

2021

StealthAUDIT®

AnyData_GoogleDrive_MyDrives User
Guide v1.0

Contents

Introduction	2
AnyData for Google Drive (My Drives).....	3
Prerequisites	3
Configuration	3
Creating a Service Account in the Google Developers Console	3
Delegating Authority to the Service Account in the Google Workspaces Admin Console	6
Enabling the APIs	8
Implementation	9
Extracting the Downloaded AnyData_GoogleDrive_MyDrives Job	9
Configuring the AnyData_GoogleDrive_MyDrives Job	10
Execution.....	13
View Results	13

Introduction

This document is designed to enable a user to install, configure, and execute AnyData_GoogleDrive_MyDrives in their environment. AnyData_GoogleDrive_MyDrives connects to a Google Workspace and scans files in user My Drives for sensitive data, including images using Optical Character Recognition (OCR). Scanning Shared Drives is not supported by this job.

AnyData then aggregates sensitive data scan results into a view within the StealthAUDIT Access Information Center (AIC), which will show the user, Drive, and folder hierarchy of the scanned Google Workspace, which files contain sensitive data, which sensitive data criteria were found, and, optionally, the specific sensitive strings of text that were found within each Google Drive.

NOTE: *In addition to downloading and scanning file formats that use extensions, this job can also scan the following Drive-native file formats: Google Doc, Google Sheet, Google Presentation, Google App Script, Google Drawing (with OCR enabled).*

NOTE: *My Drives for disabled accounts will not be scanned. To scan these My Drives, either enable all disabled accounts prior to running a scan or follow Google's recommendations for migrating files from a disabled account's My Drive to a Shared Drive (which can be scanned via the **AnyData for Google Drive (Shared Drives)** job).*

IMPORTANT: AnyData jobs do not support StealthAUDIT's job history functionality. For each AnyData job, ensure job history has been disabled (which will override global job history settings). Failure to disable job history for an AnyData job may result in data inaccuracies after multiple runs.

AnyData for Google Drive (My Drives)

This document describes the process for installing and configuring AnyData_GoogleDrive_MyDrives into an environment where the StealthAUDIT Management Platform and AIC are already installed and running.

Prerequisites

Prior to adding the AnyData_GoogleDrive_MyDrives job to your StealthAUDIT environment, confirm you have administrator rights on the StealthAUDIT server, as well as enough rights to download or copy files to the server.

You will need:

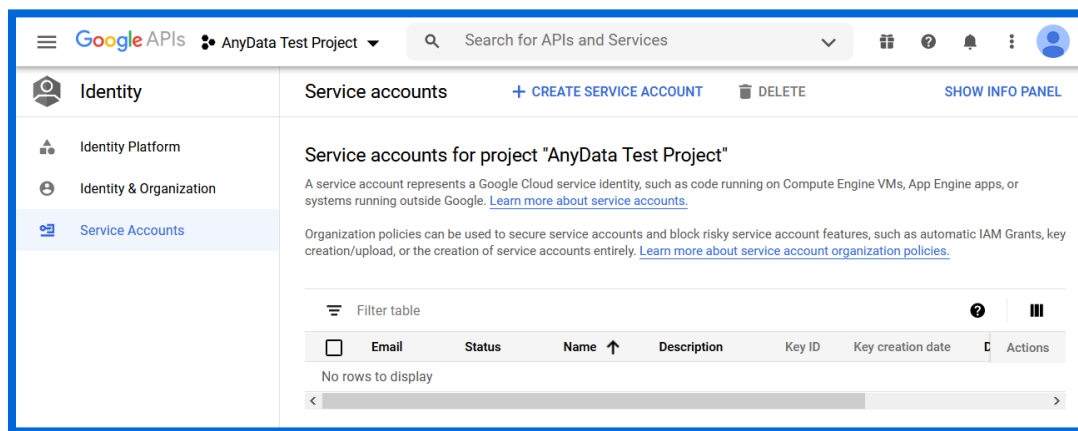
1. StealthAUDIT 11.5.0.127+
2. Access to Google Workspace, StealthAUDIT server, & SQL Server administrator accounts.
3. A Google API service account with enough permissions to download or copy files.
4. The P12 key file associated with the AnyData service account in your Google Workspace.

Should the Google API service account not exist or the P12 key file not be available, this guide will walk you through how to create both.

Configuration

Creating a Service Account in the Google Developers Console

Step 1 – Log-in to [Google Developers Console](#) with an account that has admin privileges in your Google Workspace, and navigate to **Identity > Service Accounts**.



Step 2 – Create a new project for this purpose or connect to an existing project where the new service account can be generated. Click **Create Service Account**.

Step 3 – Provide a name, ID, and a description for the service account being created, and click **Create**.

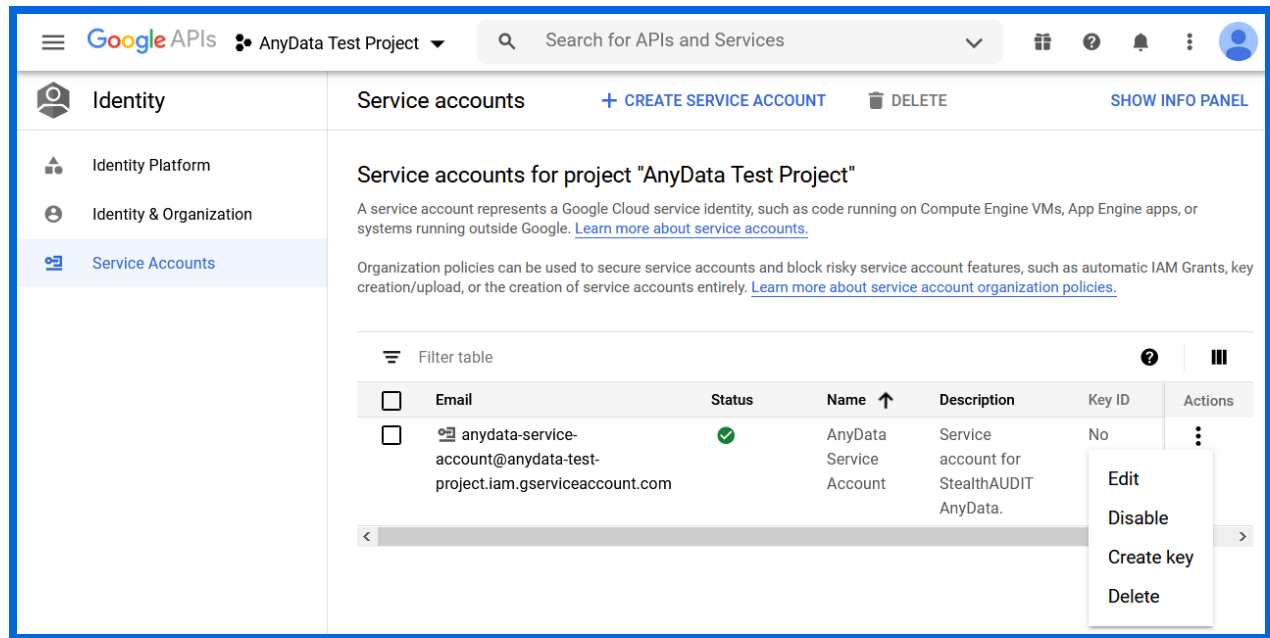
The screenshot shows the 'Create service account' wizard in the Google Cloud IAM console. The left sidebar shows the 'Identity' menu with 'Service Accounts' selected. The main content area is titled 'Create service account' and contains three steps:

- 1 Service account details**
 - Service account name:** AnyData Service Account
 - Service account ID:** anydata-service-account (with email @anydata-test-project.iam.gserviceacc)
 - Service account description:** Service account for StealthAUDIT AnyData.
 - CREATE** button
- 2 Grant this service account access to project (optional)**
- 3 Grant users access to this service account (optional)**

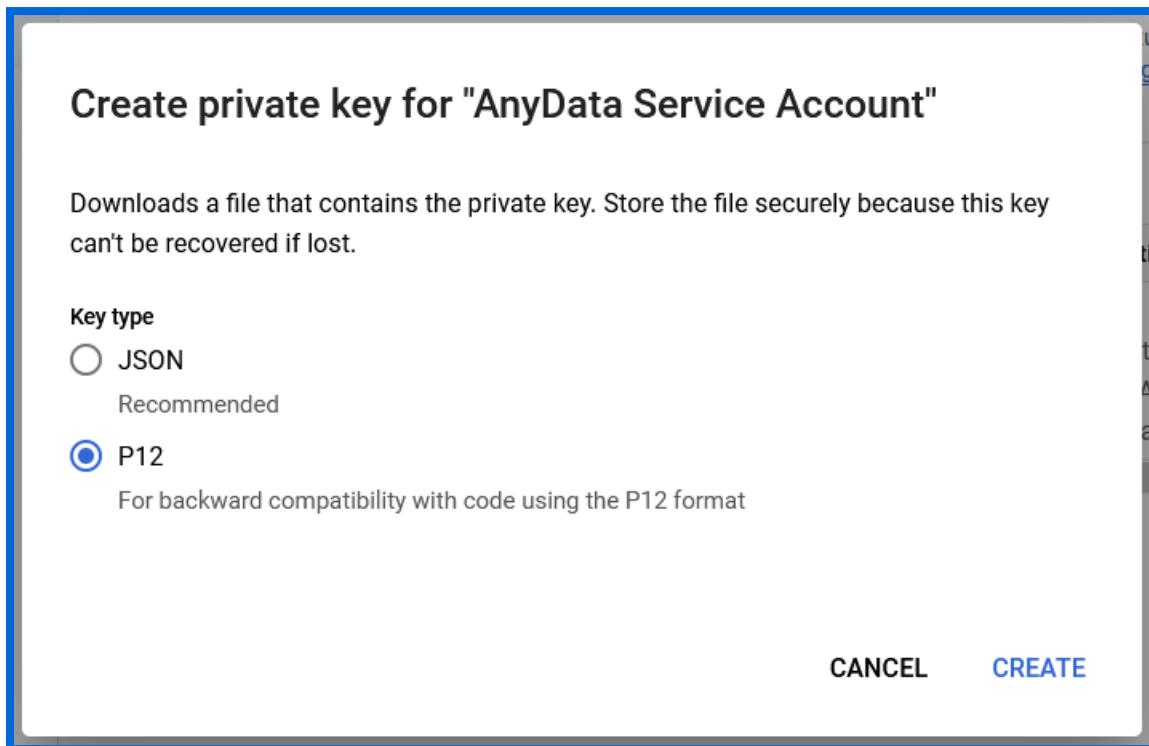
At the bottom, there are **DONE** and **CANCEL** buttons.

Step 4 – Continue through Grant this service account access to project without making any changes and click **Done** once in the Grant users access to this service account step, click **Done** without making any changes.

Step 5 – Back on the Service Accounts menu, click the vertical **ellipsis (:)** to the right of the new service account and click **Create Key**.



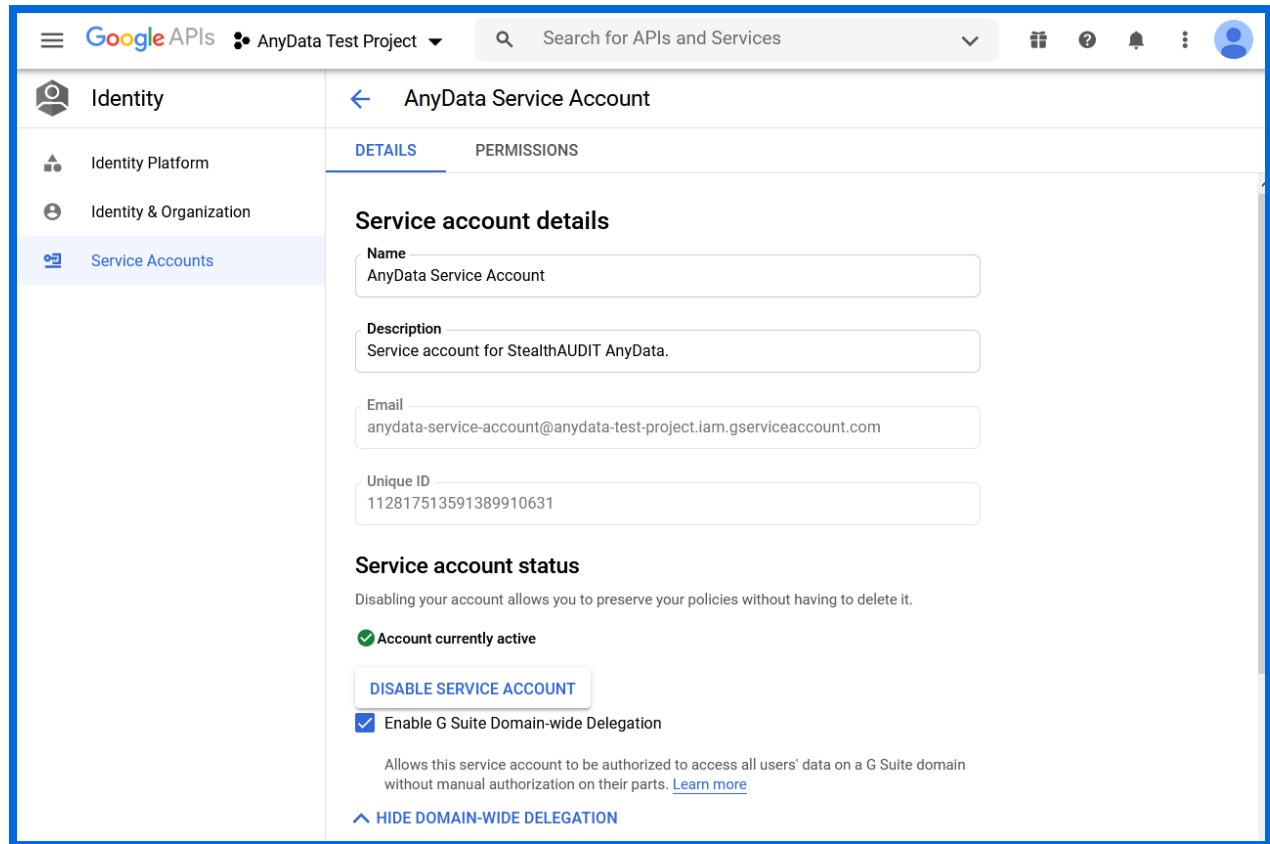
Step 6 – When prompted, choose **P12** and click **Create**. Save the file to a location you can access later and note the displayed Private Key Password.



Step 7 – Back in the Service Account menu, click the vertical **ellipsis** (:) to the right of the service account and click **Edit**. In the next screen expand the Domain-wide Delegation section and enable the **Enable G**

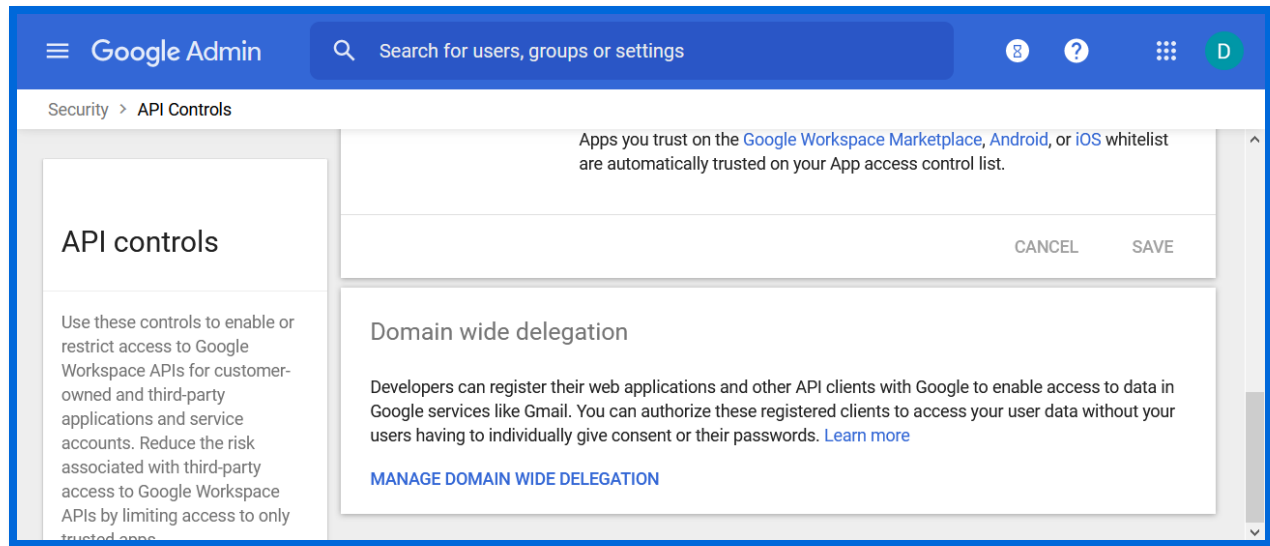
Suite Domain-wide Delegation. On the same page, locate **Service Account Details** and note the Email and Unique ID, both of which will be used later in this document. Click **Save** to return to the Service Account menu.

Remember to record the Unique ID and Email for the service account in **Step 7**.



Delegating Authority to the Service Account in the Google Workspaces Admin Console

Step 1 – Navigate to your Google Workspace’s [Admin Console](#) and log-in with an admin account. In the left sidebar, navigate to **Security > API Controls**. Locate and select **Manage Domain Wide Delegation**.



Step 2 – In Domain-wide Delegation, click **Add New**. Enter the Unique ID, from **Step 7** of the previous section in this document, in the Client ID field. Enable **Overwrite existing client ID**.

Add a new client ID

Client ID

112817513591389910631

☐ Overwrite existing client ID ?

OAuth scopes (comma-delimited)

ly, https://www.googleapis.com/auth/drive.metadata

×

OAuth scopes (comma-delimited)

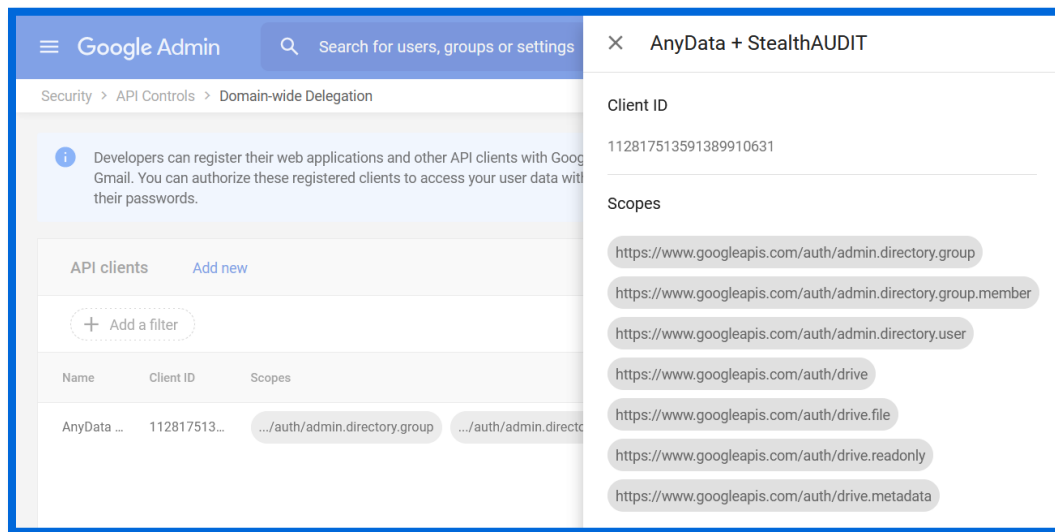
CANCEL

AUTHORIZE

In the “OAuth Scopes” field, you will enter a list of permissions (scopes) the service account will need to scan for sensitive data with AnyData. This comma separated list of scopes is as follows:

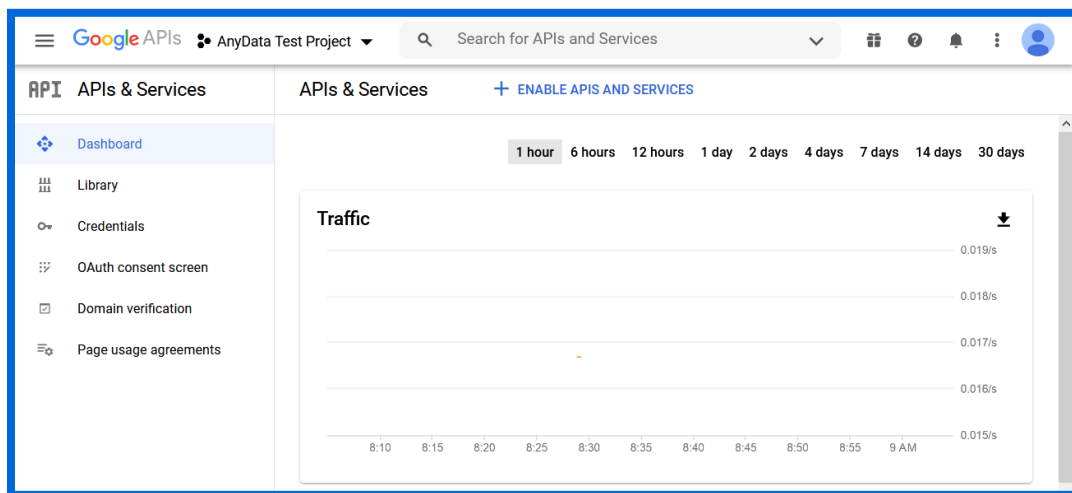

```
https://www.googleapis.com/auth/admin.directory.group,
https://www.googleapis.com/auth/admin.directory.group.member,
https://www.googleapis.com/auth/admin.directory.user,
https://www.googleapis.com/auth/drive,
https://www.googleapis.com/auth/drive.file,
https://www.googleapis.com/auth/drive.readonly,
https://www.googleapis.com/auth/drive.metadata
```

These scopes can be entered in a single field in this menu if they're comma-separated like above. Click **Authorize** to finish adding the permissions (scopes).

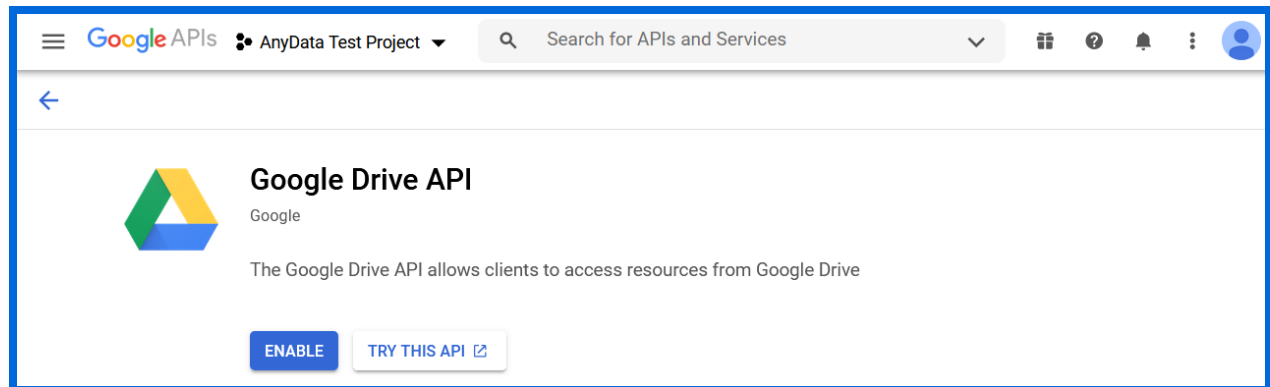


Enabling the APIs

Step 1 – Go back to the [Google Developers Console](#), and navigate to APIs & Services in the left sidebar. Click **Enable APIs and Services**.



Step 2 – You will now be in the API Library. Search for **Admin SDK API**, click on that link, and click **Enable** for the Admin SDK API. Repeat this process for the Google Drive API.

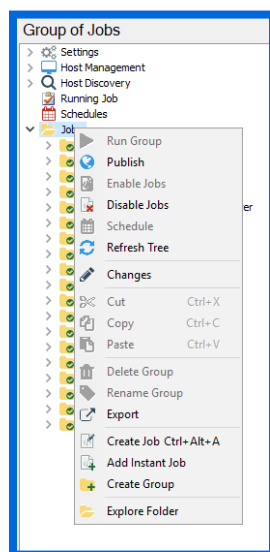


Implementation

This section will walk through how to extract the package downloaded from the Stealthbits website, how to import the AnyData_GoogleDrive_MyDrives job to StealthAUDIT, and how to configure and run the job to scan for sensitive data in Google Drive.

Extracting the Downloaded AnyData_GoogleDrive_MyDrives Job

Step 1 – Create a new Group in the StealthAUDIT job hierarchy by right-clicking **Jobs** and clicking **Create Group**. Name the group however you chose, for example: AnyData for Google Drive



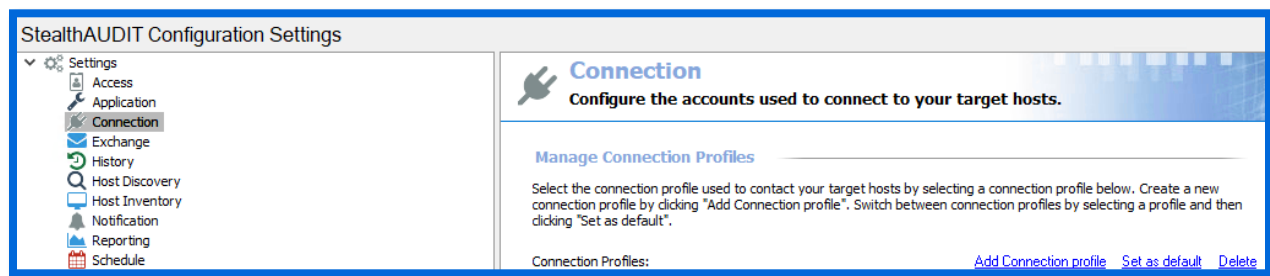
Step 2 – Right-click on the new Group and click **Explore Folder**. The directory that opens is where the AnyData_GoogleDrive_MyDrives job that has been downloaded will be placed. Extract the job to this location.

Step 3 – Right-click on the new Group and click **Refresh Tree**. The AnyData_GoogleDrive_MyDrives job should now be visible within this Group in StealthAUDIT.

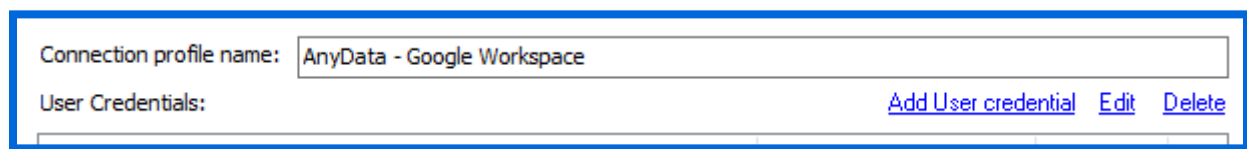
Configuring the AnyData_GoogleDrive_MyDrives Job

Now that the downloaded job has been imported to StealthAUDIT, we can configure it to scan for sensitive data in Google Drive.

Step 1 – Add a new set of credentials by navigating in the StealthAUDIT hierarchy to **Settings > Connection**. Click **Add Connection Profile**.



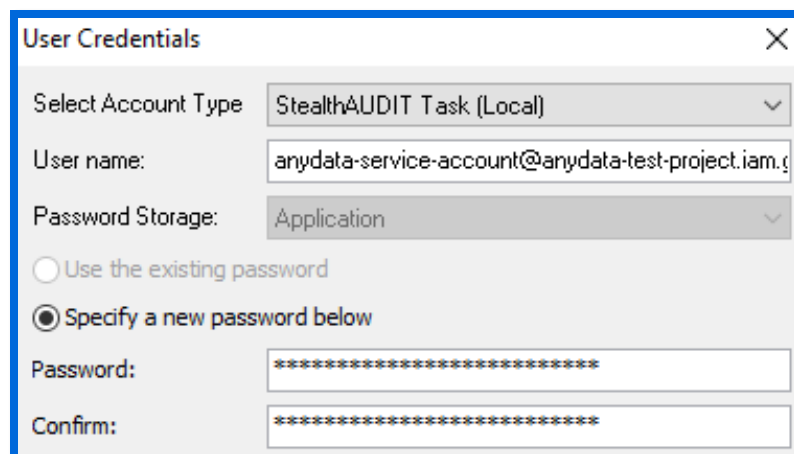
Step 2 – Name the profile however you chose, for example AnyData – Google Workspace. Click **Add User Credential**.



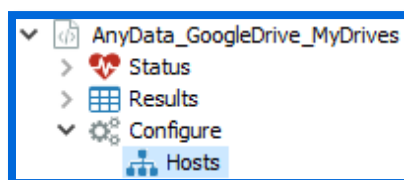
Step 3 – For this first credential's Account Type, select **Active Directory Account**. The User Name and Password should be for a user with the ability to authenticate to the SQL Server database used by StealthAUDIT. Click **OK** when finished.

IMPORTANT: It's important for the **Active Directory Account** to be the first credential in the list for this Connection Profile. If it's not, use the **Move Up** button to adjust this credential's position.

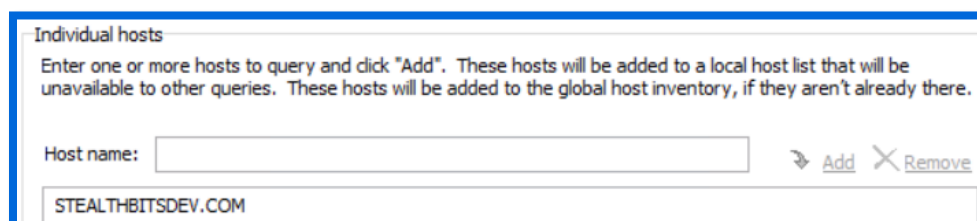
Step 4 – Click **Add User Credential** again. For this credential's Account Type, select **StealthAUDIT Task (Local)**. The User Name is the previously recorded Service Account email. The Password is the email address of an admin account for the Google Workspace. Click **OK** when finished, then click **Save**.

A screenshot of the 'User Credentials' dialog box. It has a title bar with a close button. Inside, there's a 'Select Account Type' dropdown menu set to 'StealthAUDIT Task (Local)'. Below it is a 'User name:' text box containing 'anydata-service-account@anydata-test-project.iam.g'. Then a 'Password Storage:' dropdown menu set to 'Application'. There are two radio buttons: 'Use the existing password' (unselected) and 'Specify a new password below' (selected). Below the radio buttons are two text boxes for 'Password:' and 'Confirm:', both filled with asterisks.

Step 5 – Navigate back to the AnyData_GoogleDrive_MyDrives job and navigate to the job's via **<Job Name> > Configure > Hosts**.



In the Hosts menu, locate the Individual Hosts section, use the name of your Google Workspace for the Host Name, and click **Add** then **Save**. Typically, this is the domain name and top-level domain that come after the “@” in your Google Workspace login. For example, “stealthbitsdev.com” in the case of the user “bskelly@stealthbitsdev.com”.

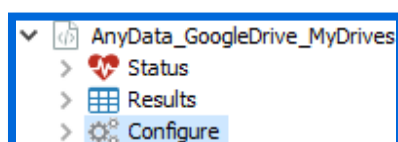
A screenshot of the 'Individual hosts' section. It has a title 'Individual hosts' and a paragraph of instructions: 'Enter one or more hosts to query and click "Add". These hosts will be added to a local host list that will be unavailable to other queries. These hosts will be added to the global host inventory, if they aren't already there.' Below this is a 'Host name:' text box. To its right are 'Add' and 'Remove' buttons. Below the text box, the domain 'STEALTHBITSDEV.COM' is entered.

Step 6 – In the StealthAUDIT job hierarchy, right-click on the AnyData_GoogleDrive_MyDrives job and click **Explore Folder**. In the directory that opens, paste the **P12 key** from the earlier configuration steps. Rename the key to **Certificate.p12**.

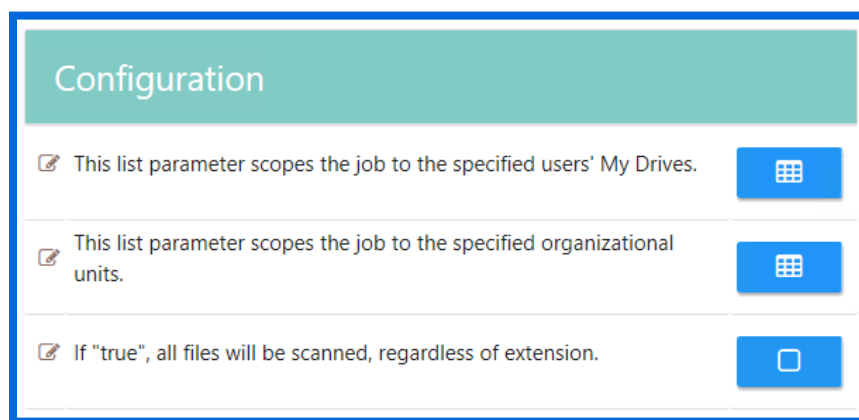
Step 7 – The following parameters can also be configured for the job:

Organizational Unit Scoping	<p>This list parameter scopes the job to the specified organizational units.</p> <p>For example, an OU named "My OU Child" nested within "My OU Parent" would be scoped to using the following path:</p> <p>/My OU Parent/My OU Child</p>
Scan All File Types	If "true", all files will be scanned, regardless of extension.
User Email Scoping	This list parameter scopes the job to the specified users' My Drives

To configure the parameters above, navigate to the job's node in the job tree.

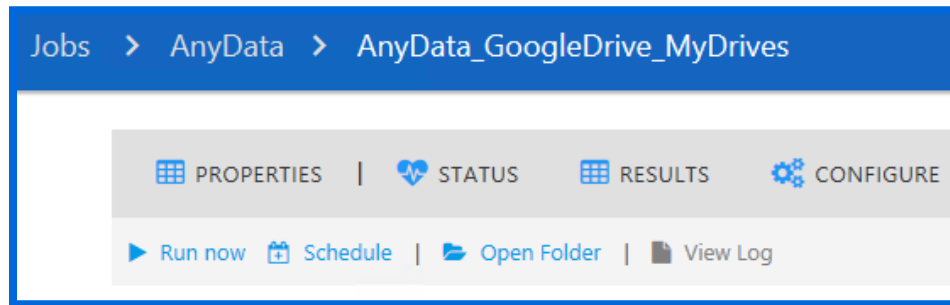


The parameters will be displayed along with other job information and can be modified in the **Configuration** section.



Execution

To execute the job, highlight the AnyData_GoogleDrive_MyDrives job in the StealthAUDIT job hierarchy, and click **Run Now** below the breadcrumb trail and other job configuration options.

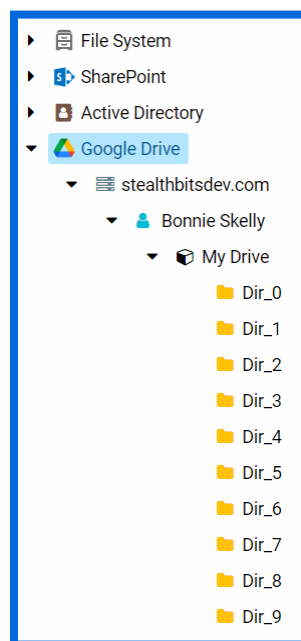


View Results

Sensitive data scan results from the AnyData_GoogleDrive_MyDrives job will be output to the Access Information Center (AIC).

Step 1 – Launch the AIC by double-clicking its icon on the StealthAUDIT server’s desktop or by navigating to its URL. Log-in as required.

Step 2 – Click on **Resource Audit** and navigate to Google Drive in the left sidebar. Expand the node, and nodes below it, to view details.



Information is broken down in a hierarchical view by **Google Drive > Organization (Google Workspace) > User > Drive > Folders**. Clicking on a scope allows you to select Sensitive Data reports in the AIC's right sidebar, which shows sensitive data found at the selected hierarchical level and below.

The screenshot displays the 'Resource Audit' interface. On the left, a tree view shows the hierarchy: File System > SharePoint > Active Directory > Google Drive > stealthbitsdev.com > Bonnie Skelly > My Drive > Dir_0. The main table lists sensitive data findings with columns: Criteria Name, Criteria Type, Path, and Count. The table shows five entries, all of type 'Pattern', located within the 'My Drive/Dir_0' folder. The right sidebar contains a 'REPORTS' section with 'Sensitive Content' selected, and a 'GROUP MEMBERSHIP' section.

Criteria Name	Criteria Type	Path	Count
US Drivers License	Pattern	Bonnie Skelly/My Drive/Dir_0/39411.txt	1
US Drivers License	Pattern	Bonnie Skelly/My Drive/Dir_0/92263.txt	1
US SSN	Pattern	Bonnie Skelly/My Drive/Dir_0/2383.txt	1
US SSN	Pattern	Bonnie Skelly/My Drive/Dir_0/30623.txt	1
US SSN	Pattern	Bonnie Skelly/My Drive/Dir_0/56379.txt	1