# 1.Directory

## 1.1 Users

### 1.1.1 Ensure more than one Super Admin account exists

*From a security point of view, having only a single Super Admin Account can be problematic if this user were unavailable for an extended period of time. Also, Super Admin accounts should never be shared amongst multiple users.* To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator
2. Go to Directory and click on Users, this will show a list of all users
3. Click on + Add a filter, select Admin role, check the Super admin box, and then select Apply
4. The list of Users displayed will only be those with the Super Admin role
5. Make sure more than one (1) user is listed

### 1.1.2 Ensure no more than 4 Super Admin accounts exist *From a security point of view, having a large number of Super Admin accounts is a bad practice. In general, all users should be assigned the least privileges needed to do their job. This includes Administrators since not everyone that needs to “Administer Something” needs to be a Super Admin. Google Workspaces provides many predefined Administration Roles and also allows the creation of Custom Roles with very granular permission selection.*

### Ensure super admin accounts are used only for super admin activities

*Use the super admin account only when needed. Delegate administrator tasks to user accounts with limited admin roles. Use the least privilege approach, where each user has access to the resources and tools needed for their typical tasks. For example, you could grant an admin permissions to create user accounts and reset passwords, but not let them delete user accounts.* To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator
2. Go to Directory and click on Users, this will show a list of all users
3. Click on + Add a filter, select Admin role, check the Super admin box, and then select Apply
4. The list of Users displayed will only be those with the Super Admin role
5. Click on + Add a filter, select Admin role, check the Delegated admin box, and then select Apply
6. Verify that there are no users in both the Super admin and Delegated admin roles

For every Super admin that is also a Delegated admin account, either create a Delegated admin account for the user of elevate or their existing non-admin account to a Delegated admin account.

## 1.2 Directory Settings

### 1.2.1 Sharing Settings

#### 1.2.1.1 Ensure directory data access is externally restricted

*If your organization uses third-party apps that integrate with your Google services, you control how much Directory information the external apps can access.*
*If you allow directory access, your users have a better experience with external apps. For example, when they use a third-party mail app, they want to find domain contacts and have email addresses automatically complete. The app needs access to Directory data to make this happen. However, this has the ability to share ALL domain AND public data with the connected third-party app.*
*Public data and authenticated user basic profile fields — Share publicly visible domain profile data with external apps and APIs. Also share the authenticated user's name, photo, and email address to enable Google Sign-In if the appropriate scopes are granted. Other non-public profile fields for the authenticated user aren't shared. All the non-public profile information of other users in the domain aren't shared. Domain and public data — (Default) Share all Directory information that's shared with your domain and public data. This information includes profile information for users in your domain, shared external contacts, and Google+ profile names and photos.* To verify this setting via the Google Workspace Admin Console:

1. Log in to https://admin.google.com as an administrator
2. Open the collapsed menu via “hamburger button \ 3 horizontal lines”
3. Under Directory, select Directory settings
4. Under Sharing settings, select External Directory sharing
5. Ensure Domain and public data is not selected
6. Select Save

# 2.Devices NA

# 3.Apps

## 3.1 Google workspace

### 3.1.1 Calendar

### 3.1.2 Drive and Docs

### 3.1.3 Gmail

### 3.1.4 Google Chat

### 3.1.5 Google Meet

NA

### 3.1.6 Groups for Business

### 3.1.7 Sites

### 3.1.8 Additional Google services

### 3.1.9 Google Workspace Marketplace

# 4.Security

## 4.1 Authentications

### 4.1.1 2-Step Verfication

### 4.1.2 Account Recovery

### 4.1.3 Advanced Protection Program

### 4.1.4 Login Challenges

### 4.1.5 Password Management

## 4.2 Access and Data Control

### 4.2.1 API Controls

### 4.2.2 Context-Aware Access

### 4.2.3 Data Protection

### 4.2.4 Google Session Control

### 4.2.5 Google Cloud Session Control

### 4.2.6 Less Secure Apps

### 4.3 Security Center

# 5.Reporting

## 5.1 Reports

### 5.1.1 User Reports

# 6.Rules

## 6.1

## 6.2

## 6.3

## 6.4

## 6.5

## 6.6

## 6.7

## 6.8