Testpassport Q&A

La meilleure qualité le meilleur service

Exam : **Google Workspace Administrator**

Title : Professional Google Workspace Administrator

Version : DEMO

1.Your company has numerous locations throughout the world. Each of these locations has multiple office managers that field questions from employees through an email alias. Some questions have not been answered by an office manager.
How can you create a system to assign conversations to different receptionists using Workspace?
A. Create a Google Groups Collaborative Inbox.
B. Use App Script to design a ticketing system that marks conversation ownership.
C. Contract with a third-party solution, such as ServiceNow.
D. Create Google Tasks and assign them to receptionists to address unanswered questions.
Answer: A

2.The company's ten most senior executives are to have their offices outfitted with dedicated, standardized video conference cameras, microphones, and screens. The goal is to reduce the amount of technical support they require due to frequent, habitual switching between various mobile and PC devices throughout their busy days. You must ensure that it is easier for the executives to join Meet video conferences with the dedicated equipment instead of whatever device they happen to have available.
What should you do?
A. Set up unmanaged Chromeboxes and set the executives' homepage to meet.google.com via Chrome settings.
B. Set up the executive offices as reservable Calendar Resources, deploy Hangouts Meet Hardware Kits, and associate the Meet hardware with the room calendars.
C. Deploy Hangouts Meet Hardware Kits to each executive office, and associate the Meet hardware with the executives' calendars.
D. Provision managed Chromeboxes and set the executives' Chrome homepage to meet. google.com via device policy.
Answer: B
Explanation:
Option B is the most suitable answer because it allows for the integration of hardware specifically designed for Google Meet with the room resources in the calendar. This will enable executives to easily book and use their office space for meetings, with the Meet hardware automatically integrated into the room's calendar resource, streamlining the process of setting up and joining video conferences.
Let's look at the other options:
A. Setting up unmanaged Chromeboxes and setting the homepage to meet.google.com doesn't necessarily streamline the process of joining a meeting as they would still need to manually enter meeting details, and the devices being unmanaged could potentially lead to other issues.
C. Associating the Meet hardware directly with the executives' calendars might seem like a good idea, but it doesn't account for the possibility of the executives having meetings outside their offices or needing to book the room for other types of meetings.
D. Provisioning managed Chromeboxes with the homepage set to meet.google.com would streamline the process of getting to the Meet homepage, but like option A, it wouldn't integrate the hardware setup with the calendar system to streamline the process of scheduling and joining meetings.
So, option B is the best choice for streamlining the process and reducing the amount of technical support needed.

3.You have configured SSO using a third-party IDP with your Google Workspace domain. An end user has reported that they cannot sign in to Google Workspace after their username was changed in the third-party SSO product. They can sign in to their other internal applications that use SSO. and no other users are experiencing issues signing in.
What could be causing the sign-in issue?
A. The SAML assertion provided by the third-party IDP is presenting a username that conflicts with the current username configured in Google Workspace.
B. The user's Google password was changed administratively, which is causing a sign-in failure.
C. The issued certificate for that user has been revoked and must be updated before the user can have another successful sign in.
D. The SAML assertion is providing the user's previous password attached to their old username.
Answer: A

4.You recently started an engagement with an organization that is also using Google Workspace. The engagement will involve highly sensitive data, and the data needs to be protected from being shared with unauthorized parties both internally and externally. You need to ensure that this data is properly secured.
Which configuration should you implement?
A. Turn on external sharing with whitelisted domains, and add the external organization to the whitelist.
B. Provision accounts within your domain for the external users, and turn off external sharing for that Org.
C. Configure the Drive DLP rules to prevent the sharing of PII and PHI outside of your domain.
D. Create a Team Drive for this engagement, and limit the memberships and sharing settings.
Answer: D
Explanation:
https://support.google.com/a/users/answer/9310352#1.1

5.Your cyber security team has requested that all email destined for external domains be scanned for credit card numbers, and if found, the email must be encrypted using your cloud-based third-party encryption provider. You are responsible for configuring to meet this request.
What should you do?
A. Create a content compliance rule on outbound mail and internal-sending mail using the predefined rule for credit card numbers, and add a custom header that your third-party encryption provider can scan for and encrypt.
B. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and check “Encrypt message if not encrypted”.
C. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and add a custom header that your third-party encryption provider can scan for and encrypt.
D. Create a content compliance rule on outbound mail using the predefined rule for credit card numbers, and check “Change route” to send to your third-party encryption provider to encrypt.
Answer: A
Explanation:
In this scenario, the goal is to ensure that all email, both sent externally and internally, which contains credit card numbers, is encrypted using a third-party encryption provider.

Option A allows you to create a content compliance rule that scans both outbound and internal-sending mails for credit card numbers. When a credit card number is detected, a custom header is added to the email which the third-party encryption provider can identify and encrypt the email accordingly.
Let's analyze other options:
B. This option only encrypts the message if it is not encrypted already, but it doesn't necessarily interface with the specific third-party encryption provider that has been mentioned in the question.
C. This option is similar to A but only focuses on outbound mail and not on internal-sending mail. It misses the part about scanning internal emails, which may still contain sensitive data like credit card numbers.
D. Changing the route to send to the third-party encryption provider seems like a viable option but would be more about rerouting the entire email to the provider rather than adding a specific header that the provider can scan for, which might not align perfectly with the encryption process required by the third-party provider.
Therefore, option A provides a more comprehensive solution that complies with the requirements set by the cybersecurity team. It allows for scanning of both outbound and internal emails, adding a custom header for the third-party provider to encrypt the mail, ensuring better security and compliance with the request.