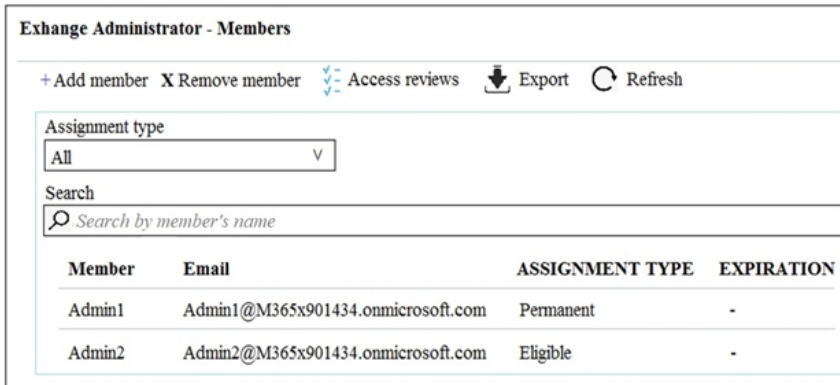


Microsoft 365 Security Administration

1. An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.



Exchange Administrator - Members

+ Add member X Remove member Access reviews Export Refresh

Assignment type: All

Search: Search by member's name

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

- A. Change the Assignment Type for Admin2 to Permanent
- B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
- C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
- D. Change the Assignment Type for Admin1 to Eligible

Answer(s): D

2. You need to recommend a solution for the user administrators that meets the security requirements for auditing. Which blade should you recommend using from the Azure Active Directory admin center?

- A. Sign-ins
- B. Azure AD Identity Protection
- C. Authentication methods
- D. Access review

Answer(s): A

3. HOTSPOT (Drag and Drop is not supported)

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Set the frequency to:

One time	v
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

A. See Explanation section for answer.

Answer(s): A

4. You need to recommend a solution to protect the sign-ins of Admin1 and Admin2. What should you include in the recommendation?

A. a device compliance policy

B. an access review

C. a user risk policy

D. a sign-in risk policy

Answer(s): D

5. You need to resolve the issue that generates the automated email messages to the IT team. Which tool should you run first?

A. Synchronization Service Manager

B. Azure AD Connect wizard

C. Synchronization Rules Editor

D. IdFix

Answer(s): B

6. Which IP address space should you include in the Trusted IP MFA configuration?

A. 131.107.83.0/28

B. 192.168.16.0/20

C. 172.16.0.0/24

D. 192.168.0.0/20

Answer(s): A

7. HOTSPOT (Drag and Drop is not supported)

How should you configure Group3? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Group type:

	▼
An Office 365 group in the Microsoft 365 admin center	
A security group in Active Directory Users and Computers	
A security group in the Azure Active Directory admin center	

Group membership criteria:

	▼
A dynamic distribution list	
A dynamic membership rule with an Advanced rule set to All users	
A dynamic membership rule with a Simple rule set to userType Equals User	

A. See Explanation section for answer.

Answer(s): A

8. HOTSPOT (Drag and Drop is not supported)

How should you configure Azure AD Connect? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User sign-in settings:

	▼
Password Synchronization with single-sign on	
Pass-through authentication with single sign-on	
Federation with Active Directory Federation Services (AD FS)	

Device options:

	▼
Hybrid Azure AD Join	
Enable Device writeback	
Disable Device writeback	

A. See Explanation section for answer.

Answer(s): A

9. You need to create Group3.

What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center

B. a mail-enabled security group in the Microsoft 365 admin center

C. a security group in the Microsoft 365 admin center

D. a distribution list in the Microsoft 365 admin center

E. a security group in the Azure AD admin center

Answer(s): A D

10. HOTSPOT (Drag and Drop is not supported)

Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ADGroup1:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

ADGroup2:	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

A. See Explanation section for answer.

Answer(s): A

11. HOTSPOT (Drag and Drop is not supported)

You are evaluating which finance department users will be prompted for Azure MFA credentials. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements

A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.

A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.

A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.

A. See Explanation section for answer.

Answer(s): A

12. Which user passwords will User2 be prevented from resetting?

A. User6 and User7

B. User4 and User6

C. User4 only

D. User7 and User8

E. User8 only

Answer(s): E

13. You need to meet the technical requirements for User9. What should you do?

A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9

B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9

C. Assign the Security administrator role to User9

D. Assign the Global administrator role to User9

Answer(s): D

14. Which role should you assign to User1?

A. Global administrator

B. User administrator

C. Privileged role administrator

D. Security administrator

Answer(s): C

15. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution:

You modify the Azure AD app and attribute filtering settings.

Does that meet the goal?

A. Yes

B. No

Answer(s): B

16. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

A. Yes

B. No

Answer(s): A

17. Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Source Anchor settings.

Does that meet the goal?

A. Yes

B. No

Answer(s): B

18. HOTSPOT (Drag and Drop is not supported)

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

verification options [\(learn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication [\(learn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60):

In contoso.com, you create the users shown in the following table.

Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

Can sign in to the My Apps portal without using MFA	V
Completed the MFA registration	
Must complete the MFA registration at the next sign-in	

User2:

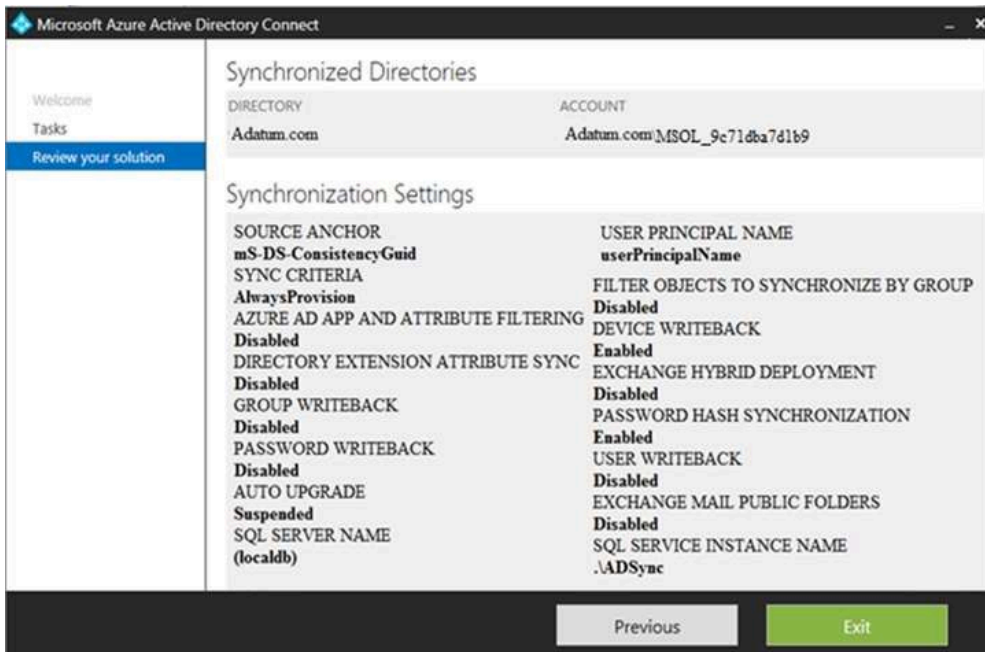
Can sign in to the My Apps portal without using MFA	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My Apps portal	

A. See Explanation section for answer.

Answer(s): A

19. HOTSPOT (Drag and Drop is not supported)

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you reset a password in Azure AD of a synced user, the password will [answer choice].

be overwritten	▼
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	▼
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

A. See Explanation section for answer.

Answer(s): A

20. You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune. You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on-premises network. What should you do first?

A. From the Azure Active Directory admin center, create a new certificate

B. Enable Application Proxy in Azure AD

C. From Active Directory Administrative Center, create a Dynamic Access Control policy

D. From the Azure Active Directory admin center, configure authentication methods

Answer(s): A

