CERTSWARRIOR

Google

Google-Workspace-Administrator
Professional Google Workspace Administrator

Questions & Answers PDF

For More Information:

https://www.certswarrior.com/

Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

Latest Version: 11.0

Question: 1

Madeupcorp.com is in the process of migrating from a third-party email system to Google Workspace. The VP of Marketing is concerned that her team already administers the corporate AdSense, AdWords, and YouTube channels using their @madeupcorp.com email addresses, but has not tracked which users have access to which service. You need to ensure that there is no disruption.
What should you do?

A. Run the Transfer Tool for Unmanaged users.
B. Use a Google Form to survey the Marketing department users.
C. Assure the VP that there is no action required to configure Google Workspace.
D. Contact Google Enterprise Support to identify affected users.

Answer: A

Explanation:
Assess the Current State: Identify which users are using the @madeupcorp.com email addresses for services like AdSense, AdWords, and YouTube.
Use the Transfer Tool for Unmanaged Users:
Access Google Admin Console: Go to admin.google.com and sign in with your administrator account.
Navigate to Tools: In the Admin console, go to "Tools" and then select "Transfer tool for unmanaged users."
Enter Domain Information: Enter the domain name (madeupcorp.com) and verify the domain.
List Unmanaged Users: The tool will generate a list of unmanaged users who are using their @madeupcorp.com email addresses.
Send Transfer Requests: Send transfer requests to these users, prompting them to accept the transfer to the managed Google Workspace account.
Follow Up: Ensure all users have accepted the transfer request to avoid any disruptions in accessing Google services with their corporate email addresses.
Verify: Confirm that the transferred accounts are now managed under the Google Workspace domain.
Reference:
Google Workspace Admin Help - Transfer tool for unmanaged users

Question: 2

Your company has an OU that contains your sales team and an OU that contains your market research team. The sales team is often a target of mass email from legitimate senders, which is distracting to their job duties. The market research team also receives that email content, but they want it because it often contains interesting market analysis or competitive intelligence. Constant Contact is often used as the source of these messages. Your company also uses Constant Contact for your own mass email marketing.

You need to set email controls at the Sales OU without affecting your own outgoing email or the market research OU.
What should you do?

A. Create a blocked senders list as the Sales OU that contains the mass email sender addresses, but bypass this setting for Constant Contact emails.
B. Create a blocked senders list at the root level, and then an approved senders list at the Market Research OU, both containing the mass email sender addresses.
C. Create a blocked senders list at the Sales OU that contains the mass email sender addresses.
D. Create an approved senders list at the Market Research OU that contains the mass email sender addresses.

Answer: A

Explanation:
Access Google Admin Console: Go to admin.google.com and sign in with your administrator account.
Navigate to Email Settings: In the Admin console, go to "Apps" > "Google Workspace" > "Gmail" > "Spam,
Phishing, and Malware".
Select the Sales OU: Ensure you are configuring settings for the Sales OU specifically.
Create a Blocked Senders List:
Add Mass Email Sender Addresses: Enter the email addresses or domains of the mass email senders that the sales team finds distracting.
Bypass for Constant Contact: Create a rule to bypass this blocked senders list for emails coming from Constant Contact. This can usually be done by setting up an exception rule within the same settings area.
Apply and Save Settings: Ensure the settings are saved and propagated to the Sales OU.
Verify Configuration: Send test emails to confirm that the Sales OU is filtering unwanted mass emails while still receiving those from Constant Contact.
Reference:
Google Workspace Admin Help - Set up email controls for your organization
Google Workspace Admin Help - Block or allow specific email addresses

Question: 3

Your organization is part of a highly regulated industry with a very high turnover. In order to recycle licenses for new employees and comply with data retention regulations, it has been determined that certain Google Workspace data should be stored in a separate backup environment.
How should you store data for this situation?

A. Use routing rules to dual-deliver mail to an on-premises SMTP server and Google Workspace.
B. Write a script and use Google Workspace APIs to access and download user data.
C. Use a third-party tool to configure secure backup of Google Workspace data.
D. Train users to use Google Takeout and store their archives locally.

Answer: C

Explanation:
Evaluate Third-Party Backup Solutions: Identify third-party tools that offer secure backup solutions for Google Workspace. Examples include Backupify, Spanning Backup, and Afi.ai.
Choose a Suitable Tool: Based on your organization's needs and compliance requirements, select a tool that offers robust data retention, secure storage, and easy recovery options.
Set Up the Backup Solution:
Create an Account: Sign up for the chosen third-party backup service.
Configure Backup Settings: Link your Google Workspace account and configure the backup settings to meet your data retention policies.
Schedule Backups: Set up regular backup schedules to ensure data is continuously backed up.
Test Backups and Recovery: Perform initial backups and test the recovery process to ensure data can be retrieved efficiently when needed.
Monitor and Maintain: Regularly monitor the backup status and maintain the system to comply with your organization's data retention regulations.
Reference:
Google Workspace Admin Help - Choose a third-party backup tool
Backupify - Google Workspace Backup

Question: 4

Your organization is on Google Workspace Enterprise and allows for external sharing of Google Drive files to facilitate collaboration with other Google Workspace customers. Recently you have had several incidents of files and folders being broadly shared with external users and groups. Your chief security officer needs data on the scope of external sharing and ongoing alerting so that external access does not have to be disabled.
What two actions should you take to support the chief security officer's request? (Choose two.)

A. Review who has viewed files using the Google Drive Activity Dashboard.
B. Create an alert from Drive Audit reports to notify of external file sharing.
C. Review total external sharing in the Aggregate Reports section.
D. Create a custom Dashboard for external sharing in the Security Investigation Tool.
E. Automatically block external sharing using DLP rules.

Answer: BD

Explanation:
Create an Alert for External Sharing:
Access Google Admin Console: Go to admin.google.com and sign in with your administrator account.
Navigate to Rules: Go to "Security" > "Alert Center" > "Manage Rules".
Create a New Rule: Select "Create Rule" and choose "Drive Audit" as the event source.
Configure Rule Settings: Set the conditions to trigger alerts when files or folders are shared externally.
Set Notification Preferences: Configure who should receive the alerts and how they should be notified.
Save the Rule: Save and activate the rule to start receiving alerts on external sharing activities.

Create a Custom Dashboard for External Sharing:
Access Security Investigation Tool: In the Admin console, go to "Security" > "Investigation Tool".
Create a New Investigation: Click "Create" and select "Drive" as the data source.
Set Up Investigation Parameters: Define the parameters to track external sharing activities (e.g., file shared externally, users involved).
Create Dashboard: Save the investigation as a custom dashboard to continuously monitor external sharing activities.
Review and Monitor: Regularly review the dashboard and set up automated reports if necessary.
Reference:
Google Workspace Admin Help - Create and manage alerts
Google Workspace Admin Help - Use the security investigation tool

Question: 5

Your organization's Sales Department uses a generic user account (sales@company.com) to manage requests. With only one employee responsible for managing the departmental account, you are tasked with providing the department with the most efficient means to allow multiple employees various levels of access and manage requests from a common email address.
What should you do?

A. Configure a Google Group as an email list.
B. Delegate email access to department employees.
C. Configure a Google Group as a collaborative inbox.
D. Configure a Google Group, and set the Access Level to Announcement Only.

Answer: C

Explanation:
Create a Google Group:
Go to the Google Groups interface.
Click on "Create Group."
Enter the group name, email address (e.g., sales@company.com), and description.
Configure Group Settings:
After creating the group, go to "Group settings."
Under "Permissions," set who can view topics, post, and join the group as per your requirement.
Set Up Collaborative Inbox:
In the Group settings, navigate to "Settings" > "Email options."
Check the box for "Enable Collaborative Inbox."
This option allows group members to assign topics, mark them as resolved, and categorize posts for better management.
Assign Roles and Permissions:
Define roles for members (e.g., Manager, Member).
Assign permissions to allow various levels of access, such as viewing and managing conversations.
Add Members:
Add the employees who need access to this group.
Go to "Manage members" and click "Add members."

Reference:
Google Groups Collaborative Inbox
Create and Configure Google Groups

CERTSWARRIOR

FULL PRODUCT INCLUDES:

Money Back Guarantee

Instant Download after Purchase

90 Days Free Updates

PDF Format Digital Download

24/7 Live Chat Support

Latest Syllabus Updates

For More Information – Visit link below:

https://www.certswarrior.com

16 USD Discount Coupon Code: U89DY2AQ