



netwrix

2021

StealthAUDIT®

AnyData_SalesforceLibraries User Guide

v1.0

Contents

Introduction	2
AnyData for Salesforce Libraries.....	3
Prerequisites	3
Configuration	3
Creating a Connected App in a Salesforce Tenant.....	3
Implementation	6
Extracting the Downloaded AnyData_SalesforceLibraries Job	6
Configuring the AnyData_SalesforceLibraries Job	7
Execution.....	9
View Results	9

Introduction

This document is designed to enable a user to install, configure, and execute AnyData_SalesforceLibraries in their environment. AnyData_SalesforceLibraries connects to a Salesforce tenant and scans files in Libraries for sensitive data, including images using Optical Character Recognition (OCR).

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

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 Salesforce Libraries

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

Prerequisites

Prior to adding the AnyData_SalesforceLibraries 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:

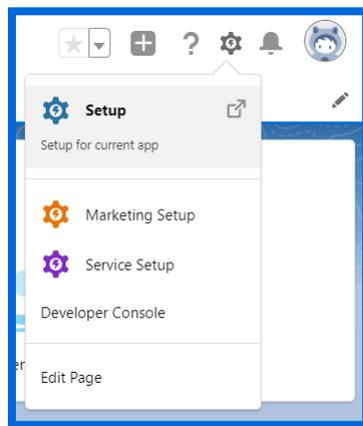
1. StealthAUDIT 11.5.0.127+
2. Access to Salesforce tenant, StealthAUDIT server, & SQL Server administrator accounts.
3. A Salesforce Connected App with enough permissions to download files in Libraries.

Should the Salesforce Connected App not exist, this guide will walk you through how to create it in the target Salesforce tenant.

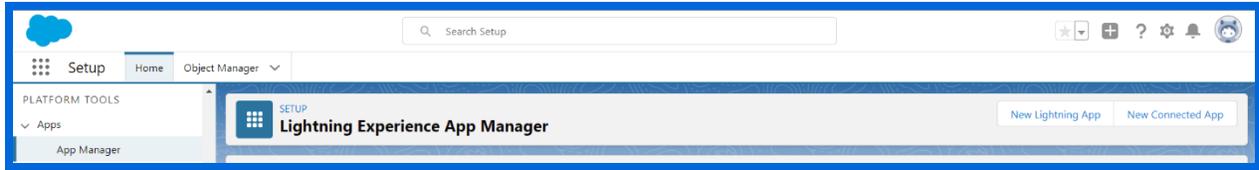
Configuration

Creating a Connected App in a Salesforce Tenant

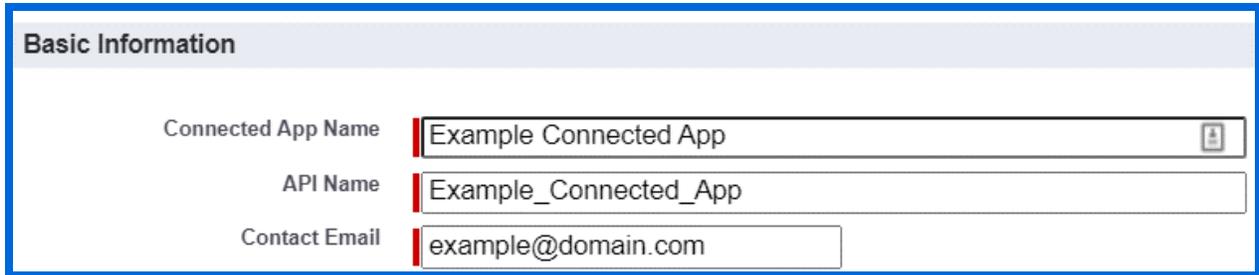
Step 1 – Log-in to the target Salesforce tenant as an admin and navigate to the **Gear Icon > Setup**.



Step 2 – In the left sidebar, navigate to **Apps > App Manager** under **Platform Tools**. Then, click **New Connected App** in the upper-right of the **Lightning Experience App Manager**.



Step 3 – Under **Basic Information**, fill out the following required fields to name the app. The email can be any email address, although it's recommended to make it the current Salesforce admin.



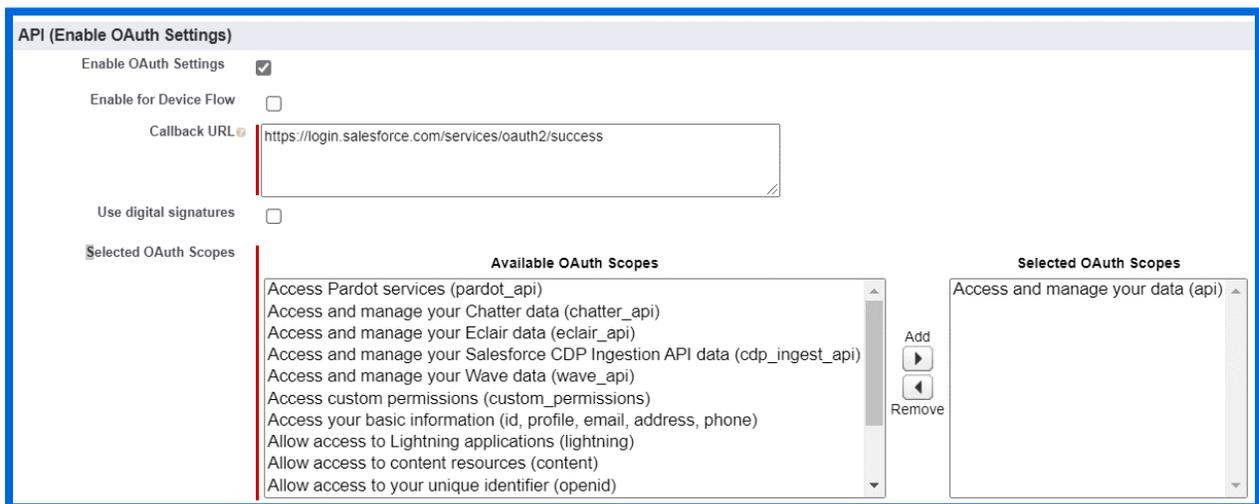
The screenshot shows the 'Basic Information' section of the app configuration. It contains three input fields:

- Connected App Name:** Example Connected App
- API Name:** Example_Connected_App
- Contact Email:** example@domain.com

Step 4 – Under **API (Enable OAuth Settings)**, enter the following value in the **Callback URL** field:

`https://login.salesforce.com/services/oauth2/success`

Step 5 – Under **API (Enable OAuth Settings)**, look for **Access and managed your data (api)** under the **Available OAuth Scopes** list. When located, highlight that row, and click the **Add** arrow so the scope moves over to the **Selected OAuth Scopes** field.



The screenshot shows the 'API (Enable OAuth Settings)' configuration page. It includes several checkboxes and a text field:

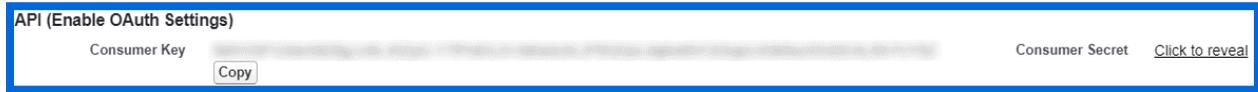
- Enable OAuth Settings:**
- Enable for Device Flow:**
- Callback URL:** `https://login.salesforce.com/services/oauth2/success`
- Use digital signatures:**

Below these are two lists of OAuth scopes:

- Available OAuth Scopes:** A list of scopes including 'Access Pardot services (pardot_api)', 'Access and manage your Chatter data (chatter_api)', 'Access and manage your Eclair data (eclair_api)', 'Access and manage your Salesforce CDP Ingestion API data (cdp_ingest_api)', 'Access and manage your Wave data (wave_api)', 'Access custom permissions (custom_permissions)', 'Access your basic information (id, profile, email, address, phone)', 'Allow access to Lightning applications (lightning)', 'Allow access to content resources (content)', and 'Allow access to your unique identifier (openid)'. The scope 'Access and managed your data (api)' is highlighted.
- Selected OAuth Scopes:** A list containing 'Access and managed your data (api)'. An 'Add' button is visible between the two lists.

Step 6 – Scroll back up to the top, click **Save**, then click **Continue**.

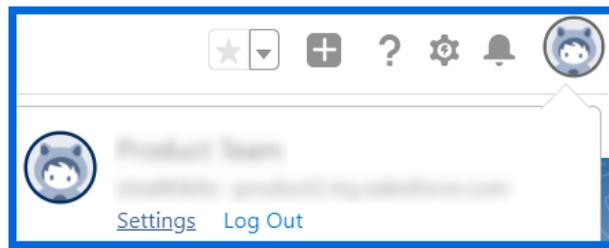
Step 7 – Scroll down and locate **API (Enable OAuth Settings)**. Note the **Consumer Key** and **Consumer Secret** (after clicking to reveal the latter). Both will be used as part of the Connection Profile in StealthAUDIT.



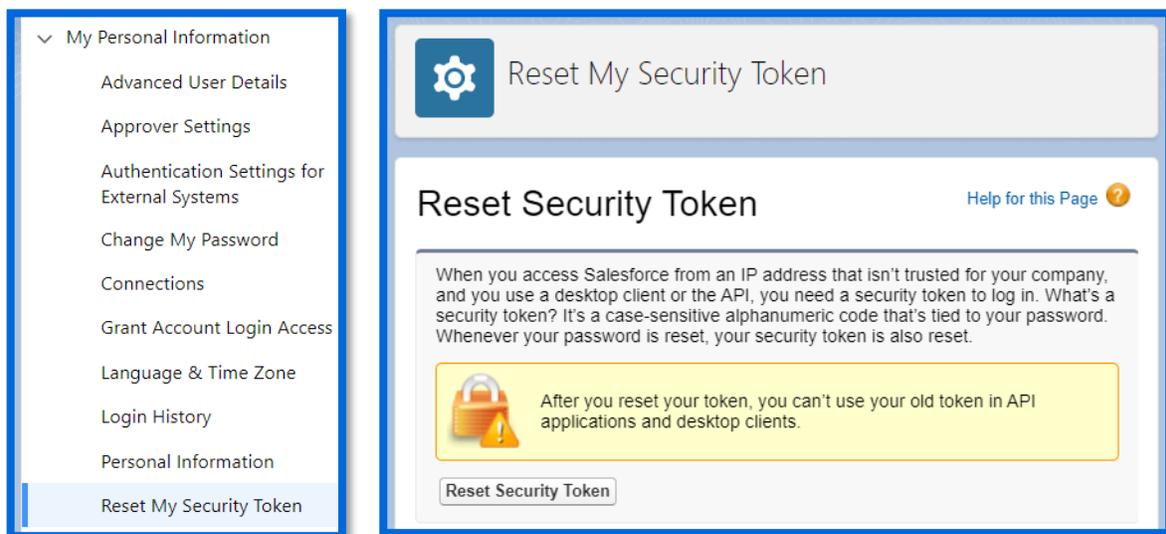
Step 8 – Finally, the Salesforce tenant's Security Token is required for API access. A tenant's Security Token is a secret value that applies to all Connected Apps, API requests, etc. If the Security Token is not known, then it must be reset to view the new one.

IMPORTANT: Resetting the Security Token to view the new one will interrupt any other Connected App or Salesforce API communications using the old Security Token.

To reset the Security Token, click on the user icon in the upper-right, then click on **Settings**.



Under **My Personal Information**, click **Reset My Security Token** followed by **Reset Security Token**.

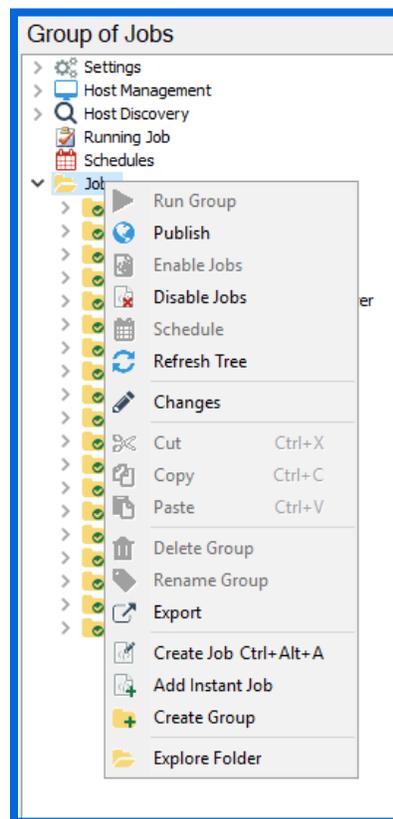


Implementation

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

Extracting the Downloaded AnyData_SalesforceLibraries 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 Salesforce



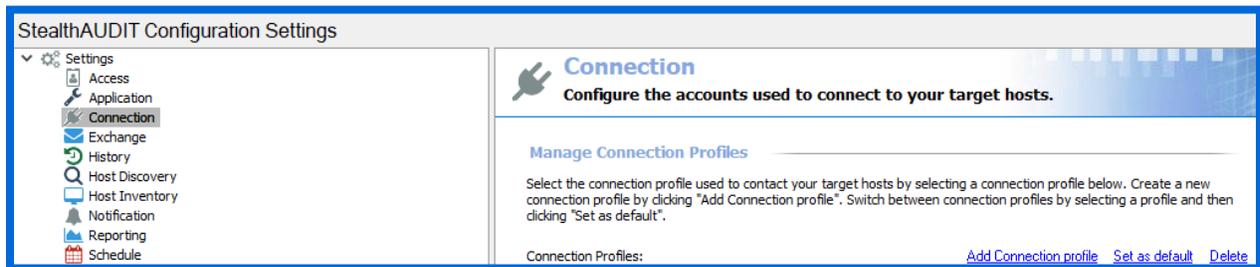
Step 2 – Right-click on the new Group and click **Explore Folder**. The directory that opens is where the AnyData_SalesforceLibraries job that has been downloaded will be placed. Extract the job to this location and make sure any files in the job folder marked as read-only have that RO flag removed.

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

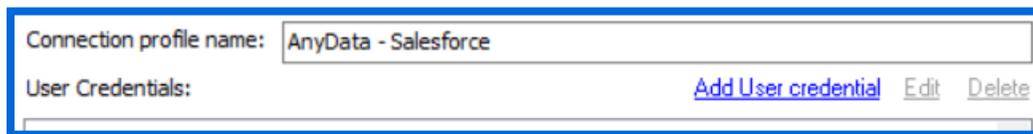
Configuring the AnyData_SalesforceLibraries Job

Now that the downloaded job has been imported to StealthAUDIT, you can configure it to scan for sensitive data in a Salesforce tenant's Libraries.

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 – Salesforce. 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.

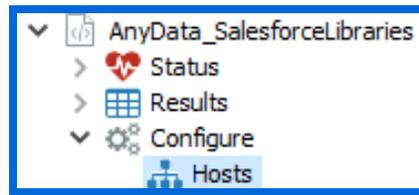
IMPORTANT: The **Active Directory Account** needs to be the first credential in the list for this Connection Profile. If it's not, use the **Move Up** button to adjust this credential's position.

Step 4 – Click **Add User Credential** again. For this credential's Account Type, select **StealthAUDIT Task (Local)**. The User Name is the previously recorded Consumer Key for the Salesforce Connected App. The Password is the previously recorded Consumer Secret for the Salesforce Connected App. Click **OK** when finished.

Step 5 – Click **Add User Credential** again. For this credential's Account Type, select **StealthAUDIT Task (Local)**. The User Name is a Salesforce admin login, and the Password is the admin's password. Click **OK** when finished.

Step 6 – Click **Add User Credential** again. For this credential's Account Type, select **StealthAUDIT Task (Local)**. The User Name is the URL of the target Salesforce tenant, and the Password is the Salesforce tenant's Security Key. Click **OK** when finished, then click **Save**.

Step 7 – Navigate back to the AnyData_SalesforceLibraries job and go to the job’s Host Selection via **[Job Name] > Configure > Hosts**.



In the Hosts menu, locate the Individual Hosts section, use the name of your Salesforce tenant for the Host Name, and click **Add** then **Save**. For example, for the tenant “example-tenant.my.salesforce”, you would add “example-tenant” to the Individual Hosts list.

Individual hosts

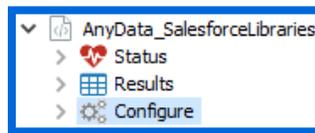
Enter one or more hosts to query and click "Add". These hosts will be added to a local host list that will be unavailable to other queries. These hosts will be added to the global host inventory, if they aren't already there.

Host name: ➔ Add ✕ Remove

Step 8 – The following parameters can also be configured for the job:

Library Scoping	This list parameter scopes the job to the specified libraries.
Scan All File Types	If "true", all files will be scanned, regardless of extension.

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.

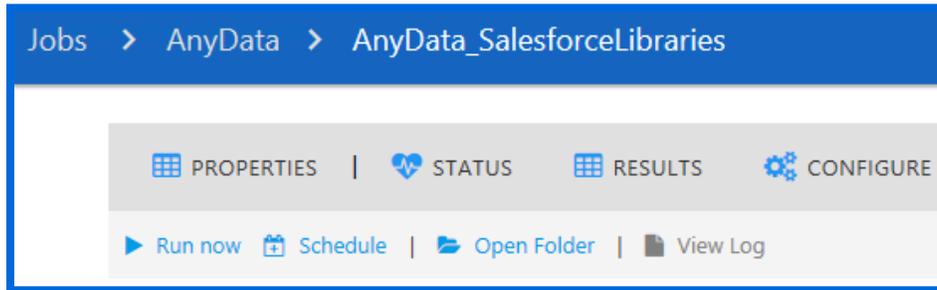
Configuration

If "true", all files will be scanned, regardless of extension. □

This list parameter scopes the job to the specified libraries. ☰

Execution

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

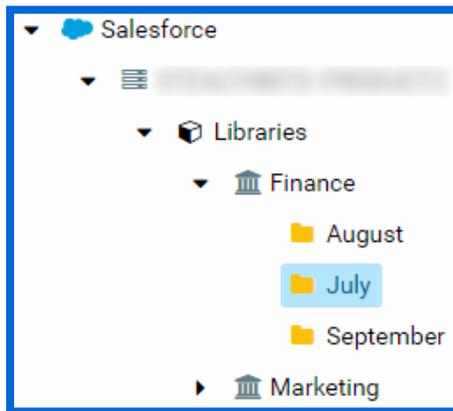


View Results

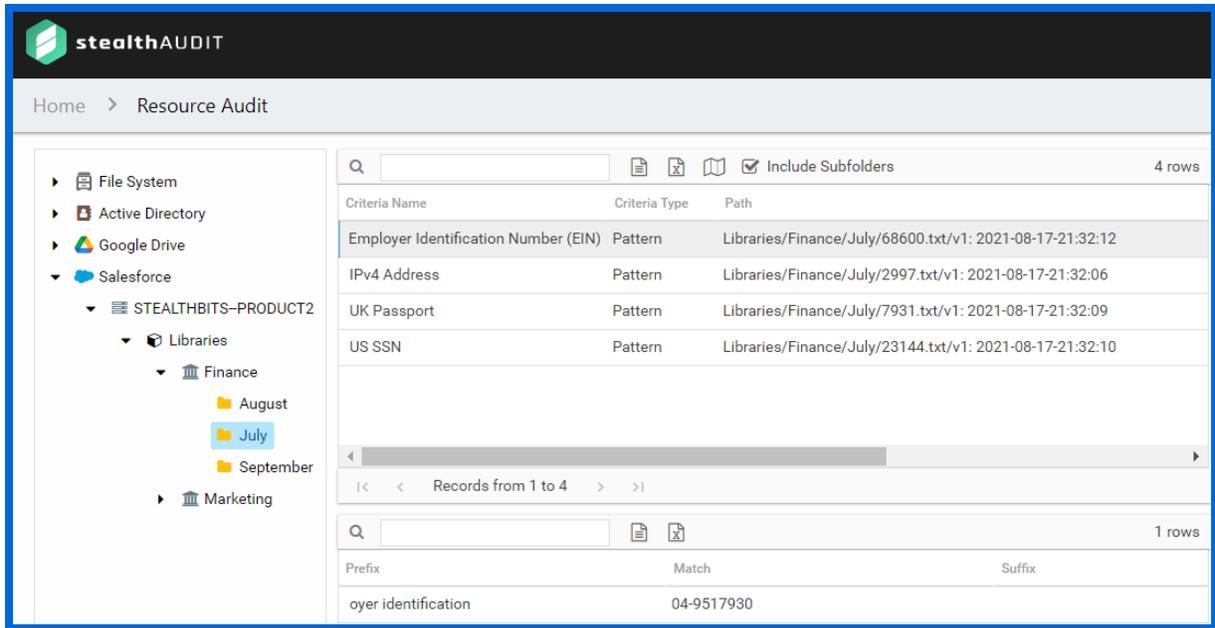
Sensitive data scan results from the AnyData_SalesforceLibraries job will be output to the Access Information Center (AIC).

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 Salesforce in the left sidebar. Expand the node, and nodes below it, to view details.



Information is broken down in a hierarchical view by **Salesforce > Tenant > Library > 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.



Home > Resource Audit

File System
Active Directory
Google Drive
Salesforce
STEALTHBITS-PRODUCT2
Libraries
Finance
August
July
September
Marketing

4 rows

Criteria Name	Criteria Type	Path
Employer Identification Number (EIN)	Pattern	Libraries/Finance/July/68600.txt/v1: 2021-08-17-21:32:12
IPv4 Address	Pattern	Libraries/Finance/July/2997.txt/v1: 2021-08-17-21:32:06
UK Passport	Pattern	Libraries/Finance/July/7931.txt/v1: 2021-08-17-21:32:09
US SSN	Pattern	Libraries/Finance/July/23144.txt/v1: 2021-08-17-21:32:10

Records from 1 to 4

1 rows

Prefix	Match	Suffix
oyer identification	04-9517930	

IMPORTANT: Salesforce Libraries support full version history for files that are re-uploaded with new information (v1, v2, etc.).

Salesforce stores each version in full, separate files, which this AnyData job can individually scan. As a result, file names are post-fixed by the file version number as well as a date/timestamp in the AIC.