CUSTOMER

SAP Cloud Platform, mobile service for app and device management

Document Version: 1.0 – 2019-01-16

Android for Work Quick Start Guide

THE BEST RUN SAP

Content

1 Introduction to Android for Work

Android for Work allows you to securely separate business and personal data and applications on your tablet or smartphone.

> **i Note**
>
> This document forms part of both the Afaria and *[[unresolved text-ref: product-long-name-nonregistered]]* document sets and therefore refers to both products. Make sure you follow the instructions for your specific product.

Android for Work provides the following:

A secure mobile experience A dedicated work profile, hardware-based encryption and sharing restrictions ensure business data - calendars, contacts, files and apps - are separate and safe from malware while personal information stays private.

Easy to manage IT has full control of all work related policies, profiles and data - from distributing apps to wiping business information - and the standard Enterprise Mobility Management (EMM) framework delivers a consistent experience across all devices.

All the apps you need Find and deploy business apps easily with Google Play and create apps quickly with the Android app framework. Seamlessly integrate with existing IT systems such as Microsoft Exchange, IBM Notes, and Google Apps for Work.

This guide provides you with all the information to:

- Enroll your enterprise into Android for Work when using *[[unresolved text-ref: product-long-name-nonregistered]]*.

  > **i Note**
  >
  > If you are using Afaria on-premise, contact SAP Support for assistance in enrolling your enterprise.

- Update the Mobile Device management console to support Android for Work
- Create and deploy Android for Work applications
- Enroll Android devices using SAP Mobile Place

2 Prerequisites

In order to set up and use Android for Work you need the following:

- Prior Afaria administration experience
- A Google account
- The following capabilities:
  - Access to the Mobile Device Management Administration console with administrator privileges
  - The ability to create Enrollment and Configuration policies
  - A managed user account
- Users:
  - An Android device running Android 5+. Refer to Android Devices for the latest information on supported devices.

3 Setting up Android for Work

Enroll in Android for Work through Google. After completing this simple setup task, you can start deploying Android for Work Apps.

To enroll, you need a Google account.

> **i Important Note**
>
> From the January release forward, Android for Work no longer supports Google Domain accounts, and only supports Android for Work accounts.
>
> To support Android for Work accounts, update the Android client to the *January client release*. Using an earlier version of the client results in the failure to inflate the managed profile and the inability of the user to install applications. There is no migration path from Google Accounts to Android for Work accounts: the enterprise must be reenrolled, and clients must also reenroll to use the new account configuration.

> **i Note**
>
> This task describes the enrollment process for the *[[unresolved text-ref: product-name-nonregistered]]*. If you are using SAP Afaria, contact SAP Support for assistance in enrolling your enterprise.

1. Log in to the*[[unresolved text-ref: product-name-nonregistered]]* administration portal and go to *Account* > *Device Setup* > *Android* >.
2. From the *Android for Work Account Configuration* area, click *Enroll*.

   You are redirected to the Google Play site.
3. From the Bring Android to work page, sign in using your Google account and then select *Get Started*.
4. From the Organization details page, enter the name of your organization
5. Review the managed Google Play agreement and then select the check box to accept the terms.
6. Select *Confirm*.
7. From the Set up Complete page, select *Complete Registration* to return to the mobile service Administration portal.
8. Under *Android for Work Account Configuration*, review the Android client's permissions and then select *Accept Permissions*.

   The client is automatically and silently updated whenever a new version is posted to Google Play. If the permissions change, an error is logged in the server logs and you must accept the new permissions in this page before the update can proceed.

   After completing this step, the status indicates "Enrolled" and the server name and Enterprise ID are displayed. Users can now enroll their Android 5.0 and above devices with Android for Work support through Mobile Place.

   > **i Note**
   >
   > You may experience a delay of up to an hour for Android for Work support to be enabled for your account. If you experience a delay, wait a little while and try again.

You can now create Android for Work configuration policies and link them to the *All Devices* group in order to start enrolling Android devices with Android for Work support (at `https://<account>.sapmobileplace.com/`). See Creating a Configuration Policy for Android for Work [page 7] for further instructions.

4 Creating a Configuration Policy for Android for Work

Create a configuration policy for scheduling device connections, collecting inventory, and configuring device and application settings for Android for Work devices.

The policy includes multiple pages, such as *Summary* and *Schedule* and device-specific policy settings, which should be completed in order. To save changes on all pages, click *Save* at the top of any page.

> **i** Note
>
> Configuration settings on the *Android* tab (*Policy* > *Edit* > *Android Configuration* > *Summary* > *Android*) have no effect on Android devices configured to use Android for Work policies.

1. On the *Policy* page, on the top toolbar, click *New* > *Configuration* > *Android* > *Android for Work*.
2. On the *Summary* page, enter the policy name.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made to support duplicate policy names are compatible with *[[unresolved text-ref: product-name-short]]* 6.6 and 7 servers.
3. Enter or select the remaining properties.
   - *Note* – add a description for the policy.
   - *State* – set to published or unpublished. Connecting devices receive only published policies.
   - *Priority* – set a user-defined value to determine which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority.
   - *Authentication* – validate the user identity against your authentication authority before allowing the policy to run. This option is available only if you have authentication enabled on the server, as defined on the *Server* > *Configuration* > *Security* page.
   - *Inventory* – select the inventory type to collect. You can view inventory information on the Device page's Device Inspector.
     - *Do not collect inventory* – no inventory collection.
     - *Hardware only* – scan collects data relating to the device's physical components, such as processors and memory cards.
     - *Software and Hardware* – scan collects hardware data and data for installed software.
4. (Optional) To configure a daily connection, define *Schedule* page properties.
5. (Optional) Configure policy pages according to your requirements.

4.1 Google Chrome Page

Configure settings for Google Chrome installed as part of Android for Work.

Setting	Description
Enable Google Chrome	Allows you to set Google Chrome settings for the configuration policy. Select *Enable Google Chrome* to make the settings on this page available.
Incognito Mode Availability	Available, Disabled, Forced. Incognito mode allows users to open incognito tabs in their browser session. In incognito tabs, cookies are disabled and no browser history is maintained. You can choose to enable incognito mode (*Available*), disable it (*Disabled*), or force all tabs to be opened in incognito mode (*Forced*).
Save browser history	Disable, Enable. Controls whether the browser saves the user's browsing history.
Password Manager	Not Enforced, Enabled, Disabled If you enable Password Manager, Google Chrome memorizes user passwords for future website logins. If you disable Password Manager, users cannot save passwords, nor use previously saved passwords. You can allow the user to configure the option, or you can specify that it is always on or always off.
Autofill	Not Enforced, Disabled Specifies whether the user can use the autofill feature to complete online forms. The first time a user fills out a form, Google Chrome automatically saves the entered information, such as the name, address, phone number, or email address, as an autofill entry. You can allow the user to configure the option, or you can specify that it is disabled.
Edit bookmarks allowed	Yes, No Bookmark editing allows users to add, edit, or remove items from their Google Chrome bookmarks bar.
Alternate error page	Not Enforced, Enabled, Disabled Controls whether Google Chrome suggests alternate pages to the user when the page they are trying to reach is unavailable. The user sees suggestions to navigate to other parts of the website or to search for the page with Google. This setting corresponds to the *Use a web service to help resolve navigation errors* Google Chrome setting. You can allow the user to configure the option, or you can specify that it is always on or always off.
Prerender Webpages	Not Enforced, Enabled, Disabled Pre-rendering web pages can speed up the user's browsing experience by allowing Google Chrome to pre-load and render linked pages. This setting corresponds to the user setting *Network action predictions* on the *Privacy* section of the **Advanced** settings tab. You can allow the user to configure the option, or you can specify that it is always on or always off.

Setting	Description
Default search provider	Not Enforced, Disabled This setting specifies whether the user can set a default search provider for the omnibox (Google Chrome's address bar) or not.
Force safe search	Yes, No Selecting *Yes* forces your users' Google searches in Google Chrome to be done with SafeSearch turned on.
Search Suggest	Not Enforced, Enabled, Disabled When users enter information into the address bar, Google Chrome can use a prediction service to help complete the web addresses or search terms. You can allow the user to configure the option, or you can specify that it is always enabled or disabled. This setting corresponds to the *Use a prediction service to help complete searches and URLs typed in the address bar* setting in Google Chrome's *Settings* page.
Safe Browsing	Not Enforced, Enabled, Disabled Specifies whether or not Safe Browsing is turned on for users. Safe Browsing helps protect users from websites that may contain malware or phishing content. You can allow users to decide whether to use Safe Browsing, or specify that it is always on or always off.
Google Translate	Not Enforced, Enabled, Disabled Lets you specify whether Google Chrome uses Google Translate, which offers content translation for web pages in languages not specified in the *Language* settings on a user's Google Chrome device. You can set Google Chrome to let users set this option in their local Google Chrome *Settings*, always offer translation, or never offer translation.
Data compression proxy	Not Enforced, Enabled, Disabled Enabling this setting can reduce cellular data usage and speed up mobile web browsing by using proxy servers hosted at Google to optimize and compress website content. You can set Google Chrome to allow the user to decide whether to use the data compression proxy, enable the data compression proxy, or disable the data compression proxy.

Proxy Settings

Setting	Description
Proxy Mode	Not Enforced, None, Auto-Detect, System, PAC Script, Manual

Setting	Description
	Specifies how Google Chrome connects to the Internet. If you leave the setting as *Not Enforced*, the user can change the proxy configuration in their Chrome *Settings*. If you choose any of the other Proxy Mode options, the user can't change the configuration. The remaining options are: **None** Google Chrome always establishes a direct connection to the Internet without passing through a proxy server. A direct connection is also the default configuration for Chrome devices if you do not set a policy and the user doesn't change the configuration. **Auto-Detect** Google Chrome determines which proxy server to connect to using the Web Proxy Autodiscovery Protocol (WPAD). **System** **PAC** Proxy Auto-detect. Always use the proxy auto-config (`.pac`) file specified in the *Proxy PAC URL* field. **Manual** Sets the server specified in the *Proxy Server* field as the proxy server to handle requests from Google Chrome. If you select this option, you need to enter the URL of the proxy server in the Proxy Server URL field below. Format the Proxy Server URL as 'IP address:port', such as '192.168.1.1:3128'. Leave it empty for any other Proxy Mode setting.
Proxy PAC URL	Available if *PAC Script* is selected. Specify the URL of the `.pac` file to use for network connections.
Proxy Server	Available if Manual is selected.

If there are any URLs that should bypass the proxy server that handles other user requests, enter them in the *Proxy Bypass URLs* list. You can set up multiple URLs.

To define a Proxy bypass URL, click *Add* from the toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to include the proxy bypass URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the proxy bypass server.

URL Blacklist and Whitelist Settings

A blacklist prevents Chrome devices from accessing specific URLs. A whitelist explicitly allows Chrome devices to access specific URLs. You can enter up to 1000 URLs for each list. URLs take the following form:

- Each URL must consist of a valid host name (such as google.com), an IP address, or an asterisk (*) in place of the host. The asterisk functions as a wildcard, representing all host names and IP addresses.
- URLs can also include:

- The URL scheme, which is http, https, or ftp, followed by ://.
- A valid port value from 1 to 65535.
- The path to the resource.
- Query parameters.

> **i Note**
>
> - To optionally disable subdomain matching, put an extra period before the host.
> - You cannot use user:pass fields, such as http://user:pass@ftp.example.com/public/file.xyz. Instead, enter http://ftp.example.com/public/file.xyz.
> - When both blacklist and blacklist exception filters apply (with the same path length), the exception filter takes precedence.
> - If an extra period precedes the host, the policy filters exact host matches only.
> - The policy searches wildcards (*) last.
> - Optional query parameters consist of a set of key-value and key-only tokens delimited by '&'. The key-value tokens are separated by '='. A query token can optionally end with a '*' to indicate prefix match. Token order is ignored during matching.
>
> For examples of valid whitelist and blacklist specifications, search for "Set Chrome policies for users" at support.google.com.

To add a URL to the blacklist or whitelist, click *Add* from the appropriate toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to include the proxy bypass URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site you want to allow or deny.

Managed Bookmark Settings

To add a bookmark, click *Add* from the toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to add the bookmark to users' available bookmarks when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
Name	Enter a name for the bookmarked site.
URL	The URL of the site to bookmark.

Geolocation Settings

Sets whether websites are allowed to track users' physical locations. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Location*. Tracking physical locations can be set by the user (*Not Enforced*), allowed by default (*Allow*), the user can be asked each time a website requests the physical location (*Ask*), or denied by default (*Block All*).

Cookie Settings

The *Default cookies setting* option determines whether websites are allowed to store browsing information, such as user site preferences or profile information. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Cookies*. Whether to allow cookies can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Cookie session only URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the cookie session-only URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow or deny cookies.

Cookie blocked URLs. Allows you to specify a list of URL patterns of sites that are not allowed to set cookies. If this policy is not set, what you specify under *Default cookie settings* will be the global default, or the user can set their own configuration.

Cookie blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the cookie-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block cookies.

Cookie allowed URLs. Allows you to specify a list of URL patterns of sites that are allowed to set cookies. If this policy is not set, what you specify under *Default cookie settings* will be the global default, or the user can set their own configuration.

Cookie allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the cookie-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow cookies.

Image Settings

The *Default images setting* option determines whether websites are allowed to display images. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Images*. Whether to display images can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Image blocked URLs. Allows you to specify a list of URL patterns of sites that are not allowed to set display images. If this policy is not set, the user can set their own configuration.

Image blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the image-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block images.

Image allowed URLs. Allows you to specify a list of URL patterns of sites that are allowed to display images. If this policy is not set, the user can set their own configuration.

Image allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the image-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow images.

JavaScript Settings

The *Default javascript setting* option determines whether websites are allowed to run JavaScript. If you disable JavaScript, some sites may not work properly.

Sets whether websites are allowed to run JavaScript. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *JavaScript*. Whether to allow JavaScript can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Javascript blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the JavaScript-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block JavaScript.

Javascript allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the JavaScript-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow JavaScript.

Popup Settings

The *Default popup setting* option determines whether websites are allowed to display pop-ups.

This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Pop-ups*. Whether to allow pop-ups can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Popup blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the pop-up-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block pop-ups.

Popup allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the pop-up-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow pop-ups.

4.2 Exchange Account Policy Page

For a user that is already defined in the Microsoft Exchange environment, sets properties for the native Microsoft Exchange ActiveSync (EAS) client.

You can use substitution variables for most of the values defined on this page. See *Substitution Variables* for more information.

Setting	Description
Enable Exchange Account	Allows you to set Exchange Account settings for the configuration policy. Enable to make the settings on this page available.

Setting	Description
Username	User's Exchange user name
Password	User's Exchange password
Domain	User's e-mail domain for the Exchange account **i Note** This is not a required field. The domain must be specified in either the *Username* field ("user@domain" or "domain\user") or the *Domain* field. If specified in the *Domain* field, Afaria appends it to the username. If it is specified in both places and the domain is different, Afaria use the one in the username field.
Email Address	User's Exchange e-mail address
Exchange host	Fully qualified domain name for the Microsoft Exchange server
Require SSL	Select *Yes* to require the use of SSL for Exchange sessions.
Trust All Certificates	Select *Yes* to allow the device to accept certificates without user intervention.
User Certificate	To add the client certificate, click *Add Certificate*, browse to select a certificate, and then specify a password for the certificate. To add a SCEP request, click *Add request*, select a CA profile from the drop-down list, and specify the common name and password for the CA. You may also specify an alt name for the certificate.
Signature	Signature for user-initiated messages. If left blank, the user can enter a signature.
Maximum attachment size (MB)	The maximum size of attachments in megabytes.
Enable tasks application	Select *Yes* to enable the Exchange Tasks application on the device.

4.3 Restrictions Page

For Android for Work devices, defines restrictions for user access to certain features.

Setting	Description
Enable Restrictions	Allows you to set restrictions for the configuration policy. Enable to make the settings on this page available.
Screen Capture	Allows you to enable or disable screen captures on the device.

Setting	Description
Enable Camera	Allows you to enable or disable the camera on the device.

4.4 Security Page

Configure password settings and provide certificates for the Android for Work profile on Android devices.

Setting	Description
Enable Password	Allows you to set password settings for the configuration policy. Enable to make the password settings on this page available.
Password Quality	The password format required, either Something, Numeric, Alphabetic, Alphanumeric, or Complex.
Minimum password length	The minimum length for the password. The range is 4 – 16 characters.
Invalid password attempts before Android for Work data wipe	The number of times a user can enter a wrong password before data wipe occurs.
Maximum idle time until lock	The maximum time that the user can configure the device to remain idle before the device screen locks. The options are: 15 sec, 30 sec, 1 min, 2 min, 5 min, 10 min, and 30 min.
Password History	The number of passwords stored in the history list. The range is 1 – 100. The default is 10.
Maximum number of days until password expires	The number of days a password remains valid. The range is 0 – 365. 0 means there is no restriction (the password does not expire). The default is 90 days. **i Note** This setting is currently not enforced by Google.
Minimum password letters Complex password format only	The minimum number of letters in the password. The range is 1 – 16.
Minimum password lowercase Complex password format only	The minimum number of lowercase letters in the password. The range is 0 – 16.
Minimum password uppercase Complex password format only	The minimum number of uppercase letters in the password. The range is 0 – 16.
Minimum password non-letter	The minimum number of non-letter characters in the password. The range is 0 – 16.

Setting	Description
Complex password format only	
Minimum password numeric Complex password format only	The minimum number of numbers in the password. The range is 1 – 16.
Minimum password complex characters Complex password format only	The minimum number of symbols in the password. The range is 1 – 16.
Smart Lock disabled	Yes or No. Select *Yes* to disable Smart Lock. Smart Lock is an Android feature that allows users to unlock their devices automatically. Default is "No".

Certificates

Configure settings for CA certificates used to authenticate connections between the Android for Work profile and your network.

To add a certificate, click *Add* from the toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to include the certificate when the policy is run. If you select *Exclude*, the certificate remains on the list but is not deployed to the device.
Certificate	To add the client certificate, click *Add Certificate*, browse to select a certificate, and then specify a password for the certificate. To add a SCEP request, click *Add request*, select a CA profile from the drop-down list, and specify the common name and password for the CA. You may also specify an alt name for the certificate. **i Note** In order to install a SCEP certificate on a device, the device must have a password. If you include a SCEP request in this policy, ensure you configure password settings on this page.

4.5 WiFi Page

Configure WiFi connections on Android for Work devices to allow users to connect wirelessly to your network. You can also choose to block users from connecting to a configured network connection.

To remove a network configuration from the Android Client, include the item you wish to delete and delete the Network SSID. The item with that Identifier will then be deleted when the Client runs this policy.

Setting	Description
Enable Wifi	Allows you to set WiFi settings for the configuration policy. Enable to make the settings on this page available.
Include/Exclude	Allows you to include or exclude the connection profile from the configuration policy.
Identifier	A system-generated ID for the network connection. This field is not editable.
Network SSID	Network Service Set Identifier (SSID). This is a name for the Wi-Fi connection as configured on the wireless router. This name is used to identify the connection in the device's Wi-Fi list. Required.
Hidden SSID	Indicates whether the SSID is hidden. If the SSID is hidden, the WiFi router does not broadcast its identity. The WiFi network is not listed on the device.
Network link security	The security protocol used to authenticate network link connections. Depending on the security protocol used, you may need one of the following: • A network WEP key 1 for WEP • A network pre-shared key for WPA/WWPA2-PSK • A CA certificate and either a client certificate or SCEP request for all version of EAP
CA Certificate	The certificate used by the router to authenticate the connection. Available if EAP is used. To add a CA certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. **i Note** A device password must be enabled.
Client certificate	The certificate used by the device to authenticate the connection. Available if EAP is used. To add a client certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. To add a SCEP request, click *Add SCEP request*, select a CA profile from the drop-down list, and specify the common name and password for the CA.

Setting	Description
	i Note A device password must be enabled.
Network identity value	The network identity value. Available if EAP is used.
Network password	The network password for authenticating the network connection. Available if EAP is used.
Network pre-shared key	A pre-shared key. Required when WAP/WAP2-PSK is used.
Network WEP key 1	A WEP key 1. Required when WEP is used.

4.6 Creating an Application Policy for Android or Android for Work Google Play Apps

Create policies for managing Android and Android for Work applications from Google Play.

- An account with Google Play. Google Play user agreements and costs are independent of *[[unresolved text-ref: product-name-nonregistered]]* operations.
- An Android for Work profile on the target device. To create a work profile, create and apply an Android for Work Configuration policy.

Policy setup is comprised of multiple pages, which should be completed sequentially. To save changes on all pages, click *Save* at the top of any page.

When you create an app policy to deploy an app to an Android for Work managed profile on a device, you can indicate if the app is to be a required or an optional app. If you set the policy to required, the app is installed in the managed profile when the policy is applied. If you set the policy to optional, the app is displayed as an available app in the managed profile and can be installed by the device user if desired.

1. On the top toolbar of the *Policy* page, click *New* > *Application* > *Android Market*.
2. On the *Summary* page, enter the policy name and an optional note and indicate whether the policy is published or unpublished.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Connecting devices receive only published policies.
3. (Optional) Select *Featured app* to tag the application as featured, which means it appears in a ticker on the home page of the device.
4. On the *General* page, select *Deploy for Android for Work devices* if you want to deploy this app to an Android for Work managed profile on a device.

   (Afaria only) If you select this option, the *Required* check box becomes available.
5. (Afaria only) Select the *Required* check box to install the application in the managed profile when the app policy is applied to the device.

If you leave this check box unselected, the app is treated as an optional app. When the app policy is applied to the device, the app is displayed as an available app in the managed profile and can be installed by the device user if desired.

6. In the *Package* field, enter the application name (`com.amazon.kindle`, for example) and click *Update* to populate the *Information* box (data retrieval is subject to data availability from the Google Play).

   When you set the Android for Work application to production mode, an Android for Work policy is automatically created and marked as "Required."

7. (Optional) On the *Categories* page, select one or more categories to be associated with the policy.

   Click *Add* to add a new category.

8. (Optional) Select *Yes* or *No* to indicate whether the selected category is a featured category.

9. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter an additional note, if required.

   > **i Note**
   >
   > The maximum length allowed for the file name is 258 characters, and the maximum image size allowed is 1MB. To enable easy download and to minimize data traffic, use smaller image files of sizes up to 100KB.
   >
   > The recommended resolution for the category image on an Android device is up to 1920 x 1080 pixels. The category image is scaled to the required resolution, without changing the aspect ratio, and is then center-cropped.

10. (Optional) In the *Available Categories* list, make changes by selecting a category and clicking *Edit*, *Delete*, *Inspect Image* or *Clear Image*.

    If you delete a category that is attached to another policy, the category is also deleted from the referring policy.

    Click *Inspect Image* to open the image in *Server* > *Category Image File* window.

    Click *Clear Image* to remove the image associated with the *Available Category*.

11. (Optional) In the *Pre-defined Categories* list, make changes by selecting a category (*Enterprise*, *Play Store*, or *All*) and clicking *Edit*, *Inspect Image* or *Clear Image*.

    Click *Inspect Image* to open the image in the *Server* > *Category Image File* window.

    Click *Clear Image* to remove the image associated with the predefined category.

12. (Optional) On the *Description Detail* page, enter a description for the application and modify the display name.

    The display name of the application is automatically updated when you upload the application package on the *General* page.

13. On the *Configuration* page, type or import your application seeding configuration data.

    Import source location is relative to the browsing computer. Importing a file overwrites the content in the data box. If you edit the file in the *[[unresolved text-ref: admin-interface-name]]* it is stored in UTF-8 format. Otherwise, it is stored in its original format.

    If you import an empty text file here, the file is not saved with the policy.

14. Click *Edit* to open the *Application Policy* > *Configuration* dialog and click *Substitution link*. The *Substitution Variables* dialog opens. The list combines predefined and user-defined substitution variables.

15. Select a substitution variable and click *Select* to add it to the application.

    If the substitution variable is not on the list, click *Add* to define it.

To delete a substitution variable from the list, select it and click *Delete*. This action deletes the user-defined variable and any associated value from all iOS and Android definitions.

16. You can now view and edit the configurations for the application and set the required values, which makes it easier for users to install applications. To edit the configurations:
    a. Select the configuration you want to edit.
    b. Click *Edit*, update the *Value* field as required, and save it.
17. On the *App Permissions* page, view the application permissions that are set for the application.

    When you set an Android for Work application to production mode, an Android for Work policy is automatically created and marked as "Required".
18. Click *Save* to save all of your changes.

5 Adding an Android Application from a Commercial App Store

Using the *[[unresolved text-ref: product-name-nonregistered]]*, an App Catalog Administrator or an App Catalog Publisher can add an Android (including Android for Work) application from a commercial app store to be published on *[[unresolved text-ref: cloud-user-interface]]*.

App Catalog Administrators and App Catalog Publishers have the following permissions:

App Catalog Administrator Role - Permissions

State	Can Edit	Available Action Items
New	Yes, except the *Info* tab and the *Multimedia* tab	Set to Trial, Request Trial, Request Production, Set to Production, Delete
Trial Requested	Yes, except the *Info* tab and the *Multimedia* tab	Approve, Reject
Trial	Yes, except the *Info* tab and the *Multimedia* tab	Request Production, Set to Production, Delete
Production Requested	Yes, except the *Info* tab and the *Multimedia* tab	Approve, Reject
Production	No	Retire
Retired	No	Delete

App Catalog Publisher Role - Permissions

State	Can Edit	Available Action Items
New	Yes, except the *Info* tab and the *Multimedia* tab	Set to Request Trial, Request Production, Delete
Trial Requested	No	None
Trial	No	Request Production
Production Requested	No	None
Production	No	None
Retired	No	None

1. Click *Applications*.
2. From the *Manage Apps* tab, click *New Application*.
3. Select *Commercial App Store* and select *Google Play*.
4. Click *Next*.
5. On the *Details* page:
   - *Country* – select a country. The Country field is disabled on Android devices.
   - *Language* – select a language.

> **Note**
>
> The languages that appear depends on the language settings set in the *Account* > *Mobile Place* > *Settings* page.

- If you select:
  - *Name* – enter the name of the application. After you save the application, you cannot edit the name of the application.
  - *URL* – copy the URL of the application from the app store.
- (Optional) *Description* - If you select:
  - *App Store*: The information in the description field is automatically populated from the app store. You cannot edit this information.
  - *Enterprise*: Enter custom description or information for this app.

> **Note**
>
> App publisher or app catalog admin can:
> - select only one type of description for the app to be published to the Mobile Place users
> - switch to any type of description at any point of time. Last save description will be published to the Mobile Place users

- (Optional) *Keywords* – enter keywords separated by commas that will help users in searching and retrieving the new application. Each keyword cannot exceed 60 characters.
- By default, *Accessible to unauthenticated users* is disabled. This option is enabled only if unauthenticated access has been enabled from *Account* > *Mobile Place* > *Settings* page. If the *Accessible to unauthenticated users* check box is selected, an application is visible to unauthenticated users only.

> **Note**
>
> *Deploy to managed devices only* and *Accessible to unauthenticated users* are mutually exclusive.

6. Click *Save*.

   The application is created.
7. Click *Groups*, and select the visibility of the application to all users, or only to selected groups.

   You can search for an existing group by typing the group name in the search groups window. Use the *Actions* icon to sort the list based on group name, or apply filters to search for a group.

   You can also create a new group, if required, by selecting the static or directory group option from the *New group* drop-down list. The newly created group is selected, by default.

   For more information on how to create groups, see *Group Management* section.
8. If you select *show the application only to selected groups*, you must select the required groups from the list or create a new group.
9. Click *Save*.
10. Click *Multimedia*. Upload an application icon or banner image by clicking *Browse*.

> **Note**
>
> A featured application must include a banner image.

The banner image must have the following properties:

- Only png, jpeg, and jpg file formats are supported.
- The recommended resolution is 1024 X 230 pixels.
- You can upload only one banner image.

11. Click *Save*.
12. Click *Categories*. To select application categories for the application, double-click or drag and drop each category from the *Available* box to the *Selected* box. To deselect categories, double-click or drag and drop the category from the *Selected* box.
13. Click *Save*.
14. Click *Settings* and select one or all of the following options:
    - *Deploy to managed users only* – the application is accessible only to managed users. This is the default setting for Android for Work applications.
    - *Mark as featured app* – the application will appear on the banner area in Mobile Place and you will be prompted to provide a banner image if you have not already done so (featured apps require a banner).
15. Click *Save*.
16. Click *Owner info* to view the owner information for the application. You can select up to five co-owners for a new application.
17. Click the *Edit App Owner* icon to change the application owner.

    > **i Note**
    >
    > Only users with App Catalog Admin role can edit the application owner.

    The *Select Owner* dialog is displayed.

    > **i Note**
    >
    > Only users who have App Catalog Admin and App Publisher roles are displayed.

18. Select the user and click *OK*.
    The app owner information is updated in the *Owner info* page.
19. Click *Add Co-Owner* to add new co-owner(s) (up to five).
    The *Select co-owners* dialog is displayed.
20. Search for co-owner by username, first name, last name, or email address. Select co-owners by selecting the checkbox beside their information.
21. Click *OK* to close the *Select Co-Owners* dialog.
22. Click *Save*.
23. Click *Supported platforms* to view the supported platform information for the application.
24. Click *Save* to save the supported platforms information.
25. Click the *Actions* icon in the *Supported Platforms* page to perform one of the following actions:
    - *Approve* – sends a request to the App Catalog Administrator to approve whether the platform state is in trial or production requested state. On approving a trial request or a production request, the *Application Notification* dialog appears. Choose whether to send the application notification to all subscribed users or to not send the notification.
    - *Reject* – sends a response to the App Catalog Administrator to reject a trial or production requested state. When a trial request or a production request is rejected, the *Reject Trial Request* or *Reject Production Request* dialog is displayed and the App Catalog Administrator must provide a reason for the rejection. Optionally, additional comments may be provided.

- *Request Trial* – sends a request to the App Catalog Administrator to publish the application in *[[unresolved text-ref: cloud-user-interface]] App Catalog* for trial users to test the app.
- *Set to Trial* – sends a request to the App Catalog Administrator to publish the application on the *[[unresolved text-ref: cloud-user-interface]] App Catalog* for allow trial users (only) to install and test the app.
- *Request Production* – sends a request to the App Catalog Administrator to publish the application on the *[[unresolved text-ref: cloud-user-interface]] App Catalog* for all end users.
- *Set to Production* – sends a request to the App Catalog Administrator to publish the application on the *[[unresolved text-ref: cloud-user-interface]] App Catalog* for all users to access and install the application. When the application is set to production, the *Application Notification* dialog appears. Choose whether to send the application notification to all subscribed users or to not send the notification.
- *Retire* – sends a request for the App Catalog Administrator to retire the application if it is in production. Once an application is retired, it is not available to end users.

  > **i** Note
  >
  > Users who have installed the app that has been retired can still use the application.

- *Delete* – Sends a request for the App Catalog Administrator to delete an application if it is in New, Trial, or Retired state. An application in request or production state cannot be deleted. If the application is in New state, the application can be deleted by the publisher as well. Because there is only one platform for the commercial app store application, the application is also deleted.

26. You can also click the *Edit* icon in the *Supported Platforms* page to edit the supported platform. The **Edit Platform** dialog is displayed.
27. For Android for Work applications: In the *Info* page, select *Deploy as Android for Work App* to set the application to be an Android for Work application. By default, Android for Work apps are deployed to all managed users.

    After setting an application to be Android for Work, the *Permissions* and *Configuration* tabs are enabled. You must perform the following steps in these tabs:

    a. Click *Permissions* to view the application permissions that are required by the application.
    b. Select *Accept all changes* to accept the permissions on behalf of end-users. This supports the silent installation of Android for Work applications and means users do not have to accept permissions for managed applications.

    > **i** Note
    >
    > After you accept the initial set of permissions for the first time, only new permissions are displayed. If there are no new permissions, the *All permissions for this application have been accepted or there are no permissions available for this application.* message is displayed.

    c. Click *Configuration* to view and change configurations, if any, which allows users to install applications without requiring them to edit configuration values. After the application is set to production, you cannot edit the configurations through the *[[unresolved text-ref: product-name-nonregistered]]* portal.

    > **i** Note
    >
    > See also *Chrome Settings* page for detailed information on configuring whether users can modify any of these settings themselves.

28. (Optional) Click *Documents* to upload a document file that provides more information about your application.

    The document file must conform to the following:

    - Only .doc, .pdf, .txt, .ppt, .pptx, and .docx file types are allowed.
    - The maximum file size of each document cannot exceed 35 Mb.

29. Click *Trial users* to add one or more trial users who can test the application before it is published to all users.
30. Click *Add Trial User*.
    The *Select Trial Users* dialog is displayed.
31. Search trial users using username, first name, last name, or email address. Select the checkbox beside the trial user(s) to add.

    > **i Note**
    >
    > Only users who have the Mobile Place User role are displayed.

32. Click *OK* to save and close the *Select Trial Users* dialog.
33. (Optional) Click *Multimedia* to add sample images (in .png, .jpeg or .jpg format) and/or videos (MP4 format) to associate with the application.
34. Click *OK* to close the *Edit Platform* dialog.
    The *Supported Platforms* page is updated with supported OS version and app version information.

6 Enrolling an Android Device

Using Mobile Place, enroll an Android device in management and access the *App Catalog*. If Android for Work policies have been linked to your device, Android for Work enrollment starts automatically when you log in to Mobile Place.

Activate your user account and log in to *[[unresolved text-ref: cloud-user-interface]]*.

Enrollment in Android for Work

For new devices, enrollment starts automatically when you log in to Mobile Place. For devices managed by *[[unresolved text-ref: product-long-name-nonregistered]]*, the *[[unresolved text-ref: product-name-nonregistered]]* credentials are used to create the managed profile.

For already enrolled devices that support Android for Work, the Android for Work profile is created automatically when your administrator assigns a configuration policy.

All application permissions for managed applications are pre-approved by your Mobile Place administrator, so there is no permission approval required.

You may experience a delay of up to an hour while the Android for Work profile is created on the device, and also while downloading an Android for Work application from Mobile Place.

> **i** Note
>
> If you cancel the prompt to install the Android for Work profile, you continue to receive prompts even if Android for Work policies have been unlinked from your device. These prompts continue until the profile is installed, the client is upgraded, or the device is re-enrolled. To get rid of these prompts, make sure that your administrator has unlinked all Android for Work policies and then re-enroll.

1. On the *[[unresolved text-ref: cloud-user-interface]]* welcome page or e-mail, tap *Enroll*.

   A seed file is downloaded and you are redirected to the *Play Store*.
2. Tap *Install* and then *Open* once the client is installed.
3. Review the administrative privileges and tap *Activate*.
   Enrollment progress is displayed on the device. For some devices, there may be suggested optional additional applications. Upon successful enrollment, the *Home* page of the Afaria client is displayed.
4. (Optional) If your administrator has created an enrollment policy in SAP Afaria MDM, enter that account information and tap *Submit*.
5. Return to Mobile Place.
   You see "Congratulations! You are enrolled!".
6. Tap *Go to App Catalog* to view the various apps that you can install on the device.
7. (Optional) Log out from Mobile Place, then log in.

   If your device is already enrolled in SAP Afaria MDM, select it, then tap *OK* to view the *App Catalog*. To enroll a new device, tap *New Device*.

For Android for Work:-

After a device is enrolled for Android for Work, only Android for Work apps are displayed in the app catalog. When the Android for Work profile is removed by unenrolling the device, performing a remote wipe or doing a factory reset, the app catalog is refreshed and all the Android apps are displayed in the app catalog.

On your device, managed applications are displayed with a small briefcase badge on them. Managed application capabilities and restrictions are configured by your Mobile Place administrator. Any data entered into the applications is encrypted internally to the application and some or all of the data may be subject to restrictions on copy-and-paste or sharing between managed applications and unmanaged applications. For any issues or concerns, please consult with your support team.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP