

# Android EMM Policies and Permissions

Android EMM (Enterprise Mobile Management) allows you to create permissions and send policies.

## Permissions Types

Permission settings may be configured on multiple levels. They are applied in this priority (low number wins).

1. Application specific permission grant (list below dropdown in Permissions tab in applications fileset properties)
2. Specific permission for all applications (configured in Policy Fileset)
3. Application default (Play Store App Fileset → Permissions tab)
4. Global default (Android Default Policy Editor)

### 1. Within Each App

After you have created a [Google Play Apps](#) Fileset:

1. Double click the Play Store App fileset
2. Permissions tab (Figure 1.1)
  1. App Default Permission - The default action devices will take when an app requests a permissions
  2. Application specific permission grant - The setting for a specific permission within this app
3. Choices
  1. Use Default - Defer to another setting
  2. Prompt - App prompts the user to approve
  3. Grant - Allowed, user can not change
  4. Deny - Not Allowed, user can no change

### 2. Policy Fileset - Permissions

You can create a policy fileset and associate that to a device to specify permission grants/denies.

See below for steps.

### 3. Global Policy

Specify the default application permission choice. (Figure 1.2)

Found under FileWave Admin → Preferences → Google → Configure Default Policy

- Unspecified
- Prompt
- Grant
- Deny

After you change the default policy, you must update the model to apply the change.


## Policies

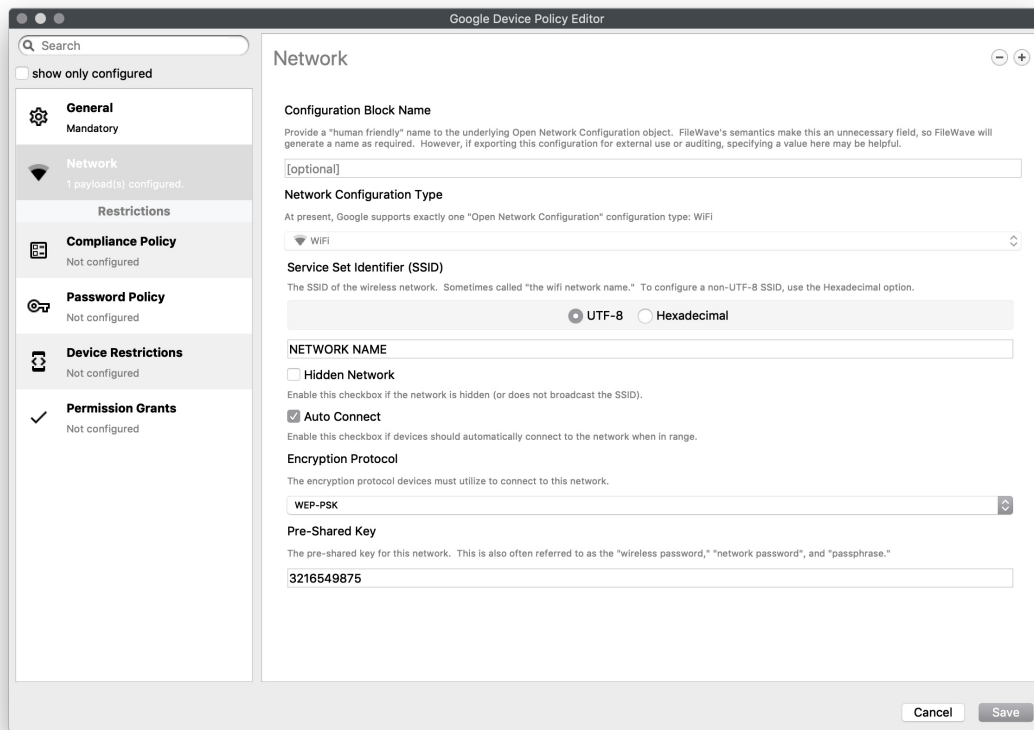
You can create a Policy for (Figure 2.1)

- Network
- Compliance
- Password
- Device Restrictions
- Permission Grants

### Network

Settings to join a WiFi network

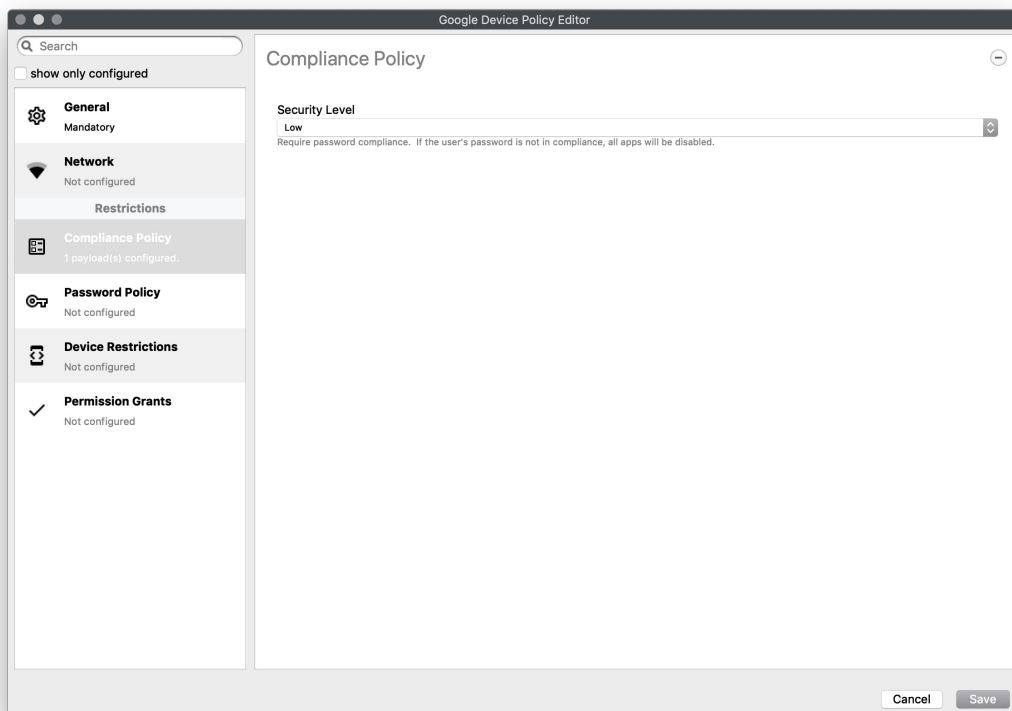
 As of 15.4, additional options have been added for DomainSuffixMatch and UseSystemCA for EAP network configuration.



## Compliance Policy

Set compliance level of associated devices.

- None - Do not enforce any compliance. When other settings are sent they can be ignored and the device will operate
- Low (Default) - Require password compliance. If not compliant, no other apps will open
- High - same as low, but additionally disables any device running below Android 7.

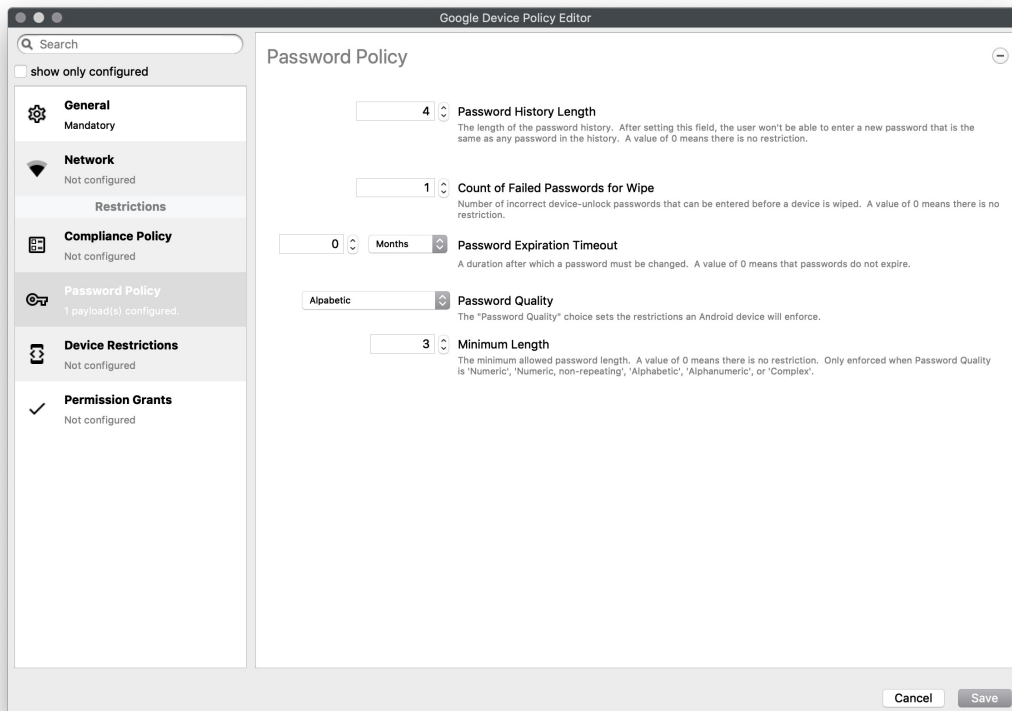


## Password Policy

Set password constraints

- Password History Length - The length of the password history. After setting this field, the user won't be able to enter a new

- password that is the same as any password in the history. A value of 0 means there is no restriction
- Count of Failed Passwords for Wipe - Number of incorrect device-unlock passwords that can be entered before a device is wiped. A value of 0 means there is no restriction.
- Password Expiration Timeout - A duration after which a password must be changed. A value of 0 means that passwords do not expire.
- Password Quality - The restrictions an Android device will enforce
  - Weak Biometric - The device must be secured with a low-security biometric recognition technology, at minimum. This includes technologies that can recognize the identity of an individual that are roughly equivalent to a 3-digit PIN (false detection is less than 1 in 1,000)
  - Password Required - A password is required, but there are no restrictions on what the password must contain.
  - Numeric - Must contain numeric characters
    - Minimum Length
  - Numeric , Non repeating - Must contain numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences.
    - Minimum Length
  - Alphabetic - The password must contain alphabetic (or symbol) characters.
    - Minimum Length
  - Alphanumeric - The password must contain both numeric and alphabetic (or symbol) characters
    - Minimum Length
  - Complex - The password must contain at least a letter, a numerical digit and a special symbol. Other password constraints, for example, passwordMinimumLetters are enforced.
    - Minimum length
    - Minimum count of letters
    - Minimum count of uppercase letters
    - Minimum count of non-alphanumerics
    - Minimum count of numerals
    - Minimum count of special symbols



## Device Restrictions

Restrict access to device functionality

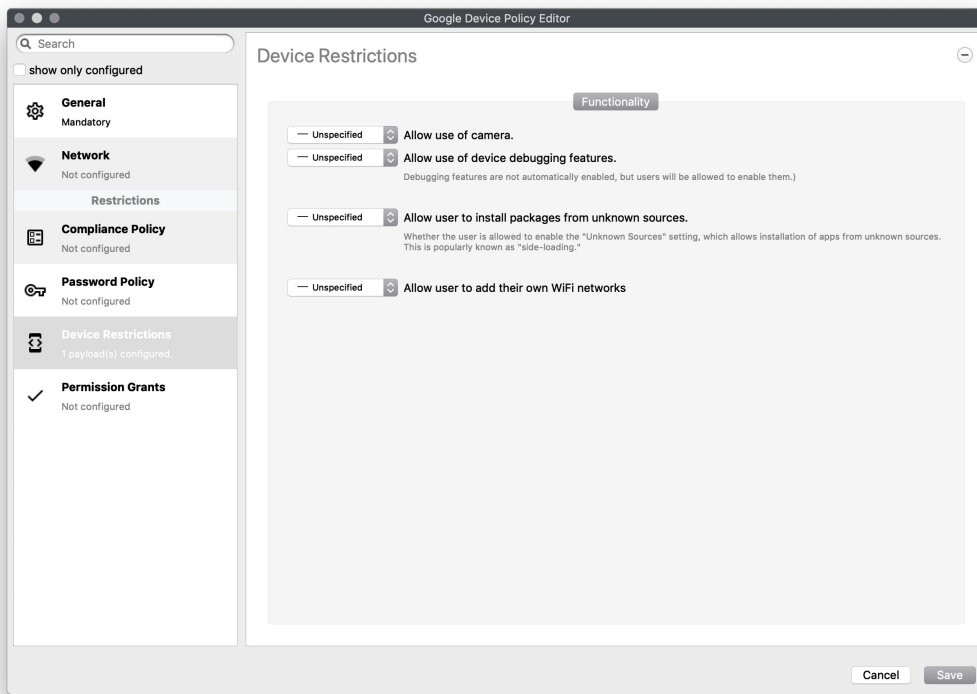
You can choose Unspecified, Allowed, Disallowed for:

- Use of camera
- Debugging
- Install packages from unknown sources
- Allow user to add own WiFi networks

As of 15.4, a new restriction for USB Data Access has been included to allow or disallow file or data transfer for Android devices.



Key Name: "usbDataAccess", Values: Unspecified / (Don't Save), Allowed / ALLOW\_USB\_DATA\_TRANSFER, Disallow File Transfer / DISALLOW\_USB\_FILE\_TRANSFER, Disallow Data Transfer / DISALLOW\_USB\_DATA\_TRANSFER.

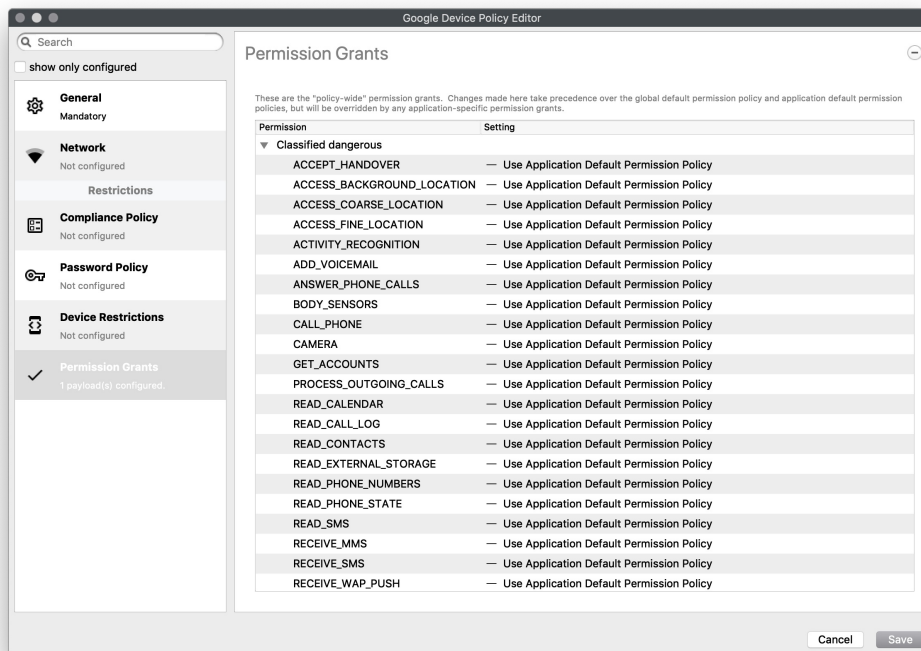


## Permission Grants

A detailed list of permission settings for settings that have been classified

- Dangerous
- Normal
- No Classification

And includes everything from allowing answering of calls, camera, NFC, vibrate, to battery status, and system alerts



Toggle to show all Permission options... Expand source

```
ACCEPT_HANDOVER
ACCESS_BACKGROUND_LOCATION
ACCESS_COARSE_LOCATION
ACCESS_FINE_LOCATION
ACTIVITY_RECOGNITION
```

ADD\_VOICEMAIL  
ANSWER\_PHONE\_CALLS  
BODY\_SENSORS  
CALL\_PHONE  
CAMERA  
GET\_ACCOUNTS  
PROCESS\_OUTGOING\_CALLS  
READ\_CALENDAR  
READ\_CALL\_LOG  
READ\_CONTACTS  
READ\_EXTERNAL\_STORAGE  
READ\_PHONE\_NUMBERS  
READ\_PHONE\_STATE  
READ\_SMS  
RECEIVE\_MMS  
RECEIVE\_SMS  
RECEIVE\_WAP\_PUSH  
RECORD\_AUDIO  
SEND\_SMS  
USE\_SIP  
WRITE\_CALENDAR  
WRITE\_CALL\_LOG  
WRITE\_CONTACTS  
WRITE\_EXTERNAL\_STORAGE  
ACCESS\_LOCATION\_EXTRA\_COMMANDS  
ACCESS\_NETWORK\_STATE  
ACCESS\_NOTIFICATION\_POLICY  
ACCESS\_WIFI\_STATE  
BLUETOOTH  
BLUETOOTH\_ADMIN  
BROADCAST\_STICKY  
CALL\_COMPANION\_APP  
CHANGE\_NETWORK\_STATE  
CHANGE\_WIFI\_MULTICAST\_STATE  
CHANGE\_WIFI\_STATE  
DISABLE\_KEYGUARD  
EXPAND\_STATUS\_BAR  
FOREGROUND\_SERVICE  
GET\_AND\_REQUEST\_SCREEN\_LOCK\_COMPLEXITY  
GET\_PACKAGE\_SIZE  
INSTALL\_SHORTCUT  
INTERNET  
KILL\_BACKGROUND\_PROCESSES  
MANAGE\_OWN\_CALLS  
MODIFY\_AUDIO\_SETTINGS  
NFC  
NFC\_TRANSACTION\_EVENT  
READ\_SYNC\_SETTINGS  
READ\_SYNC\_STATS  
RECEIVE\_BOOT\_COMPLETED  
REORDER\_TASKS  
REQUEST\_COMPANION\_RUN\_IN\_BACKGROUND  
REQUEST\_COMPANION\_USE\_DATA\_IN\_BACKGROUND  
REQUEST\_DELETE\_PACKAGES  
REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS  
SET\_ALARM  
SET\_WALLPAPER  
SET\_WALLPAPER\_HINTS  
TRANSMIT\_IR  
USE\_BIOMETRIC  
USE\_FINGERPRINT  
VIBRATE  
WAKE\_LOCK  
WRITE\_SYNC\_SETTINGS  
ACCESS\_MEDIA\_LOCATION  
BATTERY\_STATS  
BIND\_REMOTEVIEWS  
BIND\_SMS\_APP\_SERVICE  
CHANGE\_CONFIGURATION  
GET\_ACCOUNTS\_PRIVILEGED

GET\_TASKS  
GLOBAL\_SEARCH  
INSTANT\_APP\_FOREGROUND\_SERVICE  
PACKAGE\_USAGE\_STATS  
PERSISTENT\_ACTIVITY  
READ\_MEDIA\_AUDIO  
READ\_MEDIA\_IMAGES  
READ\_MEDIA\_VIDEO  
SMS\_FINANCIAL\_TRANSACTIONS  
SYSTEM\_ALERT\_WINDOW  
USE\_FULL\_SCREEN\_INTENT

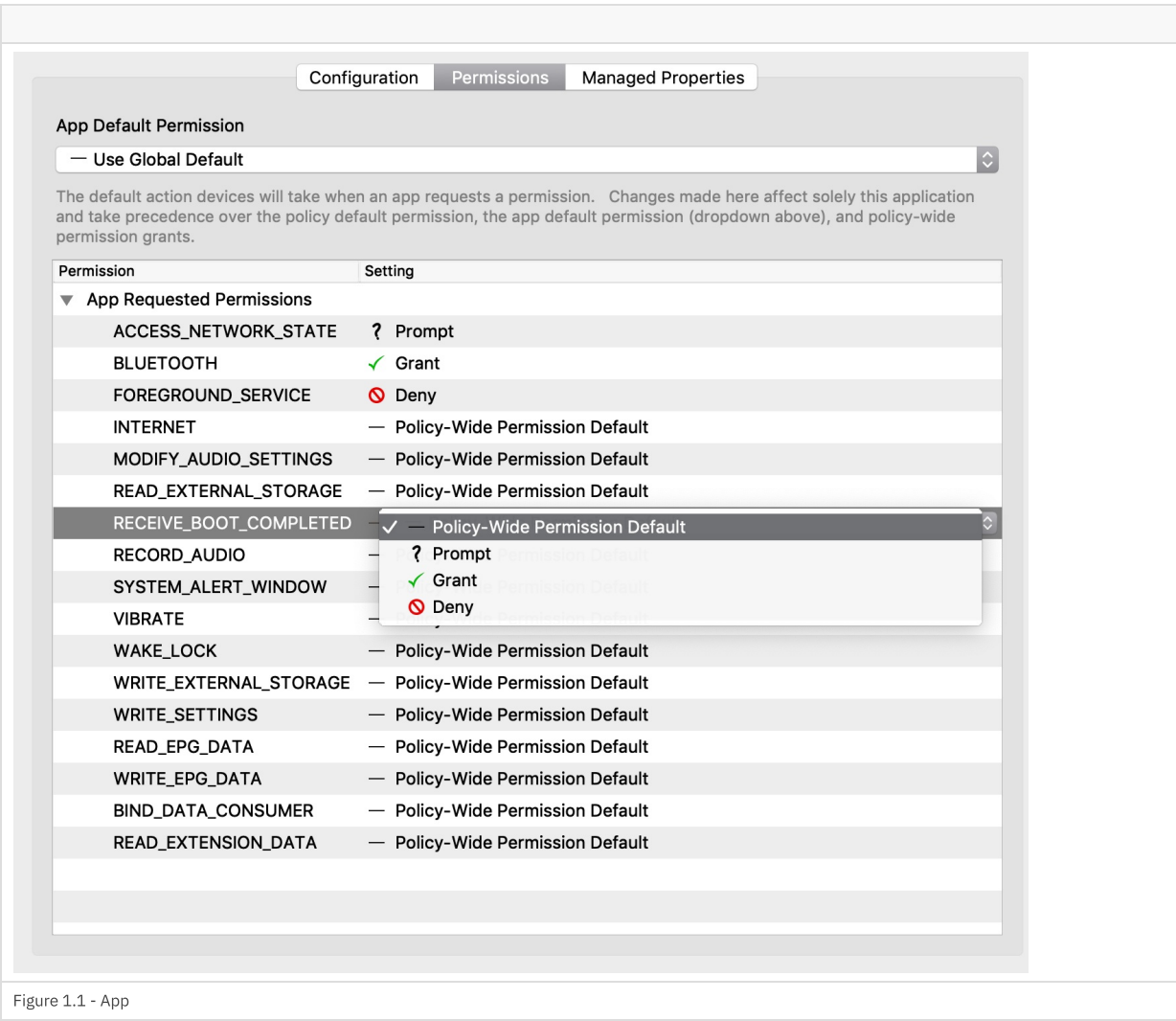


Figure 1.1 - App

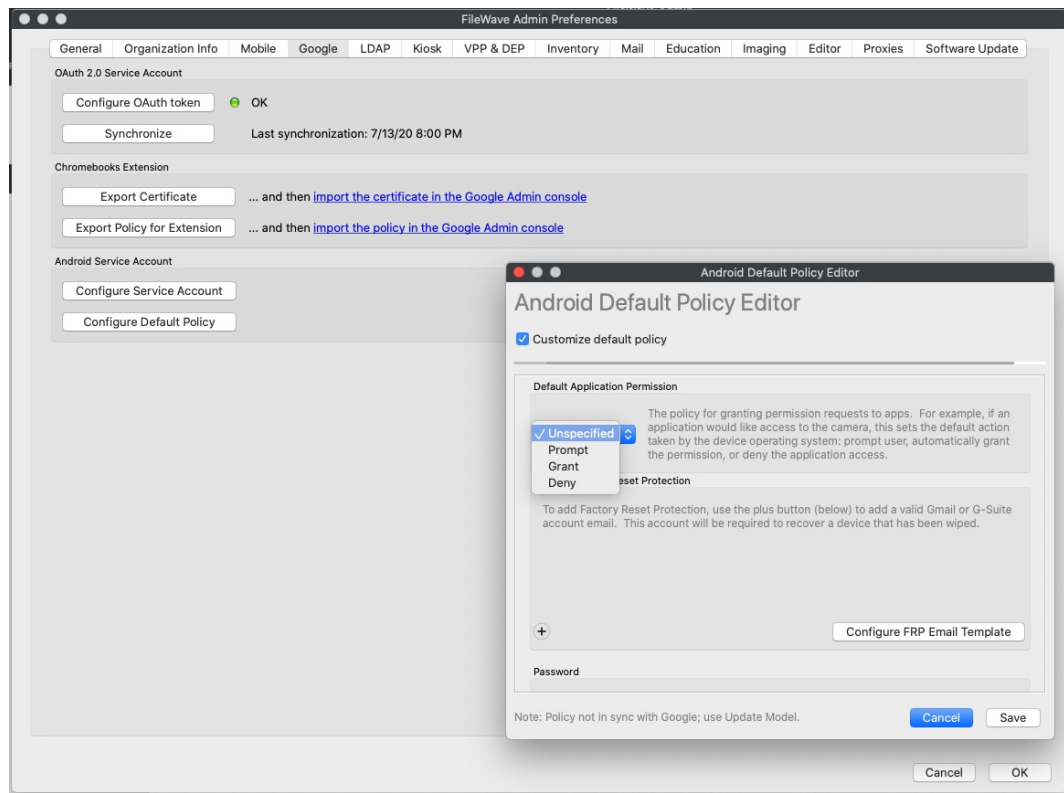


Figure 1.2 - Global

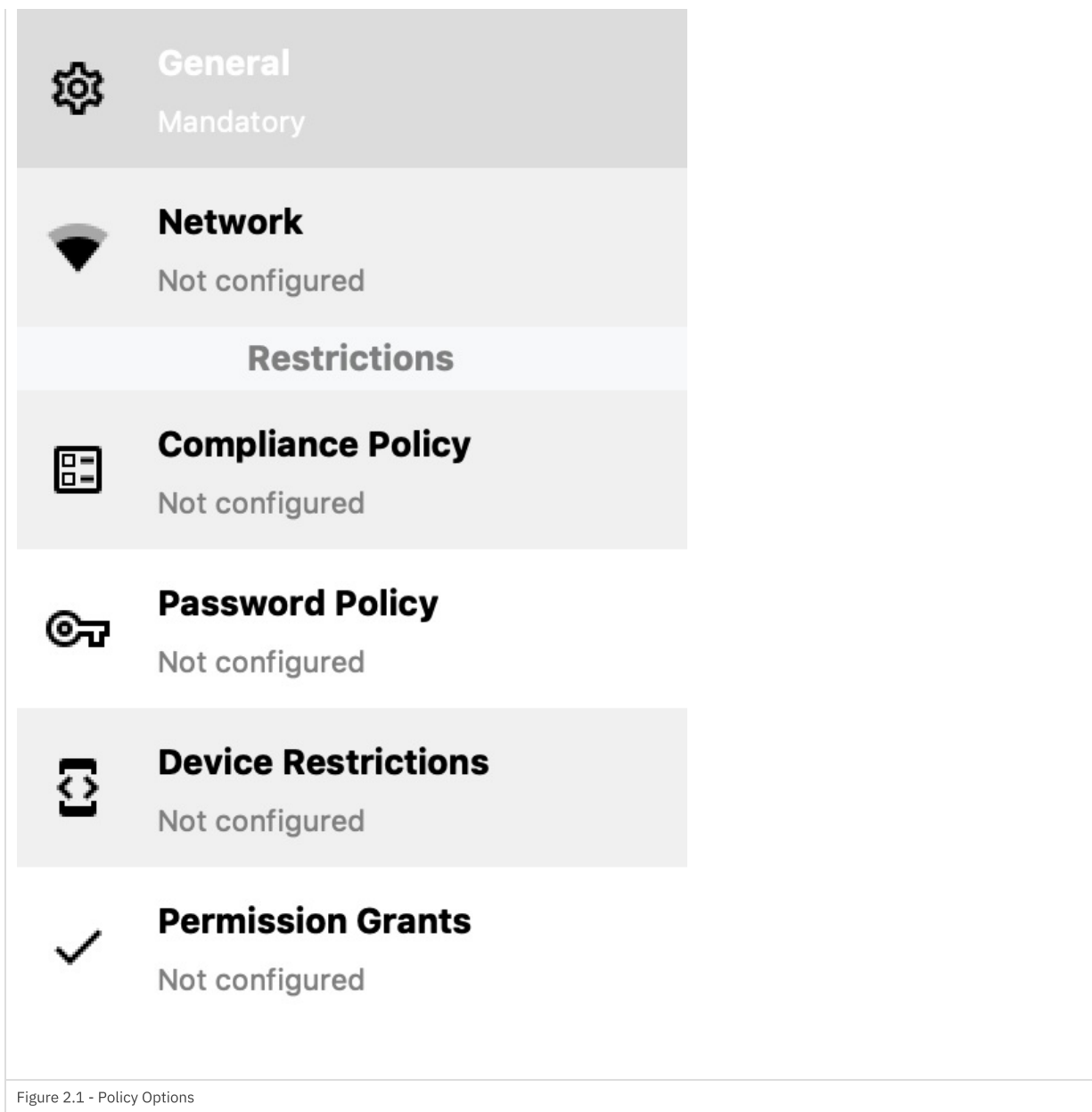
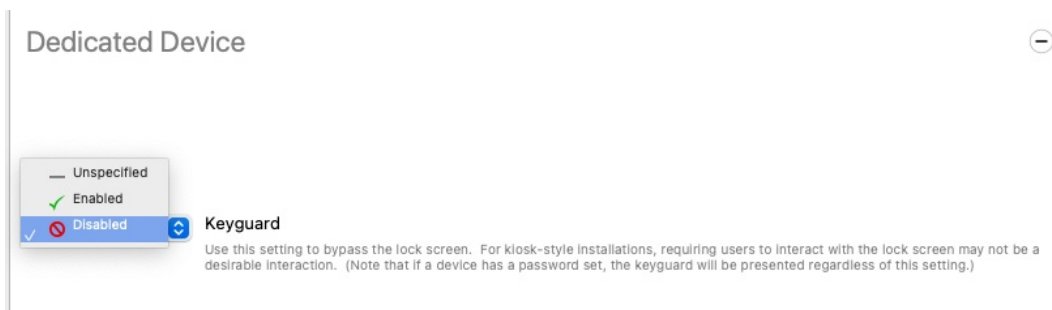


Figure 2.1 - Policy Options

## DEDICATED DEVICE

### Keyguard

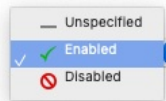
This feature enables you to lock and unlock your screen. Disabled option will bypass the lock screen.



### Custom Launcher

When enabled, it will set your device to kiosk mode. All the applications available on device screen were deployed through FileWave.



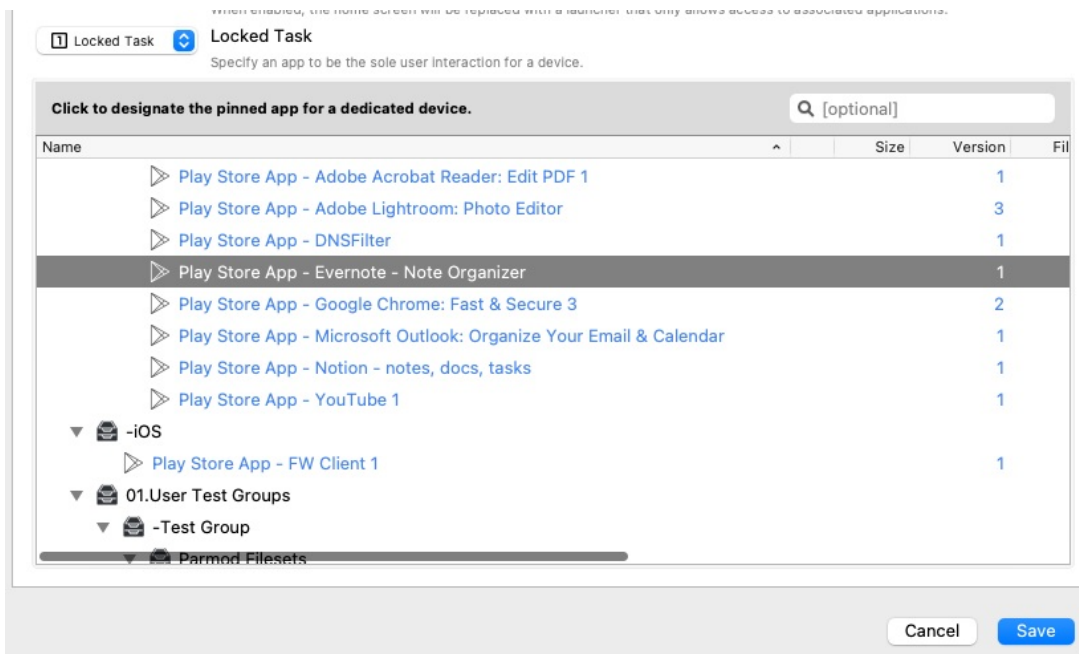


### Custom Launcher

When enabled, the home screen will be replaced with a launcher that only allows access to associated applications.

## Locked Task

This option will lock the device to open only a single app. The App must be downloaded and installed via FileWave.



Revision #7

★Created 15 June 2023 09:14:36 by Rommel Navarro

✎Updated 17 December 2024 15:08:47 by Josh Levitsky