

STEALTHbits Access Library

How-To Guide



Access Rights Reporter for Google Drive



Version 1.0
4/1/2019



Table of Contents

Introduction.....	3
StealthAUDIT® Overview	3
Access Rights Reporter for Google Drive Module	4
Prerequisites.....	4
Configuration	4
Creating the Service Account	4
Delegating Authority to the Service Account.....	8
Enabling the APIs.....	9
Implementation	9
Setting up the Module	10
Execution.....	12
Optional File Display	12
See Results	14
Identifying in the AIC	14
Access Library Overview.....	16
Legal Notice	17

Introduction

This document is designed to enable a user to install, configure, and execute the Access Rights Reporting Module (Module) for Google Drives in their environment.

This Module will connect to a Google Organization and collect a list of users, groups, group members, Drives, Drive files, and Drive permissions. The Module will then concatenate that data into a view within the StealthAUDIT® Access Information Center (AIC), which will show the permissions of accounts on individual pieces of content within the Google Drive environment.

StealthAUDIT® Overview

STEALTHbits' StealthAUDIT Management Platform helps organizations collect and analyze the data they need to answer their most difficult questions in the management and security of their critical IT infrastructure, data, and applications. Unlike point-products designed to address only a single need, StealthAUDIT is a true framework. With preconfigured solutions to address your most common requirements, as well as an extensive toolset for you to create solutions of your own, StealthAUDIT remains relevant even when your requirements change.

Key Features & Benefits:

- **Preconfigured Solution Sets** – StealthAUDIT contains out-of-the-box, ready to run Solution Sets aligning to Data Access Governance for Unstructured and Structured Data, Active Directory Management and Security, OS-level Auditing and Governance, and more.
- **Process Automation** – StealthAUDIT seamlessly ties together disparate processes, creating fully automated solutions that save time, avoid unnecessary costs, and alleviate burden on IT.
- **Governance** – Not all the data you need can be obtained from a system or application. StealthAUDIT provides both simple and sophisticated methods of retrieving and incorporating end-user feedback into the data analysis and decision-making process, including Entitlement Reviews, Self-Service Access Requests, and more.
- **Technology Integration** – StealthAUDIT can push and pull data to and from dozens of technologies (including home-grown systems) to enhance the value of existing and future technology investments.
- **Consolidated Reporting** – StealthAUDIT can report on any available dataset, enabling organizations to automate a multitude of reporting tasks, as well as view all of their reports in a single pane of glass.

Access Rights Reporter for Google Drive Module

This document describes the process for installing and configuring the Google Drive Module for the STEALTHbits Access Library into an environment where the StealthAUDIT Management Platform and the AIC are already installed and running.

Prerequisites

Prior to installing the Module, confirm you have administrator rights on the StealthAUDIT console, as well as enough rights to download or copy software to the machine on which it is hosted.

You will need:

1. Access to an administrator account
2. A service account with enough permissions to download or copy software
3. The P12 key file associated with the Google Drive tenant

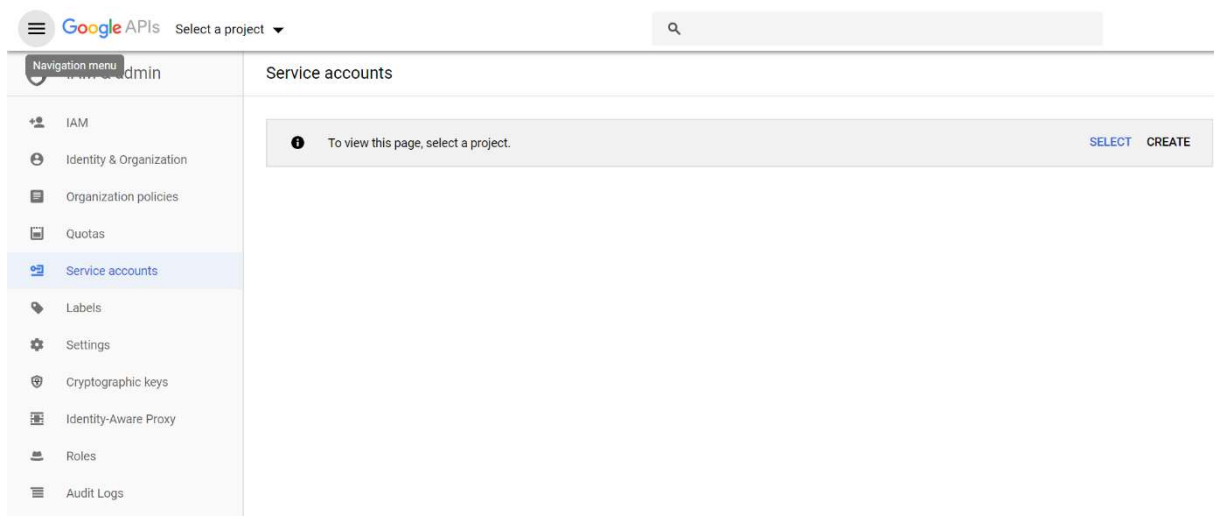
Should the service account not exist or the P12 file not be available, this guide will walk you through how to generate them.

Configuration

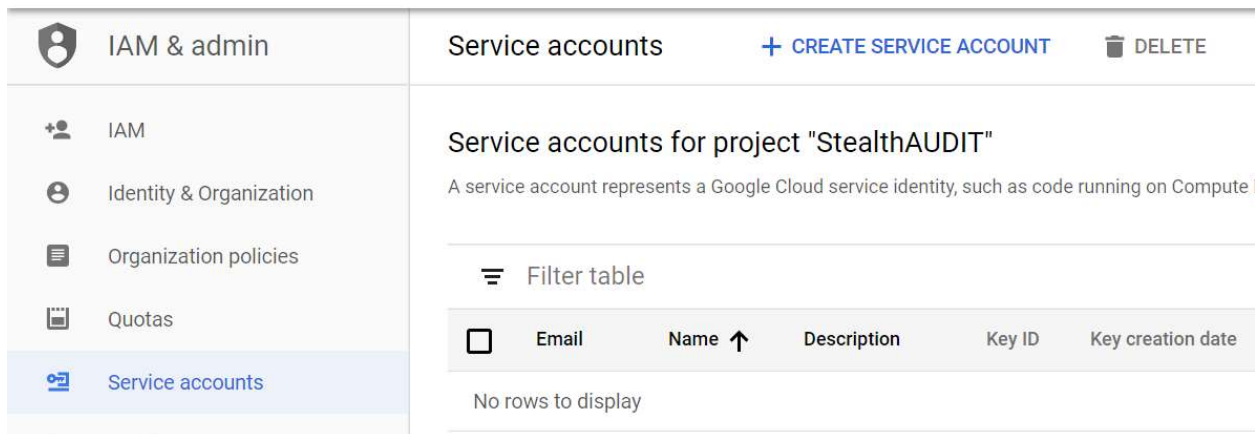
Creating the Service Account

Follow the steps below to create a Service Account:

Step 1: Log in to the [Service Account page](#) in the Google Developers Console with an account that has Administrative Privileges.

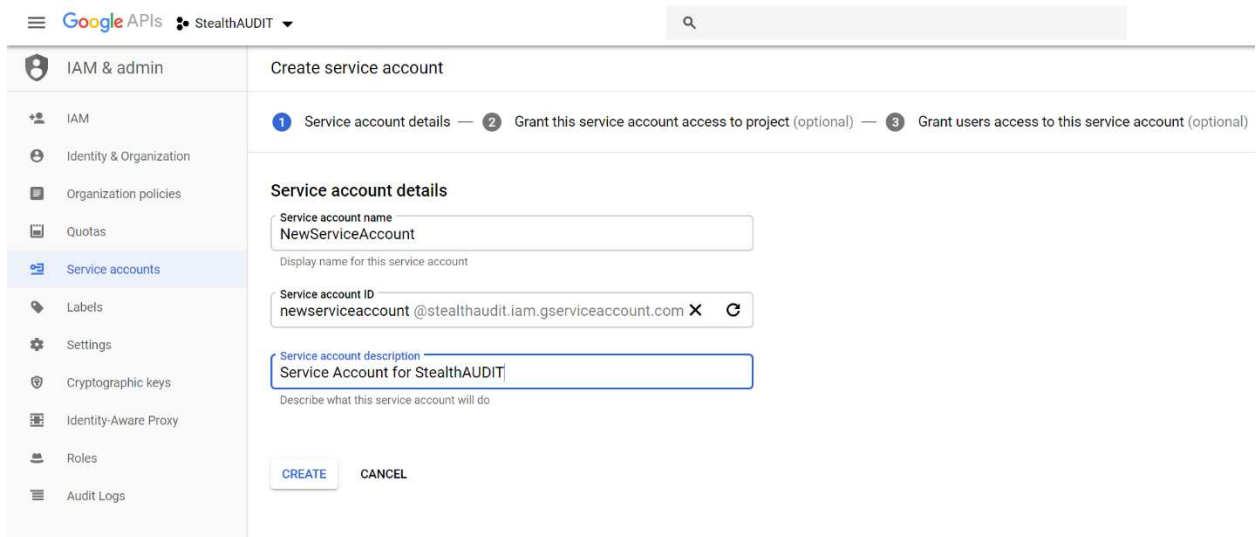


Step 2: Create a new project for this purpose or connect to an existing project where the new service account can be generated. Click "Create Service Account".



The screenshot shows the Google Cloud IAM & admin console. On the left, the 'IAM & admin' menu is open, with 'Service accounts' selected. The main content area is titled 'Service accounts for project "StealthAUDIT"'. Below the title, there is a description: 'A service account represents a Google Cloud service identity, such as code running on Compute Engine.' A 'Filter table' section is present, followed by a table with columns: 'Email', 'Name', 'Description', 'Key ID', and 'Key creation date'. The table currently shows 'No rows to display'.

Step 3: Provide a name, an ID, and a description for the account being created.



The screenshot shows the 'Create service account' wizard in the Google Cloud IAM & admin console. The left sidebar shows the 'IAM & admin' menu with 'Service accounts' selected. The main content area is titled 'Create service account' and shows a progress bar with three steps: 1. Service account details (active), 2. Grant this service account access to project (optional), and 3. Grant users access to this service account (optional). Under 'Service account details', there are three input fields: 'Service account name' (filled with 'NewServiceAccount'), 'Service account ID' (filled with 'newserviceaccount@stealthaudit.iam.gserviceaccount.com'), and 'Service account description' (filled with 'Service Account for StealthAUDIT'). At the bottom, there are 'CREATE' and 'CANCEL' buttons.

Step 4: Skip the step for “Grant this service account access to project” and continue to “Grant users access to this service account”. Click the link for “Create Key”.

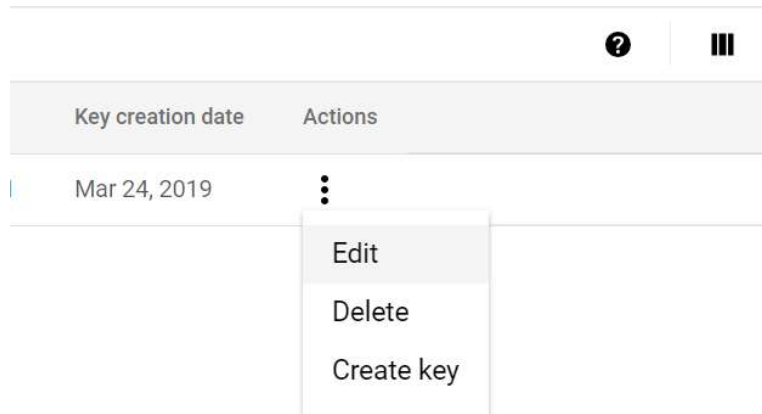
The screenshot shows the 'Create service account' wizard in the Google Cloud IAM console. The left sidebar lists navigation options: IAM & admin, IAM, Identity & Organization, Organization policies, Quotas, Service accounts (selected), Labels, Settings, Cryptographic keys, Identity-Aware Proxy, Roles, and Audit Logs. The main content area shows the progress: 'Service account details' (checked), 'Grant this service account access to project (optional)' (checked), and 'Grant users access to this service account (optional)' (current step, indicated by a blue circle with the number 3). Below the progress bar, the section 'Grant users access to this service account (optional)' is active. It includes a link to 'Learn more' and two dropdown menus: 'Service account users role' (with a help icon) and 'Service account admins role' (with a help icon). Below these, the 'Create key (optional)' section is visible, with a warning about the private key and a '+ CREATE KEY' button. At the bottom are 'DONE' and 'CANCEL' buttons.

Step 5: When prompted, choose “P12” and click “Create”.

The screenshot shows a 'Create key (optional)' dialog box. It contains the same warning about the private key as the previous screen. Under the 'Key type' section, there are two radio button options: 'JSON' (labeled 'Recommended') and 'P12' (selected). Below the 'P12' option is the text 'For backward compatibility with code using the P12 format'. At the bottom of the dialog are 'CREATE' and 'CANCEL' buttons.

Note: Keep track of where this file downloads to. This file will be required later for StealthAUDIT.

Step 6: Complete the process and return to the service account page. Once returned, click the ellipsis to the right of the newly created service account and choose "Edit".



Step 7: In the next screen expand out "Show Domain-wide Delegation" and click on "Enable G Suite Domain-wide Delegation". Fill in a value of choice for the product name field; StealthAUDIT is a recommended name. Save to return to the service account page.

- ☒ **Enable G Suite Domain-wide Delegation**
Allows this service account to be authorized to access all users' data on a G Suite domain without manual authorization on their parts. [Learn more](#)

i To change domain wide delegation, a product name for the OAuth consent screen must be configured. You can enter the product name below.

On some platforms, the email address is shown with the developer information. To select a different email address, configure consent screen.

[CONFIGURE CONSENT SCREEN](#)

Product name for the consent screen

StealthAUDIT

Assign product name.

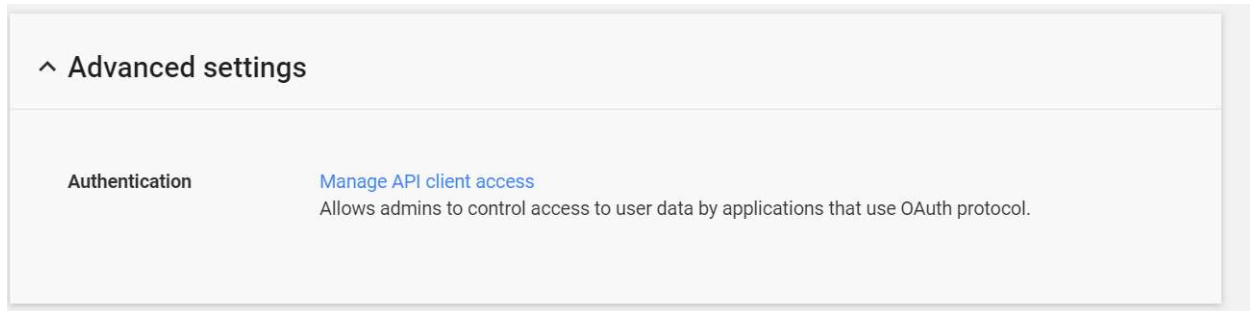
Note: Record the "Unique ID" from this page as it will be needed in a later step.

Note: Record the service account email from this page as it will be needed in a later step.

Delegating Authority to the Service Account

Follow the steps below to delegate authority to a Service Account:

Step 1: Navigate to your G Suite domain's [Admin Console](#) with an Administrator account. Click on "Security". On the Security page, click "Advanced settings", and then click "Manage API client access".



Step 2: On this page, enter the Unique ID from the provisioning process into the "Client Name" field. In the "One or More API Scopes" field you will enter a list of all permissions the service account will need in a comma separated list. Those permissions are:

- <https://www.googleapis.com/auth/admin.directory.group.member>
- <https://www.googleapis.com/auth/admin.directory.group>
- <https://www.googleapis.com/auth/admin.directory.user>
- <https://www.googleapis.com/auth/drive>

Note: For convenience, they are included in a list you can copy and paste below:

<https://www.googleapis.com/auth/admin.directory.group.member>,
<https://www.googleapis.com/auth/admin.directory.group>,
<https://www.googleapis.com/auth/admin.directory.user>,
<https://www.googleapis.com/auth/drive>

Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [Learn more](#)

Authorized API clients

The following API client domains are registered with Google and authorized to access data for your users.

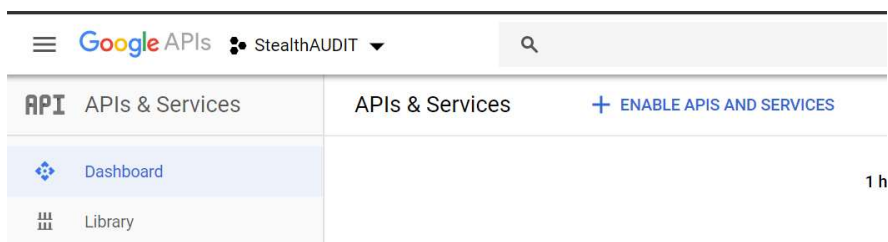
Client Name <input type="text"/> Example: www.example.com	One or More API Scopes <input type="text"/> <input type="button" value="Authorize"/> Example: http://www.google.com/calendar/feeds/ (comma-delimited)
---	---

Click "Authorize" to complete the process.

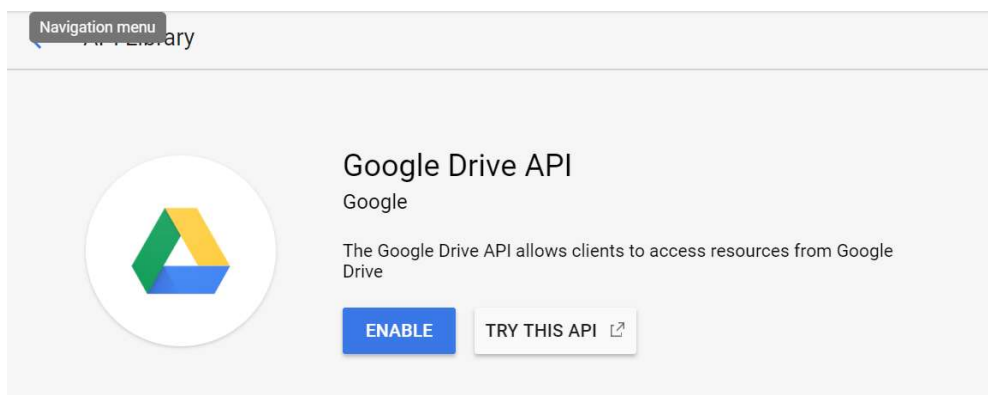
Enabling the APIs

Follow the steps below to enable the APIs:

Step 1: Navigate to the Google Developer Console API page. If your new project is not already chosen in the drop-down at the top, choose it now. Click "Enable APIs and Services".



Step 2: Search for "Admin SDK". Click on that link, and on the next page click "Enable". Repeat this process with "Google Drive API".



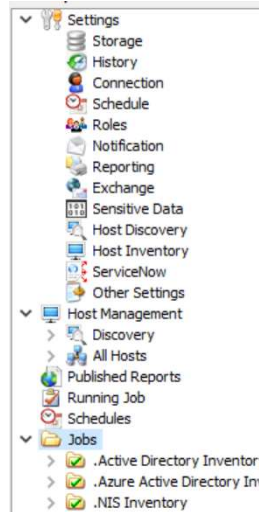
Implementation

This section will walk you through how to extract the package you have downloaded from the STEALTHbits website in the optimal way, as well as how to configure the information collected in the Configuration section appropriately to run this Module.

Extracting the Downloaded Package

Follow the steps below to extract the downloaded package:

Step 1: Create a new Group in the StealthAUDIT Job Hierarchy by right-clicking at the "Jobs" scope and choosing "Create Group". Name the group however you choose.



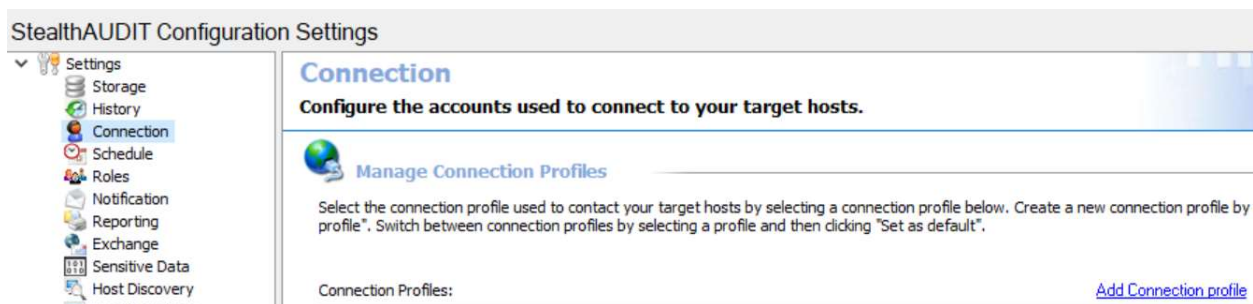
Step 2: Right-click on the new Group and choose Explore Folder. The directory that opens is where the new Job that has been downloaded will be placed. Extract the job to this location.

Step 3: Either relaunch the StealthAUDIT console, or right-click on "Jobs" and choose "Refresh Tree". Your new Module should now be visible.

Setting up the Module

Follow the steps below to set up the Module:

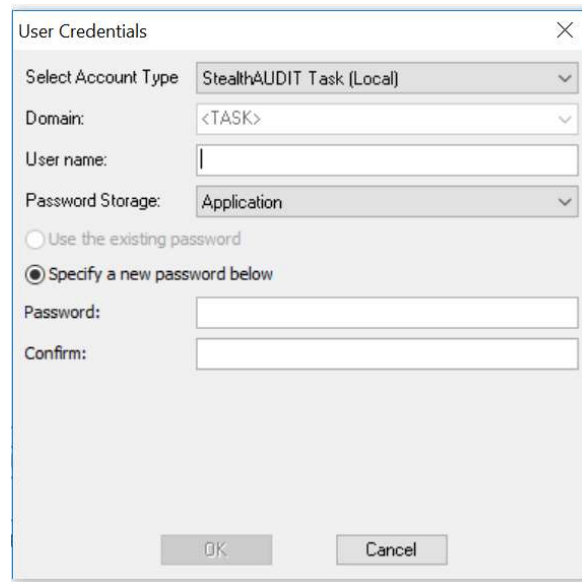
Step 1: Add a new set of credentials by navigating in the StealthAUDIT hierarchy to "Settings" -> "Connection". Click "Add Connection Profile".



Step 2: Name the profile however you choose. Click "Add User credential".



Step 3: For the Account Type, choose "StealthAUDIT Task (Local)". The User name will be the previously recorded Service Account email. The Password will be the email address of an administrator account in the Google Organization.



The "User Credentials" dialog box is shown. It has a title bar with a close button. The "Select Account Type" dropdown is set to "StealthAUDIT Task (Local)". The "Domain" dropdown is set to "<TASK>". The "User name" field is empty. The "Password Storage" dropdown is 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 fields for "Password:" and "Confirm:". At the bottom are "OK" and "Cancel" buttons.

Click "OK" when done. Then click "Save".

Step 4: Add a new entry to the StealthAUDIT Host Inventory by navigating to "Host Management" -> "All Hosts" in the StealthAUDIT hierarchy and clicking on "Add Hosts".



The screenshot shows the "All Hosts" window in the StealthAUDIT application. The left sidebar shows a tree view with "Host Management" expanded and "All Hosts" selected. The main area displays a table of hosts. The table has columns: Name, HostS, Inven, IPAddress, Subnet, DNSDomain, FQDN, OSName, OSType, and TimeZone. The first row is "GOOGLE.COM". The second row is "SBNJENGLP39" with a status of "Success", "Idle", IP "192.168.12.103", "sbitsinc.com", "SBNJENGLP39.sbitsinc.com", "Windows 10 Pro", and "UTC-05:00 E". The right sidebar shows an "Activities" panel with buttons: "Add Hosts", "View/Edit Host", "Delete Host(s)", "Import Location", "Refresh Hosts", "Save Current View", "Save Selected To List", "Schedule", "Export Data", "Suspend Host Inventory", and "External commands".

Name	HostS	Inven	IPAddress	Subnet	DNSDomain	FQDN	OSName	OSType	TimeZone
GOOGLE.COM									
SBNJENGLP39	Success	Idle	192.168.12.103		sbitsinc.com	SBNJENGLP39.sbitsinc.com	Windows 10 Pro	Windows	UTC-05:00 E

Step 5: Add a host called "google.com". Add to a host list of your choice, and choose the Connection Profile created in the previous step. Click "Finish" when done.

StealthAUDIT Host List Wizard
Specify Host List Properties

Host list options

Host List Name:

When should inventory fields be refreshed for hosts in this list?

☐ Refresh inventory every time when the host discovery query completes

By selecting this option, jobs that reference the discovery task as a host list

What credentials should be used to query these hosts?

☐ Default credentials (credentials the application is run with)

☐ Credentials in my default connection profile

☒ Credentials in this connection profile:

Step 6: In the StealthAUDIT job hierarchy, locate the newly imported Module "Access Library – Google Drives". Right-click and choose "Explore Folder".

Step 7: In the folder that pops up, paste the P12 key from the Configuration steps. Rename that key to "Certificate.p12".

Execution

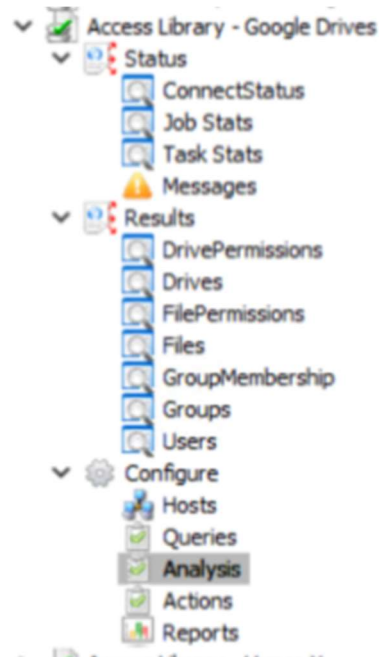
To execute, right-click on either the parent folder or job scope. Choose either "Run Group" or "Run Job" respectively. This will allow the Job to collect the necessary information and import it into the AIC.

Optional File Display

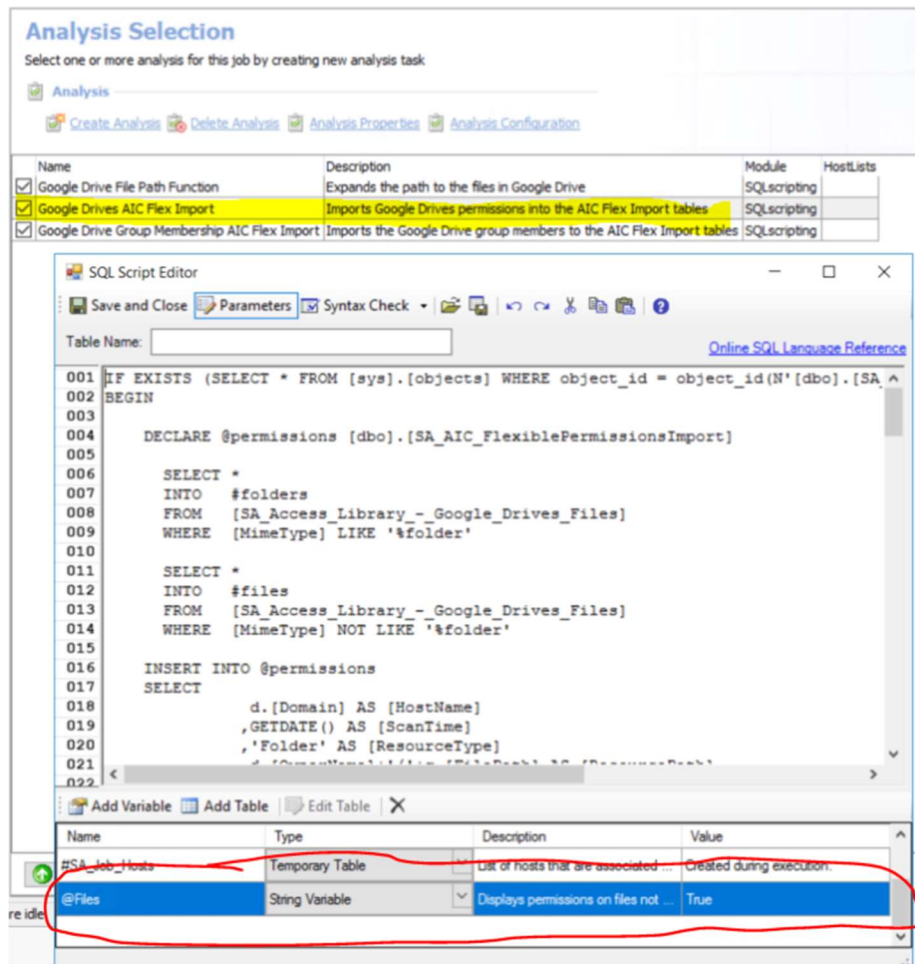
By default, this Module will display all Google Drives and all folders in the left-hand hierarchy in the AIC. Should files exist in any of these containers and those files have permissions different from the container, those files will be present in the AIC hierarchy. This can be disabled by doing the following:

Step 1: Navigate to the Module in the left-hand hierarchy of StealthAUDIT.

Step 2: Expand the job out, expand out "Configure" and then click on "Analysis"



Step 3: Click on "Google Drives AIC Flex Import" and click on "Analysis Configuration". Click "Parameters" in the new window and scroll to file a parameter named "@Files". Set this parameter to "True" to view files in the AIC and "False" to hide files.



See Results

Identifying in the AIC

Content will be output to the AIC to show access. No reports are included with this Module.

Step 1: Launch the AIC by double-clicking the icon on the desktop, navigating to the direct URL, or accessing it any other way that may be configured. Login as needed.

Step 2: Click on Resource Audit. Navigate to "Google Drives" on the left-hand hierarchy. Expand out to see additional details.

Google Drives > crmexpress.org > Malte Schoch > My Drive > Private Content

Trustee Name	Source	List	Read	Write	Delete	Manage	Applies To	Allow Mask	Deny Mask
Dave Barnett	Direct	✓	✓				favicon.ico	reader	None
Dave Barnett	Direct	✓	✓				logo.png	reader	None
Dave Barnett	Direct	✓	✓				metrotile.png	reader	None
Dave Barnett	Direct	✓	✓				Starter DesignManager.html	reader	None
Dave Barnett	Direct	✓	✓				Starter Foundation.master	reader	None
Dave Barnett	Direct	✓	✓				Starter MySiteHost.master	reader	None
Dave Barnett	Direct	✓	✓				Starter PubCollab.master	reader	None
Dave Barnett	Direct	✓	✓				Starter Publishing.master	reader	None
Dave Barnett	Direct	✓	✓				style.css	reader	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	favicon.ico	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	logo.png	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	metrotile.png	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	Starter DesignManager.html	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	Starter Foundation.master	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	Starter MySiteHost.master	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	Starter PubCollab.master	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	Starter Publishing.master	owner	None
Malte Schoch	Direct	✓	✓	✓	✓	✓	style.css	owner	None
Paul McNally	Direct	✓	✓				favicon.ico	reader	None
Paul McNally	Direct	✓	✓				logo.png	reader	None
Paul McNally	Direct	✓	✓				metrotile.png	reader	None
Paul McNally	Direct	✓	✓				Starter DesignManager.html	reader	None
Paul McNally	Direct	✓	✓				Starter Foundation.master	reader	None
Paul McNally	Direct	✓	✓				Starter MySiteHost.master	reader	None
Paul McNally	Direct	✓	✓				Starter PubCollab.master	reader	None
Paul McNally	Direct	✓	✓				Starter Publishing.master	reader	None
Paul McNally	Direct	✓	✓				style.css	reader	None

27 rows

Information is broken down in a hierarchal view by Google Drives -> Organization -> Individual -> Drive -> Folders. Clicking on a scope shows the permissions on all objects within that container.

Access Library Overview

STEALTHbits' Access Library is a site where STEALTHbits and STEALTHbits' users can post and share data access "connectors" for data repositories not natively supported within StealthAUDIT. Once validated by STEALTHbits, connectors can be posted and shared with the entire STEALTHbits community, whereby licensed StealthAUDIT users can browse and download connectors for free. The connectors and the data they collect are subsequently displayed within StealthAUDIT's Access Information Center (AIC) or used for custom reporting within StealthAUDIT.

Legal Notice

Legal Notice

The information in this publication is provided for information use only, and does not constitute a commitment from STEALTHbits of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. STEALTHbits makes no representations or warranties about the Software beyond what is provided in the License Agreement. STEALTHbits assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

The STEALTHbits logo and all other STEALTHbits product or service names and slogans are registered trademarks or trademarks of STEALTHbits Technologies, Inc. Non-STEALTHbits vendors and products referenced in this document are either registered trademarks or trademarks of those organizations in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-STEALTHbits products. Please note that this information is provided as a courtesy to assist you. While STEALTHbits tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-STEALTHbits product and contact the supplier for confirmation. STEALTHbits assumes no responsibility or liability for incorrect or incomplete information provided about non-STEALTHbits products.

© 2019 STEALTHbits Technologies, Inc.

All rights reserved.