay to email delivery. Learn more
Dynamic Delivery is only available for recipients with hosted mailboxes. Learn more

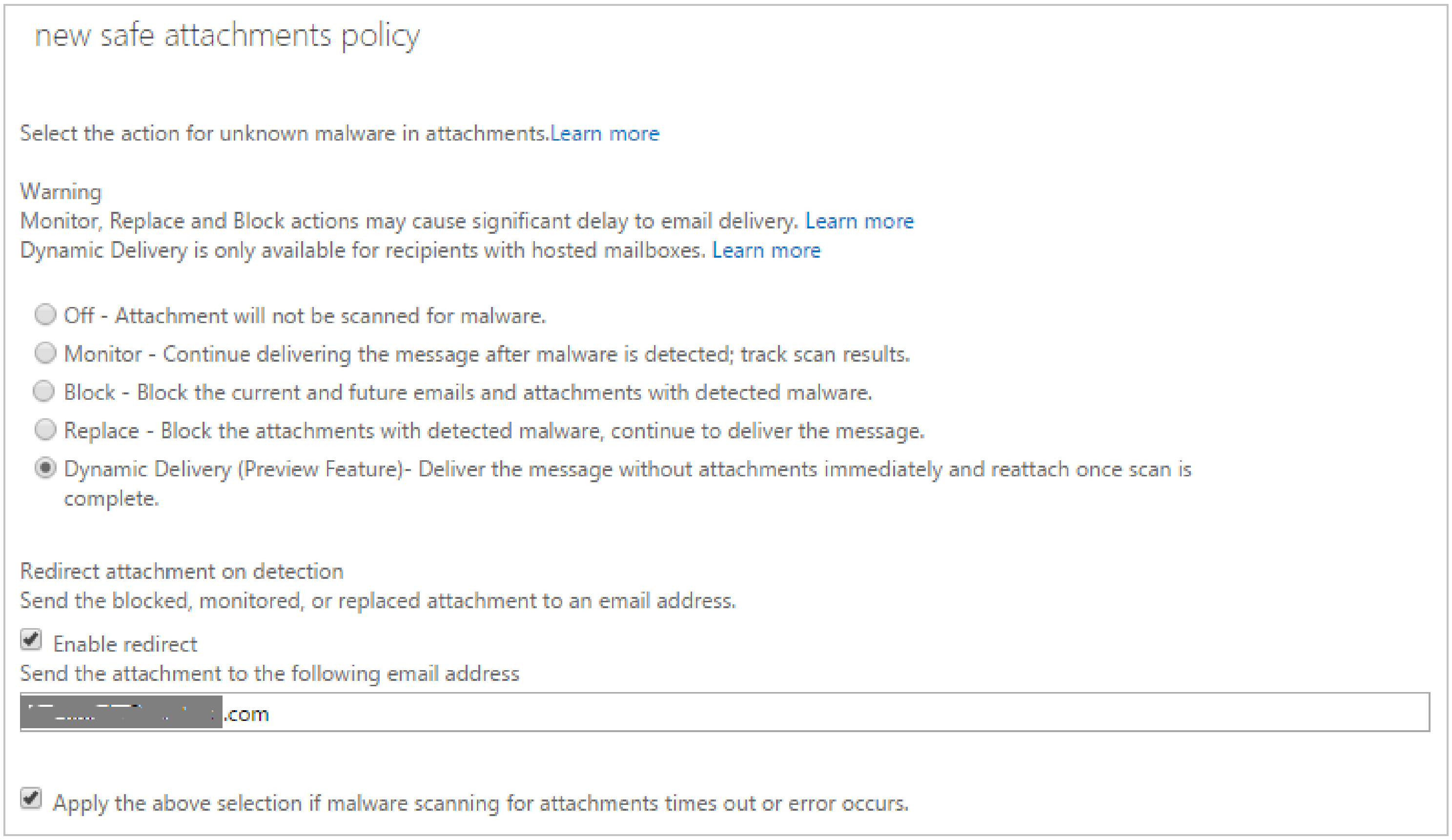
○ Off - Attachment will not be scanned for malware.
○ Monitor - Continue delivering the message after malware is detected; track scan results.
● Block - Block the current and future emails and attachments with detected malware.
○ Replace - Block the attachments with detected malware, continue to deliver the message.
○ Dynamic Delivery (Preview Feature)- Deliver the message without attachments immediately and reattach once scan is complete.

Redirect attachment on detection
Send the blocked, monitored, or replaced attachment to an email address.

□ Enable redirect
Send the attachment to the following email address

□ Apply the above selection if malware scanning for attachments times out or error occurs.

Emails can be forwarded to a designated administrator, but this is not an available action for attachments with unknown malware signatures. To forward emails to a designated administrator, check **Enable redirect** and specify the address of the administrator.



new safe attachments policy

Select the action for unknown malware in attachments.Learn more

Warning
Monitor, Replace and Block actions may cause significant delay to email delivery. Learn more
Dynamic Delivery is only available for recipients with hosted mailboxes. Learn more

○ Off - Attachment will not be scanned for malware.
○ Monitor - Continue delivering the message after malware is detected; track scan results.
○ Block - Block the current and future emails and attachments with detected malware.
○ Replace - Block the attachments with detected malware, continue to deliver the message.
● Dynamic Delivery (Preview Feature)- Deliver the message without attachments immediately and reattach once scan is complete.

Redirect attachment on detection
Send the blocked, monitored, or replaced attachment to an email address.

☑ Enable redirect
Send the attachment to the following email address

[redacted].com

☑ Apply the above selection if malware scanning for attachments times out or error occurs.

An Azure Safe Attachments policy does not block a user from clicking on the attachment in an email. The attachment is stripped from the email, so the user cannot click on it.

An Azure Safe Attachments policy does not block the body of the email. It stripsis concerned only with the attachment. You cannot configure the email and the attachment to be blocked and delete all future emails from the sender in an Azure Safe Attachments policy.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Privileged Identity Management (PIM)

**References:**

Microsoft Docs > Learn > Browse > Remediate risks with Microsoft Defender for Office 365 > Configure, protect, and detect

---

## Question #25 of 36

Question ID: 1427382

You are the Microsoft 365 Security Administrator at the Nutex Corporation. You recently initiated using PIM to protect access to Azure resources with privileged roles. You want to make all the necessary arrangements to use workflows available with PIM to request, resolve, and administer privileged access group assignments. You and your team need to understand how to leverage the workflows to build a scalable, automated, privileged access group management framework.

Which of the following statements about PIM workflows to request, resolve, and administer privileged access groups are TRUE? (Select all that apply.)

- ✗ **A)** Users of privileged access group assignments that are expiring get only one notification, 14 days before expiration.
- ✗ **B)** Notifications are not sent when administrators extend an access group assignment.
- ✗ **C)** Privileged access group assignments can only be extended but not renewed.
- ✓ **D)** Privileged access group assignment renewals are always self-initiated.
- ✓ **E)** Privileged access group assignment renewals require that the users requesting the renewals enter a business justification.

Explanation

The following statements are true:

- Privileged access group assignment renewals are always self-initiated.
- Privileged access group assignment renewals require that the users requesting the renewals enter a business justification.

Privileged access group assignment renewals are always self-initiated. When privileged users request a renewal, the administrators receive an email with the link to the request and can approve or deny it.

Privileged access group assignment renewals are used to renew access to already expired assignments. To request a renewal, go to **PIM > Privileged access groups > My Roles > Expired assignments**, click the expired assignment, and click **Renew**. You must mandatorily enter a business justification to submit the request.

Privileged access group assignments can be both extended and renewed. Extensions to group assignments can be initiated by the users or by administrators. When privileged users request an extension, administrators can either accept or deny the request. Renewals to expired group assignments can also be initiated by both users and administrators.

Users of privileged access group assignments that are expiring get three notifications, not one: 14 days before expiration, one day before expiration, and when the assignment expires. If the affected users need the access for more time, they can use the notification email or Azure portal to request an extension. Administrators can either approve or reject the request.

Notifications are sent to all the other administrators on the tenant when an authorized administrator extends an access group assignment.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Privileged Identity Management (PIM)

**References:**

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Extend or renew privileged access group assignments (preview) in Privileged Identity Management

---

## Question #26 of 36

Question ID: 1342932

You are the Azure Security Administrator at the Nutex Corporation. They have seen a spike in international business travel for their employees recently, especially in sales and operations. With employees signing in to Microsoft 365 from remote locations, you are concerned about the risks associated with unauthorized and risky sign-ins.

You plan to implement a Sign-in risk policy for your Microsoft 365 deployment.

Which of the following statements about Sign-in risk policies are TRUE? (Select all that apply.)

- ✓ **A)** The Sign-in risk policy can be configured to allow emergency access to administrators, even in the case of risky sign-ins from them.
- ✓ **B)** The Sign-in risk policy can be configured to either block or allow access if sign-ins are found to be risky.
- ✗ **C)** The Sign-in risk policy always blocks access to users whose sign-ins are found to be risky.
- ✗ **D)** Microsoft recommends that you set the risk level of Sign-in risk policies to High.
- ✓ **E)** Using the Named locations feature along with Sign-in risk policies can reduce false positives/risks detected.

Explanation

The following statements are true:

- The Sign-in risk policy can be configured to allow emergency access to administrators, even in the case of risky sign-ins from them.
- Using the Named locations feature along with Sign-in risk policies can reduce false positives/risks detected.
- The Sign-in risk policy can be configured to either block or allow access if sign-ins are found to be risky.

Sign-in risk policies can be configured to exclude user accounts, such as for emergency access or break-glass administrator accounts. With Azure AD, you can avoid scenarios that lead to a lack of administrative access by creating two or more emergency access accounts for the entire deployment. Such accounts can be used only when the regular accounts cannot sign in. Exclusions for emergency access must be periodically monitored.

A Sign-in risk policy can be emulated using a custom Conditional Access policy that includes sign-in risk as an assignment condition. If you include Named locations, specifically Trusted locations (allowed IP address ranges), false positives from these locations are reduced. A Named location in a Conditional Access policy specifies a set of IP address ranges, entire countries, or region IP addresses from which access to Azure services using MFA can be blocked for Microsoft 365 users. This is particularly used to restrict users to the corporate network when they use MFA. A single Named location can contain up to 1,200 IPv4 ranges, and on an Azure AD tenant, you can create a maximum of 90 named locations with one IP range assigned to each of them.

The Sign-in risk policy can be configured to block access, allow access, or allow access with MFA when risky sign-ins are detected. To add a Sign-in risk policy, go to Azure Active Directory > Security > Identity Protection > Overview, and click Sign-in risk policy, specify the inputs, and enforce the policy.

The Sign-in risk policy does not always block access to users whose sign-ins are found to be risky. A Sign-in risk policy can be configured to block access, allow access, or allow access with MFA when risky sign-ins are detected.

Microsoft does not recommend that you set the risk level of Sign-in risk policies to High. They recommend that you set the risk level of Sign-in risk policies to Medium or Low, specifying the amount of risk that you are willing to take. When risk levels are set to High, the policy is triggered less frequently, and this can allow attackers to get in undetected. Setting this to Medium validates users more frequently. Setting it to Low provides the best security posture for your deployment, although it can affect user productivity.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Identity Protection

**References:**

Microsoft Docs > Azure > Active Directory > Identity Protection policies > Sign-in risk policy

Microsoft Docs > Azure > Active Directory > Identity protection > How To: Configure and enable risk policies > Enable policiesMicrosoft Docs > Azure > Active Directory > Identity protection > How To: Configure and enable risk policies > Exclusions

Microsoft Docs > Azure > Active Directory > Identity Protection policies > Custom Conditional Access policy

Microsoft Docs > Azure > Active DIrectory > Identity protection > How To: Configure and enable risk policies > Choosing acceptable risk levels

---

## Question #27 of 36

Question ID: 1342926

You are the Security Administrator for Nutex Corporation's Microsoft 365 Enterprise deployment. Over the past few months, you have implemented several security measures to secure access to Microsoft 365 services.

Nutex is planning to acquire two software development companies with multiple apps and services. You need to implement a robust RBAC model to let administrators and users access the apps and services for Nutex and the companies it will acquire. You also need to allow Laura the ability to create a SQL server under nutex-core-apps in Azure. You should adhere to the principle of least priviledge.

Match the parameters required to add a role assignment for a user at a resource group scope (on the left) using the Azure PowerShell **New-AzRoleAssignment** cmdlet with their possible values (on the right).

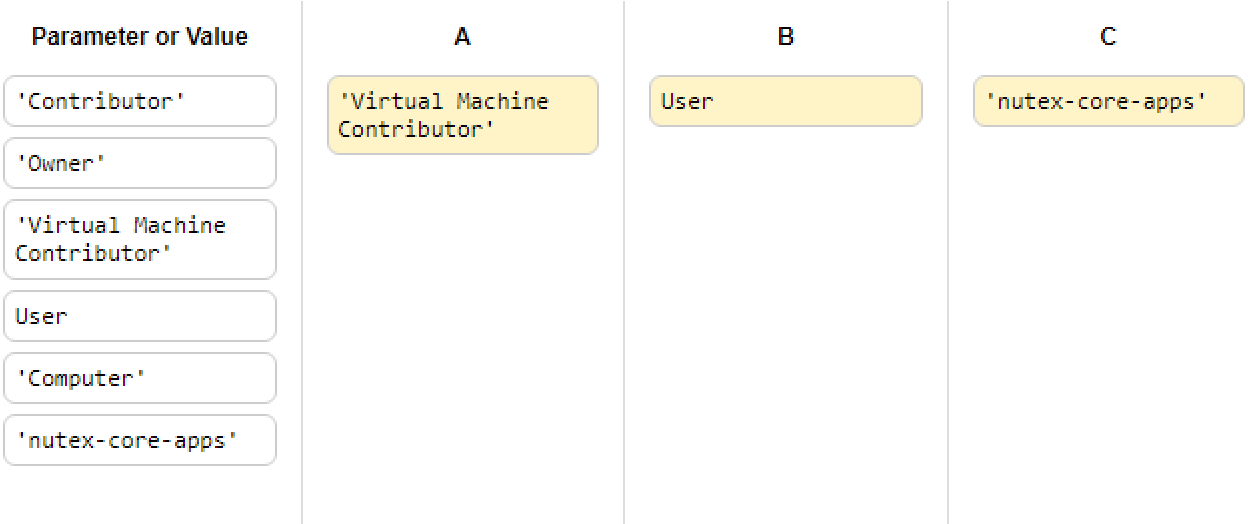
```
New-AzRoleAssignment -SignInName laura.richardson@nutex.com -RoleDefinitionName
A

-ResourceGroupName Web Admin -ObjectType B

-Scope C
```

{UCMS id=5663276575752192 type=Activity}

Explanation

You would map the parameters with their values as follows:

```
New-AzRoleAssignment -SignInName laura.richardson@nutex.com -RoleDefinitionName "Virtual Machine Contributor" -ResourceGroupName Web Admin -ObjectType User -Scope "nutex-core-apps"
```



| Parameter or Value | A | B | C |
|---|---|---|---|
| 'Contributor' | 'Virtual Machine Contributor' | User | 'nutex-core-apps' |
| 'Owner' | | | |
| 'Virtual Machine Contributor' | | | |
| User | | | |
| 'Computer' | | | |
| 'nutex-core-apps' | | | |

To manage access to Microsoft 365 apps and services, you assign roles to users, groups, service principals, or managed identities at a particular scope. The permissions required to manage access are grouped together into a role definition. After you decide upon the security principal, role, and scope, assign the role. You can add role assignments using the Azure portal, Azure PowerShell, Azure CLI, Azure SDKs, or REST APIs. You can have up to 2,000 role assignments in each subscription.

You would assign Laura the Virtual Machine Contributor role. This role allows a user to create and manage virtual machines, such as a Windows or SQL server in Azure. The Owner and Contributor roles can also create a virtual machine but will then have more rights than needed. The Owner role has all access to every resource and can assign access to those resources to other users. The Contributor role can create and manage all types of Azure resources. Unlike the Owner role, however, the Contributor role cannot grant access to those resources to others.

To add or remove role assignments, you must have Microsoft.Authorization/roleAssignments/write and Microsoft.Authorization/roleAssignments/delete permissions, such as User Access Administrator or Owner, and can use PowerShell commands in the Azure Cloud Shell or Azure PowerShell prompt. To add a role assignment for a user at a resource group scope, you must use the New-AzRoleAssignment cmdlet. Some of the parameters available with this cmdlet are RoleDefinitionName, Scope, ResourceGroupName, ObjectType, and ObjectId. The ObjectType in this scenario is User, not Computer. You are assigning the role to Laura, not the virtual machine.

The Scope in this scenario is a resource group, which is nutex-core-apps.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**

Implement role-based access control (RBAC)

**References:**

Microsoft Docs > Azure > Role-based access control > Steps to add a role assignment

Microsoft Docs > Azure > Role-based access control > Add or remove Azure role assignments using Azure PowerShell

Jeff Schertz's Blog > Locating IDs in Azure

---

## Question #28 of 36

Question ID: 1427380

You are an enterprise administrator for the Nutex Company. You want to create a new role-assignable group to expand the administrative responsibilities of select staff members and manage data loss prevention settings.

Which of the following tools could you use to complete this objective? (Choose two.)

- ✗ **A)** Azure Security Center
- ✓ **B)** Azure AD Admin Center
- ✓ **C)** Azure PowerShell
- ✗ **D)** Intune
- ✗ **E)** Azure AD Privileged Identity Management

Explanation

You can create a role-assigned group by using either the Azure AD Admin Center or PowerShell. Although it was not given as an option, you could also do this using the Azure Portal.

The following uses the **New-AzureADMSGroup** PowerShell cmdlet to create a group named **Nutex_Helpdesk_Administrators** that can be assigned to a role:

```
$group = New-AzureADMSGroup -DisplayName "Nutex_Helpdesk_Administrators" -Description "This
group is assigned to Helpdesk Administrator built-in role in Azure AD." -MailEnabled $true -
SecurityEnabled $true -MailNickName "nutexhelpdeskadministrators" -IsAssignableToRole $true
```

You can delegate role assignments to users in Azure AD Privileged Identity Management, but you cannot create role groups. Privileged Identity Management assigns admin roles to users temporarily within a configured time window.

Intune has been deprecated and replaced by Microsoft Endpoint Manager. Microsoft Endpoint Manager is part of Microsoft 365 that combines services for other legacy services such as Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. The Intune feature of Microsoft Endpoint Manager allows you to manage apps and devices, not create role- assignable groups.

Azure Security Center is not used to create user or group accounts. Azure Security Center monitors the security status of your network with a network map and reduces the attack surface across each resource by creating security policies and providing assessments.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement role-based access control (RBAC)

**References:**

Microsoft Docs > Azure > Active Directory > Create a role-assignable group in Azure Active Directory

Microsoft Docs > Learn > Browse > Secure the Microsoft 365 Messaging environment > Manage role-based-permissions in Microsoft 365 Messaging > Manage role groups

---

## Question #29 of 36

Question ID: 1355538

You have recently joined the Nutex Corporation as their Identity Administrator. Nutex uses an on-premises AD and the Azure cloud for Microsoft 365 services. They have made business partnerships with companies that need to access Nutex's apps and services on the Azure cloud. Managing access requests from thousands of partner employees manually is cumbersome. You want to implement the Identity Governance features on the Azure cloud.

Which of the following statements about the features and options available with Azure AD Identity Governance are TRUE? (Select all that apply.)

- ✓ **A)** Users can be granted access to the resources in an access package for more than five years.
- ✗ **B)** Both the Catalog owner and the access package manager can add resources to a catalog.
- ✗ **C)** Approval requests to access the access packages expire 14 days after the requests were made.
- ✓ **D)** Access packages can be deleted only if they do not have any active user assignments.
- ✗ **E)** All Azure AD administrator roles can add all types of resources to a catalog.

Explanation

The following statements are true:

- Users can be granted access to the resources in an access package for more than five years.
- Access packages can be deleted only if they do not have any active user assignments.

Lifecycle settings can be changed by the access package manager. The default length of time that a user is granted access to the resources in an Access package can be changed to a date, a number of days with a maximum of 3,660 days (10 years and 10 days), or never. To change it, go to Azure Active Directory > Identity Governance > Access packages > Policies and select the relevant policy. The expiration for the package is on the Lifecycle tab.

To ensure unrestricted active access, an access package can be deleted only when previously assigned users are not actively using the access package. To delete an access package, go to Azure Active Directory > Identity Governance > Access packages > Assignments and remove access for all users. Then click Overview and then Delete.

Only the Catalog owner, not the access package manager, can add resources to a catalog. An access package in Identity Governance is a one-time setup of resources and policies that automatically manage access to the resources in the access package. The resource can be: Membership of Azure AD security groups, Membership of Microsoft 365 Groups and Teams, Assignment to Azure AD Enterprise applications (including SaaS applications and custom-integrated applications that support federation/single sign-on and/or provisioning), and Membership of SharePoint Online sites. All access packages must be put in a container called a catalog. A catalog defines the resources that can be added to the access package. You cannot move an existing access package across catalogs.

Approval requests to access the access packages do not expire 14 days after the requests were made. You can set a duration of anywhere between 1 to 14 days for approvers to approve the requests. If the requests are not approved or are denied within this timeframe, the requests expire, and the requestors must request access again.

All Azure AD administrator roles cannot add all types of resources to a catalog. The type of resource (security group, Microsoft 365 group, app, or SharePoint Online site) depends on the type of administrator role on Azure AD. For example, Global Admin can add all types of resources, but a SharePoint Administrator can add only Microsoft 365 groups and SharePoint Online sites.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Secure Identities

**References:**

Microsoft Docs > Azure > Active Directory > Identity Governance > Create a new access package in Azure AD entitlement management

Microsoft Docs > Azure > Active Directory > Identity Governance > Change lifecycle settings for an access package in Azure AD entitlement management

Microsoft Docs > Azure > Active Directory > Identity Governance > Hide or delete an access package in Azure AD entitlement management > Delete an access package

Microsoft Docs > Azure > Active Directory > Identity Governance > Change approval and requestor information (preview) settings for an access package in Azure AD entitlement management

Microsoft Docs > Azure > Active Directory > Identity Governance > Delegation and roles in Azure AD entitlement management > Required roles to add resources to a catalog

## Question #30 of 36

Question ID: 1355539

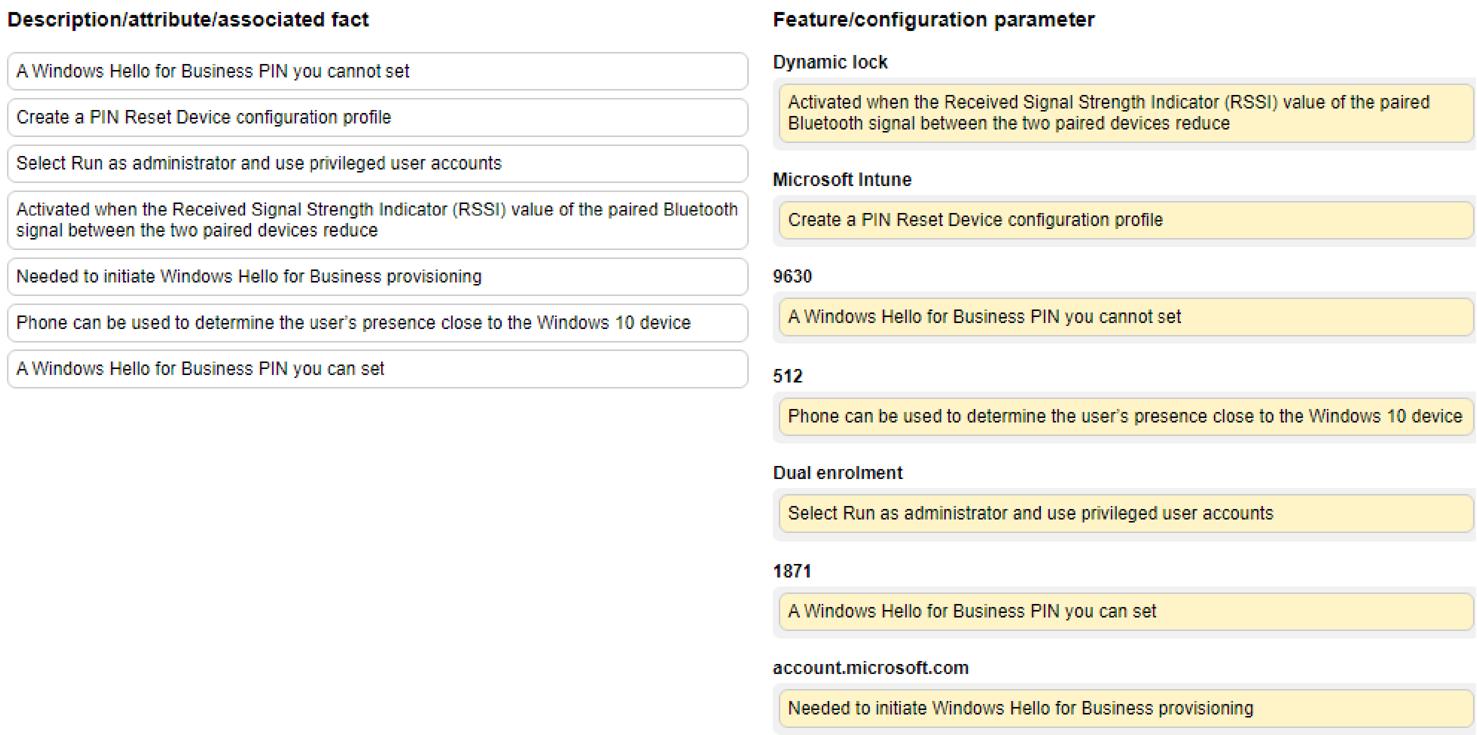
You are the Authentication Administrator for the Nutex Corporation's Microsoft 365 Enterprise deployment. Nutex has moved all its apps and services to the Azure cloud. You are tasked with implementing the most secure authentication method possible with Azure AD. Your research shows that Windows Hello for Business is the most secure method. You must now plan to deploy Windows Hello for Business for all Microsoft 365 users.

Match the description/attribute or other associated fact (on the left) with its feature/configuration parameter associated with Windows Hello for Business (on the right).

{UCMS id=5738610738331648 type=Activity}

Explanation

You would map as follows:



**Description/attribute/associated fact**

A Windows Hello for Business PIN you cannot set

Create a PIN Reset Device configuration profile

Select Run as administrator and use privileged user accounts

Activated when the Received Signal Strength Indicator (RSSI) value of the paired Bluetooth signal between the two paired devices reduce

Needed to initiate Windows Hello for Business provisioning

Phone can be used to determine the user's presence close to the Windows 10 device

A Windows Hello for Business PIN you can set

**Feature/configuration parameter**

Dynamic lock

Activated when the Received Signal Strength Indicator (RSSI) value of the paired Bluetooth signal between the two paired devices reduce

Microsoft Intune

Create a PIN Reset Device configuration profile

9630

A Windows Hello for Business PIN you cannot set

512

Phone can be used to determine the user's presence close to the Windows 10 device

Dual enrolment

Select Run as administrator and use privileged user accounts

1871

A Windows Hello for Business PIN you can set

account.microsoft.com

Needed to initiate Windows Hello for Business provisioning

Dynamic lock lets you lock a Windows 10 device when a Bluetooth device that is paired with it moves away. When this happens, the signal falls below the maximum Received Signal Strength Indicator (RSSI) value. This can make it difficult for anyone except the owner of the Windows 10 device to gain access when they are away from the device. Currently, only mobile phones are supported modes of determining the user's presence or proximity with the Windows device. You must configure a Dynamic lock policy using Group Policy. To configure dynamic lock factors go to Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business. You specify a value for the classOfDevice parameter to set the mode of determining the user's proximity. To use a phone, specify a value of 512.

PIN reset is the process of allowing users to reset their Windows Hello for Business PIN if they forget it. PIN resets are facilitated by Microsoft's PIN reset service. You can use a Group policy, Microsoft Intune policy, or Mobile Device Management (MDM) policy to let Windows 10 devices securely use the Microsoft PIN reset service. But first you must onboard the Microsoft PIN reset service to your Azure AD tenant. Also, it only works with some Enterprise and Pro editions of Windows 10.

Microsoft uses an intelligent PIN algorithm to help users select stronger PINs. The algorithm detects inputs and does not allow repeating numbers, sequential numbers, or simple patterns. It counts the number of steps required to reach the next digit, overflowing at ten (zero), and denies inputs with a constant delta between the digits. For example, the PIN 9630 has a constant delta of 7 (9 to 16, 6 to 13, 3 to 10), so is not allowed. Another example is 7036, with a constant delta of 3. An example of an allowed PIN is 1871, with deltas of 7, 9, 4. PINs of 1111, 1234, or 2233 are not allowed based on the repeating and sequential rules. PINs can be anywhere from 4 to 127 characters in length.

Dual enrolment for Windows Hello for Business enables you to enroll administrators' non-privileged and privileged credentials on their Windows 10 devices. Use the **Allow enumeration of emulated smart card for all users** Group Policy setting to configure Windows 10 devices to enumerate all enrolled Windows Hello for Business credentials. This is only supported on devices that use Windows 10 version 1709 and above. Administrator users can use non-privileged Windows Hello for Business credentials for normal tasks and select **Run as a different user** or **Run as administrator** to log in to privileged user accounts with their PINs. This feature can save time for administrators with sign-in and sign-out operations.

You can deploy Windows Hello for Business on your Windows 10 devices by choosing one of the three deployment models, cloud, hybrid, or on-premises, and choosing one key trust and one certificate trust for hybrid and on-premises deployment models. Windows Hello for Business provisioning starts immediately after the user has signed in and after the user profile is loaded, but before the user sees the desktop. You need to allow access to account.microsoft.com from your Windows 10 device to initiate Windows Hello for Business provisioning. This URL launches and completes the provisioning process.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement authentication methods

**References:**

Microsoft Docs > Windows > Security > Identity and access protection > Windows Hello for Business > Dynamic lock

Microsoft Docs > Windows > Security > Identity and access protection > Windows Hello for Business > PIN reset

Microsoft Docs > Windows > Security > Identity and access protection > Windows Hello for Business > Windows Hello for Business Frequently Asked Questions (FAQ) > Does Windows Hello for Business prevent the use of simple PINs?

Microsoft Docs > Windows > Security > Identity and access protection > Windows Hello for Business > Dual Enrollment

Microsoft Docs > Windows > Security > Identity and access protection > Windows Hello for Business > Windows Hello for Business Deployment Guide

---

## Question #31 of 36

Question ID: 1355543

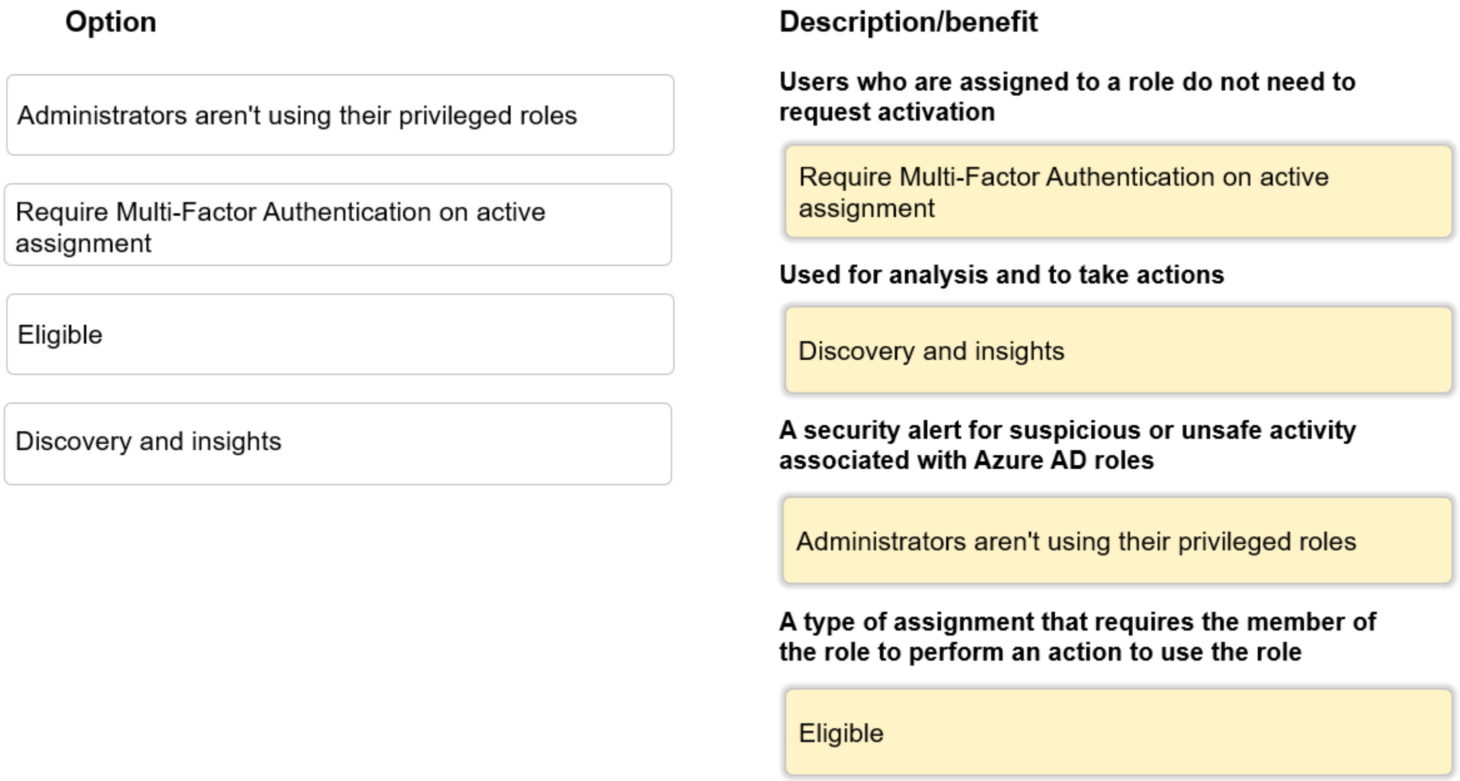
You are the Microsoft 365 Security Administrator at The Nutex Corporation. You recently initiated using PIM for protected access to Azure resources by privileged roles. You want to make some administrators eligible for a few Azure AD admin roles that use PIM.

Match the options available with implementing admin roles using PIM (on the left) with their descriptions/benefits (on the right).

{UCMS id=5657010621120512 type=Activity}

Explanation

You would map the options to their description/benefit as follows:



**Option**

Administrators aren't using their privileged roles

Require Multi-Factor Authentication on active assignment

Eligible

Discovery and insights

**Description/benefit**

**Users who are assigned to a role do not need to request activation**

Require Multi-Factor Authentication on active assignment

**Used for analysis and to take actions**

Discovery and insights

**A security alert for suspicious or unsafe activity associated with Azure AD roles**

Administrators aren't using their privileged roles

**A type of assignment that requires the member of the role to perform an action to use the role**

Eligible

Privileged Identity Management (PIM) with Azure AD can be configured to generate alerts for Azure AD roles. These alerts also contain details about how to fix and prevent the cause of the alert. Alerts are categorized by their severity:

High (requires immediate action), Medium (potential policy violation), and Low (suggesting a possisble policy change). The alerts available are:

- Administrators are not using their privileged roles
- Roles do not require multi-factor authentication for activation
- The organization does not have Azure AD Premium P2
- Potential stale accounts in a privileged role
- Roles are being assigned outside of Privileged Identity Management
- There are too many global administrators
- Roles are being activated too frequently

Using PIM, you can enforce MFA for two scenarios: Require Multi-Factor Authentication on active assignment and Require Multi-Factor Authentication on activation. Use Require Multi-Factor Authentication on active assignment to assign users to a role for a short duration (one day, for example). In this case, the assigned users do not need to request activation of the role because PIM does not enforce MFA when users use their role assignment. Use Require Multi-Factor Authentication on activation to enforce MFA for eligible users before they can activate.

With PIM, a Global administrator can make permanent/active Azure AD admin role assignments. Active assignments do not require the users to perform any action to use the role. A Global Admin can also make users eligible for Azure AD admin roles. Eligible administrators can activate the role when they need it; the permissions of the role expire in a set time duration. Also, eligible assignments require a member of the role to perform an action to use the role. The actions can include an MFA check, providing a business justification, or requesting approval from designated approvers.

The Discovery and insights (preview) option available with PIM shows the list of privileged roles and how many users are currently in those roles. You can list the assignments for a role and see the users who are assigned to that role.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Privileged Identity Management (PIM)

**References:**

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Configure security alerts for Azure AD roles in Privileged Identity Management > Security alerts

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Configure Azure AD role settings in Privileged Identity Management > Require multi-factor authentication

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Assign Azure AD roles in Privileged Identity Management

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Discovery and Insights (preview) for Azure AD roles (formerly Security Wizard)

## Question #32 of 36

Question ID: 1342933

The Nutex Corporation has seen a spike in international business travel for its employees and more contract employees working remotely, especially in sales and operations. You are the Azure Security Administrator at Nutex. With employees signing in to Microsoft 365 from remote locations, you are concerned about the risks associated with the identity of users being compromised. You are tasked with implementing the risk detection and mitigation capabilities of Azure AD Identity Protection and implementing scalable operational procedures to remediate the risks associated with user identities.

Which of the following statements about implementing the features and configuring alerts, notifications, and reporting for Azure AD Identity Protection is TRUE?

- ✗ **A)** Implementing User and Sign-in risk policies do not impact the identity secure score for your deployment.
- ✗ **B)** For Sign-in and User risk policies, you must always enforce controls to block access when risk is detected.
- ✗ **C)** You cannot configure Azure AD Identity Protection email notifications if you do not specify the recipients for the emails.
- ✓ **D)** Azure AD Identity Protection can be configured to send automated weekly email notifications with the events that were detected that week.

Explanation

Azure AD Identity Protection can be configured to send two types of automated notification emails to selected users: Users at risk detected (the users whose risk level reached the policy setting, for example if the policy is set to medium then users with a medium risk score and above will be listed), and Weekly digest (a summary of new risk detections, including risky users and sign-ins, and links to the related reports in Identity Protection).

You can configure email notifications for Azure AD Identity Protection even if you do not specify the recipients. If you do not specify recipients, users with the Global administrator, Security administrator, or Security reader roles are automatically added to the recipient list.

For Sign-in and User risk policies, you do not always have to enforce controls to block access when risk is detected. Blocking access can affect user productivity. Microsoft recommends that you allow access with appropriate additional authentication methods such as MFA or password reset. For Sign-in risk policies, you can also configure a Conditional Access policy with Sign-in risk as a condition for granular block access and allow access controls.

Implementing User and Sign-in risk policies do have an impact on the identity secure score for your deployment. Identity secure score is a number between 1 and 223 that indicates the identity security posture of your deployment. For new deployments, the identity security score is low and the dashboard lists the improvement actions that you can implement to increase the score. Implementing User and Sign-in risk policies requires that you enable controls such as MFA and password reset. Enabling these for the deployment are scored as improvement actions and improves the secure score.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement Azure AD Identity Protection

**References:**

Microsoft Docs > Azure > Active Directory > Identity protection > Azure Active Directory Identity Protection notifications

Microsoft Docs > Azure > Active Directory > Identity protection > How To: Configure and enable risk policies

Microsoft Docs > Azure > Active Directory > Identity protection > Custom Conditional Access policy

TechGenix Blog > Using Azure Active Directory Identity Protection to boost your security

Rebel Admin Blog > Protect cloud Identities with Azure Active Directory Identity Protection

---

## Question #33 of 36

Question ID: 1365723

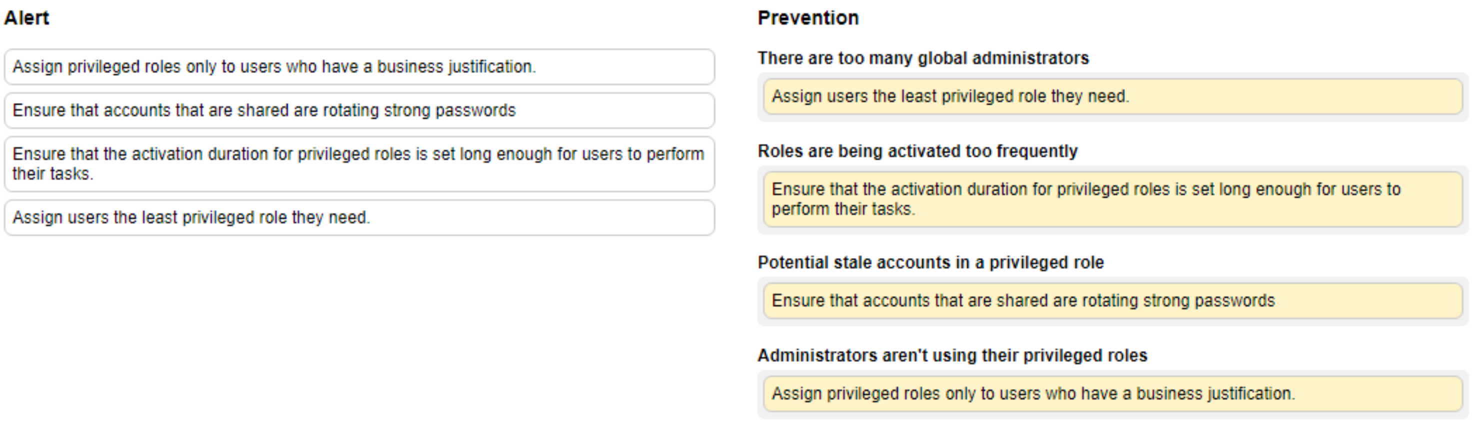
You notice several alerts in your Privileged Identity Management dashboard.

Match the security alerts with the appropriate cause.

{UCMS id=5608915157909504 type=Activity}

Explanation

You would choose the following:



**Alert**

Assign privileged roles only to users who have a business justification.

Ensure that accounts that are shared are rotating strong passwords

Ensure that the activation duration for privileged roles is set long enough for users to perform their tasks.

Assign users the least privileged role they need.

**Prevention**

**There are too many global administrators**

Assign users the least privileged role they need.

**Roles are being activated too frequently**

Ensure that the activation duration for privileged roles is set long enough for users to perform their tasks.

**Potential stale accounts in a privileged role**

Ensure that accounts that are shared are rotating strong passwords

**Administrators aren't using their privileged roles**

Assign privileged roles only to users who have a business justification.

If there is suspicious or unsafe activity in your Azure AD organization, alerts can show up in the Privileged Identity Management dashboard when triggered. The following are some of the alerts that could possibly arise:

- **Administrators aren't using their privileged roles** – This alert occurs when a user is assigned a privileged role that they do not need, and the account is not actively being used. An attacker could use this type of account to remain unnoticed. You can prevent this alert by assigning privileged roles only to users who have a business justification.
- **Potential stale accounts in a privileged role** – If accounts in a privileged role have not changed their passwords in the past 90 days, the passwords may be vulnerable to being hacked by an attacker if it is used in a service or shared account. To prevent this alert, ensure that the passwords for those accounts are periodically rotated with strong passwords. You should also review accounts with privileged roles by using access reviews to find any role assignments that are no longer needed.
- **There are too many global administrators** – When an attacker compromises a global administrator, that attacker gains all permissions. To prevent this from happening, assign users the least privileged role they need. You should review the list of users in the global administrator role regularly to see if they absolutely, positively need that role.
- **Roles are being activated too frequently** – This alert can occur when there are multiple activations to the same user's privileged role. You should ensure that their privileged role's activation duration is configured for the appropriate length of time for them to perform their tasks. You can prevent this alert by requiring multi-factor authentication for privileged roles that have accounts shared by multiple administrators.

**Objective:**

Implement and manage identity and access

**Sub-Objective:**

Implement Azure AD Privileged Identity Management (PIM)

**References:**

HYPERLINK "https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new"Microsoft Docs > Azure > Active Directory > Privileged Identity Management > Configure security alerts for Azure AD roles in Privileged Identity Management

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > View audit history for Azure AD roles in Privileged Identity Management

## Question #34 of 36

Question ID: 1427383

You are serving as an IT intern for the Nutex Company. Your manager wants you to perform a preliminary audit to confirm and record all the assignments to Azure AD roles in Privileged Identity Management, but you are not to make any changes.

Which two of the following administrator roles must you have to achieve this objective using the principle of least privilege? (Choose two.)

- ✓ **A)** Global Reader
- ✗ **B)** Compliance Administrator
- ✗ **C)** Privileged Role Administrator
- ✓ **D)** Security Administrator
- ✗ **E)** Identity Governance Administrator

Explanation

The Security Administrator and Global Reader roles can both view assignments to Azure AD roles in Privileged Identity Management. These roles grant you read rights only, which satisfies the compliance to least- privilege security practices.

While the Privileged Role Administrator role has the right to view Azure AD role assignments, it also has full management capabilities, which exceeds the authorized permission level.

The Compliance Administrator role is used to manage compliance-related features in the Microsoft 365 compliance center, Microsoft 365 admin center, Azure, and Office 365 Security & Compliance Center. It does not have access to Azure AD roles.

The role of Identity Governance Administrator is centered around managing Azure AD identity governance configuration in relation to items such as access packages, catalogs, and policies.

It does not have rights concerning Azure AD role assignments.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**

Implement Azure AD Privileged Identity Management (PIM)

**References:**

Microsoft Docs > Azure > Active Directory > Privileged Identity Management > What is Azure AD Privileged Identity Management?

Microsoft Docs > Azure > Active Directory > Azure AD built-in roles

## Question #35 of 36

Question ID: 1342915

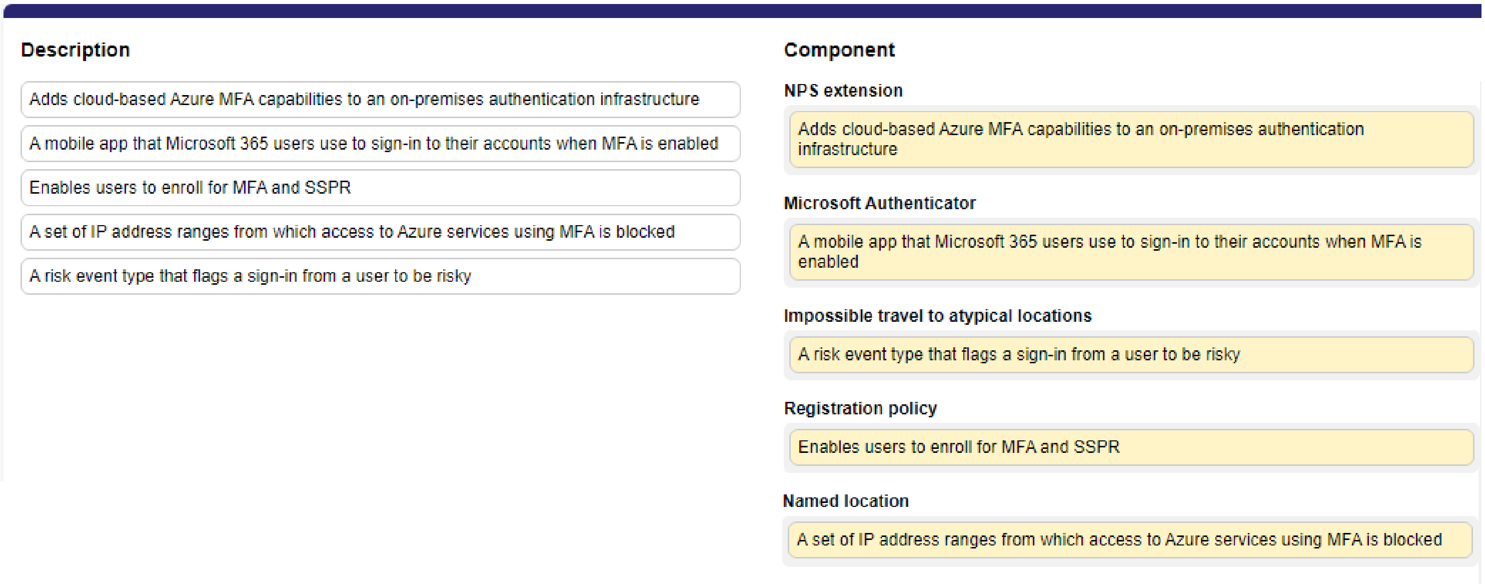
You have recently joined the Nutex Corporation as a Security Administrator for their Microsoft 365 Enterprise deployment. Nutex has recently adopted this deployment. One of your first tasks is to implement multi-factor authentication (MFA) by leveraging some of the on-premises components.

Match the components involved in deploying MFA with their descriptions.

{UCMS id=5669011397279744 type=Activity}

Explanation

You would map the components with their descriptions as follows:



**Description**

- Adds cloud-based Azure MFA capabilities to an on-premises authentication infrastructure
- A mobile app that Microsoft 365 users use to sign-in to their accounts when MFA is enabled
- Enables users to enroll for MFA and SSPR
- A set of IP address ranges from which access to Azure services using MFA is blocked
- A risk event type that flags a sign-in from a user to be risky

**Component**

**NPS extension**

Adds cloud-based Azure MFA capabilities to an on-premises authentication infrastructure

**Microsoft Authenticator**

A mobile app that Microsoft 365 users use to sign-in to their accounts when MFA is enabled

**Impossible travel to atypical locations**

A risk event type that flags a sign-in from a user to be risky

**Registration policy**

Enables users to enroll for MFA and SSPR

**Named location**

A set of IP address ranges from which access to Azure services using MFA is blocked

If you are using on-premises legacy, RADIUS, or AD FS applications that do not authenticate directly with Azure AD, you will need additional extensions and infrastructure to use the features of the cloud-based Azure multi-factor authentication (MFA). For on-premises RADIUS applications, you will need to use an NPS extension. With an NPS extension, you can add phone call, text message, or phone app verification as the second layer of authentication. This accomplishes a hybrid deployment of MFA.

Microsoft Authenticator is a mobile app that Microsoft 365 users use to sign-in to their accounts when MFA is enabled. This app is available for both Android and iOS phones. With Microsoft 365 MFA, in addition to a password that users must enter, a second layer of authentication is required, which can be one of the following: a verification code sent as a text message to a phone, a phone call with a verification code, the Microsoft Authenticator smartphone app or similar, or an OAuth hardware token that generates random time-limited verification codes. You would choose a second layer of authentication that suits your Microsoft 365 users.

You can leverage Azure's automated risk detection and remediation policies to protect your users' identities. You can create policies to force password changes when there is a threat of compromised identity or to require MFA when Azure deems a sign-in to be risky, which includes leaked credentials, sign-ins from anonymous IP addresses, impossible travel to atypical locations, sign-ins from unfamiliar locations, sign-ins from infected devices, and sign-ins from IP addresses with suspicious activities. Impossible travel to atypical locations flags sign-ins based on the location from which the user recently signed in.

With Azure MFA, Registration policy is a way to enforce how Microsoft 365 users will register their second layer of authentication method – phone, app, or hardware token. With the recent introduction of a Combined Registration Experience, users can register once and specify a second method for MFA and self-service password reset (SSPR). Users must register with MFA within 14 days of rolling out the Registration policy.

A named location is a Conditional Access Policy that specifies a set of IP address ranges or entire countries or regions from which access to Azure services using MFA can be blocked for Microsoft 365 users. Using this is particularly useful in restricting users to the corporate network when they use MFA. A single named location can contain up to 1,200 IPv4 ranges, and on an Azure AD tenant you can create a maximum of 90 named locations with one IP range assigned to each. Named locations can also be Trusted locations (allowed IP address ranges). You can add lists of countries or regions if you want to block MFA by countries and regions.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement authentication methods

**References:**

Microsoft Docs > Azure > Active Directory > Authentication > Plan an Azure AD Multi-Factor Authentication deployment

Microsoft Docs > Azure > Active Directory > Authentication > Integrate your existing Network Policy Server (NPS) infrastructure with Azure AD Multi-Factor Authentication

Microsoft Docs > Azure > Active Directory > User help > What is the Microsoft Authenticator app?

Microsoft Docs > Azure > Active Directory > Identity protection > What is Identity Protection?

Microsoft Docs > Azure > Active DIrectory > Authentication > Enable combined security information registration in Azure Active Directory

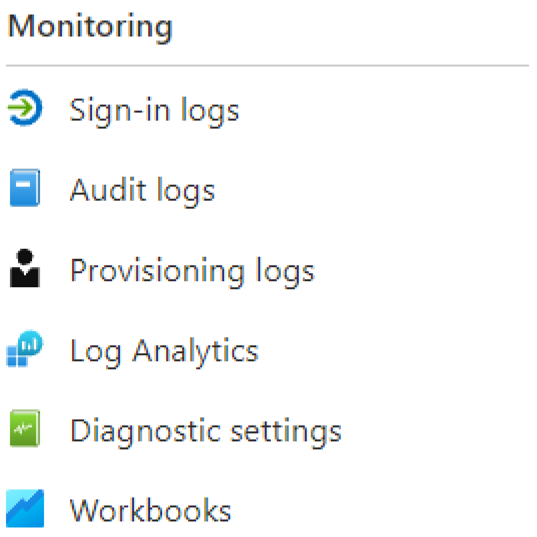
Microsoft Docs > Azure > Active Directory > Conditional Access > Using the location condition in a Conditional Access policy > Named locations

## Question #36 of 36

Question ID: 1427378

You are an enterprise administrator for the Nutex Company. You recently created a Conditional Access policy in an effort to tighten up security for your Azure AD environment. The helpdesk is reporting that users are getting an error message when they attempt to access several of their assigned applications. You suspect that the Conditional Access policy is unnecessarily restricting them.

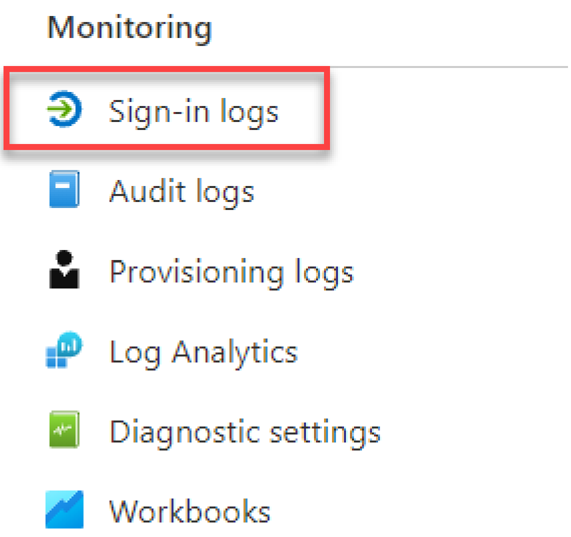
Click on the monitoring menu item in the Azure portal that will provide the necessary information to determine the problem.



- ✗ **A)** 24,138,287,175
- ✗ **B)** 24,219,287,250
- ✗ **C)** 24,263,287,290
- ✗ **D)** 24,181,287,214
- ✗ **E)** 24,98,287,129
- ✓ **F)** 24,57,287,90

Explanation

You would choose the Sign-in logs option:



If users are being denied access to applications or resources, the denials will be listed in the sign-in events logs, which can be viewed under the **Monitoring** section in the Azure AD portal. The **Sign-in logs** option provides insight into how resources are used by your users. Once a sign-in failure event has been located, you can select the **Conditional Access** tab, which will then show the specific policy that denied the user access.

The **Audit logs** option contains information about changes applied to tenant users and groups, as well as any updates applied to tenant resources.

The **Provisioning logs** option includes activities performed by provisioning services, such as ServiceNow, Adobe, or Workday. For example, you can see which users from Workday were successfully created in Active Directory.

The **Log Analytics** option allows you to edit and run log queries involving the Azure Monitor logs.

The **Diagnostic settings** option provides diagnostic and auditing information for Azure resources and the Azure platform they depend on.

The **Workbooks** option involves the creation of interactive and analytic report narratives.

**Objective:**
Implement and manage identity and access

**Sub-Objective:**
Implement conditional access

**References:**

Microsoft Docs > Azure > Active DIrectory > Conditional Access > Troubleshooting sign-in problems with Conditional Access