

## SC-300 Dumps

### Microsoft Identity and Access Administrator

<https://www.certleader.com/SC-300-dumps.html>



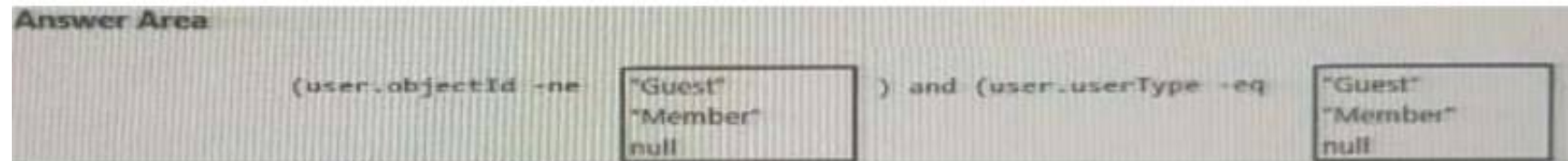
### NEW QUESTION 1

- (Exam Topic 1)

You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

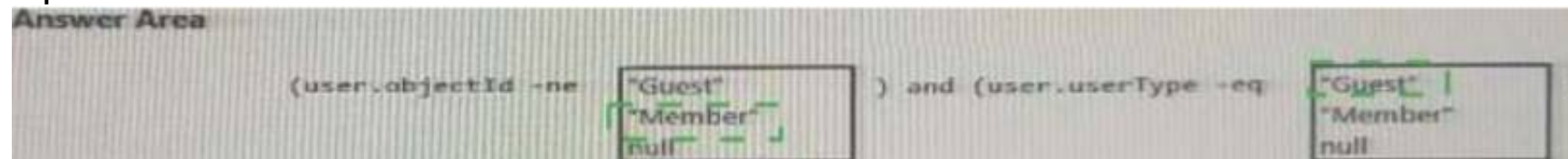
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



### NEW QUESTION 2

- (Exam Topic 1)

You need to meet the authentication requirements for leaked credentials. What should you do?

- A. Enable federation with PingFederate in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Enable password hash synchronization in Azure AD Connect.
- D. Configure an authentication method policy in Azure AD.

**Answer:** C

**Explanation:**

Reference:

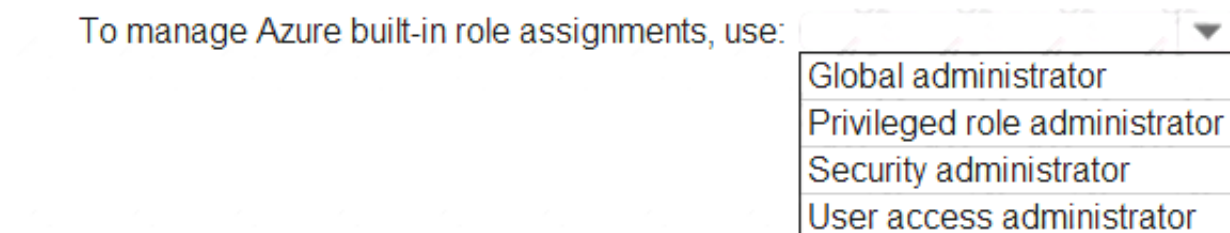
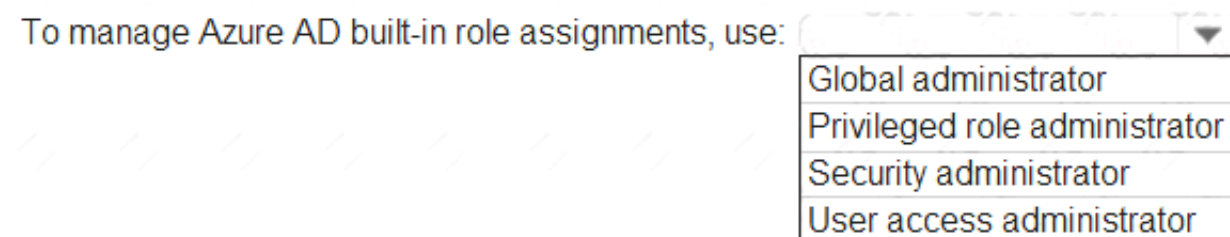
<https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>

### NEW QUESTION 3

- (Exam Topic 1)

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal> <https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

### NEW QUESTION 4

- (Exam Topic 1)

You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements. What should you configure?

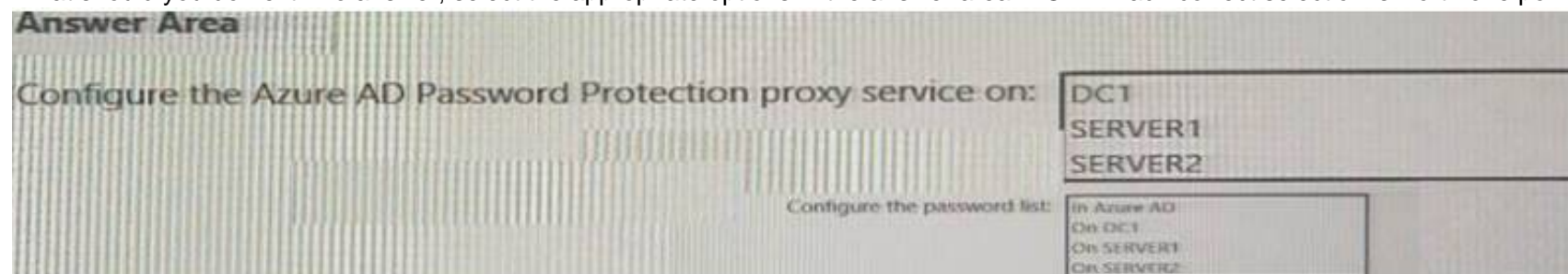
- A. named locations that have a private IP address range
- B. named locations that have a public IP address range
- C. trusted IPs that have a public IP address range
- D. trusted IPs that have a private IP address range

**Answer:** B

#### NEW QUESTION 5

- (Exam Topic 1)

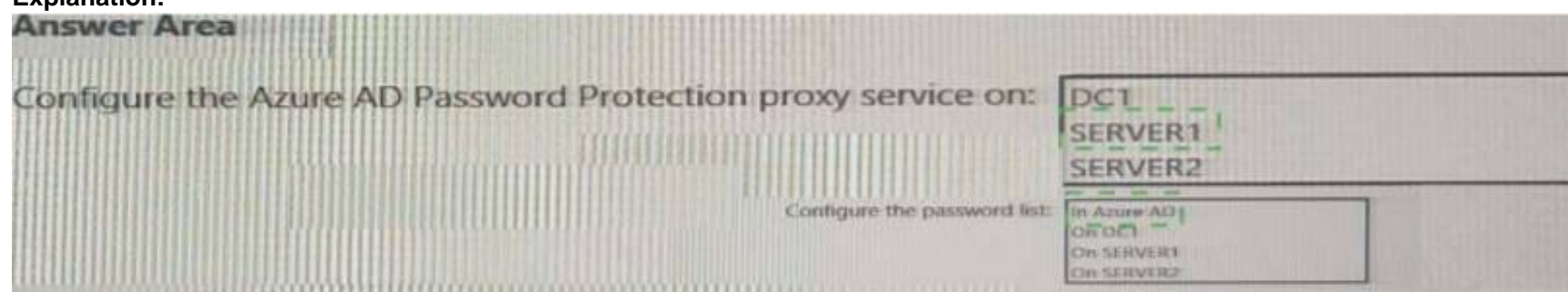
You need to implement password restrictions to meet the authentication requirements. You install the Azure AD password Protection DC agent on DC1. What should you do next? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



#### NEW QUESTION 6

- (Exam Topic 1)

You need to configure the detection of multi staged attacks to meet the monitoring requirements. What should you do?

- A. Customize the Azure Sentinel rule logic.
- B. Create a workbook.
- C. Add an Azure Sentinel playbook.
- D. Add Azure Sentinel data connectors.

**Answer:** D

#### NEW QUESTION 7

- (Exam Topic 3)

You have an Azure Active Directory (Azure AD) tenant named conto.so.com that has Azure AD Identity Protection enabled. You need to Implement a sign-in risk remediation policy without blocking access. What should you do first?

- A. Configure access reviews in Azure AD.
- B. Enforce Azure AD Password Protection.
- C. implement multi-factor authentication (MFA) for all users.
- D. Configure self-service password reset (SSPR) for all users.

**Answer:** D

#### NEW QUESTION 8

- (Exam Topic 3)

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Configure password protection for Windows Server Active Directory.

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>

#### NEW QUESTION 9

- (Exam Topic 3)

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for tailed Azure AD user sign-in attempts. You need to ensure that a new security administrator receives the alerts instead of you. Solution: From Azure monitor, you modify the action group. Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

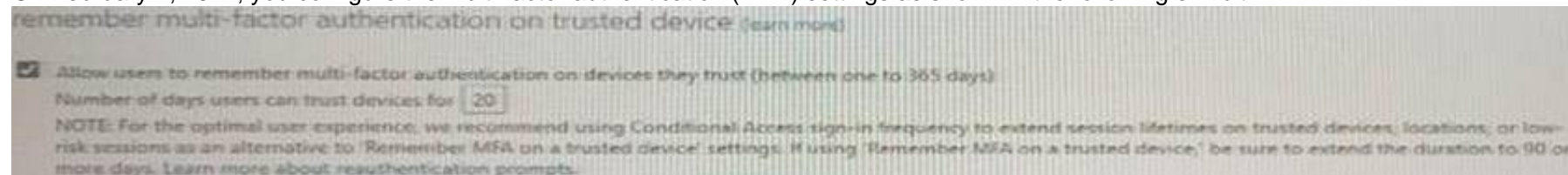
#### NEW QUESTION 10

- (Exam Topic 3)

You create the Azure Active Directory (Azure AD) users shown in the following table.

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.



The users authentication to Azure AD on their devices as shown in the following table.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

On February 26, 2021, what will the multi-factor auth status be for each user?

A)

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

B)

Name	Multi-factor auth status
User1	Enabled
User2	Enabled
User3	Enabled

C)

Name	Multi-factor auth status
User1	Enforced
User2	Enforced
User3	Enforced

D)

Name	Multi-factor auth status
User1	Disabled
User2	Enforced
User3	Enforced

- A. Option A
- B. Option B
- C. Option C
- D. Option D

**Answer: B**

#### NEW QUESTION 10

- (Exam Topic 3)

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User1, and User3,

You create a group named Group1. You add User2 and User3 to Group1.

You configure a role in Azure AD Privileged identity Management (PIM) as shown in the application administrator exhibit. (Click the application Administrator tab.)



### Role setting details - Application Administrator

Privileged Identity Management | Azure AD roles

Edit

#### Activation

Setting	State
Activation maximum duration (hours)	5 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	Yes
Approvers	0 Member(s), 1 Group

#### Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on activation	No
Require justification on active assignment	Yes

Group1 is configured as the approver for the application administrator role. You configure User2to be eligible for the application administrator role. For User1, you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click Assignment tab)

### Add assignments

Privileged Identity Management | Azure AD roles

Membership

Setting

Assignment type ⓘ

☒ Eligible
 ☐ Active

Maximum allowed eligible duration is 3 month(s).

Assignment starts \*

01/01/2021

12:00:00 AM

Assignment ends \*

01/31/2021

11:59:00 PM

For each of the following statement, select Yes if the statement is true, Otherwise, select No. NOTE: Each correct selection is worth one point.

#### Answer Area

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 is assigned the Application administrator role automatically.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 requests to be assigned the Application administrator role, only User3 can approve the request.	<input checked="" type="radio"/>	<input type="radio"/>
If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 14

- (Exam Topic 3)

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM). While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights. You need to ensure that the IT department users only have access to the Security administrator role when required. What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments afterfrom the Role settings details
- B. Expire active assignments afterfrom the Role settings details
- C. Assignment type toActive
- D. Assignment type toEligible

Answer: D

Explanation:

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

NEW QUESTION 16

- (Exam Topic 3)

You have a Microsoft 365 tenant. All users have mobile phones and laptops. The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access. You plan to implement multi-factor authentication (MFA). Which MFA authentication method can the users use from the remote location?

- A. a verification code from the Microsoft Authenticator app
- B. security questions
- C. voice
- D. SMS

Answer: B

NEW QUESTION 19

- (Exam Topic 3)

You have a Microsoft 365 E5 tenant. You purchase a cloud app named App1. You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud app Security. Which four 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.

Actions

From Microsoft Cloud App Security, create a session policy.

Create a conditional access policy that has session controls configured.

Publish App1 in Azure Active Directory (Azure AD).

Implement Azure AD Application Proxy.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.

>

<

Answer Area

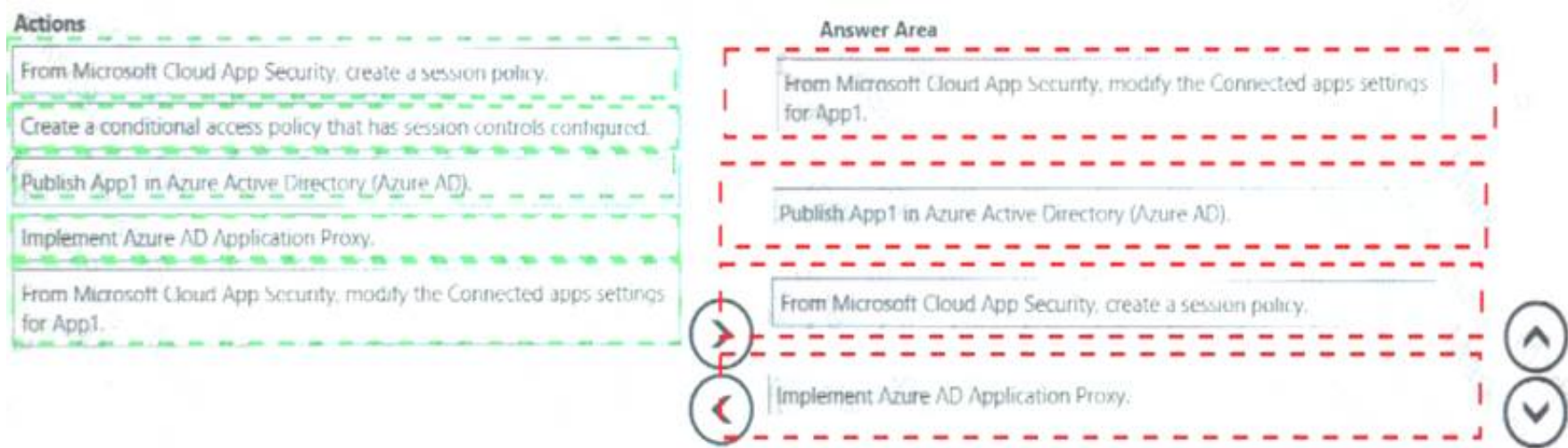
↑

↓

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



## NEW QUESTION 20

- (Exam Topic 3)

You have a Microsoft 365 tenant.

You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Require MFA for all users

Assignments

Users and groups ⓘ

All users

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only On

Create

Control user access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☒ Require multi-factor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy ⓘ  
[See list of policy protected client apps](#)

☐ Require password change (Preview) ⓘ

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)



Privileged Identity Management
ContosoAzureAD
User Administrator

# Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

## Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s) 0 Group

## Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

ContosoAzureAD
Identity Governance
Privileged Identity Management
ContosoAzureAD

# User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments
Active assignments
Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope	Membership
User Administrator				
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory	Direct
Admin3	Admin3@m365x629615.onmicrosoft.com	User	Directory	Direct

For each of the following statement, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

## Answer Area

Statements	Yes	No
Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.	<input type="radio"/>	<input type="radio"/>
Admin2 can request activation of the User administrator role for a period of two hours.	<input type="radio"/>	<input type="radio"/>
If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements

Yes

No

Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request.

☒
☐

Admin2 can request activation of the User administrator role for a period of two hours.

☐
☒

If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.

☒
☐

**NEW QUESTION 25**

- (Exam Topic 3)

You have a Microsoft 365 tenant named contoso.com. Guest user access is enabled.

Users are invited to collaborate with contoso.com as shown in the following table.

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

From the External collaboration settings in the Azure Active Directory admin center, you configure the Collaboration restrictions settings as shown in the following exhibit.

Collaboration restrictions

- ☐ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☒ Allow invitations only to the specified domains (most restrictive)

 Delete

☒ TARGET DOMAINS

☐ Outlook.com

From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE:Each correct selection is worth one point.

Statements

Yes

No

User1 can accept the invitation and gain access to the enterprise application.

☐
☐

User2 can access the enterprise application.

☐
☐

User3 can accept the invitation and gain access to the SharePoint site.

☐
☐

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Yes

Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.

Box 2: Yes

Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.

Box 3: No

Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

**NEW QUESTION 26**

- (Exam Topic 3)

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU). What should you configure?

- A. an access review

- B. the terms or use
- C. a linked subscription
- D. a user flow

**Answer:** D

#### NEW QUESTION 27

- (Exam Topic 3)

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain.

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections. What should you include in the recommendation?

- A. Azure AD Application Proxy
- B. an Azure AD Password Protection proxy
- C. Network Policy Server (NPS)
- D. a pass-through authentication proxy

**Answer:** C

#### NEW QUESTION 31

- (Exam Topic 3)

Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active

Directory (Azure AD) tenant named contoso.com by using Azure AD Connect. Azure AD Connect is installed on a server named Server 1.

You deploy a new server named Server2 that runs Windows Server 2019.

You need to implement a failover server for Azure AD Connect. The solution must minimize how long it takes to fail over if Server1 fails.

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.

**Actions**

- On Server1, run export for all connectors.
- On Server2, run export for all connectors.
- On Server2, run full import for all connectors.
- On Server2, run delta synchronization for all connectors.
- On Server2, install Azure AD Connect.
- On Server1, configure the staging mode.

**Answer Area**

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Actions**

- On Server1, run export for all connectors.
- On Server2, run export for all connectors.
- On Server2, run full import for all connectors.
- On Server2, run delta synchronization for all connectors.
- On Server2, install Azure AD Connect.
- On Server1, configure the staging mode.

**Answer Area**

On Server2, run export for all connectors.

On Server2, run delta synchronization for all connectors.

On Server1, run export for all connectors.

#### NEW QUESTION 33

- (Exam Topic 3)

You have an Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

For which groups can you create an access review?

- A. Group1 only
- B. Group1 and Group4 only
- C. Group1 and Group2 only
- D. Group1, Group2, Group4, and Group5 only
- E. Group1, Group2, Group3, Group4 and Group5

**Answer:** D

**Explanation:**

You cannot create access reviews for device groups. Reference:

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

**NEW QUESTION 38**

- (Exam Topic 3)

You have an on-premises datacenter that contains the hosts shown in the following table.

Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

You have an Azure Active Directory (Azure AD) tenant that syncs to the Active Directory forest. Multi-factor authentication (MFA) is enforced for Azure AD.

You need to ensure that you can publish App1 to Azure AD users.

What should you configure on Server and Firewall1? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.

Service to install on Server4:

Azure AD Application Proxy
The Azure AD Password Protection DC agent
The Azure AD Password Protection proxy service
Web Application Proxy in Windows Server

Rule to configure on Firewall1:

Allow incoming HTTPS connections from Azure AD to Server4.
Allow incoming IPsec connections from Azure AD to Server4.
Allow outbound HTTPS connections from Server4 to Azure AD.
Allow outbound IPsec connections from Server4 to Azure AD.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>

**NEW QUESTION 41**

- (Exam Topic 3)

You have a Microsoft 365 tenant.

Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).

You need to receive an alert if a registered application gains read and write access to the users' email. What should you do? To answer, select the appropriate options in the answer area.

NOTE:Each correct selection is worth one point.



Tool to use:

Azure AD Identity Protection
Identity Governance
Microsoft Cloud App Security
Microsoft Endpoint Manager

Policy type to create:

App discovery
App protection
Conditional access
OAuth app
Sign-in risk
User risk

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy>

**NEW QUESTION 45**

- (Exam Topic 3)

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant

Users sign in to computers that run Windows 10 and are joined to the domain.

You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO). You need to configure the computers for Azure AD Seamless SSO.

What should you do?

- A. Enable Enterprise State Roaming.  
B. Configure Sign-in options.  
C. Install the Azure AD Connect Authentication Agent.  
D. Modify the Intranet Zone settings.

**Answer:** D

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start>

**NEW QUESTION 46**

- (Exam Topic 3)

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

- A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured  
B. an Azure AD conditional access policy that has session controls configured  
C. an Azure AD conditional access policy that has client apps conditions configured  
D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad>

**NEW QUESTION 49**

- (Exam Topic 3)

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

In Azure AD, you add a new enterprise application named Appl. Which groups can you assign to App1?

- A. Group1 and Group
- B. Group2 only
- C. Group3 only
- D. Group1 only
- E. Group1 and Group4

**Answer:** A

#### NEW QUESTION 52

- (Exam Topic 3)

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for tailed Azure AD user sign-in attempts. You need to ensure that a new security administrator receives the alerts instead of you. Solution: From Azure AD, you create an assignment for the Insights at administrator role. Does this meet the goal?

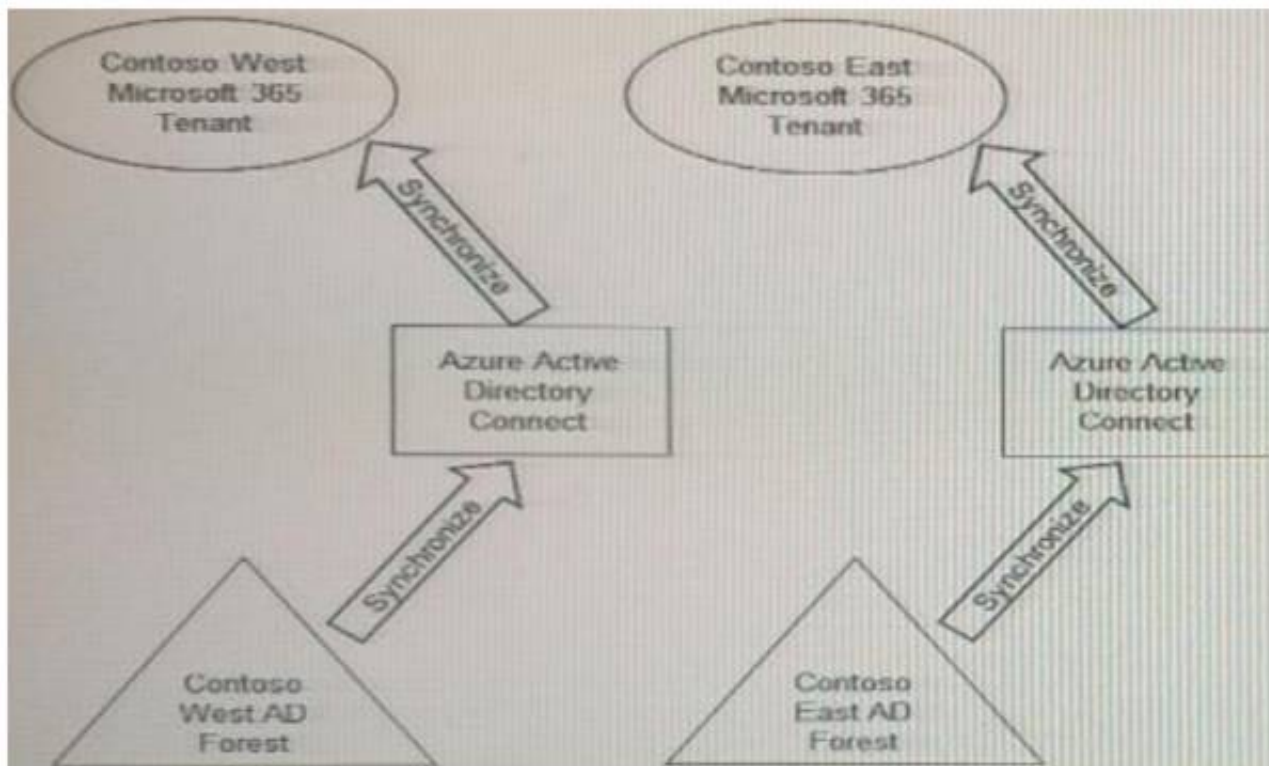
- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 53

- (Exam Topic 3)

Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture for both divisions is shown in the following exhibit.



You need to assign users from the Contoso East division access to Microsoft SharePoint Online sites in the Contoso West tenant. The solution must not require additional Microsoft 365 licenses.

What should you do?

- A. Configure The exiting Azure AD Connect server in Contoso Cast to sync the Contoso East Active Directory forest to the Contoso West tenant.
- B. Configure Azure AD Application Proxy in the Contoso West tenant.
- C. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync theContoso East Active Directory forest to the Contoso West tenant.
- D. Create guest accounts for all the Contoso East users in the West tenant.

**Answer:** D

#### NEW QUESTION 55

- (Exam Topic 3)

You have an Azure Active Directory (Azure AD) tenant.

You need to review the Azure AD sign-ins log to investigate sign ins that occurred in the past. For how long does Azure AD store events in the sign-in log?

- A. 14 days
- B. 30 days
- C. 90 days
- D. 365 days

**Answer:** B

#### NEW QUESTION 58

- (Exam Topic 3)

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit. (Click theExhibittab.)

### Custom smart lockout

Lockout threshold ⓘ 5 ✓

Lockout duration in seconds ⓘ 3600 ✓

### Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Contoso  
Litware  
Tailwind  
project  
Zettabyte  
MainStreet



### Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

You are evaluating the following passwords:

- Pr0jectlitw@re
- T@ilw1nd
- C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd
- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

**Answer: C**

#### Explanation:

Reference:

<https://blog.enablingtechcorp.com/azure-ad-password-protection-password-evaluation>

### NEW QUESTION 62

- (Exam Topic 3)

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com. You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

Which four 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.

Actions	Answer Area
Sign in to the Microsoft 365 admin center.	
Create a self-signed user account in the Azure AD tenant.	
From the Microsoft 365 admin center, add the domain name.	
Respond to the Become the admin message.	
From the Microsoft 365 admin center, remove the domain name.	
Create a TXT record in the contoso.com DNS zone.	

A.



Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover>

NEW QUESTION 63

- (Exam Topic 3)

You have a Microsoft 365 tenant.

In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

- A. an access policy in Microsoft Cloud App Security.
- B. Terms and conditions in Microsoft Endpoint Manager.
- C. a conditional access policy in Azure AD
- D. a compliance policy in Microsoft Endpoint Manager

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

NEW QUESTION 64

- (Exam Topic 3)

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements.

- Identify sign-ins by users who ate suspected of having leaked credentials.
- Rag the sign-ins as a high risk event.
- Immediately enforce a control to mitigate the risk, while still allowing the user to access applications. What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app-enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require multi-factor authentication
- Grant access but require password change

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To classify leaked credentials as high-risk, use:

- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app-enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require multi-factor authentication
- Grant access but require password change

NEW QUESTION 69

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your SC-300 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/SC-300-dumps.html>