

# Associate Google Workspace Administrator

## Section 1: Managing user accounts, domains, and Directory (~22% of the exam)

### 1.1 Managing the user life cycle.

#### Considerations include:

- Manually creating user accounts.
- Automating the provisioning and deprovisioning of users.
- Using a third-party identity provider (IdP) to provision and authorize users.
- Configuring basic SAML SSO.
- Configuring GCDS.
- Modifying user attributes (e.g., names, email addresses, passwords, aliases).
- Deleting, suspending, restoring, and archiving accounts.
- Transferring ownership of data to another account.
- Assigning licenses.
- Administering passwords (e.g., password resets, forcing password changes, monitoring password strength).

### 1.2 Designing and creating organizational units (OUs).

#### Considerations include:

- Designing the OU hierarchy in alignment with an organizational structure while following Google-recommended practices.
- Creating and managing OUs for hierarchical user management.

### 1.3 Managing groups.

#### Considerations include:

- Designing a groups hierarchy.
- Creating and managing distribution lists.
- Creating and managing shared mailboxes (Collaborative Inbox).
- Creating and managing dynamic groups.
- Creating and managing security groups.

## **1.4 Managing domains.**

### **Considerations include:**

- Adding and verifying primary and secondary domains.
- Managing domain aliases.
- Configuring MX records for email routing.

## **1.5 Managing buildings and resources.**

### **Considerations include:**

- Creating buildings and rooms in bulk.
- Creating and managing new resources for booking and scheduling.
- Establishing resource booking permissions.
- Creating features to add specific details to resources (e.g., capacity, whiteboard, wheelchair accessible).

## **Section 2: Managing core Workspace services (~20% of the exam)**

### **2.1 Configuring Gmail.**

#### **Considerations include:**

- Configuring MX records for email routing.
- Configuring basic mail routing scenarios for split and dual delivery.
- Using content compliance rules to filter and route emails based on their content.
- Configuring spam, phishing, and malware settings (e.g., allowlist, denylist, inbound gateway, IP allowlist).
- Managing email attachment size limits and blocked file types.
- Configuring Gmail forwarding and POP/IMAP access.
- Implementing Google-recommended email security practices (e.g., SPF, phishing prevention, DKIM, DMARC).
- Migrating email data to and from Gmail (e.g., when migrating from other email providers).
- Delegating Gmail access to other users.
- Managing compliance footers and email quarantines.

## **2.2 Configuring Google Drive and Docs.**

### **Considerations include:**

- Configuring default sharing options for new files, folders, and Docs (e.g., internal versus external sharing, Drive trust rules).
- Configuring Drive settings to limit external sharing based on organizational policies.
- Managing target audiences.
- Creating, managing, and sharing custom Docs templates.
- Enabling Docs add-ons.
- Creating and managing Shared Drives.
- Setting and adjusting storage quotas for individual users or OUs.
- Installing and configuring Google Drive for desktop.
- Transferring ownership of files and folders to other users.
- Managing Drive Labels.
- Enabling and disabling offline access.

## **2.3 Configuring Google Calendar.**

### **Considerations include:**

- Creating and managing resource calendars (e.g., meeting rooms, equipment).
- Configuring booking policies for resources.
- Delegating calendar and resource access to another user.
- Configuring shared calendars for teams or groups.
- Managing external sharing options for calendars.
- Configuring Calendar to support third-party web conferencing tools.
- Canceling and transferring events to another user.
- Preventing invitations from unknown senders.

## **2.4 Configuring Google Meet.**

### **Considerations include:**

- Enabling or disabling Meet for an organization or specific OUs.
- Configuring Meet safety settings.
- Configuring Meet video settings (e.g., quality, recordings, transcripts).
- Enabling and managing Stream settings.

## **2.5 Configuring Google Chat.**

### **Considerations include:**

- Enabling or disabling Chat for an organization or specific OUs.
- Configuring Chat settings in the Admin console (e.g., chat history, space settings, allowing outside domains to join Chat spaces, moderation).
- Managing Chat invite settings.
- Adding Chat apps.<sup>3</sup>

## **2.6 Configuring Gemini for Google Workspace.**

### **Considerations include:**

- Enabling or disabling Gemini for an organization or specific OUs.
- Assigning Gemini licenses to specific users or groups.
- Enabling Alpha features.
- Monitoring Gemini adoption.

## **2.7 Supporting Workspace development.**

### **Considerations include:**

- Identifying use cases for AppSheet and Apps Script (e.g., task automation).
- Enabling AppSheet for an organization or specific OUs.

## **Section 3: Managing data governance and compliance (~14% of the exam)**

### **3.1 Using Google Vault for eDiscovery and data retention.**

#### **Considerations include:**

- Identifying the differences between Gmail content compliance and DLP rules.
- Configuring DLP rules to prevent unauthorized sharing or loss of sensitive data.
- Creating and configuring automatic DLP rules and actions based on content detectors (e.g., credit card numbers, personally identifiable information) or regular expressions.
- Applying DLP rules to specific Workspace services (e.g., Gmail, Drive, Chat).
- Customizing DLP notification messages.

### **3.2 Creating and managing data loss prevention (DLP) rules.**

#### **Considerations include:**

- Installing and configuring the command line interface (CLI) for Kubernetes (kubectl)
- Deploying a Google Kubernetes Engine cluster with different configurations (e.g., Autopilot, regional clusters, private clusters, GKE Enterprise)
- Deploying a containerized application to Google Kubernetes Engine

### **3.3 Creating and managing Drive trust rules.**

#### **Considerations include:**

- Limiting sharing to specific OU groups, domains, or users.
- Blocking sharing of certain OU groups, domains, or users.
- Allowing or restricting sharing outside an organization (e.g., visitors, external users). 4

### **3.4 Determining how to store and export your environment's data.**

#### **Considerations include:**

- Managing Google Takeout settings (e.g., allowing or restricting certain data types).
- Using the Data Export tool.
- Choosing a geographic location for your data.
- Configuring legal and compliance settings based on industry regulations.

### **3.5 Classifying data.**

#### **Considerations include:**

- Identifying use cases for applying labels to data (e.g., user classification, DLP, default classification, AI classification).
- Applying Drive Labels.
- Applying Gmail Labels.

## **Section 4: Managing security policies and access controls (~20% of the exam)**

### **4.1 Securing user access.**

#### **Considerations include:**

- Enforcing strong password policies and two-step verification (2SV) rules.
- Configuring password policies and recovery options (e.g., security questions, verification codes).
- Configuring 2SV methods (e.g., Google Authenticator app, text message, passkeys).

- Managing context-aware access policies.
- Applying security policies and access controls to specific OUs.
- Creating and managing security groups that control access to resources (e.g., files, calendars).
- Assigning prebuilt and custom administrative roles to users (e.g., super admin, groups admin, user management admin) and delegating specific administrative tasks.

#### **4.2 Reporting, auditing, and investigating security risks and events.**

##### **Considerations include:**

- Investigating and analyzing logs and security events by using the Security Investigation Tool.
- Identifying security risks and threats by using the security center.
- Identifying gaps in security-related configurations by using the security health page in the security center.
- Creating activity rules and alerts.

#### **4.3 Enabling additional Google and third-party applications.**

##### **Considerations include:**

- Managing the Marketplace allowlist.
- Deploying and restricting Google Workspace Marketplace and Google Play Store applications.
- Configuring SAML in third-party applications.
- Managing access to additional Google services (e.g., AdSense and YouTube) for a specific set of users.
- Removing connected applications and sites.
- Implementing automatic releases of browser extensions to OUs within a domain.

### **Section 5: Managing endpoints (~10% of the exam)**

#### **5.1 Managing mobile devices.**

##### **Considerations include:**

- Determining when to use a basic, advanced, or third-party mobile management solution.
- Applying security policies to mobile devices by using Google basic mobile management.
- Maintaining visibility and control over registered devices, including both company-owned and bring your own device (BYOD).
- Onboarding mobile devices from former employees.

## **5.2 Managing Chrome browsers.**

### **Considerations include:**

- Applying Chrome browser policies (e.g., oine access, update policies).
- Enrolling browsers and applying policies.
- Managing extensions and apps (e.g., allowing, blocking, force-installing).

## **Section 6: Troubleshooting common issues (~14% of the exam)**

### **6.1 Identifying and diagnosing Workspace issues.**

#### **Considerations include:**

- Navigating the Admin console to access audit logs.
- Interpreting log entries to identify error messages, unusual activity, or paerns related to an issue.
- Checking the Google Workspace Status Dashboard for service disruptions or outages.
- Recommending a solution related to mail delivery issues (e.g., implementing mail policy changes).

### **6.2 Troubleshooting and resolving common issues.**

#### **Considerations include:**

- Troubleshooting problems with user accounts, passwords, or access to services.
- Troubleshooting email delivery problems (e.g., undelivered messages, spam ltering issues).
- Troubleshooting issues with email forwarding, lters, or labels.
- Analyzing message headers or email audit logs by using Workspace tools, security investigation tools, or the Google Admin Toolbox (e.g., SPF, DMARC, DKIM).
- Troubleshooting Calendar events that are not syncing or displaying correctly (e.g., Apple Calendar, Outlook).
- Troubleshooting issues with calendar sharing or managing permissions.
- Troubleshooting Calendar issues with sharing free/busy information.
- Troubleshooting Drive issues with sharing and managing permissions.
- Resolving problems with Drive for Desktop.
- Recovering accidentally deleted les in Drive.
- Troubleshooting Drive oine access issues.
- Diagnosing network performance issues (e.g., video and sound quality) by using the Meet quality tool.
- Troubleshooting Meet issues (e.g., users unable to access Meet events).

### **6.3 Using support resources.**

#### **Considerations include:**

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