AZ-500 Exam Topics Review Questions

Updated: 6/7/2021

https://cybersecurityhoy.files.wordpress.com/2021/06/az-500-exam-all.pdf

Updated: 6/7/2021

Contents

1. Stored access policy

You have an Azure Storage account named Sa1 in a resource group named RG1. Users and applications access the blob service and the le service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the le service and the blob service.

You need to revoke all access to Sa1.

Solution: You generate new SASs. Does this meet the goal? No

Instead, you should create a new stored access policy. To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy.

Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

2. Same as 1

3. Connect HDInsight to your on-premises network

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network. You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.

Solution: You deploy the On-premises data gateway to the on-premises network. Does this meet the goal? NO

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

✑ Create Azure Virtual Network.

✑ Create a custom DNS server in the Azure Virtual Network.

✑ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

✑ Configure forwarding between the custom DNS server and your on-premises DNS server.

References: https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

4. Same as 3

5. Password hash synchronization with seamless single sign-on (SSO)

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant. You need to recommend an integration solution that meets the following requirements:

✑ Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant Minimizes the number of servers required for the solution.

Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign into Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

For **pass-through authentication**, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests.

References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

6. Synchronization Rules Editor

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

Use the Synchronization Rules Editor and write attribute-based filtering rule. References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

7. Conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

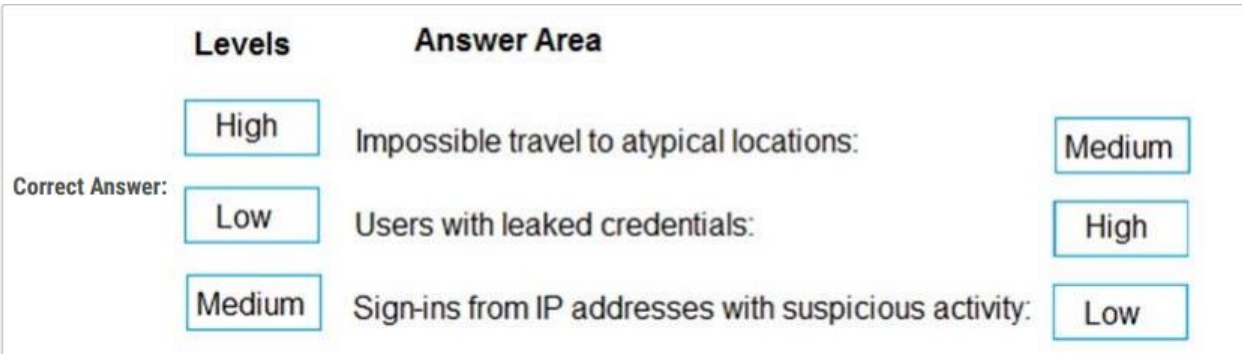
You need to identify the risk level of the following risk events:

✑ Users with leaked credentials

✑ Impossible travel to atypical locations

✑ Sign-ins from IP addresses with suspicious activity

Which level should you identify for each risk event?



Correct Answer:

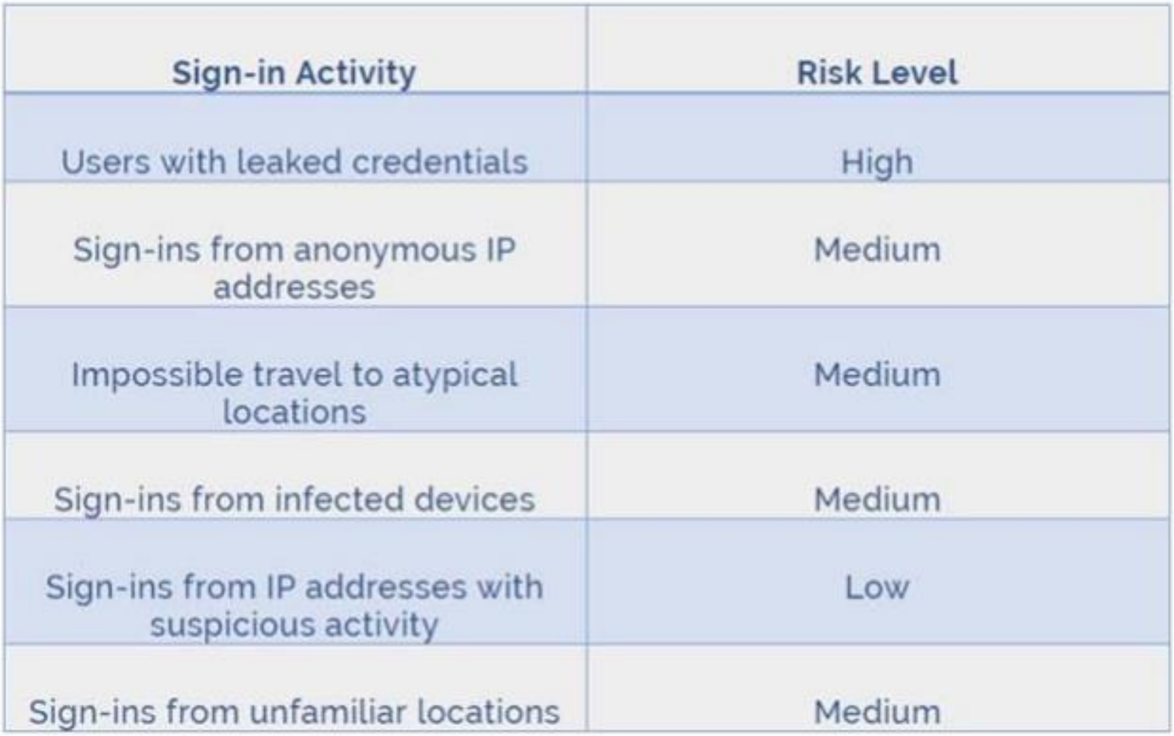
Levels	Answer Area	
High	Impossible travel to atypical locations:	Medium
Low	Users with leaked credentials:	High
Medium	Sign-ins from IP addresses with suspicious activity:	Low

Azure AD Identity protection can detect six types of suspicious sign-in activities:

1. Users with leaked credentials
2. Sign-ins from anonymous IP addresses

3. Impossible travel to atypical locations
4. Sign-ins from infected devices
5. Sign-ins from IP addresses with suspicious activity
6. Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks: High, Medium & Low



Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

8. Azure AD Identity Protection user risk policy

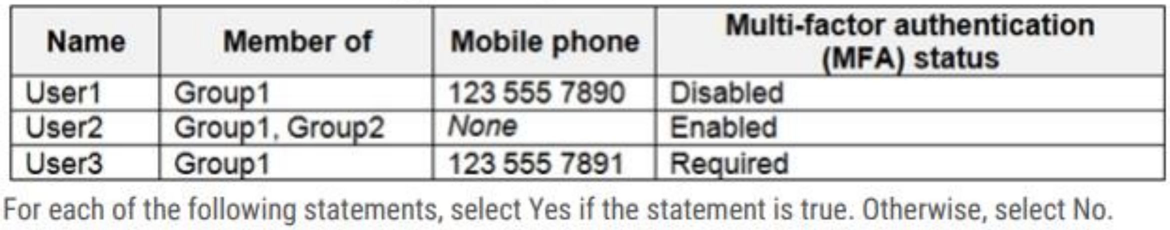
You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

✑ Assignment: Include Group1, Exclude Group2

✑ Conditions: Sign-in risk of Medium and above

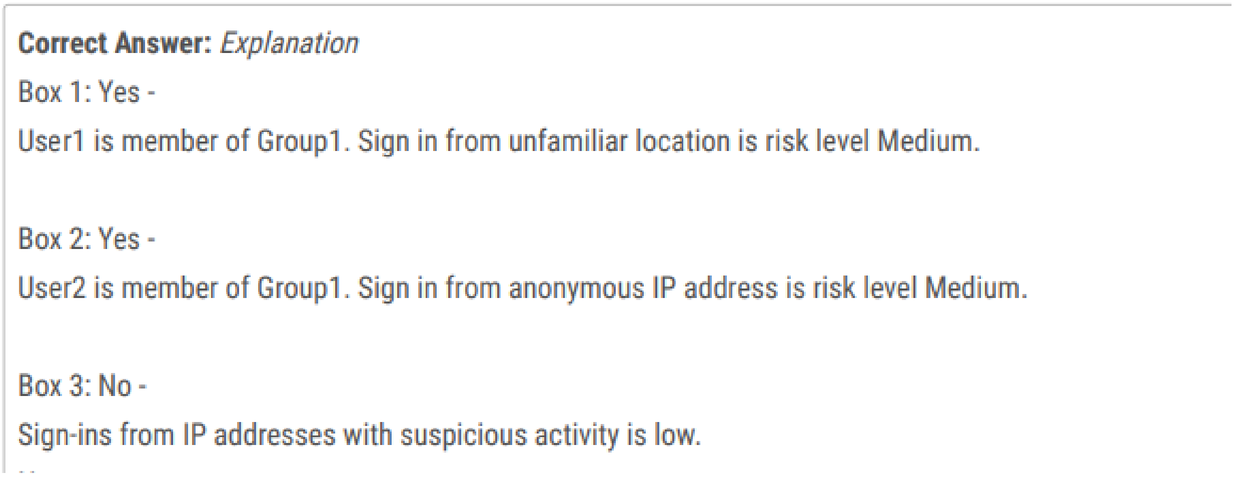
Access: Allow access, Require password change

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table:



Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	*None*	Enabled
User3	Group1	123 555 7891	Required

For each of the following statements, select Yes if the statement is true. Otherwise, select No.



Correct Answer: *Explanation*

Box 1: Yes -

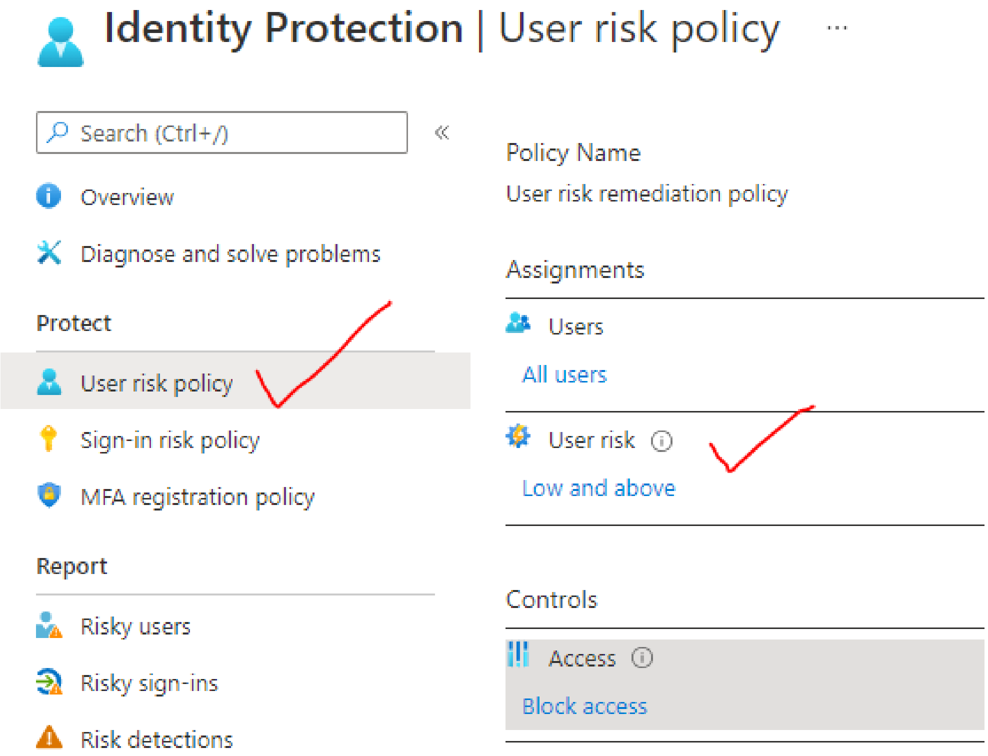
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

Box 2: Yes -

User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.

Box 3: No -

Sign-ins from IP addresses with suspicious activity is low.



Identity Protection | User risk policy

Policy Name
User risk remediation policy

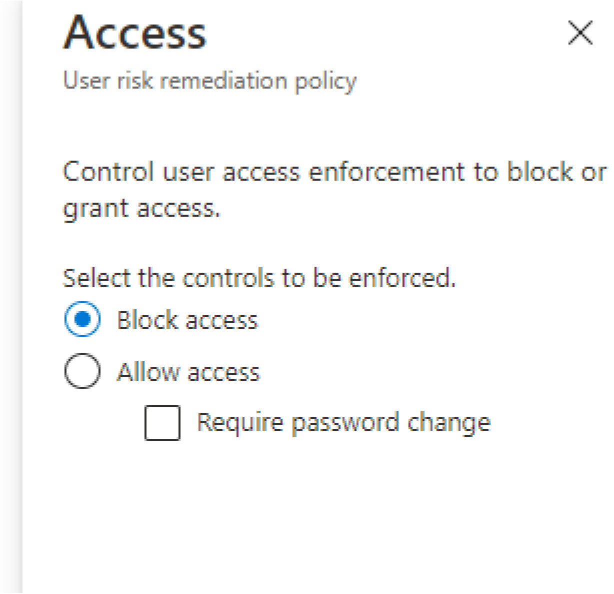
Assignments

Users
All users

User risk
Low and above

Controls

Access
Block access



Access

User risk remediation policy

Control user access enforcement to block or grant access.

Select the controls to be enforced.

● Block access

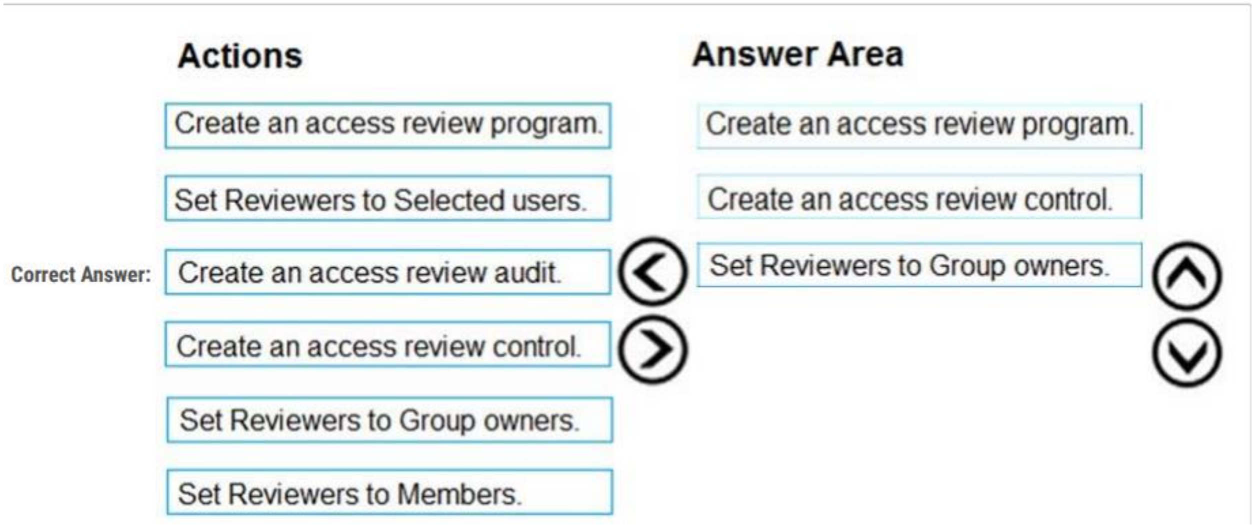
○ Allow access

□ Require password change

9. Access Review

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Correct Answer:

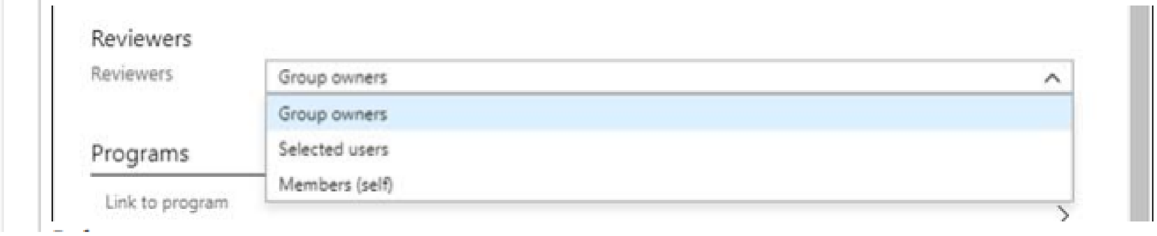
Actions	Answer Area
Create an access review program.	Create an access review program.
Set Reviewers to Selected users.	Create an access review control.
Create an access review audit.	Set Reviewers to Group owners.
Create an access review control.	
Set Reviewers to Group owners.	
Set Reviewers to Members.	

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



Reviewers

Reviewers: Group owners

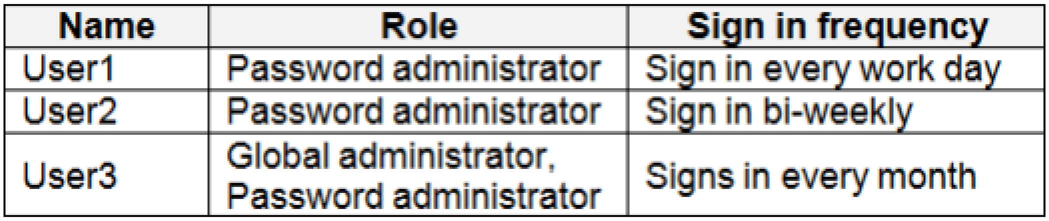
References:

https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

https://docs.microsoft.com/en-us/azure/activedirectory/governance/manage-programs-controls

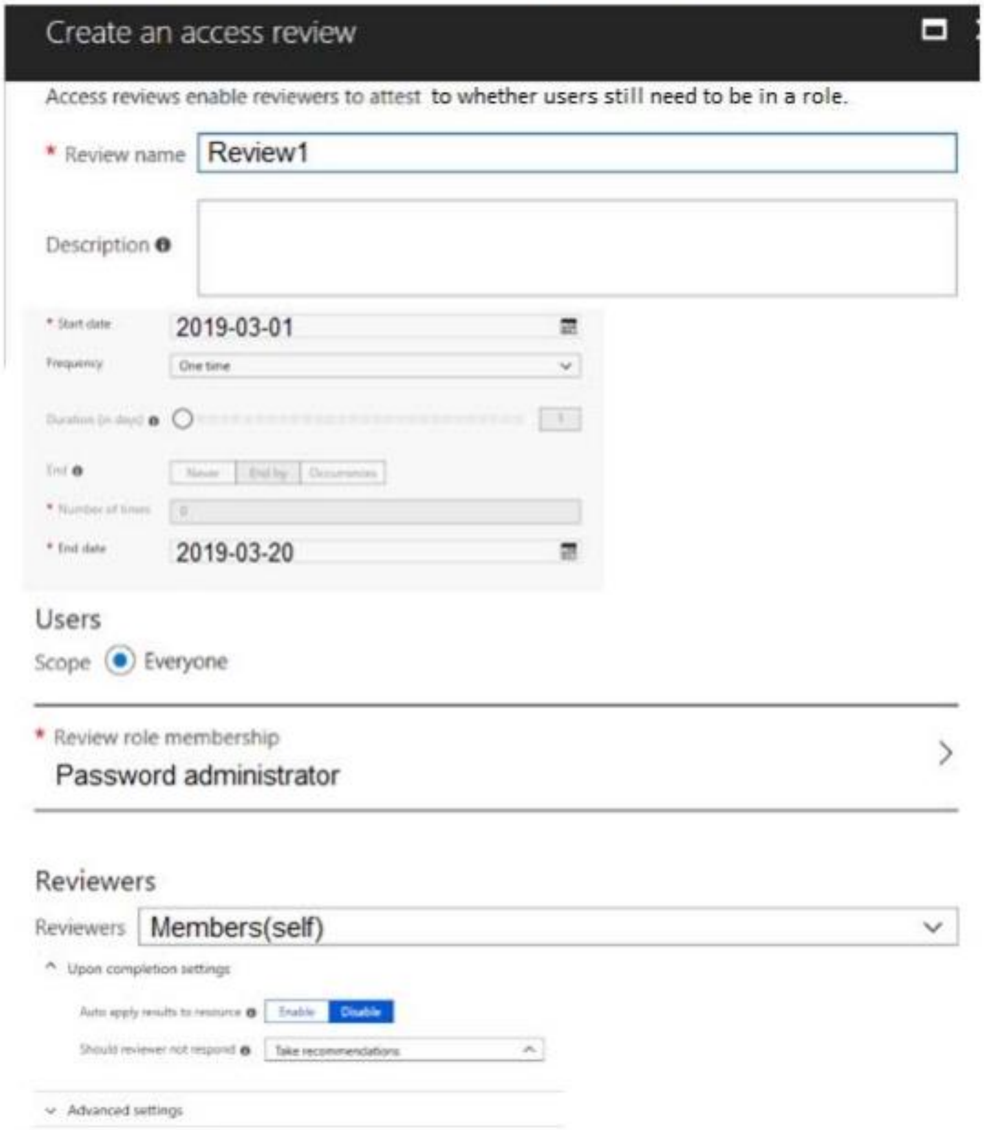
10. Access Review

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.



Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.



Create an access review

Access reviews enable reviewers to attest to whether users still need to be in a role.

* Review name: Review1

Description

* Start date: 2019-03-01

Frequency: One time

Duration (in days) ○ 1

End: Never | End by | Occurrences

* Number of times: 0

* End date: 2019-03-20

Users

Scope ● Everyone

* Review role membership: Password administrator

Reviewers

Reviewers: Members(self)

Upon completion settings

Auto apply results to resource: Enable | [✓ Disable]

Should reviewer not respond: Take recommendations

Advanced settings

Correct Answer: *Explanation*

Box 1: User3 only -

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

References:

https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review