#### **Common Security Settings**

1. What are some best practices for reinforcing and monitoring the security of your domain?
2. Disable access to less secure apps
3. View and manage your users' security settings
4. Set up 2-step verification
5. All of the above
6. The IT manager at your organization wants to know the advantages of using 2-step verification for your organization. What should you say? (Choose 2)
7. It'll greatly reduce the risk of unauthorized access if a user's password is compromised
8. We wouldn't have to manage individual user IDs and passwords for each user
9. It would be a great opportunity to make sure everyone is the organization has a security key
10. It'll reinforce our domain’s password security by requiring our users to enter an additional code or use a security key to sign in
11. The IT manager at your organization hasn't had a chance to explore the admin console yet but wants to know what individual security settings he can manage for a user. What are some examples you could give him? (Choose 3)
12. Require a password change
13. Determine if the user is enrolled in 2-step verification
14. Review a user's administrative access
15. Temporarily disable the user's login challenge for 10 minutes
16. Where do you go to manage your users' password strength?
17. Security > Password monitoring
18. Security > Password management
19. Users > Account
20. Reports > Security
21. Your organization has decided to enforce 2-step verification in 2 weeks. What actions should you keep in mind when enforcing 2-step verification? (Choose 3)
22. You'll want to provide a lead time for users to enroll before enforcement
23. You'll want to confirm that all of your users are enrolled before enforcement
24. When you create new user accounts after enforcement, you will want to allow them a grace period before they need to enroll otherwise they will be locked out of their accounts
25. Enforcing 2-step verification will not affect your users as they can still opt-out.

#### **SSO**

1. Your IT manager has just informed you that your organization has an account now with Asana and would like you to enable Single Sign On with the application. Where in the admin console would you go to configure a third-party pre-integrated cloud application, like Asana, as your service provider?
2. Apps > SAML apps > plus sign (+) > SETUP MY OWN CUSTOM APP from the Enable SSO for SAML Application window
3. Security > Set up single sign-on (SSO) for SAML applications and provide the necessary information
4. Apps > SAML apps > plus sign (+) > Select Asana from the list of predefined applications
5. What of the following are true of the Secure LDAP service? (Choose 3)
6. User's authenticate against a local directory to gain access to G Suite services
7. It allows you to connect your LDAP-based applications and services to G Suite
8. It reduces maintenance as directory information is consolidated into one directory
9. Users authenticate against the G Suite directory to gain access to LDAP compliant applications and services
10. When adding a pre-integrated SAML application to your G Suite account, which of the following must you add/upload the Service Provider's configuration? (Choose 3)
11. Google Certificate
12. SSO URL
13. Change Password URL
14. Entity ID URL
15. When using a third party IdP which of the following is disabled/hidden in G Suite?  
      
    A. Password monitoring  
    B. Password reuse policy  
    C. Require password change  
    D. Password recovery

#### **Application Security**

1. Your organization wants to prevent any external application from accessing Gmail and Drive data. How would you ensure such access is prevented?
2. Disable API access from the Gmail and Drive service settings
3. From Security > API Permissions, disable API access to the Gmail and Drive APIs. Ensure Trust domain owned apps is disabled
4. Disable Gmail and Drive API access from the top level organization settings
5. From Security > API Permissions, disable API access to the Gmail and Drive APIs. Ensure Trust domain owned apps is enabled
6. You have been asked to create a whitelist of Marketplace apps to restrict which apps a user can install onto their devices. What must you do first?
7. Get your users to Install the Marketplace whitelist app onto each device
8. Add the names of all the trusted applications to each user's device policy
9. Change the Marketplace settings to allow users to install only whitelisted applications from G Suite Marketplace
10. Complete a Domain install for each application that you want to whitelist
11. What is the expected behavior when a user tries to install a Marketplace app that has not been whitelisted?
12. Users can not attempt to install an application that is not on the whitelist because they only see whitelisted apps in the Marketplace
13. User's can install an app that is not on the whitelist but they cannot allow it access to their data so it will not work
14. When the user attempts to install the app they will see a message advising that the app cannot be installed because it has not been whitelisted
15. What happens to already installed applications if you block API access from the Security > API Permissions section?
16. Already installed applications that use the blocked API will continue to work indefinitely
17. Already installed applications that use the blocked API will continue to work until the user next signs in to G Suite
18. Already installed applications that use the blocked API will continue to work until the application needs a new OAuth token
19. Already installed applications will stop working and OAuth tokens will be revoked

#### **Security Tools**

1. Where would you go to review security recommendations for your organization?
2. Security investigation tool
3. Security dashboard
4. Alert Center
5. Security health page
6. Which of the following statements is NOT TRUE about the alert center?
7. The alert center includes additional in-depth details that enable you to take action to resolve numerous issues that might affect your organization
8. The alert center enables you to view alerts and alert details directly in the admin console
9. The alert center consolidates all admin created email alerts into one place
10. Some alerts in the alert center are similar to the admin email alerts, but the alert center does not include a comprehensive set of alerts that match each of the admin alerts
11. When examining messages in the security investigation tool what actions can you apply to a message? (Choose 3)
12. Delete message
13. Mark message as spam
14. Forward to self
15. View header
16. You have been asked by your CEO to provide a list of all administrators that have used the security investigation tool together with details of the searches they have performed in the last month. Where can you find that information?
17. Users Account Activity log
18. The Admin Audit log
19. Users Security log
20. Access Transparency Audit log