MATRIX42
SMARTER WORKSPACE – BETTER LIFE

Silverback by Matrix42

Android for Work Enablement

Version 3.1.0

15/01/2016

Copyright © 2000 - 2015 Matrix42 AG

This documentation is copyright protected. All rights are reserved by Matrix42 AG.

Any other use, in particular the disclosure to third parties, storage in a data system, dissemination, processing, presentation, performance and demonstration are prohibited. This applies to the entire document, as well as parts thereof.

Subject to change. Reprint, also in excerpts, is permitted only with the written consent of Matrix42 AG.

The software described in this document is subject to a permanent development due to which there may be differences in the documentation and the actual software. This documentation is not entitled to the actual functionality of the software.

Apple and **Mac OS X** are registered trademarks of Apple Inc.
Citrix® software or **Citrix® server** are Trademarks and Registered Trademarks of Citrix Systems, Inc. in the United States and other countries.
cygwin is copyrighted by Red Hat Inc. 1996-2003.
expat is copyrighted by Thai Open Source Software Center Ltd.
gSOAP is copyrighted by Robert A. van Engelen, Genivia, Inc. All rights reserved.
Iconv is copyrighted by 1999-2003 Free Software Foundation, Inc.
Iperf is copyrighted by the University of Illinois, except for the gnu_getopt.c, gnu_getopt_long.c, gnu_getopt.h files, and inet_aton.c, which are under the GNU General Public License.
Libmspack (C) 2003-2004 by Stuart Caie <kyzer@4u.net>.
OpenSSL This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
PuTTY is copyrighted by Simon Tatham. Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, and CORE SDI S.A.
RSA Data Security, Inc. MD5 Message-Digest Algorithm is copyrighted by RSA Data Security Inc. Created 1991. All rights reserved.
rsync is an open source utility that provides fast incremental file transfer. rsync is freely available under the GNU General Public License version 2.
runcontrol The Initial Developer of the Original Code is James Clark. Portions created by James Clark are Copyright (c) 1998 James Clark. All rights reserved.
SNMP++ Copyright (c) 1996 Hewlett-Packard Company.
VMware, the **VMware "boxes" logo and design, Virtual SMP, VMotion vSphere, vSphere Hypervisor (ESXi), ESX, View, ThinApp, vCenter** and **vCloud** are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.
Windows, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and **Windows Server 2012** are registered trademarks of Microsoft Corporation.

Others, at this point not explicitly listed, company, brand and product names are trademarks or registered trademarks of their respective owners and are subject to trademark protection.

Table of Contents

1. Overview 4
1.1. What is Android for Work? 4
1.2. How does Silverback Integrate with Android for Work? 4
2. Creating a Google Managed Domain 5
2.1. Signing up for a Managed Domain 5
2.2. Verify Domain Ownership 7
3. EMM Token for existing Google Managed Domain 11
3.1. Generate a Token 11
4. Creating the API Project 13
4.1. Enabling EMM API Functionality 13
4.2. Create the Service Account Credentials 15
4.3. Enable Directory Management via Silverback 22
5. Pairing Silverback to the Managed Domain 25
5.1. Pairing Android for Work Management 25
5.2. Pairing Directory API Management 28

Android for Work Enablement

1. Overview

1.1. What is Android for Work?

Android for Work is Google's approach to standardize the management for Android devices in enterprise environments across all hardware manufacturers.

Android for Work provides a logically data separated work area managed by corporate IT in parallel to the personal area on a single Android device. The private and Android for Work area share the same user interface to allow the user native UI experience. All Android for Work applications are differentiated by an orange briefcase icon ('badged apps') and can be easily identified as work application by the end-user.

1.2. How does Silverback Integrate with Android for Work?

At a high level, a Google Managed Domain is created (or an existing Google Apps account also), and then this is "paired" with Silverback by Matrix42, allowing the server to manage users and settings.

Special API Projects are created in the Google Managed Domain and then Silverback is configured to work with these projects.

From this point forward, the management of apps and settings for devices is done via the Silverback Admin Console.

This document will go through the process of enabling Android for Work for your devices from start to finish.

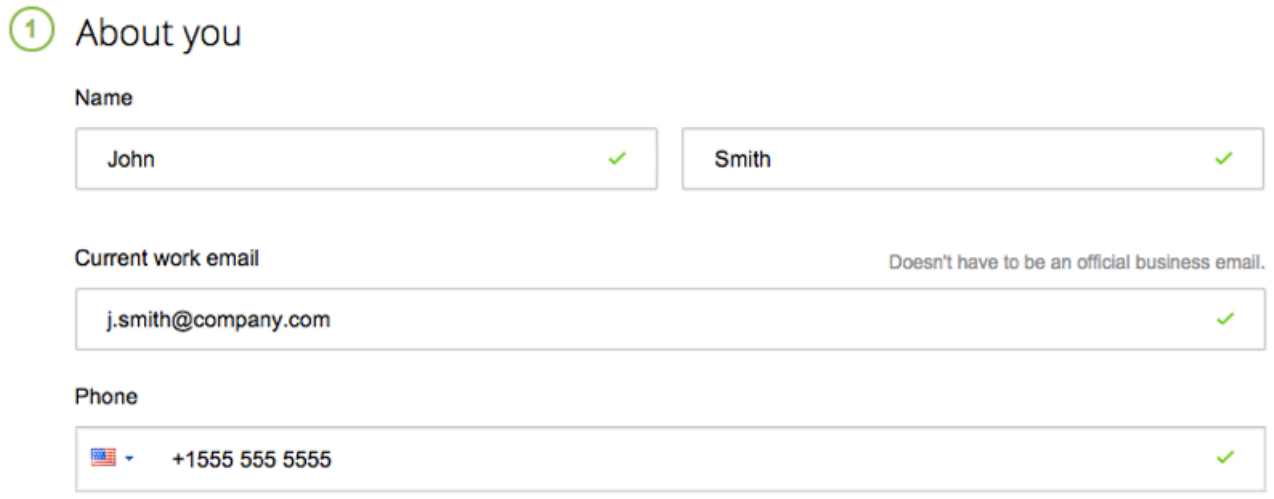
2. Creating a Google Managed Domain

2.1. Signing up for a Managed Domain

This step is not required if you already have a Google Apps account or Managed Domain.

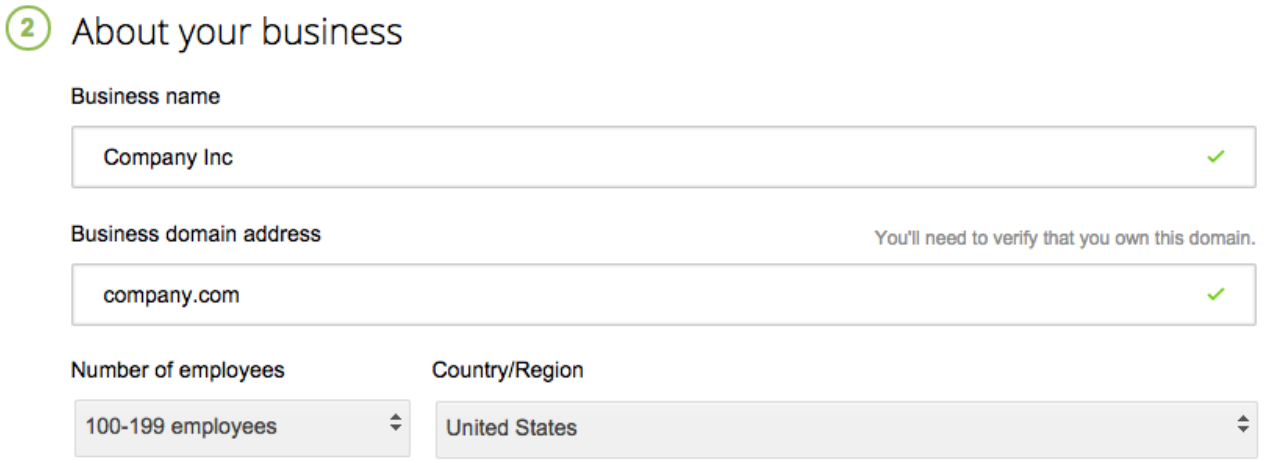
Begin by first navigating to the Android for Work sign-up page, located here: https://www.google.com/a/signup/u/0/?enterprise_product=ANDROID_WORK

In the **About you** section, enter the personal information including your First and Last name, current work email (this does not need to match the domain you are signing up for), and phone number.

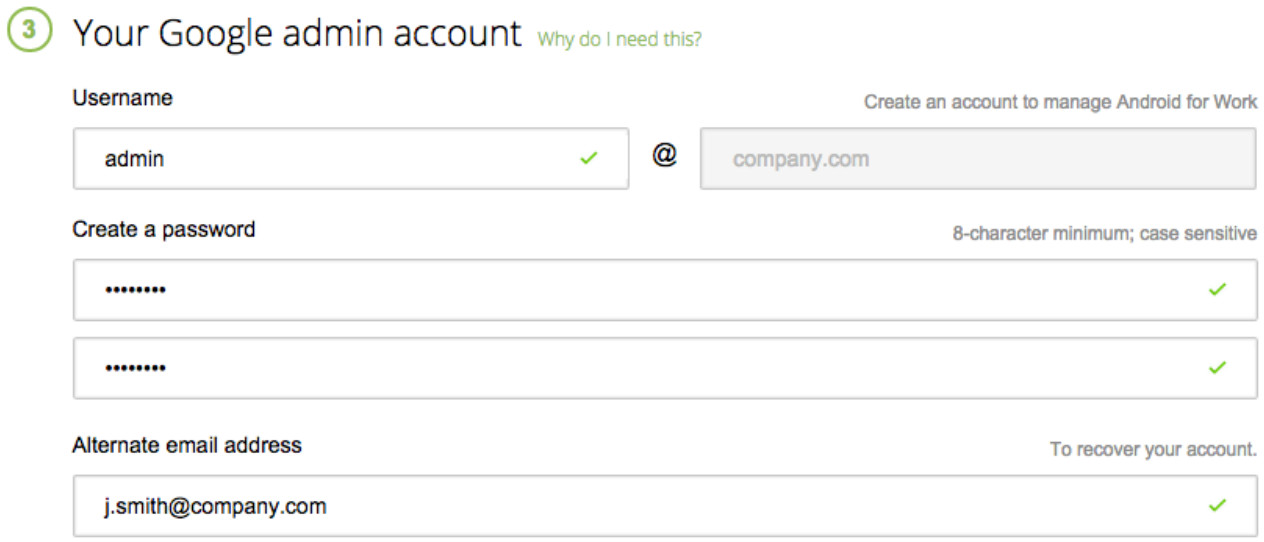


In the **About your business** section, enter your business name and the business domain address. **This domain must match the domain you want your users to enrol with, e.g. company.com.** You will also need to verify that you own this domain, this is typically done by creating a DNS entry with Google will check for, and this will prove that you manage the domain. Enter the other information such as number of employees and country/region.

Android for Work Enablement



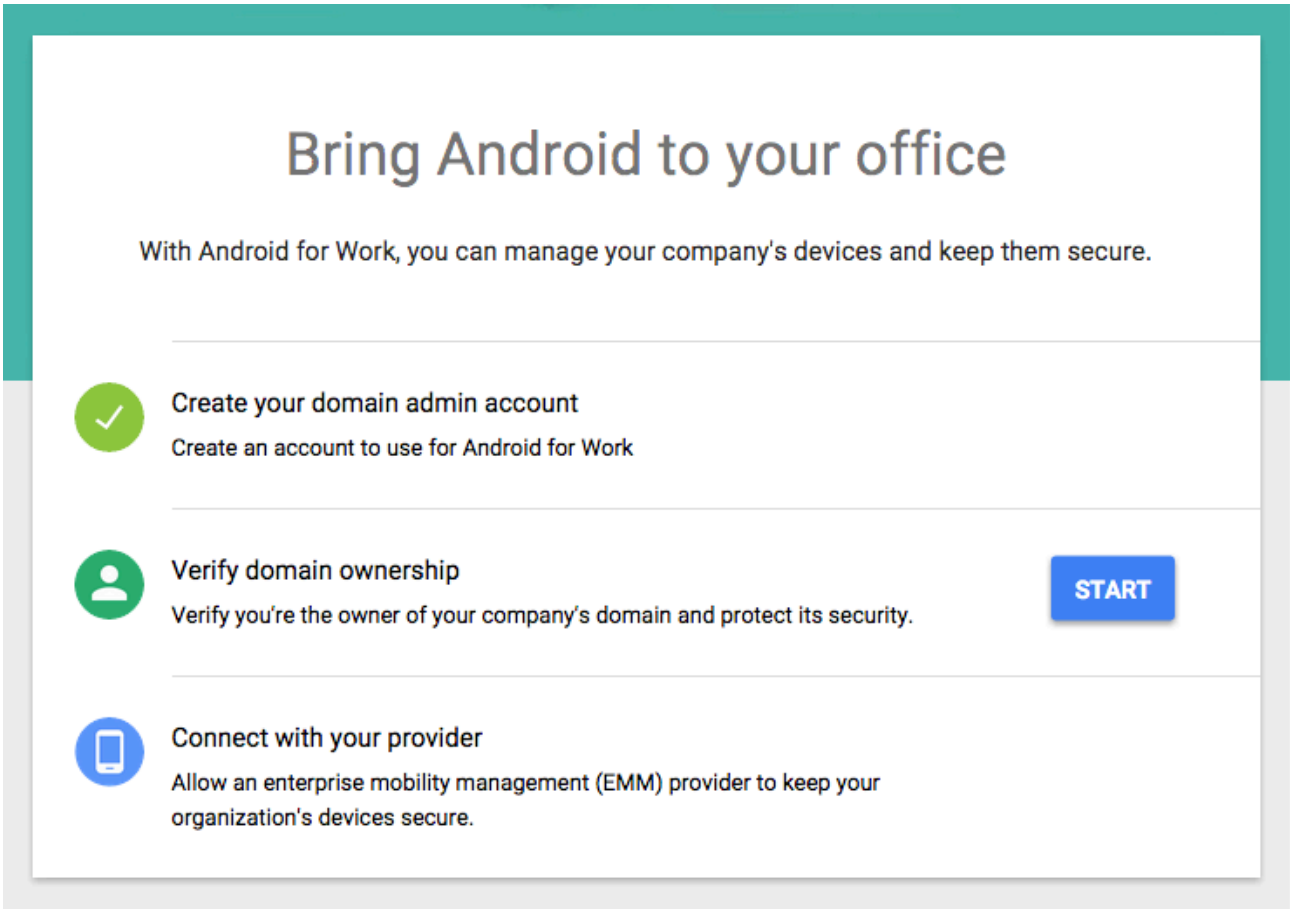
In the **Your Google admin account** section, you will be creating the administrative account for your Managed Domain. This is the account that will be used for the rest of the document and will be the “Master” account.



In the final section, enter the security verification and read and agree to the required agreements.

2.2. Verify Domain Ownership

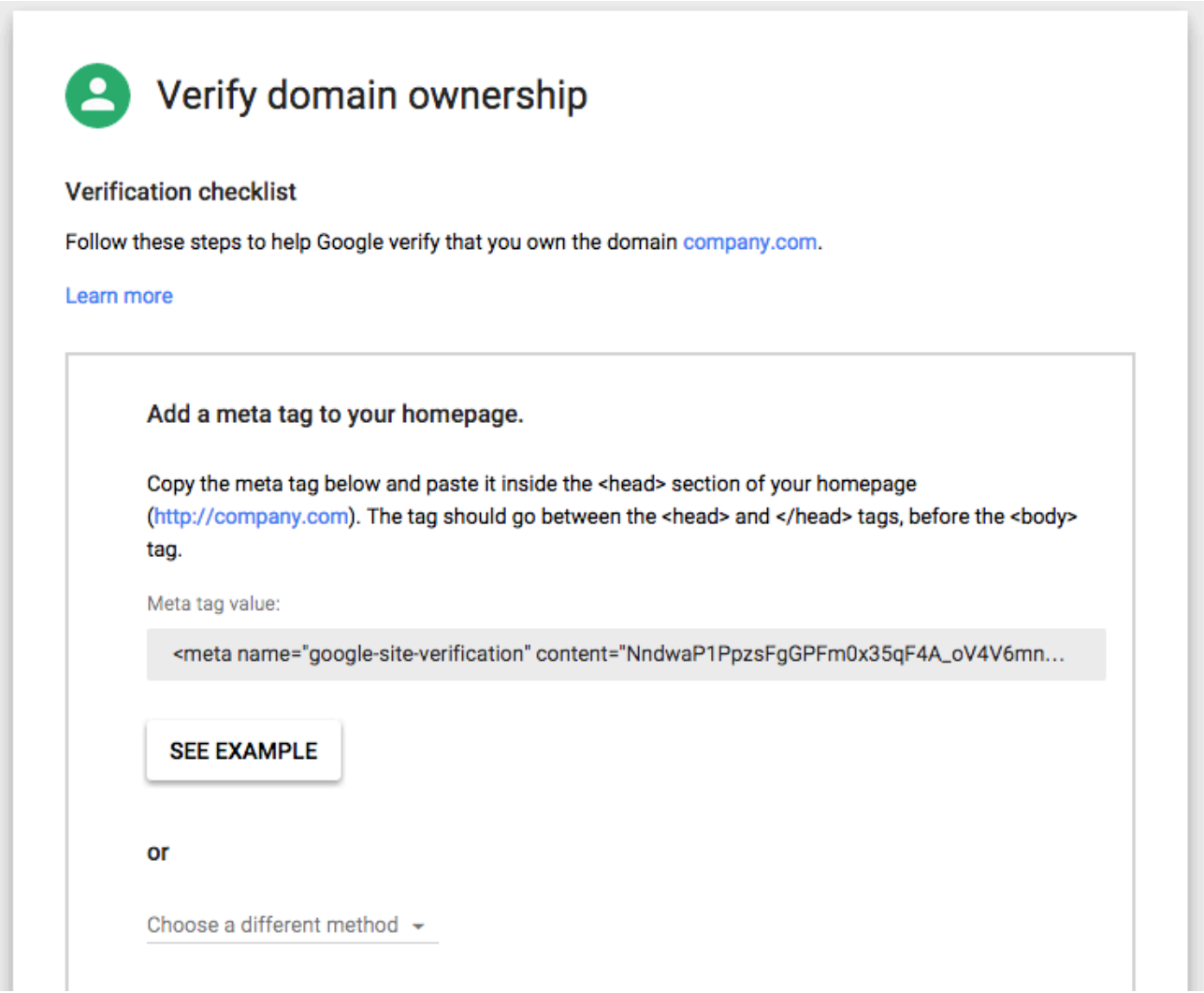
After the sign up is completed, you will be required to verify that you own the Domain Name provided. Click Start next to Verify domain ownership to star this process:



Android for Work Enablement

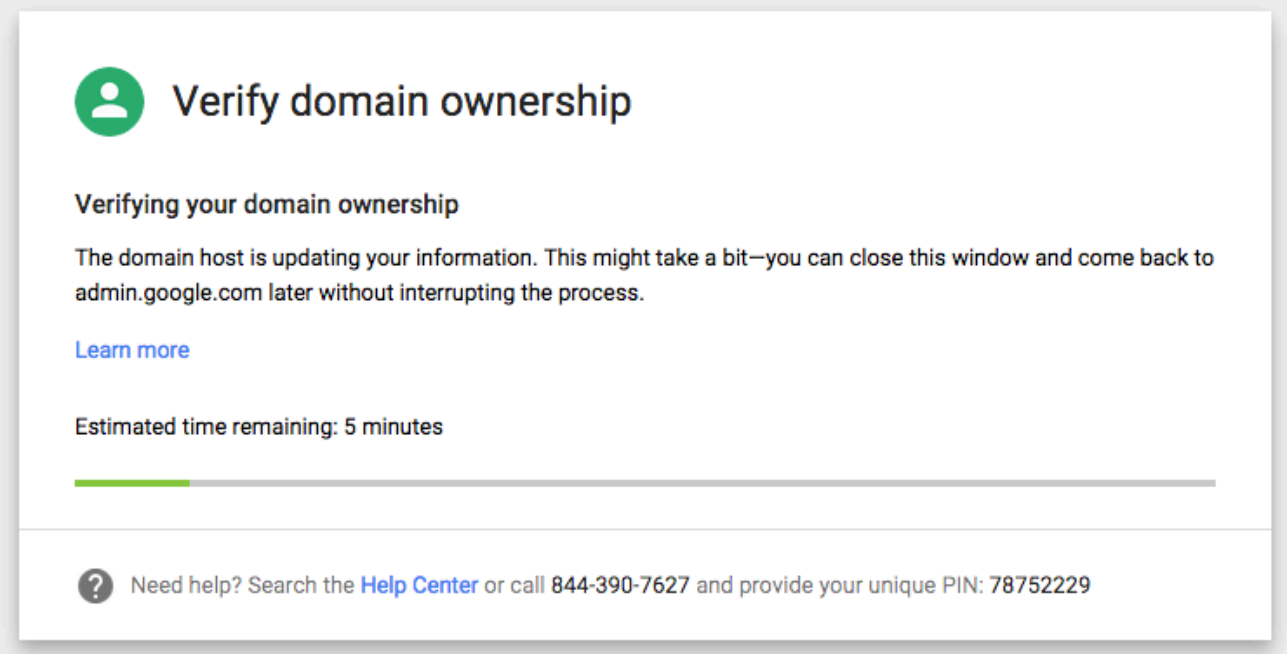
You will be required to verify your domain. This can be done in several ways and you should select the method that suits your needs. The domain can be verified by adding content to your home page or by altering your DNS settings by adding an entry that Google can verify. Select your verification method and follow the steps.

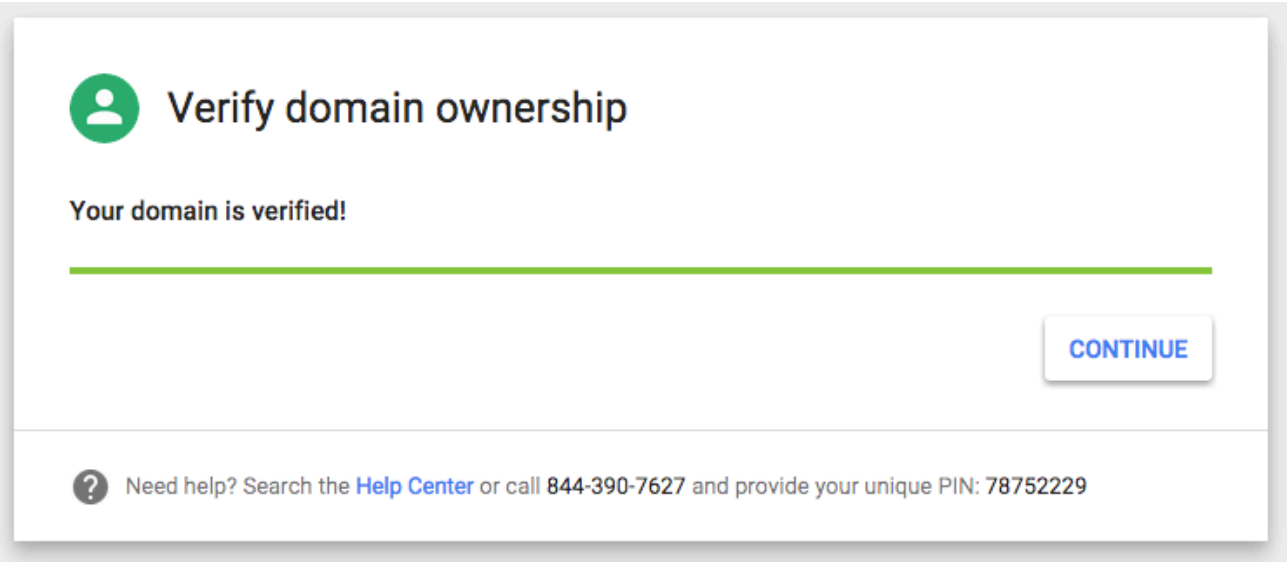
You can select “Choose a different method” if the method selected does not suit your needs:



Android for Work Enablement

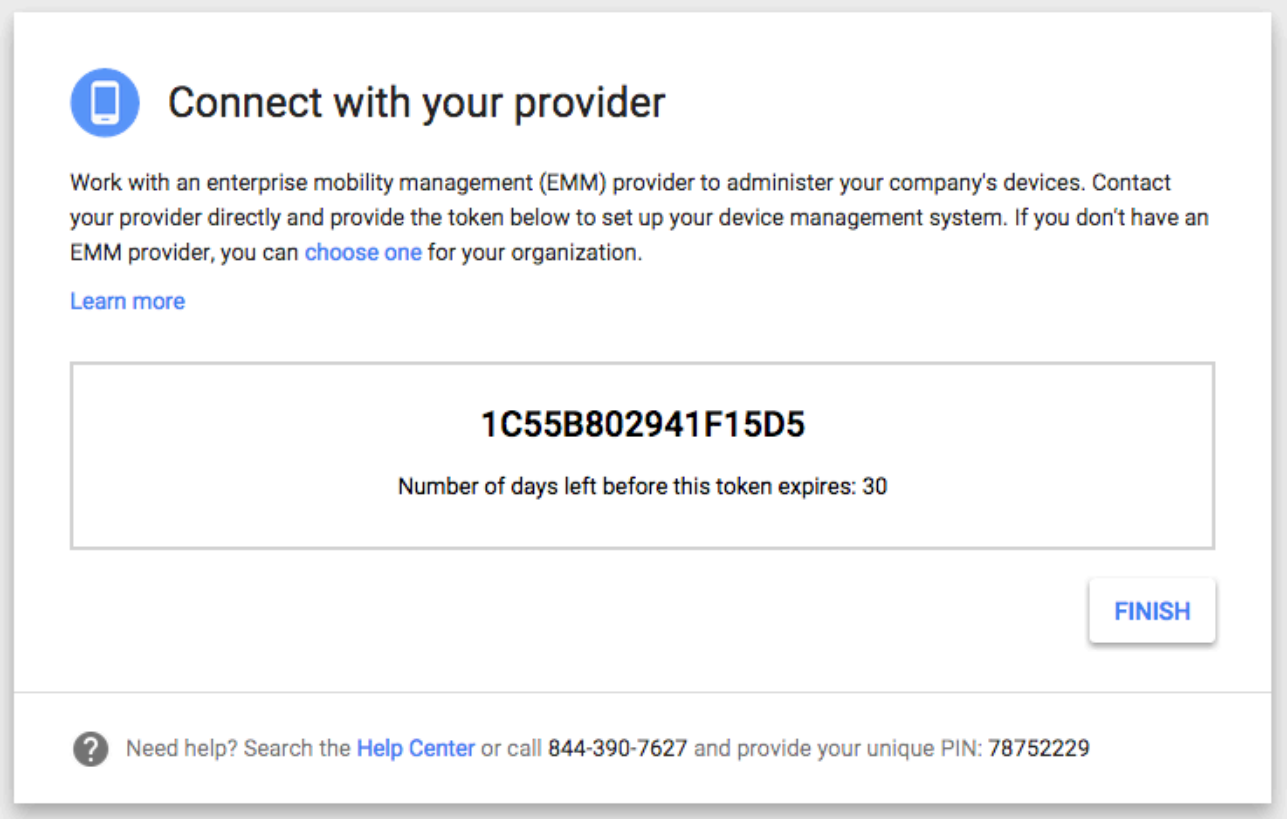
After choosing your verification method and activating, Google will attempt to verify your input. Wait for the process to change to verified to continue:





Android for Work Enablement

After being verified, you will be presented with an EMM token number which will expire in 30 days. You should copy this token so that it can be entered when configuring Silverback.



3. EMM Token for existing Google Managed Domain

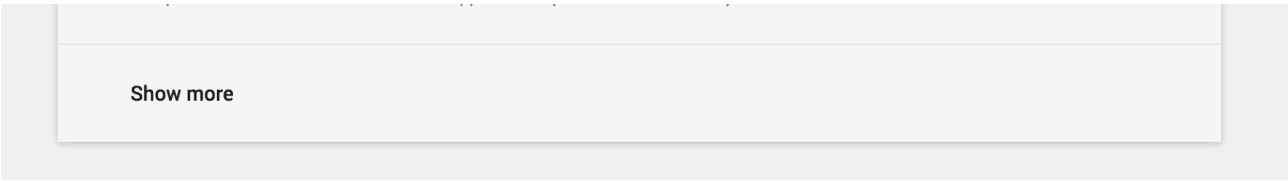
This section is not required if you acquired your EMM Token from the section above. This is only to be followed if you have a Google Apps Business account or have previously created your Google Managed Domain as above.

3.1. Generate a Token

1 Login to your Google Account Admin Page at: https://admin.google.com

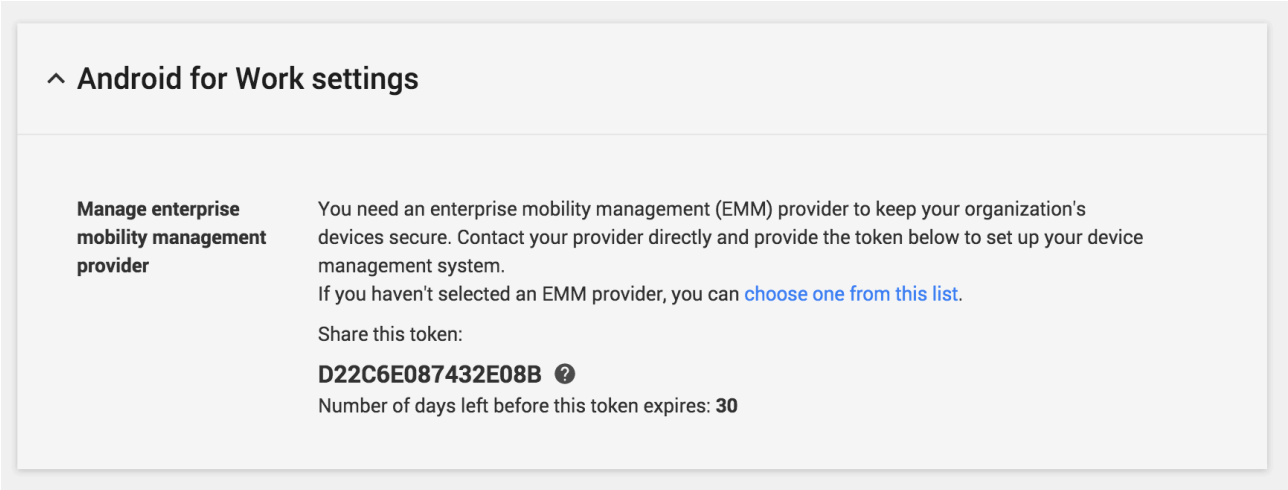
2 Click Security from the menu:

3 Click Show More:



Android for Work Enablement

4 Click Android for Work Settings:



5 Copy the Token value from this page and record it for later steps.

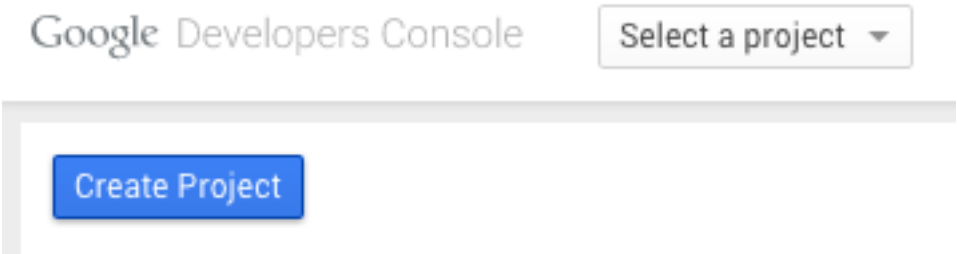
4. Creating the API Project

Silverback requires an API Project and associated service account to manage Android for Work settings for your Google Managed domain. This section is required whether you already have a Google Apps Business account, or you created a Google Managed Domain in the above step.

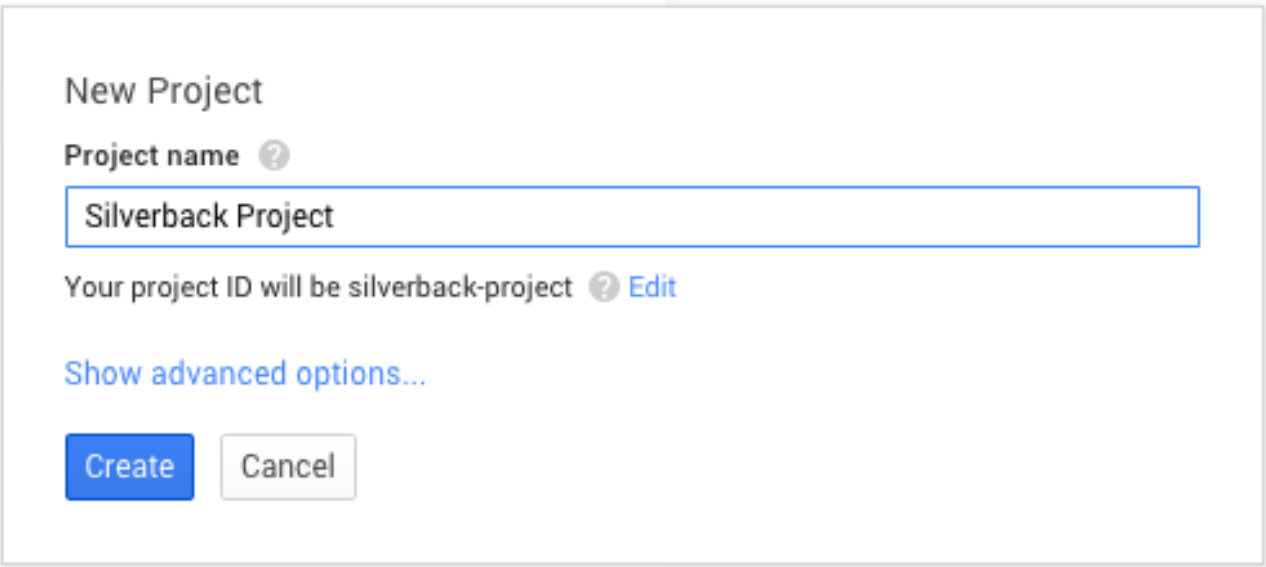
4.1. Enabling EMM API Functionality

6 Navigate to the URL: https://console.developers.google.com/project to create your project which Silverback will use to manage your Android for Work settings.

7 From this page, click Create Project:

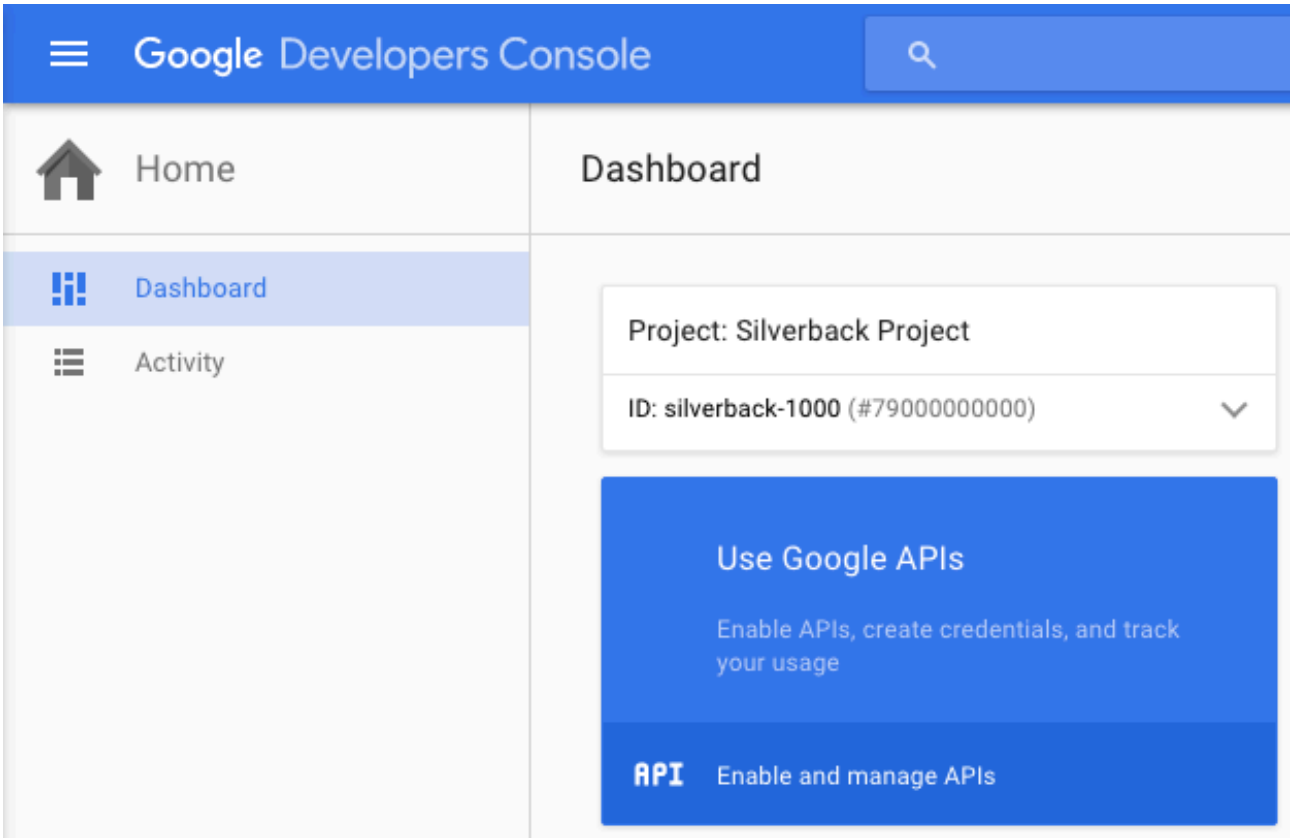


8 Enter a Project Name, the value entered is not critical, but as you may have multiple projects in future, it's recommended to name this project with a value that will be easily identifiable as your Android for Work deployment:

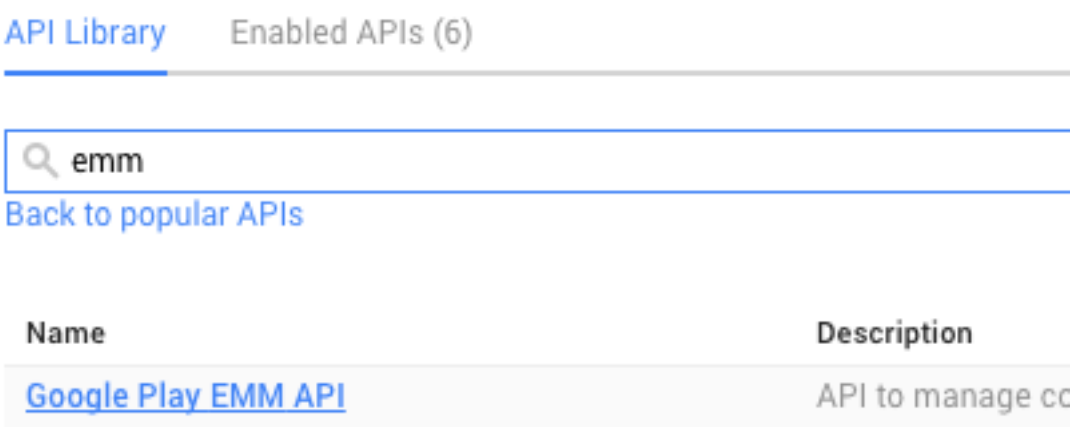


Android for Work Enablement

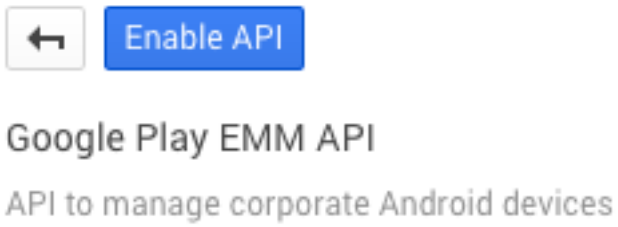
9 After the project is created, you will be taken to the project dashboard, Click on “Enable and manage APIs”.



10 To enable Android for Work Management for Silverback, Enter “EMM” in the API search field and when “Google Play EMM API” is visible, click it:

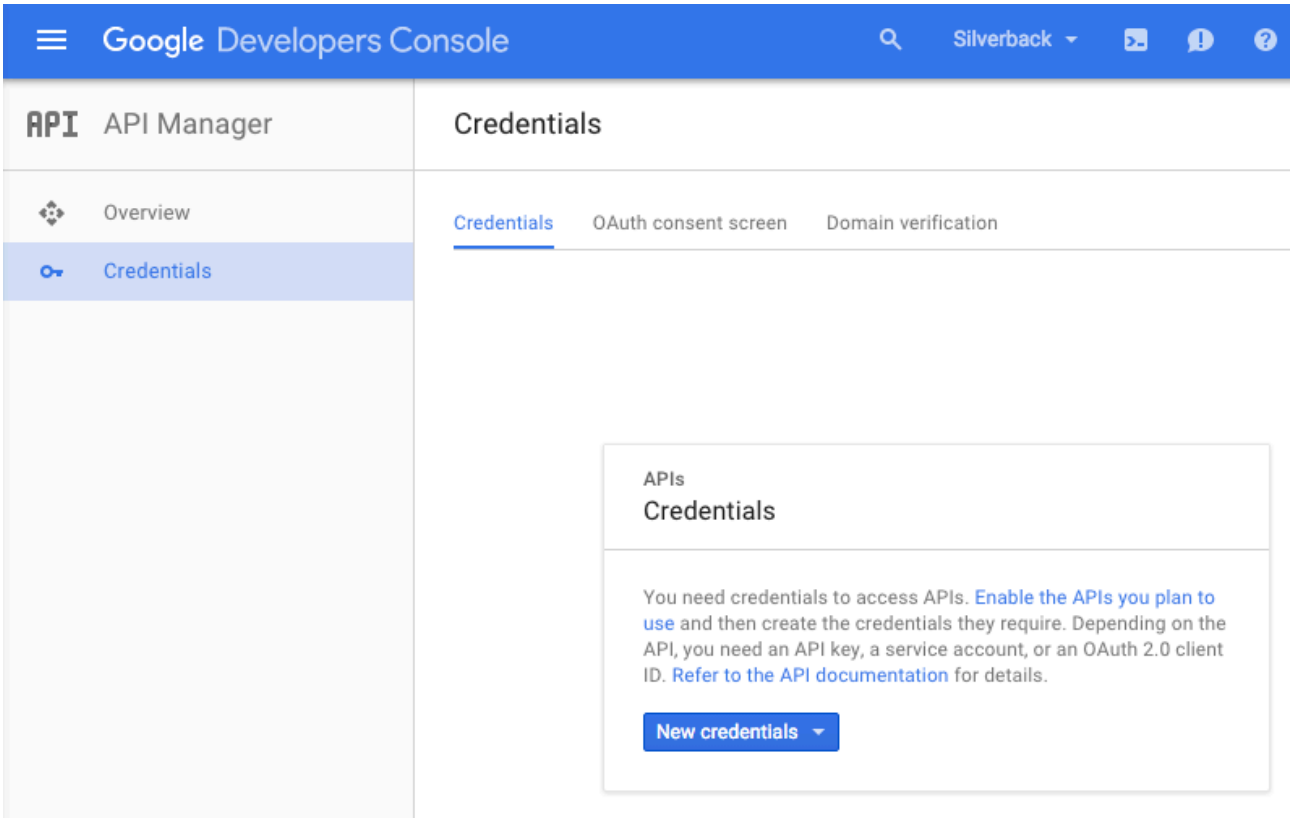


11 From the resulting screen, click “Enable API”:



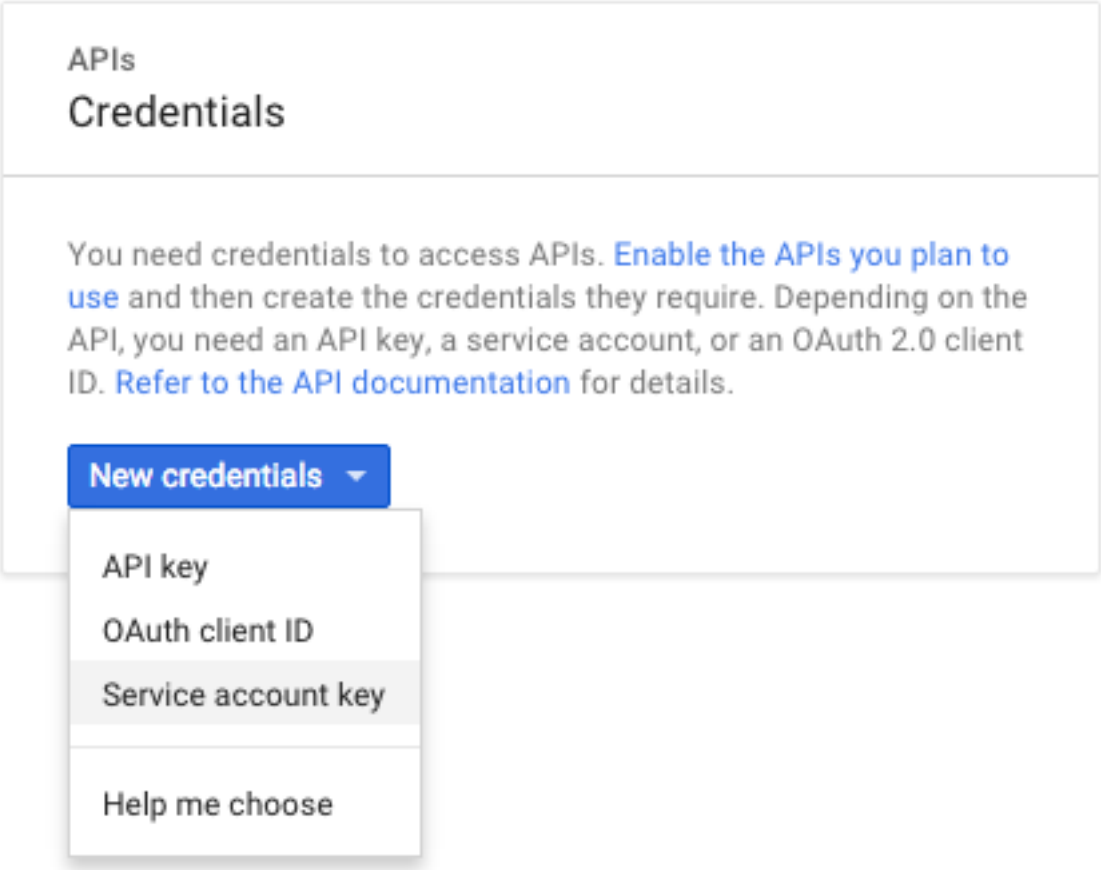
4.2. Create the Service Account Credentials

1 After enabling the API, a service account must be created so that Silverback can manage the settings for you. From the Developer Console in the step above, click on Credentials and then New credentials:



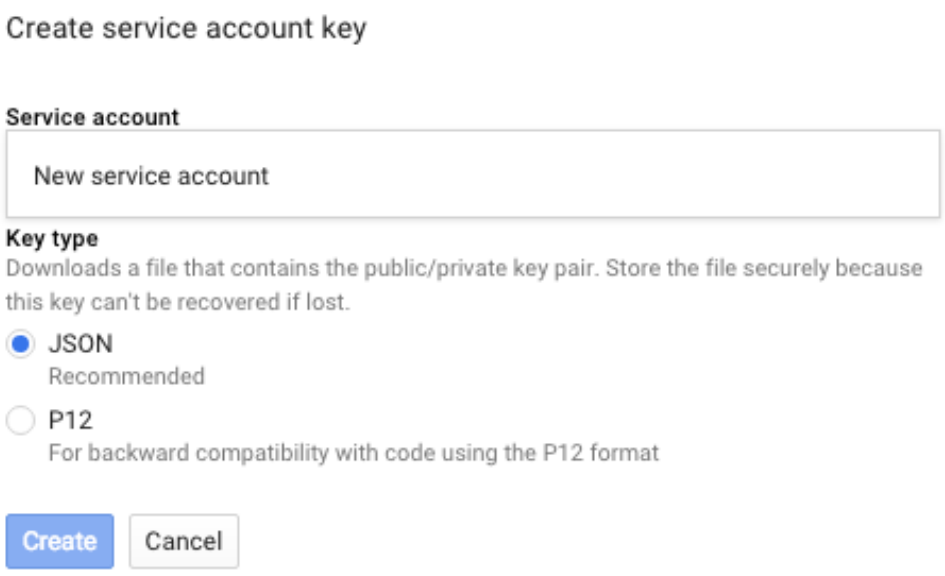
Android for Work Enablement

2 From the select list, choose Service account key:

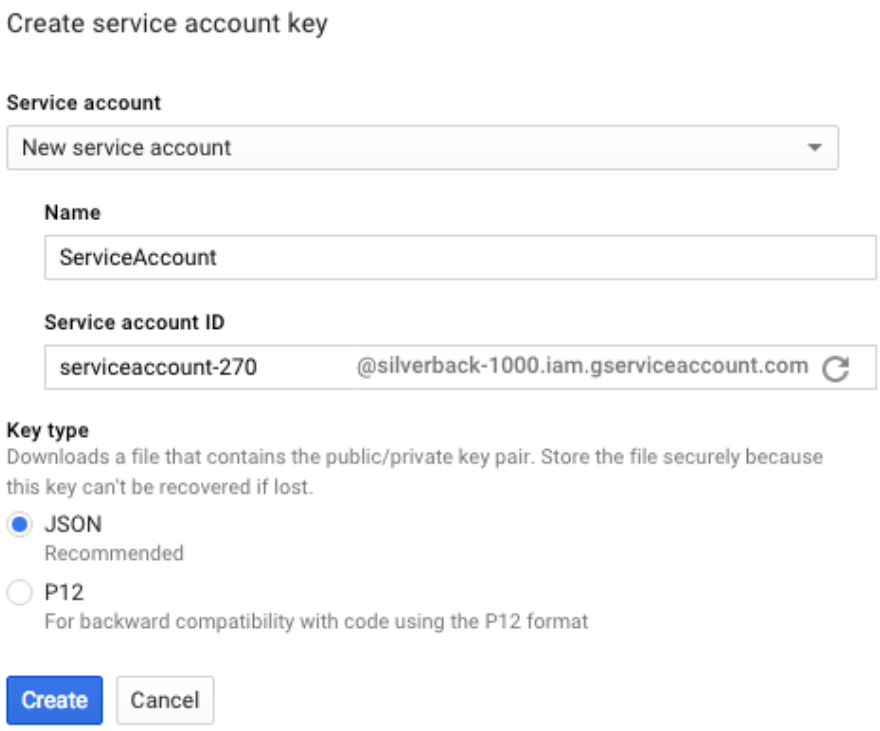


Android for Work Enablement

3 Click the Service account select list and click New service account:

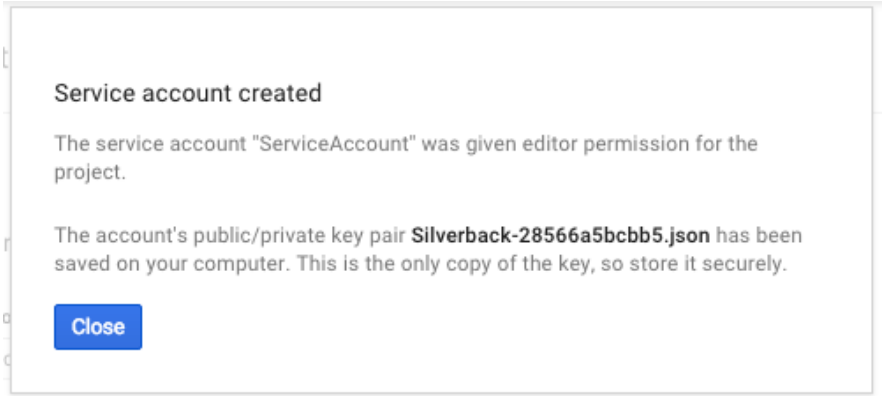


4 Enter a Service account name and then choose JSON and click create:



Android for Work Enablement

5 Confirm the prompt:



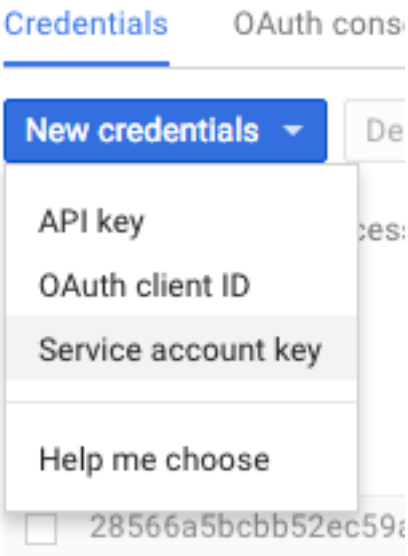
6 This will download a JSON formatted file, which will contain the Client ID and Email needed for future steps. Open the downloaded JSON payload, and copy the value for both client_id and client_email:

Silverback-28566a5bcbb5.json — Edited

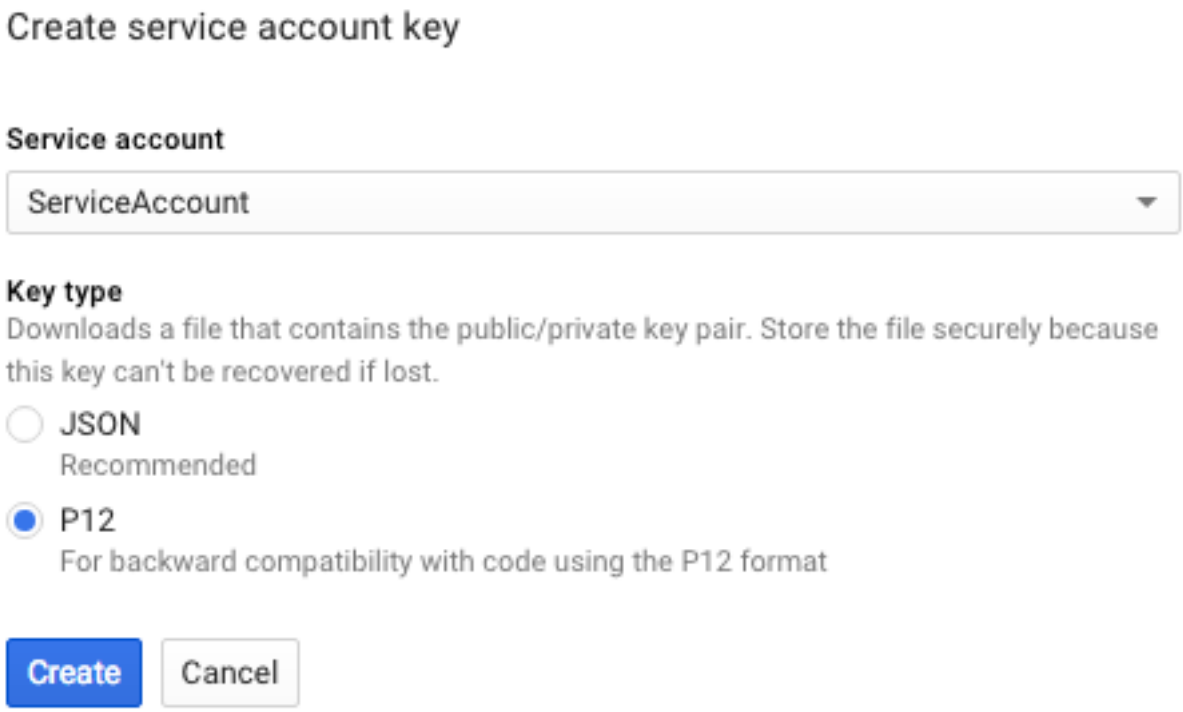

```
{
  "type": "service_account",
  "project_id": "silverback-1000",
  "private_key_id": "28566a5bcbb52ec59acb689002f0c8fc444322d8",
  "private_key": "-----BEGIN PRIVATE KEY-----
\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCyOtF9SopUUxP7\ngig6zxc4AK3cLvaL/
ObPWgUK1urlDNRxbseSs8go5i+JcNe1n30+ynZEr7Ik59Ms\nb9sqFba56unvO2oOyKZXS5vHBm7TF
+il9LUilEWNXOkNABrMfaDYpZnh+FHgFCij\nLGf8kmZkGjCuMwW1cwTCajtRJLyuI2fos8l2cR6gi9DO+Y
+iHERb059f/Gk00axR\nD9zkyyVf2++fmwVIvC++6UrtfCKylIWAJXMDMiMH361E7SqlsYMmlwTmL+8OyeDt
\niDWXMCouI9I1WCw0JKCkEawCRShO6wx21QEfD1nQzjfQRYNbFbQPJ/mbrEfmUvyZ
\nNCU5Iuy7AgMBAAECggEAL1SnZVpyOcqGN/hsrpFoXRrxENP37V0P/mithh9k6cbq
\nuSNaBzySzVIh6qYosyjjdF9tJzPlc/vaDtAoGBAMuChtyV0s1kgDMI7x8S
\nzFGRZzxMd2OuK6tWrgZXkAx6rO5yVVUVWUsq6nb86Qz7OpSH4TepT8kfGJJRlii8\nOt/
+ZgX1UOCITDaxYLOO+MIqq3LUWz9gvA/bKu9cBe1Rwyf71jlyvinTBOhRdgN0\n5w4j80t3o0ypV/yuaoxf/
MGi\n-----END PRIVATE KEY-----\n",
  "client_email": "serviceaccount-270@silverback-1000.iam.gserviceaccount.com",
  "client_id": "111195123249486749 66",
  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://accounts.google.com/o/oauth2/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/
serviceaccount-270%40silverback-1183.iam.gserviceaccount.com"
}
```

Android for Work Enablement

7 From the resulting screen, click “New credentials” and then “Service account key”:

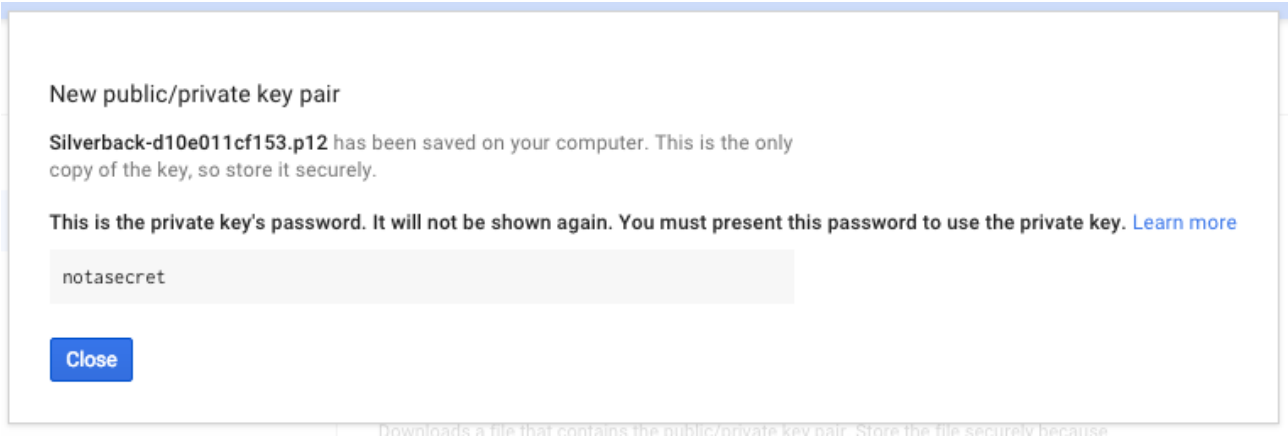


8 From the resulting screen, select the service account you created previously, and choose P12 as the Key type:

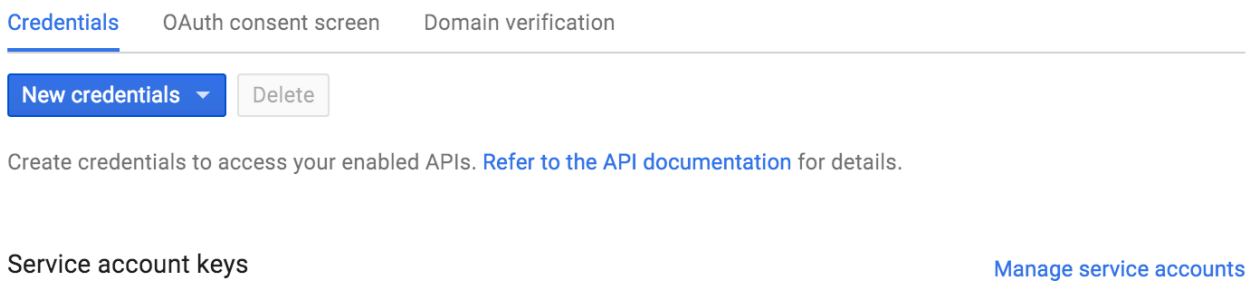


Android for Work Enablement

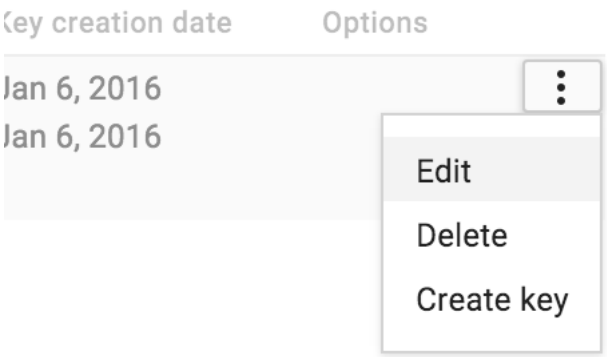
9 A certificate file will download; this file must be kept for later configuration. A password is generated with this file and should be noted so that it can be entered later:



10 From the resulting screen, click Manage Service Accounts:

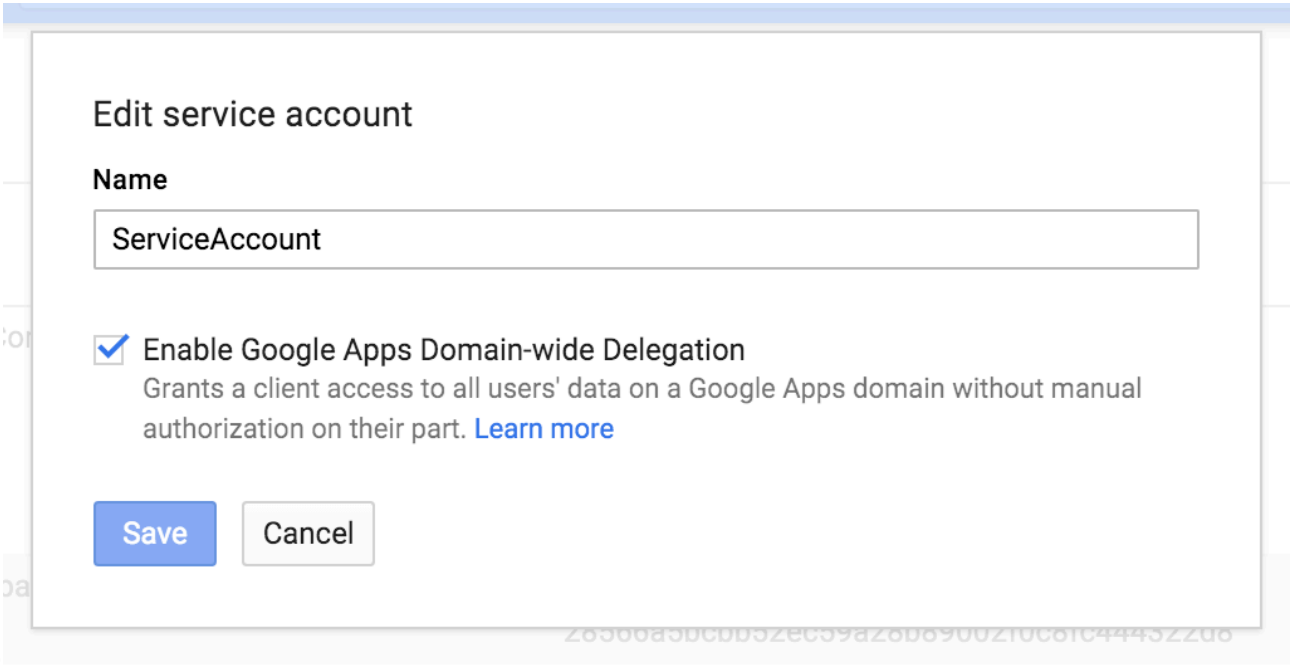


11 From the resulting screen, click the menu button for the service account, and click Edit:



Android for Work Enablement

12 Check the value to enable Google Apps Domain-Wide Delegation and click Save:



13

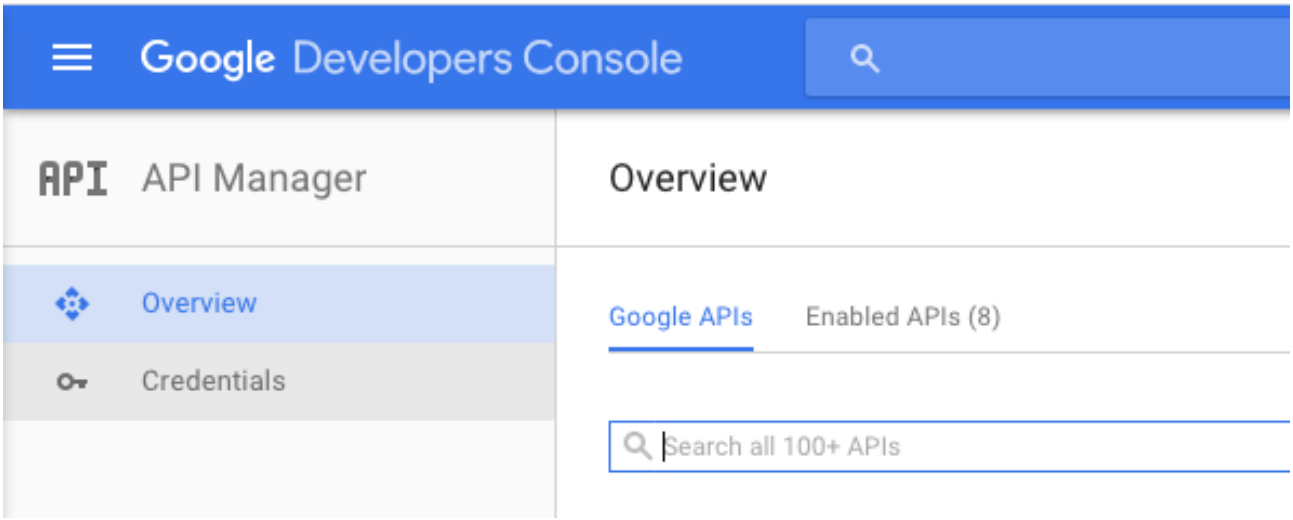
At the end of these Service Account steps you should have:

- Client ID for Service Account (from JSON Payload)
- Email Address for Service Account (from JSON Payload9)
- P12 Certificate File for Service Account and Associated Password

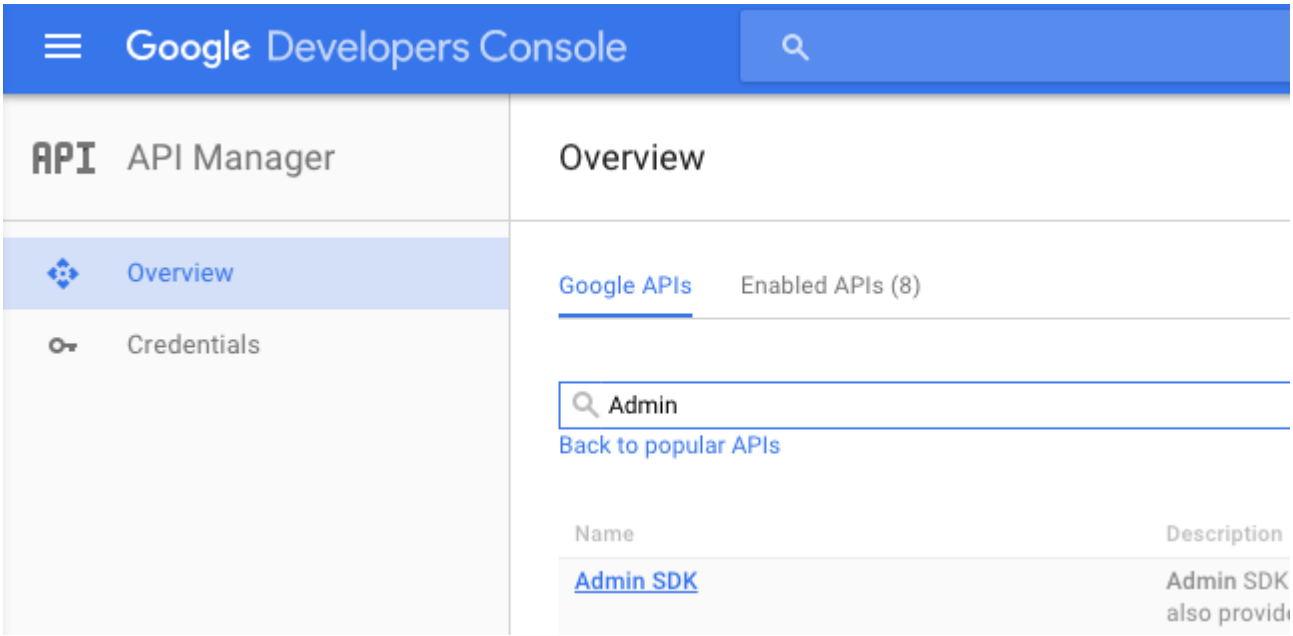
4.3. Enable Directory Management via Silverback

The following step is only required if you want Silverback to manage your Google Managed Domain users automatically. This is recommended if you do not already have a Google Apps Business account and therefor have no users in your account. This process enables Silverback to create and manage users for you automatically when they enrol.

1 To enable this API, from the developer console, click on Overview:

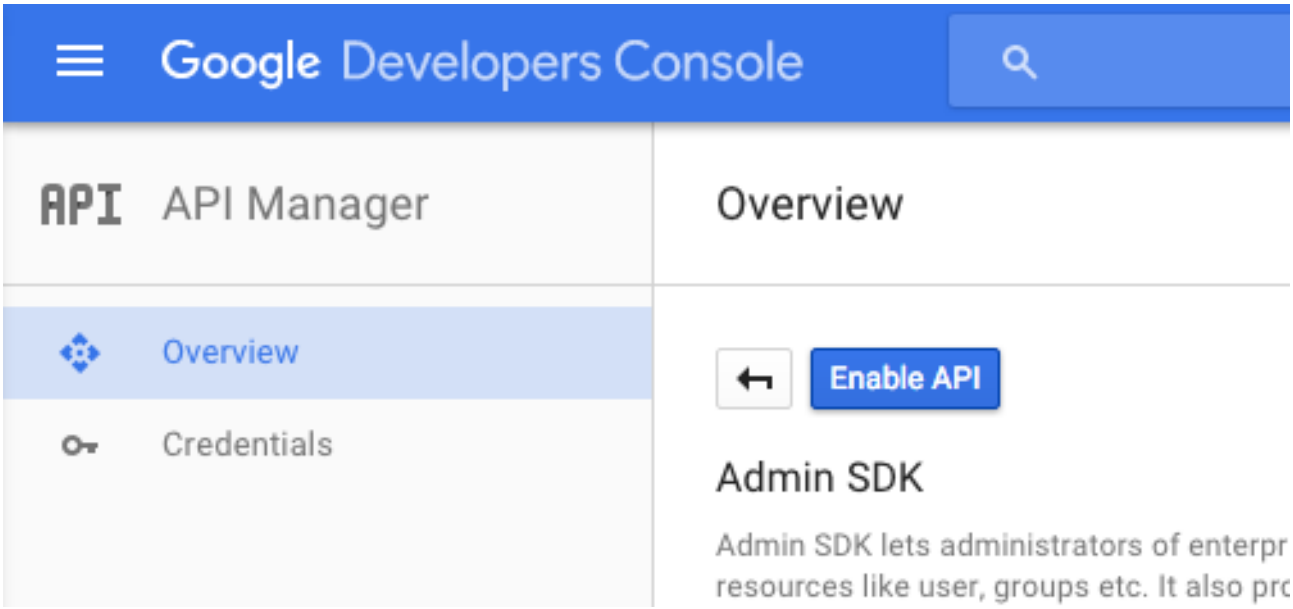


2 In the search box, enter “Admin” and click on “Admin SDK”:

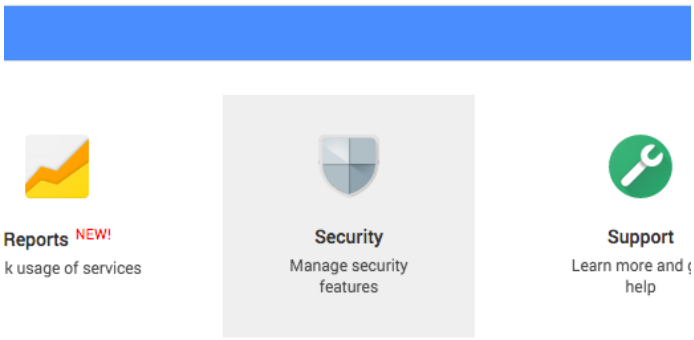


Android for Work Enablement

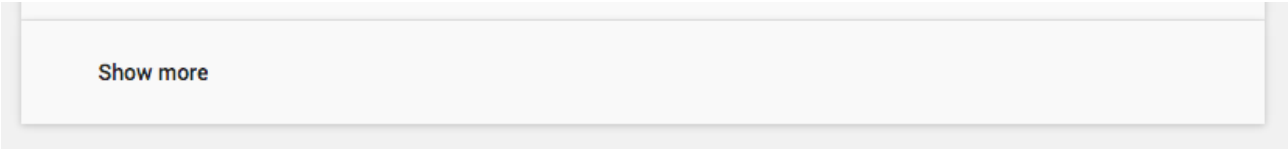
3 Click “Enable API” from the resulting screen:



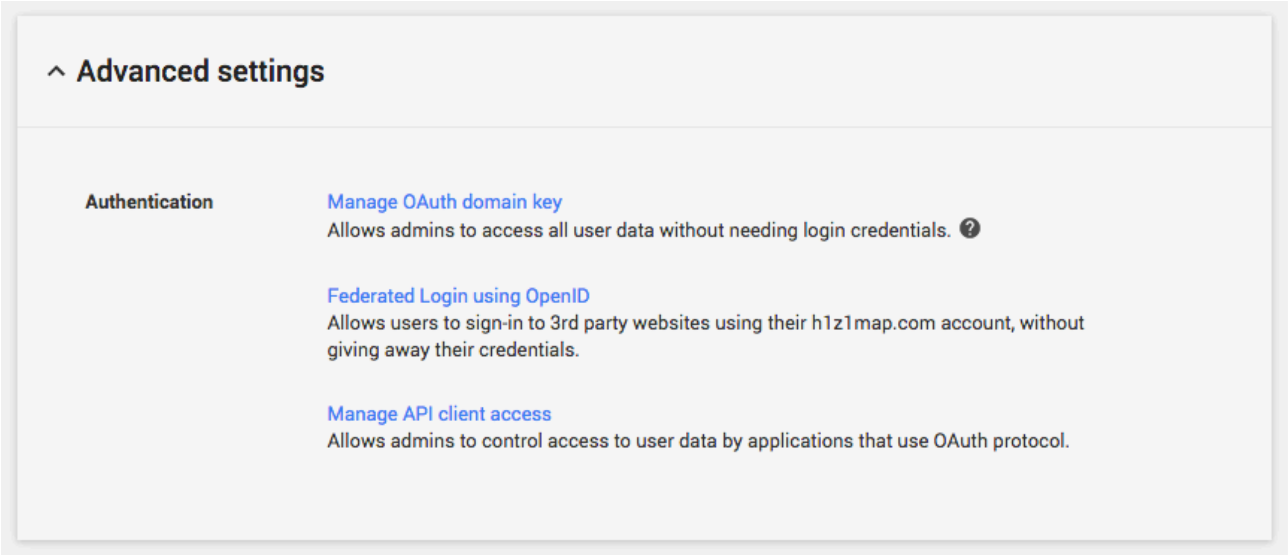
4 Navigate to the Google Apps Admin Page at https://admin.google.com/ and select “Security” from the main page:



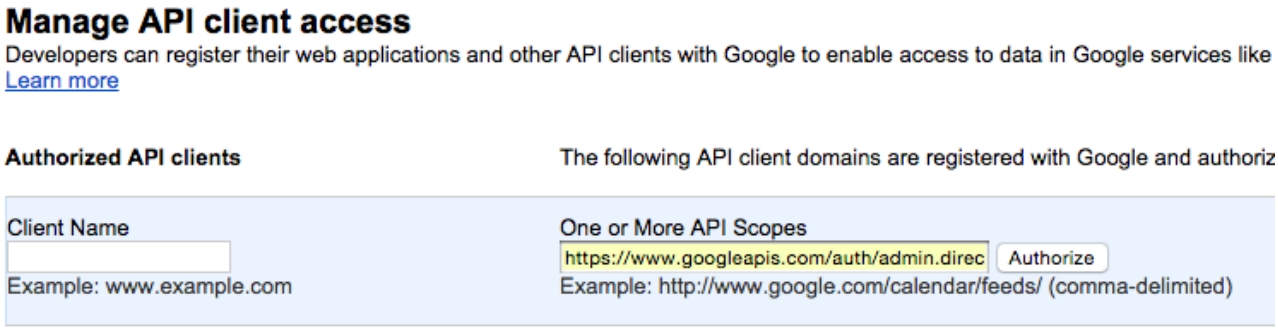
5 Click on “Show more”



6 Click on “Manage API client access”:



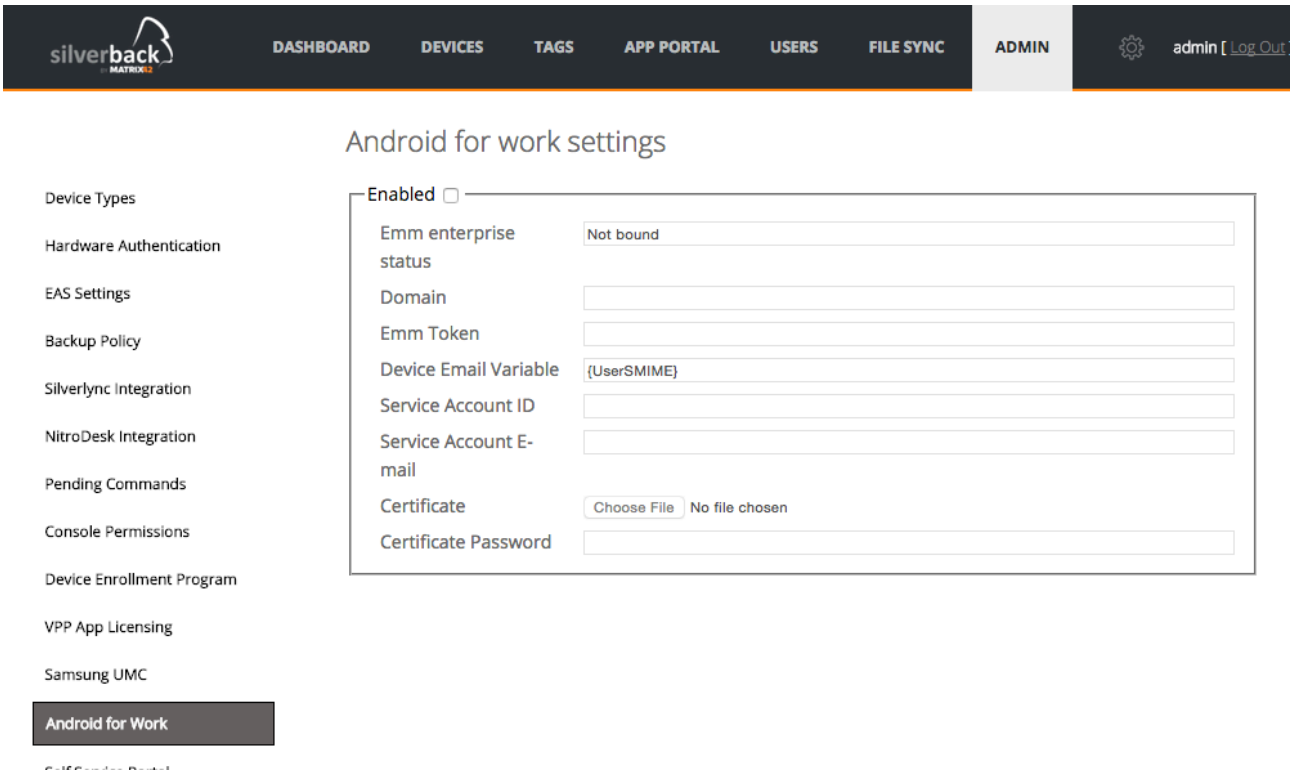
7 On the resulting page, enter the Client ID value previously recorded in the “Client Name” field, and enter https://www.googleapis.com/auth/admin.directory.user in the “One or More API Scopes” field, then click Authorize:



5. Pairing Silverback to the Managed Domain

5.1. Pairing Android for Work Management

1 To pair Silverback to your Google Managed Domain, login to the Silverback admin console. Click on the Admin Tag and the Android for Work section:

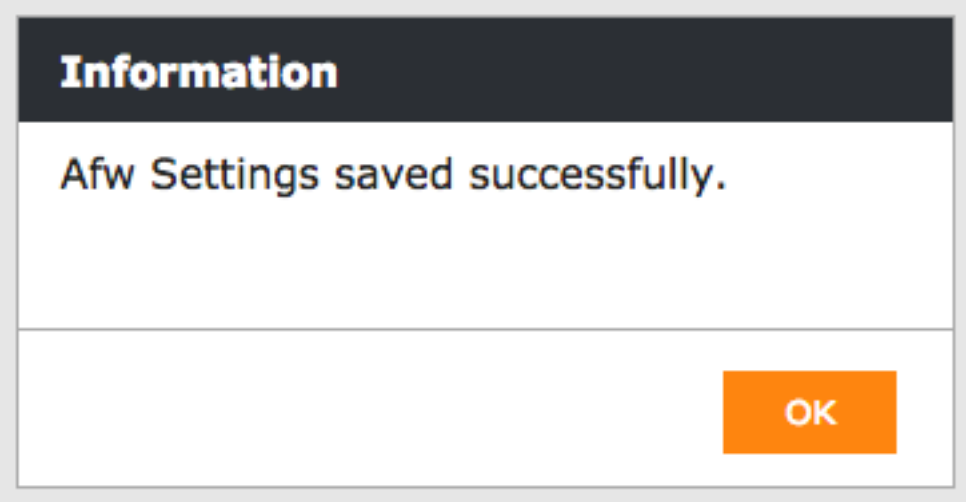


Android for Work Enablement

2 Tick “Enabled” to enable the form, and then enter the following information in the page:

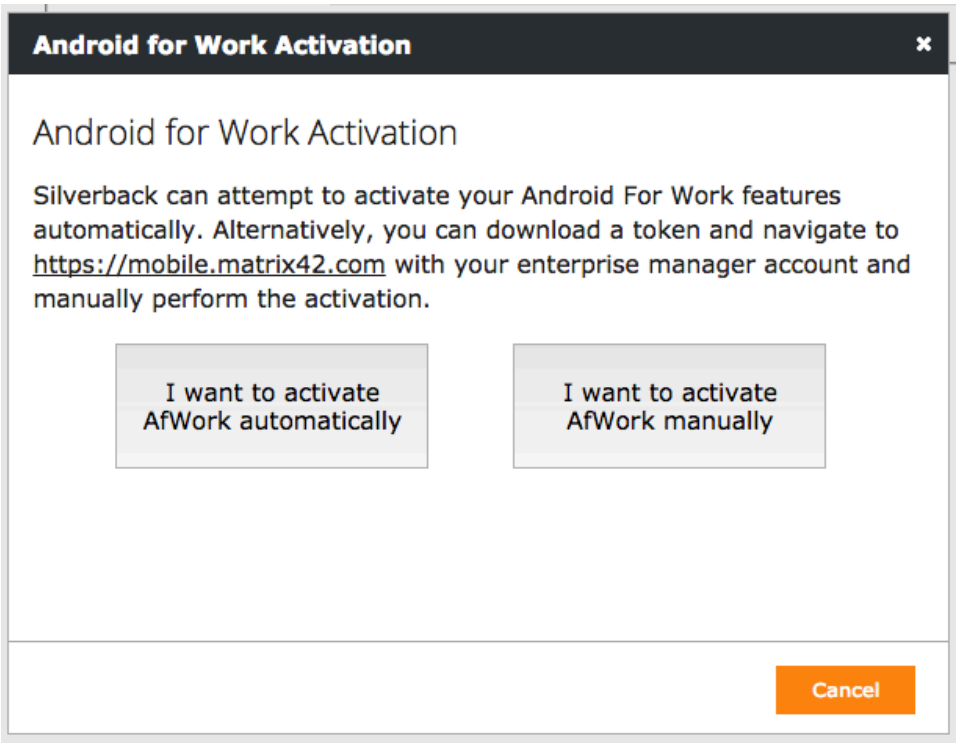
Setting	Value
Domain	The Domain name for the company, e.g. company.com, this must match the domain used for the sign up in the previous steps
EMM Token	This is the EMM Token presented to you on sign-up. If you need to see the token again, navigate to the Google Admin page, select Security and then Android for Work settings to view the token
Device email variable	The system variable used for user’s email addresses. This will be the value used when creating the user’s Google account. This can be any system variable, but it’s important to note that Silverback will automatically append the Domain value to the end. E.g. If “user01” is the Device Email Variable, then the user created will be user01@company.com”
Service Account ID	The Client ID value previously generated
Service Account E-mail	The Client Email address previously generated
Certificate	The P12 Certificate file downloaded when creating the Service Account previously
Certificate Password	The password on the P12 Certificate file. Google assigns this by default and displays the value to you.

3 After the information above is entered, click Save. If the settings validate correctly, the confirmation screen will show. Click OK:

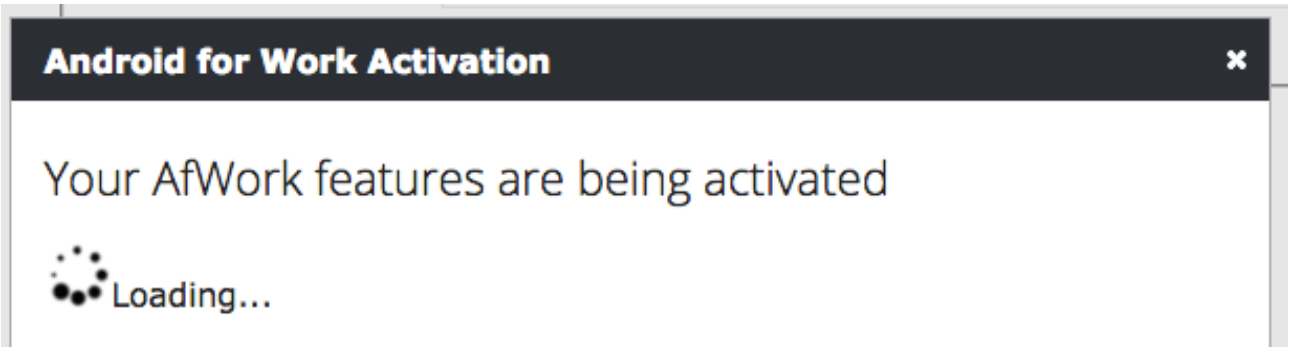


Android for Work Enablement

4 At this point, the settings are not yet activated, click Activate to begin this process and select “I want to activate AfWork Automatically”:



5 If prompted, enter your Matrix42.com account credentials to activate Android for Work. Silverback will indicate that Activation is in progress:



6 After this is completed, you will be returned to the main Android for Work settings page, and you can now optionally enable the Directory API if needed.

5.2. Pairing Directory API Management

If directory integration is needed, and enabled as part of the Enable Directory Management via Silverback section, you need to configure Directory API settings. The following table explains the settings and their purpose:

Note: The default password must be strong; however these requirements change from time to time. If you have issues creating users in Android for Work, try increasing the complexity of the password.

Setting	Description
Send User Password	Android for Work Directory API can pre-configure accounts with both username and password. Disabling this will prevent Silverback from sending a password on user creation.
Use User Password	When a user is created via the Directory API, Silverback will send a password to use for the account. This checkbox allows you to send the password the user used to create the enrolment via the SSP.
Default Password	If the user's password is not available, or the above setting is disabled, Silverback will use this default value. The value can be communicated to users to use for Android for Work activation.
Admin Email	When Silverback sends requests to the API, it will impersonate an admin on the Google Managed Domain. Authentication is handled by the service account, but it will use this email address as the user making these changes. This must be the email of a user with Administrator rights on the Google Managed Domain.

After enabling Directory API integration and populating the settings, save the changes to enable this.