Google Cloud

Professional Google Workspace Administrator

Certification exam guide

A Professional Google Workspace Administrator transforms business objectives into tangible Google Workspace configurations, policies, and security practices as they relate to users, content, and integrations. Through their understanding of their organization's infrastructure, Google Workspace Administrators let people work together, communicate, and access data in a secure and efficient manner. Operating with an engineering and solutions mindset, Google Workspace Administrators use tools, programming languages, and APIs to automate workflows, educate end users, and increase operational efficiency while they advocate for Google Workspace and its toolset.

Related job roles: IT systems administrator, cloud solutions engineer, collaboration engineer, systems engineer.

Section 1: Managing objects (~20% of the exam)

1.1 Managing account lifecycles by using provisioning and deprovisioning processes. Considerations include:

- Transferring ownership data to another account
- Provisioning users based on a process determined by an organization's policy (for example, where to list accounts)
- Provisioning and deprovisioning accounts, including:
    - Creating, reviewing, updating, deleting accounts (CRUD [create, read, update, and delete] operations).
    - Adding users (for example, individual, bulk, and automated)
    - Offboarding accounts (for example, suspending, deleting, and recovering)
    - Editing user attributes (for example, renaming, passwords, and aliases)
    - Creating administrative roles (for example, default roles, and custom roles)
- Revoking account access outside of a typical organizational policy (for example, security reasons and personnel issues)
- Configuring, monitoring, troubleshooting, and updating lifecycle management by using Google Cloud Directory Sync (GCDS)

    - Auditing and reviewing GCDS (for example, interpreting log data)

1.2 Configuring Google Drive. Consideration include:

- Managing the lifecycle of shared drives based on user requests and organizational policies (for example, OU [organizational unit] placements)
- Configuring shared drive permissions, given specific requirements or scenarios
- Implementing shared drive membership permissions based on organizational policies
- Transferring user data from one user's drive to another drive
- Applying security best practices for shared drives based on the business need

1.3 Managing calendar and calendar resources. Considerations include:

- Creating and managing calendar resources
- Managing and delegating calendar access and resources
- Managing the lifecycle of both individual and shared calendars (for example, differentiating between an individual's calendar and a calendar resource)
- Configuring Google video conference room options (for example, Jamboard, Google Meet)
- Scheduling Google Meet conferences and livestream meetings or events
- Monitoring usage reports and recommending changes
- Troubleshooting calendar issues

1.4 Configuring and managing Groups for business. Considerations include:

- Configuring memberships and advanced settings, including:
    - Adding users to groups
    - Implementing current Google Workspace APIs
    - Automating tasks by using Apps Script
- Using a Google group to apply membership permissions for a shared drive
- Creating specific types of Google-native groups (for example, dynamic, security, identity-mapped, and POSIX)
- Implementing Google group security access controls to restrict members
- Troubleshooting issues in a Google group (for example, calendar invites not expanding, invites unable to be sent to a group)

Section 2: Configuring services (~18% of the exam)

2.1 Implementing and managing Google Workspace configurations based on corporate policies. Considerations include:

- Assigning and configuring permissions to Google Workspace tools by using organizational units (OUs) and Google groups
- Modifying OU policies
- Implementing application and security settings according to OU inheritance and override settings in parent OUs
- Delegating granular Identify and Access Management (IAM) administrator roles and permissions to users in a domain
- Implementing security configuration options for installing or using Google Cloud Marketplace applications or add-ons
- Configuring Drive labels for data organization
- Configuring a Rapid Release or Scheduled Release for feature releases
- Configuring Google Meet to align with corporate policies and requirements
- Creating and configuring security and data region settings
- Implementing security integration protocols and addressing questions and objections from users
- Managing content compliance rules
- Investigating and remediating an issue by using Security Health Analytics check results

2.2 Configuring Gmail. Considerations include:

- Configuring basic mail routing scenarios for split delivery
- Configuring a mail host
- Configuring end-user access to Gmail by using Google Workspace Sync for Microsoft Outlook (GWSMO) or email client (for example, POP, IMAP, Thunderbird, Outlook)
- Configuring POP and IMAP access to align with corporate policies and requirements
- Configuring administrator access for mail forwarding by using advanced Gmail settings (for example, compliance rules, default routing, APIs)
- Managing and understanding all available spam controls (for example, allowlist, denylist, inbound gateway, and IP allowlist)
- Enabling email delegation for an OU
- Managing Gmail archives

Section 3: Troubleshooting (~24% of the exam)

3.1 Troubleshooting mail delivery problems reported by users. Considerations include:

- Determining whether user behavior or a broader issue (for example, rules, or Cloud Data Loss Prevention [DLP]) is causing an error
- Determining whether an issue is an expected behavior (for example, a missing attachment, or an attachment filter issue)
- Auditing and reviewing mail flow structure and end-user actions to determine the root cause of delivery issues
- Analyzing message headers or email audit logs by using Google Workspace tools or security investigation tools
- Recommending and/or implementing an appropriate course of action related to mail delivery issues (for example, implementing mail policy changes)

3.2 Troubleshooting and collecting logs and reports needed to engage with the support team. Considerations include:

- Documenting steps taken by end user to reproduce an issue
- Collecting appropriate log file types
- Searching for known issues and application status
- Generating HAR files

3.3 Identifying, classifying, troubleshooting, and mitigating basic email attacks. Considerations Include:

- Configuring:
    - Blocked senders
    - Email allowlist
    - Objectionable content
    - Phishing settings
    - Spam settings
    - Gmail safety settings
    - Administrator quarantine
    - Attachment compliance
    - Secure transport compliance
- Implementing Sender Policy Framework (SPF); Domain-based Message Authentication, Reporting, and Conformance (DMARC); Mail Transfer Agent Strict Transport Security (MTA-STS); and DomainKeys Identified Mail (DKIM) to secure email transmission

- Investigating whether custom configurations are responsible for any issues or vulnerability (for example, email allowlist and IP addresses)
- Investigating the scope of email attacks by using available Google Workspace email tools
- Analyzing message contents for common attack patterns (for example, name, domain, and brand spoofing)
- Mitigating successful attacks and preventing future attacks by using Google Workspace email tools (for example, identifying the issue and responding)

3.4 Troubleshooting Google Workspace access and performance issues. Considerations include:

- Identifying why a user is having an issue when they access a single Google application (for example, Drive)
- Identifying the root cause of a performance issue when accessing a Google Workspace application (for example, a known issue, an outage, a network, or a device)
- Analyzing, evaluating, and modifying settings to ensure delivery of critical emails (for example, specific IP ranges, X-headers)
- Troubleshooting authentication issues that users reported
- Troubleshooting issues that users reported when they set up Google Workspace on a mobile device
- Troubleshooting Google Meet video call issues from the administrator console
- Troubleshooting Google Meet device issues by using the administrator console
- Troubleshooting network configuration issues to ensure high-quality meetings by using Google Meet
- Troubleshooting Jamboards
- Troubleshooting access to Google Workspace services (for example, Gmail and Drive)
- Troubleshooting data visibility issues by enabling/disabling licenses or services
- Investigating access issues in applications for OUs
- Interpreting and responding to alerts in the Alert Center API

Section 4: Data access and authentication (~24% of the exam)

4.1 Configuring policies for all devices (for example, mobile device, desktop, Chrome OS, Google Meet Hardware, Jamboard, Google Voice, and browser). Considerations include:

- Configuring:
    - Chrome user and browser policy settings
    - ChromeOS device policy settings (for example, Enterprise)

    - Windows 10 login and device policies (for example, Google Credential Provider for Windows (GCPW)
    - Managed Chrome browsers (for example, Chrome Browser Cloud Management)
    - Basic device management
    - Basic and advanced device management for Android and iOS
    - Company-owned device management for Android and iOS
    - Context-aware access policies
    - Personal device settings for Android and iOS (for example, password, advanced, device approvals, application management, and insights)
- Enabling Endpoint Verification security by using BeyondCorp

4.2 Configuring and implementing Gmail DLP and sharing access control lists (ACLs) based on governance policies. Considerations include:

- Identifying areas of improvement for secure collaboration based on data exfiltration reports
- Scanning emails by using Gmail DLP
- Implementing Gmail DLP policies to prevent the over-sharing of sensitive data
- Configuring and implementing Gmail DLP options for data classification
- Configuring and implementing data classification settings on Drive
- Implementing context-aware access policies based on data governance policies
- Configuring settings to limit external sharing on Drive based on organizational policies
- Configuring settings to limit email delivery based on organizational policies
- Configuring and implementing client-side encryption services for Drive

4.3 Managing third-party applications. Considerations include:

- Implementing automatic releases of a browser extension to OUs within the domain
- Implementing security configuration options for installing or using Google Cloud Marketplace applications or add-ons
- Reviewing and authorizing user requests for a new Google Workspace Marketplace application, Google Play, or a Chrome extension
- Pushing an application to a user's phone by using Google's mobile device management (MDM)
- Configuring Google as a Security Assertion Markup Language (SAML) provider for a third-party application
- Deploying password-vaulted apps
- Deploying and restricting Google Workspace Marketplace and Google Play Store applications
- Granting API access to applications
- Integrating third-party user provisions

- Integrating third-party marketplace applications to specific OUs in Google Workspace
- Managing access to additional Google services (for example, AdSense and YouTube) for a specific set of users
- Revoking third-party author access
- Removing connected applications and sites

4.4 Configuring user authentication. Considerations include:

- Configuring:
    - 2-step Verification for the administrator and high-risk accounts (for example, requiring a physical key or not allowing SMS)
    - 2-step Verification for low-risk and standard accounts (for example, Google Authenticator)
    - Google-side connection to third-party single sign-on (SSO) providers
    - Google Multi-IdP options for SSO
    - Basic SAML SSO configuration for third-party application authentication when Google is the SSO provider
    - Third-party SSO for Google Workspace
    - Access control based on the use of the security functionality within API Controls
    - Google session control based on a company's legal policies
- Implementing basic user security controls (for example, password length enforcement)
- Implementing security aspects of identity management, perimeter security, and data protection

Section 5: Supporting business initiatives (~14% of the exam)

5.1 Using Vault to support legal initiatives. Considerations Include:

- Configuring retention rules based legal security policies (for example, setting retention rules, placing legal holds, exporting data for additional processing and review, auditing reports, and searching a domain's data by user account, OU, date, or keyword)
- Assisting with or creating:
    - Legal matters to hold data
    - Export matter content (data) for analysis
    - Delegation protocols for Vault access
    - Google Workspace content by using Vault (searching)
    - Legal holds for Google Workspace content by using Vault
    - Vault audit reports (running)

5.2 Creating and interpreting reports for the business. Considerations include:

- Generating and interpreting user adoption reports (for example, Work Insights)
- Investigating issues by using the Alert Center
- Investigating and monitoring a service outage for a specific Google Workspace application
- Investigating issues by using data objects and metrics available within activity reports
- Configuring group alerts triggered by a specific event
- Creating and reviewing audit logs
- Using BigQuery to combine multiple Google Workspace logs and usage reports to provide actionable insights

5.3 Supporting data import and export. Considerations include:

- Assisting with off-boarding employees and transferring data (for example, Drive, Calendar, and Google Data Studio)
- Migrating Gmail data between Google Workspace accounts
- Exporting data from Google Workspace offline or to other platforms