PassQueen
a.k.a dumpsqueen.com

Microsoft Identity and Access Administrator

Microsoft SC-300

Version Demo

Total Demo Questions: 37

Total Premium Questions: 374

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Configure and manage a Microsoft Entra ID	60
Topic 2, Implement and manage identities	75
Topic 3, Implement and manage authentication	113
Topic 4, Implement and manage access management for apps	63
Topic 5, Plan and implement identity governance	48
Topic 6, Mix Questions	2
Topic 7, Case Study 1	2
Topic 8, Case Study 2	4
Topic 9, Case Study 3	2
Topic 10, Case Study 4	3
Topic 11, Case Study 5	2
Total	374

QUESTION NO: 1

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

You need to bulk create 25 new user accounts by uploading a template file. Which properties are required in the template file?

A. displayName, identityIssuer, usageLocation, and userType

B. accountEnabled, givenName, surname, and userPrincipalName

C. accountEnabled, displayName, userPrincipalName, and passwordProfile

D. accountEnabled, passwordProfile, usageLocation, and userPrincipalName

ANSWER: C

Explanation:

accountEnabled, displayName, userPrincipalName, and passwordProfile are the required properties for creating cloud-only user accounts through the bulk-upload template. The user principal name supplies the unique sign-in name for each new account, while the display name provides the user's directory display value. The accountEnabled value determines whether the newly created identity is permitted to sign in. A password profile supplies the initial password configuration required for a new cloud user, including the initial password and, where applicable, the requirement to change that password at first sign-in.

These values are the core creation properties needed to establish a usable Microsoft Entra ID user object. The bulk-create process uses a comma-separated values template that maps its required columns to the corresponding directory user attributes. Administrators can include additional profile, organization, contact, and location values when needed, but they are not required merely to create the account. In the downloaded template, password-related input may be presented with a friendly column name such as an initial password, while its directory representation corresponds to the password profile used during user creation.

For Microsoft's bulk user-creation procedure and template guidance, see Bulk add users in Microsoft Entra ID. The required user-creation properties are also documented in the Microsoft Graph create user API reference.

QUESTION NO: 2

You have a Microsoft Entra ID tenant that contains an on-premises web application named App1.

You plan to publish App1 by using Microsoft Entra Application Proxy.

Which two actions are required before users can access App1 through Application Proxy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Install an Application Proxy connector.

B. Publish App1 by configuring an internal URL and an external URL.

C. Configure an inbound firewall rule from the internet to the connector server.

D. Deploy Microsoft Entra Connect Sync on the connector server.

E. Create an Azure VPN Gateway.

ANSWER: A B

Explanation:

You must install an **Application Proxy connector** on a Windows Server that can reach the internal application. The connector establishes outbound connections to the Application Proxy service and relays requests to App1. You must also publish App1 as an Enterprise Application Proxy application and configure its internal URL and external URL.

Application Proxy does not require inbound firewall connections to the connector server, Azure VPN Gateway, or Microsoft Entra Connect Sync. Microsoft Entra Connect Sync is used for directory synchronization and is unrelated to publishing an on-premises application through Application Proxy. See Add an on-premises application for remote access through Application Proxy and Install and register a connector.

QUESTION NO: 3

You have a Microsoft Entra tenant.

You need to create a Conditional Access policy to manage administrative access to the tenant. The solution must ensure that administrators are authenticated by using a phishing-resistant multi-factor authentication (MFA) method.

Which three authentication methods should you include in the solution? Each correct answer presents a complete solution.

A. Windows Hello for Business

B. a FIDO2 security key

C. certificate-based authentication (multi-factor)

D. voice call

E. SMS

F. email OTP

G. certificate-based authentication (single-factor)

ANSWER: A B C

Explanation:

Microsoft Entra Conditional Access can enforce an *authentication strength*, including the built-in Phishing-resistant MFA strength. This strength is intended for high-value scenarios such as administrative access because it requires authentication methods that are bound to the user or device and resist credential phishing and replay attacks. Windows Hello for Business meets this requirement by using device-bound cryptographic credentials, typically protected by a biometric gesture or PIN. A FIDO2 security key also provides phishing resistance through public-key cryptography and origin binding, which helps prevent use on a fraudulent sign-in site. Certificate-based authentication (multi-factor) qualifies when the certificate credential is combined with an additional factor, such as a PIN, to satisfy the multifactor requirement. Configure the Conditional Access policy to target the applicable directory roles and require the Phishing-resistant MFA authentication strength. This ensures that an administrator must use one of the approved phishing-resistant methods when the policy applies. Microsoft documents the methods included in this built-in authentication strength and guidance for deploying it to protect privileged accounts. See Authentication strengths in Microsoft Entra ID and Certificate-based authentication in Microsoft Entra ID.

QUESTION NO: 4 - (HOTSPOT)

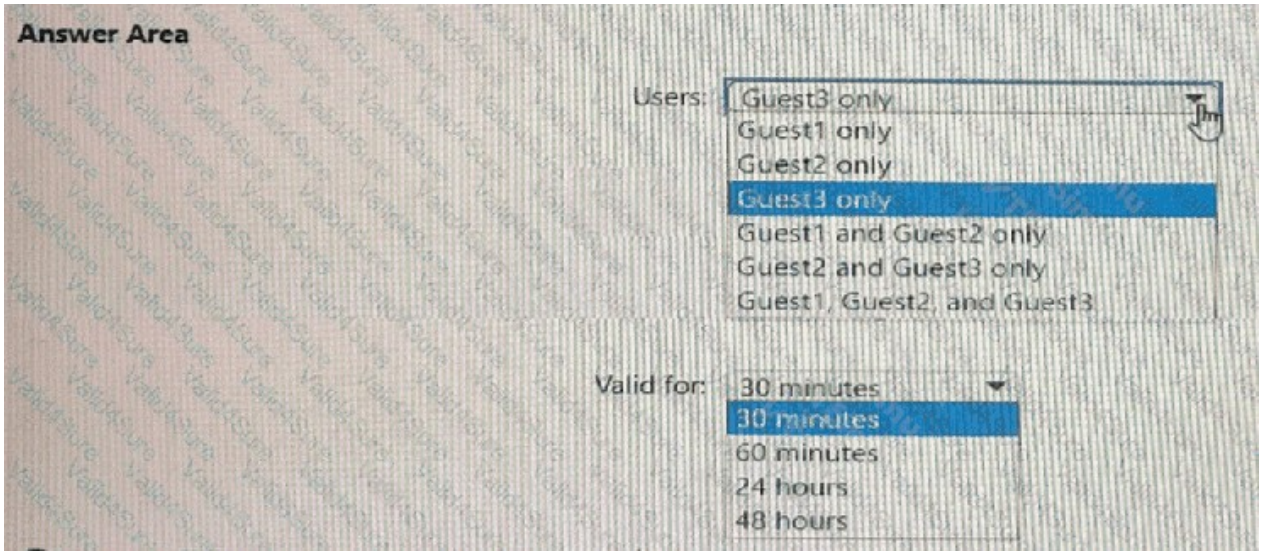
You have an Azure AD tenant named contoso.com that has Email one-time passcode for guests set to Yes.

You invite the guest users shown in the following table.

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



ANSWER:

Explanation:

Email one-time passcode authentication provides a way for B2B collaboration guests to access shared resources when they do not have an identity that Microsoft Entra ID can use for normal federation or Microsoft-account sign-in. In this scenario, the gmail.com guest is a personal Google-account user. That email address does not inherently provide a Microsoft Entra organizational identity or a Microsoft account identity for the invitation redemption flow. Because email one-time passcode is enabled for guests in contoso.com, Microsoft Entra ID sends this guest a verification code to the invited email address.

The passcode is intended to prove control of that mailbox during the sign-in and redemption process. Microsoft documents that an email one-time passcode is valid for 30 minutes and can be used only once. After the code is redeemed or expires, the guest must obtain another code if one is needed for a subsequent authentication attempt. Consequently, the correct selections are **Guest3 only** and **30 minutes**. Microsoft's guest-authentication behavior and the email one-time-passcode process are described in Email one-time passcode authentication for B2B guest users. The broader invitation and redemption behavior for external collaboration users is documented in B2B collaboration invitation redemption.

QUESTION NO: 5

You need to locate licenses to the A. Datum users. The solution must need the technical requirements.

Which type of object should you create?

A. A Dynamic User security group

B. An OU

C. A distribution group

D. An administrative unit

ANSWER: A

Explanation:

A Dynamic User security group is the appropriate object when licensing must be assigned automatically according to user attributes. In Microsoft Entra ID, dynamic groups evaluate a membership rule continuously. For example, a rule can include users whose department, country, job title, or a supported custom/extension attribute has a specified value. When an

applicable user attribute changes, Entra ID recalculates membership and adds or removes the user without an administrator manually maintaining the group.

Microsoft Entra group-based licensing can then assign a product license to that security group. Users who become members through the dynamic rule inherit the group's license assignment, and users who no longer satisfy the rule have the group-derived assignment removed, subject to any other direct or group-based assignments that apply. This approach centralizes licensing, supports attribute-driven automation, and scales effectively for an organization such as A. Datum.

Microsoft documents that licenses can be assigned to security groups and Microsoft 365 groups, including groups with dynamic membership. Dynamic membership rules and their supported user properties are documented in Dynamic membership rules for groups in Microsoft Entra ID. For the licensing workflow and requirements, see Assign licenses to users by group membership in Microsoft Entra ID.

QUESTION NO: 6

You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Global Administrator
User2	User Administrator
User3	Groups Administrator
User4	*None*

From the tenan1, you configure a naming policy for groups.

Which users are affected by the naming policy?

A. User2 only

B. User3only

C. User2 and User3 only

D. User3 and User4 only

E. User1, User2, and User3 only

F. User1, User2, User3, and User4

ANSWER: D

Explanation:

User3 and User4 only are affected by the Microsoft 365 group naming policy. A group naming policy enforces organizational naming standards whenever users create or edit Microsoft 365 groups. It can add required prefixes and suffixes to group names and can block specified custom words. The policy is enforced for group-creation experiences across Microsoft 365 workloads that create Microsoft 365 groups, helping ensure names remain consistent and suitable for discovery and governance.

Microsoft documents an explicit exemption for users assigned the Global Administrator or User Administrator Microsoft Entra roles. Those roles can create groups without being constrained by the configured group naming policy. Based on the roles shown, User1 is a Global Administrator and User2 is a User Administrator, so they are exempt. User3, who has the Groups Administrator role, is not one of the documented naming-policy exemptions; therefore, the policy applies when User3 creates a group. User4 has no exempt administrative role and is also subject to the policy. For implementation and scope details, see Microsoft 365 group naming policy and Microsoft Entra group naming policy guidance.

QUESTION NO: 7

You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.

B. From PowerShell, run Set-ADSyncScheduler.

C. From PowerShell, run Start-ADSyncSyncCycle.

D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

ANSWER: A

Explanation:

To synchronize users in the Adatum organizational unit, use the Microsoft Azure Active Directory Connect wizard and select **Customize synchronization options**. This path exposes the synchronization configuration settings, including the ability to change the selected Active Directory domains and organizational units. In the wizard, the administrator can select the appropriate Active Directory forest, open the domain and OU filtering settings, and include the Adatum OU in the synchronization scope. After the configuration is applied, Azure AD Connect Sync evaluates objects within that selected scope and synchronizes eligible users to Microsoft Entra ID during its next synchronization cycle.

OU filtering is appropriate when only a defined subset of on-premises Active Directory users should be synchronized, such as users stored in a dedicated OU. Microsoft recommends using the Azure AD Connect wizard to modify this filtering configuration rather than attempting to alter synchronization rules directly. The selected OU must also be included in the scope for any required dependent objects, such as groups or contacts, according to the organization's identity design. For details, see Microsoft Entra Connect Sync filtering configuration and custom installation and configuration options.

QUESTION NO: 8

You have a Microsoft Entra ID tenant that contains a user named User1.

You need to enable User1 to reset their password by using self-service password reset (SSPR).

Which two authentication methods can be enabled for SSPR? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Authenticator

B. mobile phone

C. Windows Hello for Business

D. Temporary Access Pass

E. device compliance status

ANSWER: A B

Explanation:

Microsoft Authenticator and **mobile phone** are supported authentication methods for Microsoft Entra self-service password reset. Administrators configure the available methods in the Authentication methods policy and configure SSPR for the appropriate users or groups. A user must register the required number of methods before they can use SSPR.

Security questions can be available only for selected user populations, but methods such as Windows Hello for Business and Temporary Access Pass are not methods used to complete an SSPR reset. Windows Hello for Business is a passwordless sign-in method, and a Temporary Access Pass is intended to bootstrap registration or recovery of other authentication methods. See How self-service password reset works and Authentication methods in Microsoft Entra ID.

QUESTION NO: 9

You have an Azure AD tenant and a .NET web app named App1.

You need to register App1 for Azure AD authentication.

What should you configure for App1?

A. the executable name

B. the bundle ID

C. the package name

D. the redirect URI

ANSWER: D

Explanation:

The redirect URI is required when registering a .NET web application for Microsoft Entra ID (formerly Azure AD) authentication. It identifies the endpoint in App1 to which Microsoft Entra ID returns the user's browser after the user successfully authenticates and authorizes the application. The application uses this return location to receive the authorization response and complete the sign-in flow, typically at a callback endpoint such as `https://app1.contoso.com/signin-oidc`. For security, the URI sent in an authentication request must match one of the redirect URIs registered on the app registration; this prevents tokens or authorization responses from being redirected to an untrusted destination. In the Azure portal, this value is configured under the app registration's Authentication settings, using the Web platform type for a server-side .NET web app. The URI should use HTTPS in production and be an exact registered callback address used by the application's OpenID Connect middleware. Microsoft documents redirect URIs and their matching requirements at Redirect URIs in the Microsoft identity platform. For the app-registration configuration process, see Quickstart: Register an application with the Microsoft identity platform.

QUESTION NO: 10

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

You need to identify users that are eligible for the Cloud Application Administrator role.

Which blade in the Privileged Identity Management settings should you use?

A. Azure resources

B. Privileged access groups

C. Review access

D. Azure AD roles

ANSWER: D

Explanation:

Azure AD roles is the correct PIM area because Cloud Application Administrator is a Microsoft Entra ID directory role, rather than an Azure resource role or a role associated with a privileged access group. In Privileged Identity Management, the Azure AD roles blade provides management and reporting for Microsoft Entra directory-role assignments. From there, an administrator can open the role assignments view and filter or select the eligible assignment state to identify users who can activate the Cloud Application Administrator role when needed. Eligible assignments provide just-in-time access: the user does not hold the role permanently but can activate it subject to the configured PIM policy, such as approval, multifactor authentication, justification, and time limits. Microsoft's directory-role PIM documentation describes using the Microsoft Entra roles area to manage eligible and active assignments, while the Cloud Application Administrator role is documented as a Microsoft Entra built-in role. See Assign Microsoft Entra roles in PIM and Cloud Application Administrator permissions.

QUESTION NO: 11

You have a Microsoft Entra ID P2 tenant that contains an enterprise application named App1.

Guest users are assigned to App1.

You need to review guest access to App1 every 90 days and automatically remove access when a reviewer denies access or does not respond.

Which two access review settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure a recurrence of every 90 days.

B. Enable auto apply results to resource.

C. Configure the review as a one-time review.

D. Disable recommendations.

E. Require users to accept terms of use.

ANSWER: A B

Explanation:

You should configure the access review with a **recurrence of every 90 days** and enable **auto apply results to resource**. A recurring application access review presents guest access assignments to the selected reviewers on the required schedule. The 90-day recurrence meets the periodic review requirement.

Automatically applying the results removes the application assignment when the review outcome is deny. The review can also be configured with an appropriate setting for users who do not respond, such as denying access, so that unanswered reviews result in removal when the review completes. Without automatic application, the review produces decisions but does not remove the users' access to App1. For more information, see Review access to applications and Microsoft Entra access reviews overview.

QUESTION NO: 12

You have a Microsoft Entra ID tenant.

You need to prevent users from authenticating to Microsoft 365 by using device code flow.

The solution must continue to allow browser-based authentication.

What should you configure?

A. a Conditional Access policy that targets device code flow and blocks access

B. a Conditional Access policy that blocks legacy authentication clients

C. a user risk policy that requires a secure password change

D. an authentication methods policy that disables SMS

ANSWER: A

Explanation:

You should configure a **Conditional Access policy that targets device code flow and blocks access**. Conditional Access includes an authentication flows condition that can target device code flow. A policy configured with this condition and a block-access grant control prevents authentication requests that use a device code.

The policy does not block browser-based authentication unless browser access is also included in the policy scope. This provides a targeted control for device-code authentication, which can be useful when an organization wants to reduce the risk associated with device-code phishing attacks. For more information, see Conditional Access authentication flows.

QUESTION NO: 13

You have a Microsoft Entra ID tenant that is synchronized with an on-premises Active Directory domain by using Microsoft Entra Connect Sync.

You plan to deploy password hash synchronization.

Which two statements are true about password hash synchronization? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Users can authenticate to cloud resources when the on-premises network is unavailable.

B. The plaintext password is never synchronized to Microsoft Entra ID.

C. Every cloud sign-in is validated by an on-premises authentication agent.

D. Password hash synchronization requires Active Directory Federation Services (AD FS).

E. Users must use a different password for cloud applications.

ANSWER: A B

Explanation:

Password hash synchronization synchronizes a hash derived from the on-premises Active Directory password hash to Microsoft Entra ID. The plaintext password is not synchronized to Microsoft Entra ID. Users can then authenticate to cloud resources by using Microsoft Entra ID without relying on an on-premises authentication agent for each sign-in.

Password hash synchronization also supports leaked credential detection in Microsoft Entra ID Protection because Microsoft can evaluate synchronized password hashes against known compromised credential data. Pass-through authentication differs because it validates passwords through on-premises authentication agents during sign-in. See Implement password hash synchronization and Microsoft Entra ID Protection risk detections.

QUESTION NO: 14

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

You configure self-service password reset (SSPR) by using the following settings:

• Require users to register when signing in: Yes

• Number of methods required to reset: 1

What is a valid authentication method available to users?

A. home phones

B. mobile app notification

C. a mobile app code

D. an email to an address in your organization

ANSWER: A

Explanation:

home phones is a valid telephone-based method for self-service password reset when a user has registered a phone number for password reset. Requiring users to register when signing in ensures that users are prompted to provide the information needed for the enabled SSPR authentication methods before they need to reset a password. Because the policy requires only one method to reset, a registered phone-based verification method can satisfy the reset requirement by receiving a verification call or code, depending on the phone method configuration.

SSPR is designed to let users prove their identity through registered authentication information and then create a new password without help-desk intervention. Microsoft documents phone-based authentication as an SSPR method and explains that the number of methods required by the SSPR policy determines how many registered methods a user must complete during a reset. With the requirement set to one, one successfully completed registered phone verification is sufficient. See How self-service password reset works in Microsoft Entra ID and Enable self-service password reset.

QUESTION NO: 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 use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed 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: A

Explanation:

Yes is correct. In Azure Monitor, an alert rule determines the condition that triggers an alert, while an action group determines what happens after that alert is triggered, including who receives its notifications. An action group can contain one or more notification actions, such as email, SMS, push notifications, voice calls, webhooks, Azure Functions, or ITSM actions. For this requirement, the administrator can edit the action group associated with the Azure AD sign-in alert rule, remove or replace the existing email recipient, and add the new security administrator's email address. Future alert instances that invoke that action group will then send the email notification to the new recipient. This approach changes alert delivery without requiring changes to the sign-in log query, the alert condition, or the alert rule's evaluation frequency. Azure Monitor action groups are designed to be reusable, so the same updated recipient configuration can also apply to every alert rule that uses that action group. For details, see Manage action groups in Azure Monitor and Azure Monitor alerts overview.

QUESTION NO: 16

You create a Log Analytics workspace.

You need to implement the technical requirements for auditing.

What should you configure in Azure AD?

A. Company branding

B. Diagnostics settings

C. External Identities

D. App registrations

ANSWER: B

Explanation:

Diagnostics settings is correct because Microsoft Entra ID uses diagnostic settings to route its audit and monitoring logs to an Azure Monitor destination, including a Log Analytics workspace. After a diagnostic setting is created, the administrator selects the relevant log categories, such as AuditLogs, and sends them to the workspace. This makes directory audit events available for retention, querying, correlation, alerting, workbooks, and integration with broader Azure Monitor and security operations processes.

Audit logs record changes and administrative activities in the tenant, such as modifications to users, groups, applications, roles, and policies. Configuring the diagnostic setting provides the required export pipeline from Microsoft Entra ID to the already-created workspace; merely viewing audit information in the portal does not establish that workspace destination. The setting can also send other Entra log categories when needed, but AuditLogs is the key category for an auditing requirement. Microsoft documents the process for configuring Entra diagnostic settings and choosing Log Analytics as a destination at Configure diagnostic settings for Microsoft Entra ID. Details about the audit log data and its uses are available in Microsoft Entra audit logs.

QUESTION NO: 17

You need to modify the settings of the User administrator role to meet the technical requirements. Which two actions should you perform for the role? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Select Require justification on activation

B. Set all assignments to Active

C. Set all assignments to Eligible

D. Modify the Expire eligible assignments after setting.

E. Select Require ticket information on activation.

ANSWER: C D

Explanation:

Set all assignments to Eligible because an eligible Microsoft Entra Privileged Identity Management assignment does not provide standing administrative access. Instead, the assigned user activates the User administrator role only when it is needed, which implements just-in-time privileged access. This is the appropriate assignment type when the requirement is for users to request or activate administrative permissions as needed rather than retain them continuously.

Modify the Expire eligible assignments after setting because eligible role assignments can be configured with an expiration period. Setting the eligible-assignment expiration to the required period, up to one year when that is the stated requirement, ensures that eligibility is available for the intended duration and then must be renewed or reassigned. These settings work together: eligibility enables on-demand activation, while the expiration configuration limits how long that eligibility remains valid. Microsoft documents that eligible assignments require activation before the role can be used and that role settings can control eligible-assignment expiration. See Assign Microsoft Entra roles in Privileged Identity Management and Configure Microsoft Entra role settings in Privileged Identity Management.

QUESTION NO: 18

You have a Microsoft Entra tenant that contains a terms of use (ToU) named Terms1. You create a Conditional Access policy named Policy1 to deploy Terms1. You need to configure Policy1 to require users to accept Terms1. Which settings should you configure for Policy1?

A. Conditions

B. Session

C. Grant

D. Target resources

ANSWER: C

Explanation:

You should configure **Grant** controls in Policy1. Microsoft Entra Terms of Use is enforced through a Conditional Access policy's grant controls, which determine requirements a user must satisfy before access to a targeted resource is allowed. In the policy's Grant section, select **Require terms of use** and choose the Terms1 agreement. When an in-scope user accesses an application covered by the policy, Microsoft Entra presents Terms1 if the user has not already accepted the version that applies to them. The user must accept the agreement to satisfy the access requirement and continue to the resource. Terms of Use can also be configured with settings such as requiring users to expand the agreement, requiring reacceptance after a period, and requiring acceptance again after the document is updated. Those agreement settings define the acceptance experience, while the Conditional Access Grant control is what applies the agreement during sign-in. For implementation guidance, see Microsoft Entra Terms of Use and Conditional Access grant controls.

QUESTION NO: 19

You have a Microsoft Entra ID tenant.

You create a Conditional Access policy that requires the Phishing-resistant MFA authentication strength.

Which two authentication methods can satisfy the policy? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. FIDO2 security key

B. Windows Hello for Business

C. SMS

D. Voice call

E. Microsoft Authenticator verification code

ANSWER: A B

Explanation:

FIDO2 security keys and **Windows Hello for Business** can satisfy the Phishing-resistant MFA authentication strength. These methods use cryptographic authentication that is bound to the user and the legitimate sign-in service, which helps prevent credential phishing and replay attacks.

SMS, voice calls, and one-time passcodes from an authenticator app can provide multifactor authentication, but they do not meet the phishing-resistant requirement. Authentication strengths allow administrators to require a specific set of methods through a Conditional Access grant control. For more information, see Authentication strengths and Passwordless authentication options.

QUESTION NO: 20

You have a Microsoft Entra ID tenant that contains an enterprise application named App1.

You need to investigate why a user was denied access to App1 during sign-in.

Which two locations can provide information about the Conditional Access evaluation for the sign-in? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the Sign-in logs

B. the Conditional Access insights and reporting workbook

C. the Audit logs

D. access reviews

E. the provisioning logs

ANSWER: A B

Explanation:

The **Sign-in logs** contain a Conditional Access tab that identifies the policies evaluated for an individual sign-in and shows the result of each policy. The **Conditional Access insights and reporting workbook** provides aggregated reporting and analysis of Conditional Access policy activity when the required logs are sent to a Log Analytics workspace.

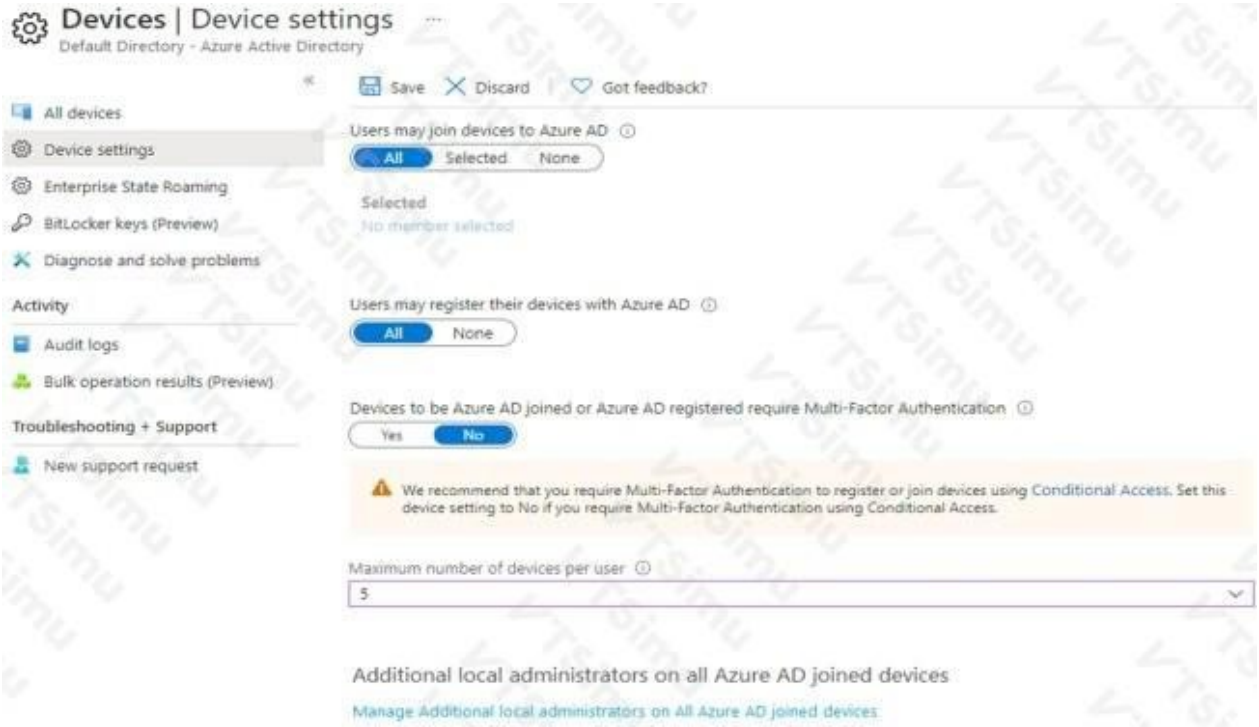
Audit logs record directory changes, such as policy creation or modification, but do not provide the per-sign-in Conditional Access evaluation needed to investigate the denied request. Access reviews and provisioning logs also do not contain Conditional Access policy results. See Sign-in logs in Microsoft Entra ID and Conditional Access insights and reporting workbook.

QUESTION NO: 21 - (HOTSPOT)

You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	**None**

You have the Device Settings shown in the following exhibit.



User1 has the devices shown in the following table.

Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

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 join four additional Windows 10 devices to Azure AD.	○	○
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

ANSWER:

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	○
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Explanation:

Azure AD device settings govern both how many devices an individual user can join and which identities receive local administrator rights on Azure AD-joined Windows devices. The configured maximum device-join value is applied per user. Because User1 has only the qualifying number of existing Azure AD-joined devices shown in the device table, User1 remains within the configured limit when joining four more Windows 10 devices. This is evaluated against the Azure AD join limit, rather than treating every device relationship as an Azure AD join.

The setting that requires Multi-Factor Authentication to join devices or register devices is a tenant-level device configuration. An administrator with the applicable tenant administrative privileges can modify this device setting. This permits Admin1 to set the requirement to Yes, which causes MFA to be required during the relevant device join or registration scenarios.

Local administrator membership on an Azure AD-joined device is not automatically granted merely because an identity exists in the tenant or has a role unrelated to the configured additional local device administrators list. By default, the Azure AD user who joins a Windows device becomes its local administrator, and tenant administrators or users explicitly configured as additional local administrators can also receive that access. Since Admin2 is not included in the applicable additional local-administrator assignment, Admin2 is not a local administrator on Device3.

Microsoft documents these controls in Manage device identities using the Microsoft Entra admin center and explains local administrator behavior for joined devices in Manage the local administrators group on Microsoft Entra joined devices.

QUESTION NO: 22

You have a Microsoft Entra ID tenant.

You need to require multi-factor authentication (MFA) for access to Microsoft 365 from all locations except the corporate network.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a named location that contains the corporate public IP address ranges.

B. Exclude the corporate named location from the Locations condition of the Conditional Access policy.

C. Include the corporate named location in the Locations condition of the Conditional Access policy.

D. Configure the corporate named location as a trusted authentication method.

E. Create a device filter that excludes all corporate devices.

ANSWER: A B

Explanation:

You should create a **named location** that contains the organization's public corporate IP address ranges and configure the Conditional Access policy to **exclude that named location** from its Locations condition. The policy then applies to sign-ins from all other locations and can use Require multifactor authentication as its grant control.

Named locations provide a reusable way to define network locations by IP address ranges or countries and regions. Excluding the corporate named location ensures that users connecting from the listed corporate egress IP addresses are not targeted by this particular MFA policy. For more information, see Conditional Access location condition and Named locations in Conditional Access.

QUESTION NO: 23 - (DRAG DROP)

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You need to ensure that User1 can create access reviews for groups, and that User2 can review the history report for all the completed access reviews. The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role 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.

ANSWER:

Explanation:

Assign User1 the **Identity Governance Administrator** role. This Microsoft Entra role is designed for identity-governance work and permits the user to create and manage access reviews. Access reviews are an Identity Governance capability used to periodically validate whether people still need access to group memberships, applications, and privileged resources. The role provides the required administrative capability without granting broad control over unrelated tenant settings, users, subscriptions, or security configuration. This directly follows least privilege because User1 receives permissions specifically intended to administer the access-review lifecycle.

Assign User2 the **Global Reader** role. Global Reader is a read-only Microsoft Entra directory role that allows a user to view administrative settings and reporting information across the tenant, including information needed to review completed access-review history. Since User2 only needs to inspect the history report rather than create, modify, configure, or take action on access reviews, a read-only role is appropriate. The tenant-wide visibility of Global Reader also ensures that the user can review history for completed access reviews regardless of the resource or review scope involved.

These assignments separate the ability to administer access reviews from the ability to examine their completed historical results. Microsoft documents the permissions and responsibilities of directory roles in the Microsoft Entra built-in roles reference. For access-review administration details, see Manage access reviews.

QUESTION NO: 24

You have the Azure resources show in the following table.

Name	Description
User1	User account
Group1	Security group that uses the Dynamic user membership type
VM1	Virtual machine with a system-assigned managed identity
App1	Enterprise application
RG1	Resource group

To Which identities can you assign the Contributor role for RG1?

A. User1 only

B. User1 and Group1 only

C. User1 and VW1 only

D. User1, VM1, and App1 only

E. User1, Group1, Vm1, and App1

ANSWER: E

Explanation:

User1, Group1, Vm1, and App1 is correct because Azure role-based access control (Azure RBAC) role assignments can be made to Microsoft Entra security principals at a resource group scope such as RG1. A user account, such as User1, can receive a role assignment directly. A security group, such as Group1, can also be assigned the Contributor role, allowing members to receive the permissions through group membership. App1 is represented by a service principal for an enterprise application, which is a supported principal type for Azure RBAC assignments. Vm1 can receive the role assignment through its system-assigned managed identity. A system-assigned managed identity is a service principal created in Microsoft Entra ID for the Azure resource, enabling the virtual machine to authenticate to Azure services without storing credentials in code or configuration. Contributor grants management access to Azure resources within RG1, but does not grant permission to assign Azure roles. Assigning the role at the RG1 scope makes its permissions apply to resources contained in that resource group. Microsoft documents the supported Azure RBAC security principal types and managed identity behavior in Azure RBAC overview and Managed identities for Azure resources overview.

QUESTION NO: 25

You have a Microsoft Entra ID P2 tenant.

You plan to use entitlement management to govern access to company resources.

Which three resource types can you add to an entitlement management catalog? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. enterprise applications

B. Microsoft 365 groups

C. SharePoint Online sites

D. Conditional Access policies

E. administrative units

ANSWER: A B C

Explanation:

Enterprise applications, **Microsoft 365 groups**, and **SharePoint Online sites** are supported catalog resource types. A catalog is a container for resources that can later be included in access packages. Access packages assign the appropriate role or permission for each catalog resource to approved requestors.

After the resources are added to a catalog, an access package can bundle access to those resources and apply assignment policies, approval workflows, expiration, and access reviews. Conditional Access policies and administrative units are Microsoft Entra configuration objects, but they are not resources that can be added to an entitlement management catalog. For more information, see Create and manage a catalog of resources in entitlement management.

QUESTION NO: 26

You create a new Microsoft 365 E5 tenant.

You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).

What should you configure?

A. a sign-in risk policy

B. a user risk policy

C. an MFA registration policy

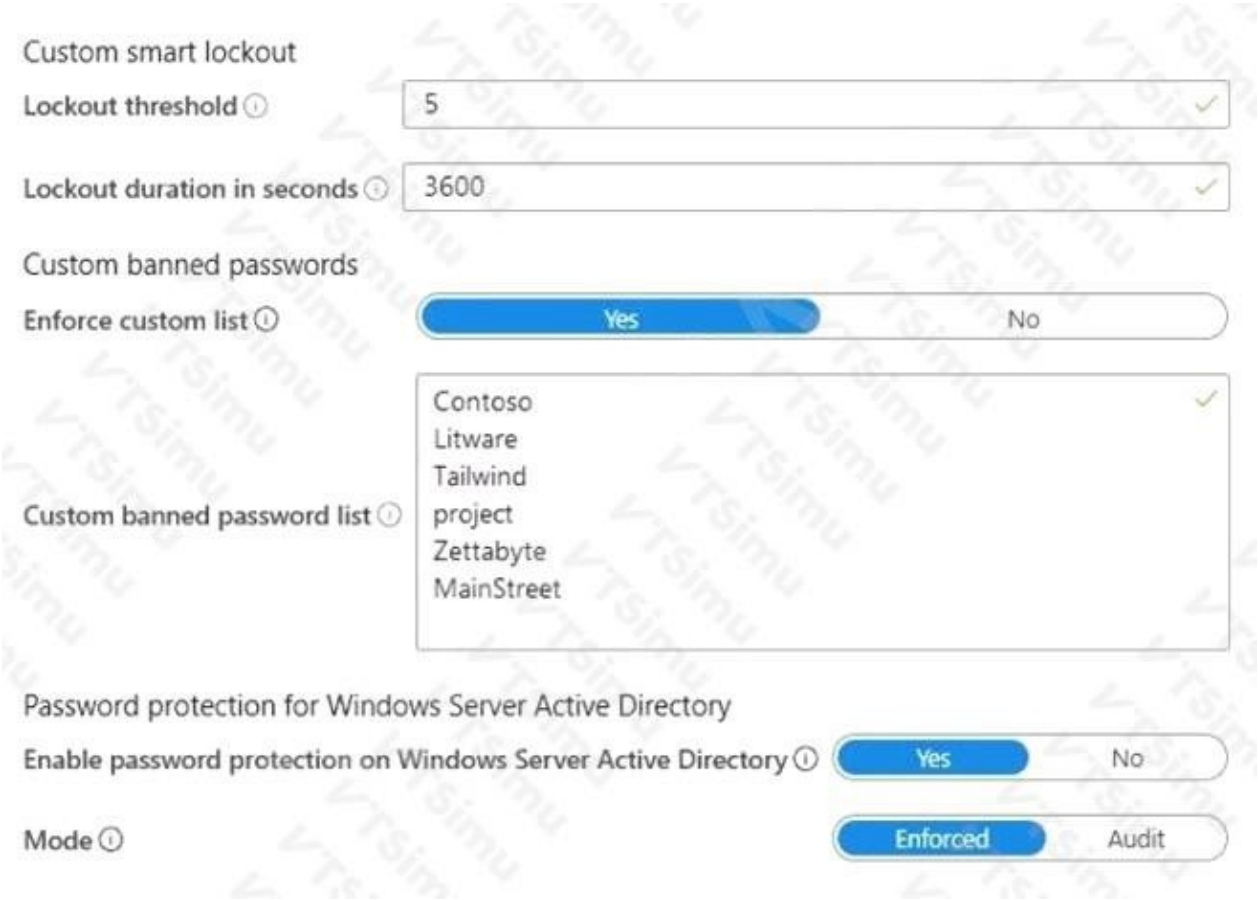
ANSWER: A

Explanation:

a sign-in risk policy is the appropriate configuration because Microsoft Entra ID Protection evaluates risk associated with each authentication attempt. An anonymous IP address is a Microsoft Entra sign-in risk detection, typically identified when a user authenticates through an anonymizing proxy, such as Tor, or another IP source that obscures the user's normal location. A sign-in risk policy can target users and configure the required action for qualifying sign-ins. Setting the policy to require multifactor authentication ensures that a user whose sign-in is assessed at the selected risk level must successfully complete MFA before access is granted. This directly addresses the requirement because the control is evaluated during the portal sign-in, rather than only assessing long-term account compromise indicators or requiring users to register authentication methods. Microsoft recommends using risk-based Conditional Access policies to automatically challenge potentially risky sign-ins with MFA and reduce the chance that compromised credentials can be used from suspicious network sources. For details about anonymous IP address detections, see Microsoft Entra ID Protection risk detections. For configuring sign-in risk policies, see Configure Microsoft Entra ID Protection risk policies.

QUESTION NO: 27

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



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:

C0nt0s0, Pr0jectlitw@re, and T@ilw1nd will be blocked. Microsoft Entra Password Protection evaluates passwords against both the global banned-password list and the configured custom banned-password list. Its evaluation is deliberately resilient to common attempts to evade a banned term. Before comparison, the service performs normalization that accounts for typical character substitutions, such as using `0` for `o`, `1` for `i`, and `@` for `a`. Therefore, the password strings still correspond to the configured banned names and terms after normalization.

Password Protection also uses fuzzy matching rather than requiring an exact, case-sensitive textual match. This helps prevent otherwise predictable variations of organizational names, project names, and other custom banned terms from being accepted merely because a user has changed characters or capitalization. In this configuration, each listed password contains a normalized form of a banned custom term, so each receives a sufficiently high banned-password score and is rejected. For implementation details, see Password ban lists in Microsoft Entra ID and Microsoft Entra Password Protection password evaluation.

QUESTION NO: 28 - (DRAG DROP)

DRAG DROP

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.

You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 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.

Select and Place:

ANSWER:

Explanation:

To use **contoso.com** as the default domain suffix for new Microsoft 365 users, first add **contoso.com** as a custom domain in the Microsoft 365 admin center or Microsoft Entra admin center. Adding it begins the ownership-validation process and provides the DNS information required to prove that the organization controls the domain.

Next, create the specified TXT record in the public DNS zone that is hosted by the domain registrar or DNS provider. A TXT record is commonly used because it establishes domain ownership without changing mail flow or other production DNS services. After the TXT record has propagated, successfully verify the domain name in Microsoft 365. Verification allows the tenant to use the custom domain as an accepted and managed domain.

Finally, set **contoso.com** to primary. The primary domain is automatically selected as the default domain suffix when administrators create new users, so new accounts receive names such as **user@contoso.com**. The original **contoso.onmicrosoft.com** domain is the tenant's initial Microsoft-managed domain and should remain available rather than

being removed. Microsoft documents the process of adding, verifying, and making a custom domain the default domain at Add a domain to Microsoft 365 and Domains FAQ.

QUESTION NO: 29

You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.

You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.

You need to download the Azure AD log that contains conditional access policy data.

What should you export from Azure AD?

A. sign-ins in JSON format

B. sign-ins in CSV format

C. audit logs in JSON format

D. audit logs in CSV format

ANSWER: A

Explanation:

sign-ins in JSON format is the appropriate export. Microsoft Entra ID sign-in logs record each interactive and non-interactive authentication attempt and include Conditional Access evaluation information. For a sign-in event, this includes the Conditional Access status and policy-level details showing the policies evaluated and their results. This is the operational data a SIEM needs to investigate how Conditional Access was applied to authentication activity, identify blocked or successful access attempts, and correlate policy outcomes with users, applications, devices, locations, and risk signals.

JSON is well suited to third-party SIEM ingestion because it retains structured sign-in event properties, including nested Conditional Access policy information, in a machine-readable format. A SIEM can parse these properties and use them for searches, correlations, dashboards, detections, and long-term analysis. Microsoft documents Conditional Access information as part of the sign-in log details and supports downloading sign-in log data from the Microsoft Entra admin center. For continuous production monitoring, organizations can also send sign-in logs to Azure Monitor Logs, Event Hubs, or a storage account through diagnostic settings, enabling downstream SIEM integration.

See Microsoft Entra sign-in logs and Microsoft Entra diagnostic settings.

QUESTION NO: 30

You have a Microsoft Entra ID P2 tenant.

You plan to configure Privileged Identity Management (PIM) for the Global Administrator role.

You need to require users to provide a justification and complete multifactor authentication when they activate the role.

Which two role settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Require justification on activation

B. Require multifactor authentication on activation

C. Require approval to activate

D. Expire eligible assignments after

E. Require access reviews

ANSWER: A B

Explanation:

Configure **Require justification on activation** and **Require multifactor authentication on activation** in the role activation settings for the Global Administrator role. These settings apply when an eligible user requests just-in-time activation of the role. PIM records the supplied justification and requires the user to complete MFA before the role becomes active.

Assignment expiration controls how long an assignment remains eligible or active, but it does not require a justification or MFA at the time of activation. Access review settings provide periodic governance over assignments and are not an activation-time control. See Configure Microsoft Entra role settings in PIM and Activate Microsoft Entra roles in PIM.

QUESTION NO: 31 - (SIMULATION)

You have an Azure subscription that is linked to a Microsoft Entra tenant named contoso.com. The subscription contains a group named Group1 and a virtual machine named VM1.

You need to meet the following requirements:

• Enable a system-assigned managed identity for VM1.

• AddVM1 to Group1.

How should you complete the PowerShell script? To answer, drag the appropriate cmdlets to the correct targets. Each cmdlet 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.

ANSWER: See the explanation for the answer

Explanation:

Select the following cmdlets for the two blanks:

The completed script is:

`Update-AzVM -IdentityType SystemAssigned` enables the VM's system-assigned managed identity. That identity is represented in Microsoft Entra ID by a service principal, so `Get-AzADServicePrincipal` retrieves its object ID for use as the group member reference.

QUESTION NO: 32

You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.

You enable combined registration in interrupt mode.

You create a new user named User1.

Which two authentication methods can User1 use to complete the combined registration process? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. a FID02 security key

B. a hardware token

C. a one-time passcode email

D. Windows Hello for Business

E. the Microsoft Authenticator app

ANSWER: C E

Explanation:

a one-time passcode email and **the Microsoft Authenticator app** are supported in the combined security-information registration experience for the respective SSPR and MFA/SSPR registration requirements. Combined registration provides a single registration journey for users who need both Microsoft Entra multifactor authentication and self-service password reset. An email address can be registered as an SSPR authentication method, allowing the user to receive a verification code for password-reset operations. This is relevant because SSPR is enabled for the tenant.

The Microsoft Authenticator app is a supported combined-registration method and provides an MFA-capable method through push notifications or verification codes. It can also be used for SSPR verification, so it supports the stronger MFA requirement while contributing to the user's password-reset security information. In interrupt mode, the registration prompt is presented during sign-in when the user must provide the required security information, rather than waiting for the user to visit the Security info page voluntarily. Microsoft documents the unified registration experience and its supported methods in Combined security information registration. The method capabilities for MFA and SSPR are detailed in Authentication methods in Microsoft Entra ID.

QUESTION NO: 33

You have a Microsoft Entra ID tenant that contains an enterprise application named App1.

App1 supports System for Cross-domain Identity Management (SCIM) provisioning.

You plan to configure automatic user provisioning from Microsoft Entra ID to App1.

Which two values must you obtain from App1 before you configure provisioning? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. tenant URL

B. secret token

C. redirect URI

D. application ID

E. verified domain name

ANSWER: A B

Explanation:

You must obtain the **tenant URL** and a **secret token** from App1. The tenant URL identifies the SCIM endpoint to which Microsoft Entra ID sends provisioning requests. The secret token is used by the provisioning service to authenticate to that endpoint.

These values are entered on the Provisioning page for the enterprise application before the connection can be tested and provisioning can be started. A redirect URI and an application ID are used for application authentication configurations such as OAuth or OpenID Connect, but they do not provide the SCIM endpoint and credential required for automatic provisioning. For more information, see Automate user provisioning to SaaS applications with Microsoft Entra ID.

QUESTION NO: 34

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

A. the Set -KindohsProductKcy cmdlct

B. the Update-MgGroup cmdlet

C. the Set-MgUserLicense cmdlet

D. the Update-MgUser cmdlet

ANSWER: C

Explanation:

The **Set-MgUserLicense cmdlet** is the appropriate tool for removing the individually assigned Office 365 Enterprise E3 licenses at scale. Group-based assignment of Microsoft 365 Enterprise E5 adds the E5 entitlement but does not automatically remove a separate direct license assignment already present on each user. Direct assignments must therefore be explicitly removed. Microsoft Graph PowerShell supports this through `Set-MgUserLicense`, which accepts licenses to add and licenses to remove for a user. A script can obtain the E3 SKU ID, iterate through the affected users, and pass that SKU ID in the `-RemoveLicenses` collection while supplying an empty `-AddLicenses` collection. This provides a repeatable, bulk administrative approach for all 2,500 users rather than requiring individual portal actions. The E5 licenses remain available because their source is the group assignment, independent of removal of the direct E3 assignments. Microsoft documents the cmdlet and its `RemoveLicenses` parameter in the Set-MgUserLicense reference. Licensing assignment concepts, including direct and group-based assignments, are also covered in Microsoft Entra group-based licensing documentation.

QUESTION NO: 35

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

You plan to bulk invite Azure AD business-to-business (B2B) collaboration users.

Which two parameters must you include when you create the bulk invite? Each correct answer presents part of

the solution

NOTE: Each correct selection is worth one point.

A. email address

B. redirection URL

C. username

D. shared key

E. password

ANSWER: A B

Explanation:

Bulk invitation of Microsoft Entra B2B collaboration users uses a specially formatted comma-separated values (CSV) file. The required columns are **email** and **redirectUrl**, which correspond to the email address and redirection URL parameters. The email address identifies the external person who will receive the B2B invitation. It must contain a valid address for the guest so Microsoft Entra ID can create the guest invitation and send the invitation message.

The redirection URL specifies the destination to which the guest is sent after they accept the invitation and complete the redemption process. Including a suitable application or organization URL provides a defined post-redemption experience and is mandatory in the bulk-invitation CSV format. Additional columns, such as display name, invitation message, or user type, can be supplied when appropriate, but they are optional. The bulk-invite workflow validates that the required email and redirect URL values are present for each invitation record before processing the upload. Microsoft documents the required CSV fields and provides a downloadable template in the bulk invitation guidance: Bulk invite B2B collaboration users. For background on guest collaboration and invitation redemption, see B2B collaboration overview.

QUESTION NO: 36 - (SIMULATION)

Task 7

You need to lock out accounts for five minutes when they have 10 failed sign-in attempts.

ANSWER: See the explanation for the answer

Explanation:

In the Microsoft Entra admin center, configure **Smart lockout** as follows:

1. Go to **Protection** > **Authentication methods** > **Password protection**.
2. Under **Smart lockout**, set **Lockout threshold** to `10`.
3. Set **Lockout duration in seconds** to `300` (five minutes).
4. Select **Save**.

This locks users out after 10 failed sign-in attempts for five minutes.