Number: Associate Google Workspace Administrator
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: Associate Google Workspace Administrator

Exam Name: Associate Google Workspace Administrator

Exam A

QUESTION 1
The current data storage limit for the sales organizational unit (OU) at your company is set at 10GB per user. A subset of sales representatives in that OU need 100GB of storage across shared services. You need to increase the storage for only the subset of sales representatives by using the least disruptive approach and the fewest configuration steps. What should you do?

A. Move the subset of users to a sub-OU, and assign a 100GB storage limit to that sub-OU.
B. Instruct the subset of users to store their documents in a Shared Drive with a 100GB limit.
C. Change the storage limit of the sales OU to 100GB.
D. Create a configuration group, and add the subset of users to that group. Set the group storage limit to 100GB.

Correct Answer: A
Section:
Explanation:
By moving the subset of sales representatives to a sub-organizational unit (OU) and assigning a 100GB storage limit to that sub-OU, you can efficiently increase the storage for those users without affecting the rest of the sales team. This approach allows you to target the specific users that require more storage, maintaining minimal disruption and configuration steps.

QUESTION 2
Your company's security team should be able to investigate unauthorized external file sharing. You need to ensure that the security team can use the security investigation tool and you must follow the principle of least privilege. What should you do?

A. Grant the super admin role to a delegate from the security team.
B. Create a pre-built reporting role. Assign the role to the security team alias.
C. Share the Drive audit log with the security team.
D. Create a custom admin role with security center privileges. Assign the role to the individual security team members.

Correct Answer: D
Section:
Explanation:
By creating a custom admin role with security center privileges, you can ensure that the security team has the necessary access to investigate unauthorized external file sharing while adhering to the principle of least privilege. This approach provides the security team with the specific permissions they need without granting unnecessary broader privileges, such as those associated with the super admin role.

QUESTION 3
Users at your company are reporting that they are not receiving some emails in their corporate Gmail account. You have checked the Google Workspace Status Dashboard and you found no service disruptions. You need to identify the root cause of the problem and resolve the mail delivery issues. What should you do? (Choose two.)

A. Use Email Log Search (ELS) to identify specific delivery failures.
B. Verify whether the organization's Mail Exchange (MX) records are correctly configured.
C. Check the users' spam folders to determine whether emails are being misdirected.
D. Investigate the Gmail log events for error messages or unusual patterns.
E. Check the senders' IP addresses in the inbound mail gateway.

Correct Answer: A, B
Section:
Explanation:

Use Email Log Search (ELS): ELS allows you to trace email delivery and identify issues, such as undelivered or bounced messages. This is an essential tool for identifying the root cause of mail delivery issues.
Verify whether the organization's Mail Exchange (MX) records are correctly configured: Incorrect MX records could prevent emails from being delivered to the organization's Gmail accounts. It's important to verify that these records are set up properly to ensure smooth email delivery.

QUESTION 4
Your organization is concerned about unauthorized access attempts. You want to implement a security measure that makes users change their password if there are twenty or more failed login attempts within one hour. You want to use the most effective and efficient approach. What should you do?

A. Set up a Chrome action rule to restrict users from defined ChromeOS actions after twenty failed password attempts.
B. Create an activity rule for user log events, define a time period and threshold, and select an Action for the rule to force a password change.
C. Create an activity rule for live-state data sources that meets the required time period and threshold to identify users who need to change their password.
D. Enable email alerts to notify users that they need to change their password.

Correct Answer: B
Section:
Explanation:
Creating an activity rule for user log events allows you to monitor failed login attempts within a specific time period (such as one hour) and set a threshold (like twenty attempts). This rule can automatically trigger an action, such as forcing a password change, when the defined threshold is met. This is the most effective and efficient approach to addressing unauthorized access attempts while ensuring that security measures are enforced without manual intervention.

QUESTION 5
An employee using a Workspace Enterprise Standard license was terminated from your organization. You need to ensure that the former employee no longer has access to their Workspace account and preserve access to the former employee's documents for the manager and the team.
You want to minimize license cost. What should you do?

A. Delete the former employee's Workspace account.
B. Suspend former employee's Workspace account.
C. Reset the password of the former employee and keep their Workspace license active.
D. Switch the license type of the former employee's Workspace account to an Archived User license.

Correct Answer: D
Section:
Explanation:
Switching the former employee's account to an Archived User license ensures that their data and documents are preserved, and access is retained for the manager and team without incurring the full cost of an active Workspace license. Archived User licenses are a cost-effective way to maintain access to documents while preventing unauthorized access to the account.

QUESTION 6
Your organization's employees frequently collaborate with external clients and vendors by using Google Meet. There are active instances of unsupervised meetings within your organization that do not have a host, and unsupervised meetings that continue after an event has completed. You want to end all meetings that are being used inappropriately as quickly as possible. What should you do?

A. End all unsupervised meetings by using the Google Meet APIs.
B. Enable Host Management for Google Meet, and train internal host employees how to end meetings for everyone.
C. Turn off Google Meet in the Admin console for your organization. Turn Google Meet back on after two minutes.
D. Identify and end all unsupervised meetings by using the security investigation tool.

Correct Answer: A
Section:
Explanation:

Using the Google Meet APIs allows you to programmatically end all unsupervised meetings quickly. This approach is the most effective for managing unsupervised meetings in real-time, especially if there are multiple such meetings happening across the organization. It provides a centralized method to monitor and take action on these meetings, ensuring security and preventing misuse.

QUESTION 7
Your organization uses live-streaming to host large Google Meet meetings. You need to limit the participation to affiliated Google Workspace domains by using the Admin console. What should you do?

A. Add the Trusted Workspace domain names in the Stream dialog box.
B. Turn off live streaming to Youtube.
C. Add participants to an organizational unit (OU). Turn on live streaming.
D. Turn on in-house live streaming. Invite users from affiliated domains.

Correct Answer: C
Section:
Explanation:
By organizing participants into an organizational unit (OU) in the Admin console, you can control access to live streaming and ensure that only users from affiliated Google Workspace domains are allowed to participate in the live-streamed meetings. Turning on live streaming within this context will ensure that the meeting is restricted to the appropriate participants from the specified domains.

QUESTION 8
You are configuring email for your company's Google Workspace account. The company wants to prevent certain types of files from being sent or received as email attachments in the simplest and most cost-effective way. What should you do?

A. Adjust the maximum message size limit to prevent large files from being sent or received.
B. Enable the Security Sandbox in Gmail to automatically quarantine emails with suspicious attachments.
C. Scan all incoming and outgoing emails for malicious attachments by using an industry standard third-party email security solution.
D. Configure an attachment compliance rule in Gmail settings to block specific file types.

Correct Answer: B
Section:
Explanation:
Configuring an attachment compliance rule in Gmail allows you to specifically block certain types of files from being sent or received as email attachments. This approach is simple and cost-effective because it leverages Google Workspace's built-in functionality without requiring third-party solutions or advanced configurations. You can easily specify which file types to block, ensuring that your organization is protected from undesirable attachments.

QUESTION 9
Your organization has a Shared Drive with 150 users organized as a group. All users of the group need to be able to add and edit files, but the ability to move, delete, and share content must be limited to a single user. You need to configure the shared drive to meet these requirements efficiently.
What should you do?
Your organization has a Shared Drive with 150 users organized as a group. All users of the group need to be able to add and edit files, but the ability to move, delete, and share content must be limited to a single user. You need to configure the shared drive to meet these requirements efficiently.
What should you do?

A. Create a folder inside the shared drive. Share the files with the group by using the share function.
B. Create a folder inside the shared drive. Share the folder link with the group.
C. In the Admin console, assign Contributor access for the shared drive to each user. Assign Content Manager access for the shared drive to the single user.
D. In the Admin console, assign Contributor access for the shared drive to the group. Assign Content Manager access for the shared drive to the single user.

Correct Answer: D
Section:

Explanation:
By assigning Contributor access to the group, all 150 users will be able to add and edit files in the shared drive. Assigning Content Manager access to the single user ensures that only that person has the ability to move, delete, and share content within the shared drive. This approach efficiently meets the requirement of limiting certain administrative privileges while allowing the group to collaborate on content.

QUESTION 10
Your company wants to minimize distractions and inappropriate content in their Google Chat spaces. You need to give trusted employees the ability to remove messages and ban users from specific Chat spaces. What should you do?

A. Assign the trusted employees as moderators for the relevant Chat spaces.
B. Create a data loss prevention (DLP) rule that blocks inappropriate content from being shared
C. Use the security investigation tool to audit and monitor Chat messages.
D. Disable all Chat spaces except those specifically approved by management.

Correct Answer: A
Section:
Explanation:
Assigning trusted employees as moderators for the relevant Chat spaces will give them the necessary privileges to remove messages and ban users when needed. This is the most efficient way to control inappropriate content and maintain a positive and productive environment within the spaces. Moderators can take action to address issues directly without requiring more complex or restrictive solutions.

QUESTION 11
Your organization acquired a small agency. You need to create user accounts for these new employees. The new users must be able to use their new organization's email address and their email address with the sub-agency domain name. What should you do?
Your organization acquired a small agency. You need to create user accounts for these new employees. The new users must be able to use their new organization's email address and their email address with the sub-agency domain name. What should you do?

A. Redirect the acquired domain to Google's MX records and add the account as a ''send as'' address.
B. Set up the acquired agency as a secondary domain from the Manage domains page.
C. Set up the acquired agency as a user alias domain from the Manage domains page.
D. Set up the acquired agency as a secondary domain and swap it to the primary domain.

Correct Answer: C
Section:
Explanation:
Setting up the acquired agency as a user alias domain allows users to have their new organization's email address while still being able to send and receive emails using their previous email address with the sub-agency domain. This approach efficiently ensures they can use both email addresses without requiring additional configuration for separate accounts.

QUESTION 12
You are designing a group structure for your company that will be used to grant access to a specific shared drive. You need this solution to automatically add and remove employees based on their job role. What should you do?

A. Create a security group. Add all employees with the desired job role. Grant the security group access to the shared drive.
B. Create a distribution list. Add all employees with the desired job role. Grant the distribution list access to the shared drive.
C. Create a dynamic group. Set the membership criteria to the desired job role. Grant the dynamic group access to the shared drive.
D. Create a configuration group. Add users on an exception basis. Grant the configuration group access to the shared drive.

Correct Answer: C
Section:
Explanation:

A dynamic group automatically manages its membership based on user attributes, such as job role. This approach ensures that employees are automatically added or removed from the group based on their role, minimizing manual effort and ensuring that the group always reflects the current team composition. Granting this dynamic group access to the shared drive ensures that the right users have the appropriate permissions without requiring constant manual updates.

QUESTION 13
You are migrating your organization's email to Google Workspace. Your organization uses the terramearth.com email domain. You need to configure Google Workspace to receive emails sent to terramearth.com. What should you do?

A. Add terramearth.com as a primary, secondary, or alias domain in Google Workspace. Update the Mail Exchange (MX) records with your domain registrar to direct mail flow to Google's mail servers.
B. Establish a Transport Layer Security (TLS) connection between your company's existing mail servers and Google's mail servers
C. Configure an email address in Google Workspace to capture emails sent to unverified domains, including terramearth.com.
D. Create a domain alias for terramearth.com in Google Workspace. Configure email forwarding to redirect emails to the new Google Workspace accounts.

Correct Answer: A
Section:
Explanation:
To receive emails for your domain (terramearth.com) in Google Workspace, you need to add the domain to Google Workspace as either a primary, secondary, or alias domain, depending on your organization's requirements. After adding the domain, you must update the Mail Exchange (MX) records at your domain registrar to point to Google's mail servers. This step is essential to ensure that emails are correctly routed to Google Workspace.

QUESTION 14
Your organization is migrating their current on-premises email solution to Google Workspace. You need to ensure that emails sent to your domain are correctly routed to Gmail. What should you do?

A. Change the Mail Exchange (MX) records in your current email domain's DNS settings to point to Google's mail servers.
B. Set up email forwarding from your on-premises email provider to Gmail.
C. Create a content compliance rule to filter and route incoming emails.
D. Configure SPF, DKIM, and DMARC records in your current email domain's DNS settings.

Correct Answer: A
Section:
Explanation:
To ensure that emails sent to your domain are correctly routed to Gmail, you need to update the Mail Exchange (MX) records in your domain's DNS settings to point to Google's mail servers. This is a critical step in the migration process, as it ensures that all incoming email traffic is directed to Google Workspace after the switch.

QUESTION 15
Your compliance team has observed that employees at your organization are frequently resetting their passwords and is concerned about account hijacking. You need to create a solution to notify the compliance team whenever a user updates or resets their password. What should you do?

A. Create and enforce a new password policy for all users in your organization.
B. Move all compliance team members into a separate organizational unit (OU). Create and enforce a new password policy for the members of this OU.
C. Create an activity rule that is triggered by the User's password changed event. Add compliance team members as email recipients.
D. Create a new alert by using user log events. Check that the challenge type is ''Password'', and add the compliance team as email recipients.

Correct Answer: C
Section:
Explanation:
Creating an activity rule that triggers on the 'User's password changed' event allows you to automatically notify the compliance team whenever a user updates or resets their password. This approach is efficient because it directly ties the event to the rule and sends alerts without requiring manual monitoring or additional steps. By adding the compliance team as email recipients, you ensure they are promptly notified of any changes.

QUESTION 16
Multiple users in your organization are reporting that Calendar invitations sent from a specific department are not being received. You verified that the invitations are being sent and there are no error messages in the sender's logs. You want to troubleshoot the issue. What should you do?

A. Analyze the message headers of the sent invitations by using the Google Admin Toolbox to identify any delivery issues.
B. Verify that the senders in the specific department have the necessary permissions to share their calendars externally and send invitations outside of the organization.
C. Disable and re-enable the Calendar service for the affected users to refresh their connection.
D. Check the affected users' Calendar settings to confirm whether they have accidentally blocked invitations from the specific department.

Correct Answer: A
Section:
Explanation:
Using the Google Admin Toolbox to analyze the message headers of the sent invitations helps you identify if there are any issues with the delivery of the invitations, such as misrouted messages or issues with email delivery to the affected users. This approach will give you detailed information on what might be causing the issue, even if no error messages appear in the sender's logs.

QUESTION 17
The names and capacities of several conference rooms have been updated. You need to use the most efficient way to update these details.
What should you do?

A. Export the resource list to a CSV file, make the changes, and re-import the updated file.
B. Edit each resource in the Google Admin console.
C. Add the modified rooms as new resources. Tell employees not to use old rooms.
D. Delete the existing resources and recreate the resources with the updated information.

Correct Answer: A
Section:
Explanation:
Exporting the resource list to a CSV file, making the necessary updates, and then re-importing the file is the most efficient method for updating multiple conference rooms at once. This approach allows you to make bulk updates quickly without needing to edit each resource individually or delete and recreate rooms. It also ensures that the updated information is applied to all affected rooms at once.

QUESTION 18
You are configuring Chrome browser security policies for your organization. These policies must restrict certain Chrome apps and extensions.
You need to ensure that these policies are applied on the devices regardless of which user logs into the device. What should you do?

A. Configure the allowed list of apps in the Devices page in the apps and extensions settings.
B. Configure the Chrome user setting to require users to sign in to use Chrome apps and extensions.
C. Configure the Policy Precedence to override the domain-wide policy applied for apps and extensions.
D. Require 2SV for user logins.

Correct Answer: A
Section:
Explanation:
To ensure that Chrome apps and extension policies are applied regardless of which user logs into the device, you should configure the allowed list of apps in the Devices section of the apps and extensions settings. This policy applies at the device level, ensuring that the restrictions are enforced for any user who logs into that device, providing consistent security across the organization.

QUESTION 19
Your company's help desk is receiving technical support tickets from employees who report that messages from known external contacts are being sent to the spam label in Gmail. You need to correct the issue and ensure delivery of legitimate emails without introducing additional risk as soon as possible. What should you do?

A. Ask employees to select the messages in Gmail that are being delivered to spam and mark them as Not spam.
B. Contact the external senders, and tell them to authenticate their sent mail by using domain-based message authentication, reporting, and conformance (DMARC).
C. Turn off more aggressive spam filtering in spam policies that are applied to the users' organizational unit and add the senders' mail system IP addresses to the email allowlist.
D. Create an address list of approved senders so messages from these users bypass Gmail's spam filters and recipients can decide whether they are spam or not.

Correct Answer: A
Section:
Explanation:
Asking employees to mark legitimate emails as 'Not spam' helps train Gmail's spam filter to correctly identify these senders as trusted. This is a quick and effective way to correct the issue without introducing any additional risk or changes to the email filtering settings. Over time, Gmail will learn to recognize these senders as legitimate, reducing the likelihood of their messages being misclassified as spam in the future.

QUESTION 20
Your organization collects credit card information in customer files. You need to implement a policy for your organization's Google Drive data that prevents the accidental sharing of files that contain credit card numbers with external users. You also need to record any sharing incidents for reporting. What should you do?

A. Create a data loss prevention (DLP) rule that uses the predefined credit card number detector, sets the action to ''block external sharing'', and enables the ''Log event'' option.
B. Enable Gmail content compliance, and create a rule to block email attachments containing credit card numbers from being sent to external recipients.
C. Implement a third-party data loss prevention solution to integrate with Drive and provide advanced content detection capabilities.
D. Configure a data retention policy to automatically delete files containing credit card numbers after a specified period.

Correct Answer: A
Section:
Explanation:
A data loss prevention (DLP) rule with the predefined credit card number detector will help you identify and prevent the accidental sharing of files that contain sensitive credit card information. Setting the action to 'block external sharing' ensures that such files cannot be shared externally. Enabling the 'Log event' option will record any incidents of external sharing for auditing and reporting purposes, fulfilling both the security and reporting requirements.

QUESTION 21
You are investigating a potential data breach. You need to see which devices are accessing corporate data and the applications used. What should you do?

A. Analyze the audit log in the Admin console for device and application activity.
B. Analyze the security investigation tool to access device log data.
C. Analyze the Google Workspace reporting section of the Admin console.
D. Analyze the User Accounts section in the Google Admin console.

Correct Answer: A
Section:
Explanation:
The audit log in the Google Admin console provides detailed information about device and application activity, which is crucial for investigating a potential data breach. You can see which devices have accessed corporate data, as well as which applications were used, giving you a comprehensive view of any unauthorized or suspicious activities. This is the most appropriate and efficient tool for this investigation.

QUESTION 22
Your organization is implementing a new customer support process that uses Gmail. You need to create a cost-effective solution that allows external customers to send support request emails to the customer support team. The requests must be evenly distributed among the customer support agents. What should you do?

A. Create a Google Group, enable collaborative inbox settings, set posting permissions to ''Anyone on the web'', and add the customer support agents as group members.

B. Use delegated access for a specific email address that represents the customer support group, and add the customer support team as delegates for that email address.
C. Create a Google Group, add the support agents to the group, and set the posting permissions to ''Public.''
D. Set up an inbox for the customer support team. Provide the login credentials to the customer support team.

Correct Answer: A
Section:
Explanation:
A Google Group with collaborative inbox settings allows you to evenly distribute support request emails among the team. By setting the posting permissions to ''Anyone on the web,'' external customers can send emails directly to the group, and the emails will be distributed to the support agents as tasks. This is a cost-effective solution that also provides an organized way to manage and track customer support requests.

QUESTION 23
Your organization has enabled Google Groups for Business to let employees create and manage their own email distribution lists and web forums. You need to ensure that users cannot join external Google Groups with their Google Workspace accounts without interrupting internal group usage. What should you do?

A. Set the setting for Google Groups for Business called Accessing groups from outside this organization to Private.
B. In Additional Google Services, turn Google Groups OFF at the root organizational unit.
C. Use the Directory API to change the settings of user-created groups to disable features that allow external users to access, view, or post on groups.
D. Set the setting for Google Groups for Business called Default for permission to view conversations to All organization users.

Correct Answer: A
Section:
Explanation:
By setting the Accessing groups from outside this organization to Private, you prevent users from joining external Google Groups while still allowing internal users to use Google Groups within the organization. This setting ensures that only members of your organization can join and interact with internal groups, effectively stopping external access without affecting internal group usage.

QUESTION 24
You manage Chrome Enterprise browsers for your large organization. You want to ensure that specific extensions are automatically installed on all managed Chrome Enterprise browsers. What should you do?

A. Allowlist the specific Chrome browser extensions.
B. Configure a script to deploy the extensions upon user login.
C. Publish the extensions in the Chrome Web Store.
D. Force-install the extensions through Chrome browser policies.

Correct Answer: D
Section:
Explanation:
Using Chrome browser policies, you can force-install specific extensions on all managed Chrome Enterprise browsers. This ensures that the desired extensions are automatically installed on users' browsers without requiring manual installation. This approach is the most efficient and scalable solution for managing extensions across a large organization.

QUESTION 25
You need to grant a specific set of users in your company access to YouTube, and you want to restrict their access to Merchant Center. What should you do?

A. Enable YouTube for all users in the company. Individually restrict access to Merchant Center for specific Groups or organizational units (OUs).
B. Create YouTube and Merchant Center as custom web apps. Apply access policies at the Group or organizational unit (OU) level.
C. Contact Google Support and request that they enable YouTube access for the specific set of users and restrict their access to Merchant Center.
D. Enable access to YouTube at the Group or organizational unit (OU) level for the subset of users. Disable access to Merchant Center.

Correct Answer: D
Section:
Explanation:
By enabling YouTube access at the Group or organizational unit (OU) level, you can target a specific set of users, allowing them to access YouTube. Simultaneously, you can disable access to Merchant Center for those same users, ensuring they can access YouTube but not Merchant Center. This approach uses Google Workspace's built-in capabilities to manage access based on user groups or organizational units.

QUESTION 26
Your organization is about to conduct its biannual risk assessment. You need to help identify security risks by quickly reviewing all security settings for Gmail, Drive, and Calendar. What should you do?

A. In the reporting section of the Admin console, review the Gmail, Drive, and Calendar reports.
B. In the alert center, review all of the alerts.
C. In each individual organizational unit (OU), review the security settings.
D. In the Google Admin console, review the security health page.

Correct Answer: D
Section:
Explanation:
The security health page in the Google Admin console provides an overview of security settings and highlights potential risks across various services, including Gmail, Drive, and Calendar. This page offers a consolidated view of the security posture of your organization, making it the most efficient option for quickly identifying security risks in preparation for a risk assessment.

QUESTION 27
You need to ensure that data owned by former employees remains available in Google Vault. You want to use the most cost-effective solution.
What should you do?

A. Migrate the former employees' Gmail to their manager(s) by using the data migration service during the deletion process. Transfer the former employees' Google Drive files to a new owner.
B. Change the Google account passwords of the former employees.
C. Suspend the former employees' Google accounts. Create an organizational unit (OU). Move the former employees into that OU.
D. Assign an Archived User license to the former employees' Google accounts.

Correct Answer: C
Section:
Explanation:
Suspending the accounts of former employees while moving them to a dedicated organizational unit (OU) ensures that their data remains in Google Vault and accessible without the need for additional licenses. This is a cost-effective solution because suspending the account keeps the data intact but prevents the employees from accessing their accounts.

QUESTION 28
A user is experiencing intermittent issues accessing their Gmail inbox. Sometimes their Gmail loads slowly, and other times the user encounters error messages that haven't been documented. You need to effectively troubleshoot this recurring problem. What should you do?

A. Check the Google Workspace Status Dashboard for any reported service disruptions.
B. Instruct the user to generate a HAR file the next time they experience slowness or an error.
C. Instruct the user to try to access Gmail from another device or network to see if the issue persists.
D. Instruct the user to clear their browser cache and cookies.

Correct Answer: B
Section:
Explanation:
A HAR file (HTTP Archive) records detailed information about the user's network activity, including HTTP requests and responses. This file can help diagnose issues with Gmail loading slowly or errors occurring, especially

when they are intermittent. By generating a HAR file, you can provide valuable data for troubleshooting the issue and pinpoint any underlying network or browser-related issues.

QUESTION 29
You are managing the buildings and resources for your organization. You need to create several conference rooms with a capacity of 10 people each, equipped with a whiteboard and projector, and wheelchair accessible. You want to ensure the process is efficient. What should you do?

A. Automate room creation by using a third-party app from the Google Workspace Marketplace.
B. Create a CSV file and add all resources. Write a script using the Workspace API to reference the CSV file and create all the resources.
C. Create each conference room individually in the Google Admin console. Add the features for each room.
D. Use the Google Admin console to bulk upload the rooms. Create a resource with the specified features and apply the features to that resource.

Correct Answer: B
Section:
Explanation:
Using a CSV file to list all the conference rooms and a script to automate their creation via the Workspace API is the most efficient solution. This approach allows you to batch-create the rooms with the specified attributes (capacity, whiteboard, projector, wheelchair accessible) without manually inputting each room individually. It minimizes manual effort and ensures consistency across all room configurations.

QUESTION 30
A user in your organization received a spam email that they reported for further investigation. You need to find out more details and the scope of this incident as quickly as possible. What should you do?

A. Conduct a Vault search to find this email and identify if additional users were affected.
B. Conduct a search to find all emails sent by the sender by using the Gmail API.
C. Conduct an Email reports search to find this email and all of the email's recipients.
D. Conduct a search in the security investigation tool to find this email, and identify whether additional users were affected.

Correct Answer: D
Section:
Explanation:
The security investigation tool is specifically designed for investigating security incidents like spam and phishing emails. It allows you to search for emails, review their details, and determine the scope of the incident, including identifying whether other users were affected. This tool is the most appropriate and efficient way to respond to the incident.

QUESTION 31
You work at a large organization that prohibits employees from using Google Sites. However, a task force comprised of three people from five different departments has recently been formed to work on a project assigned by the Office of the CIO. You need to allow the users in this task force to temporarily use Google Sites. You want to use the least disruptive and most efficient approach. What should you do?

A. Turn Google Sites access on for each of the 15 users in the task force.
B. Create a configuration group for the task force's 15 users. Grant Google Sites access to the group.
C. Place the 15 task force users into a new organizational unit (OU). Turn on Google Sites access for the OU.
D. Create an access group for the task force's 15 users. Grant Google Sites access to the group.

Correct Answer: C
Section:
Explanation:
Creating a new organizational unit (OU) for the task force members and turning on Google Sites access for that OU is the least disruptive and most efficient approach. It allows you to target only the users in the task force, granting them temporary access to Google Sites without impacting the rest of the organization. This solution also provides clear control over the access, which can be easily modified when the task force's work is completed.