2021

StealthAUDIT®

AnyData_Box User Guide v1.0

300 Spectrum Center Drive, Suite 200, Irvine, California | (949) 407-5125

Contents

Introduction

This document is designed to enable a user to install, configure, and execute AnyData_Box in their environment. AnyData_Box connects to an organization’s Box.com account and scans files 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 folder hierarchy of the scanned Box account, which files contain sensitive data, which sensitive data criteria were found, and, optionally, the specific sensitive strings of text that were found.

NOTE: *Files shared from external organizations will not be downloaded or scanned.*

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 Box

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

Prerequisites

Prior to adding the AnyData_Box 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:

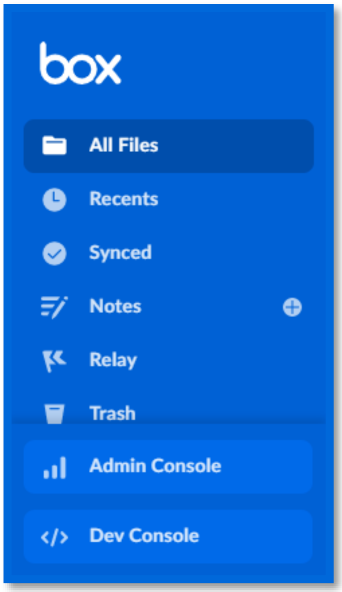
1. StealthAUDIT 11.5.0.127+
2. Access to Box.com, StealthAUDIT server, & SQL Server administrator accounts.
3. A Box App with enough permissions to download files.

Should the Box App not exist, this guide will step through how to create it in the target Box account.

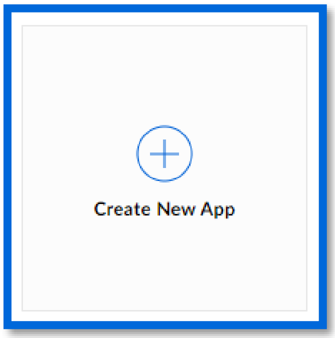
Configuration

Creating a Box App

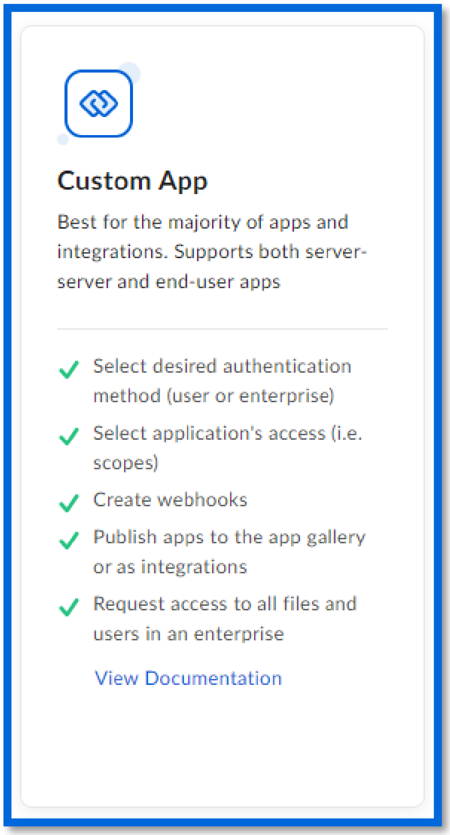
Step 1 – Log-in to the Box account as an admin and navigate to the **Dev Console** via the left sidebar.



Step 2 – Click on **Create New App** in **My Apps**.



Step 3 – Select **Custom App** when prompted for the app type. In the Custom App menu, select **Server Authentication (Client Credentials Grant)** and give the app any name.

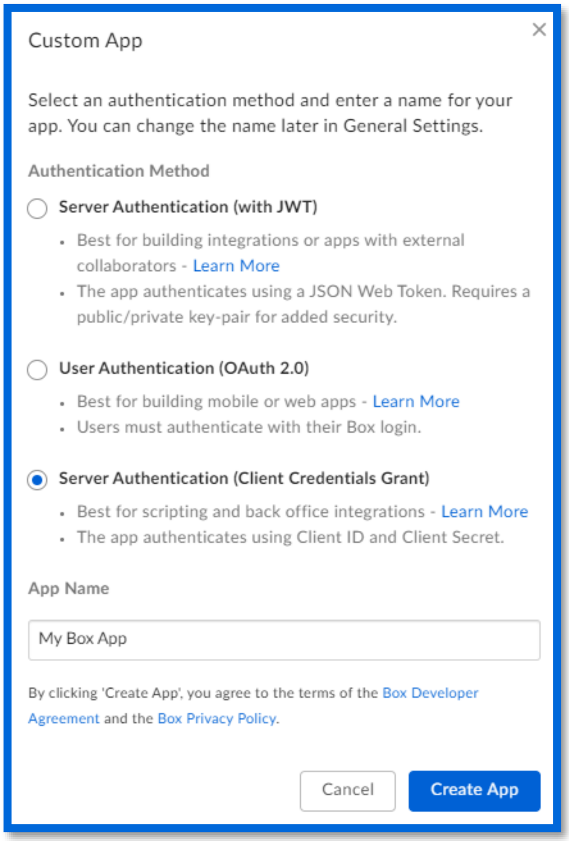


Custom App

Best for the majority of apps and integrations. Supports both server-server and end-user apps

- ✓ Select desired authentication method (user or enterprise)
- ✓ Select application's access (i.e. scopes)
- ✓ Create webhooks
- ✓ Publish apps to the app gallery or as integrations
- ✓ Request access to all files and users in an enterprise

View Documentation



Custom App ×

Select an authentication method and enter a name for your app. You can change the name later in General Settings.

Authentication Method

○ Server Authentication (with JWT)
- Best for building integrations or apps with external collaborators - Learn More
- The app authenticates using a JSON Web Token. Requires a public/private key-pair for added security.

○ User Authentication (OAuth 2.0)
- Best for building mobile or web apps - Learn More
- Users must authenticate with their Box login.

● Server Authentication (Client Credentials Grant)
- Best for scripting and back office integrations - Learn More
- The app authenticates using Client ID and Client Secret.

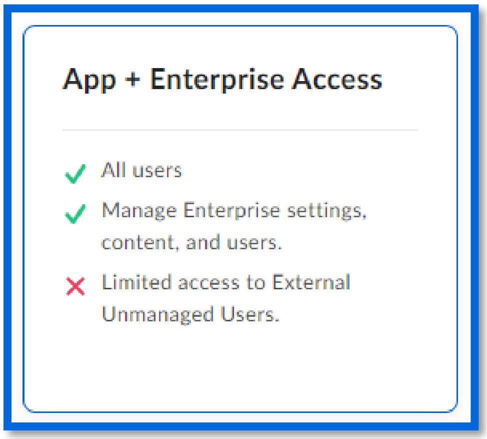
App Name

My Box App

By clicking 'Create App', you agree to the terms of the Box Developer Agreement and the Box Privacy Policy.

Step 4 – After clicking **Create App**, you will be redirected to the new app's **Configuration** page. On this page, take note of the **Client ID** and **Client Secret** (via the **Fetch Client Secret** button).

Step 5 – Under **App Access Level**, select **App + Enterprise Access**.



App + Enterprise Access

✓ All users

✓ Manage Enterprise settings, content, and users.

✗ Limited access to External Unmanaged Users.

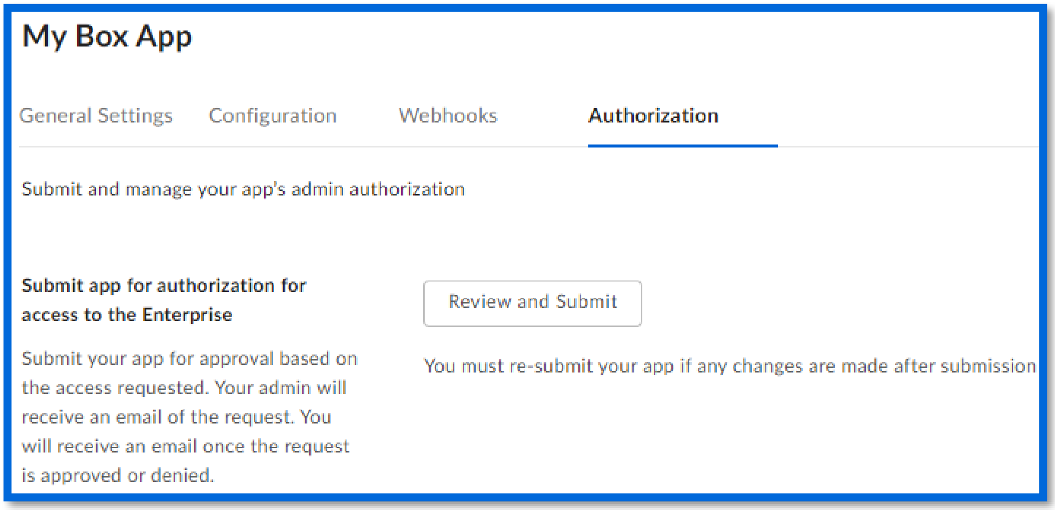
Step 6 – Under **Application Scopes**, enable the following:

- Read all files and folders stored in Box
- Write all files and folders stored in Box
- Manager users
- Manager groups
- Manager enterprise properties

Step 7 – Under **Advanced Features**, enable the following:

- Make API calls using the as-user header
- Generate user access tokens

Step 8 – Click **Save Changes**, then navigate to the app’s **Authorization** tab at the top of the page. Click **Review and Submit**, give the app a description, and click **Submit**.



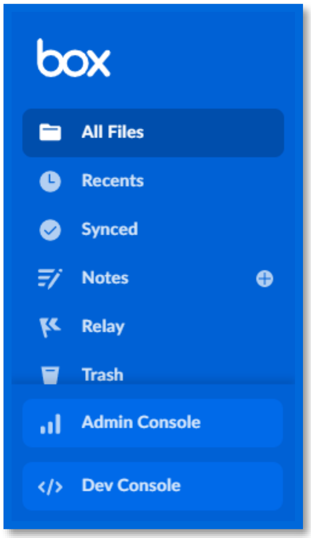
Submit and manage your app’s admin authorization

Submit app for authorization for access to the Enterprise

Submit your app for approval based on the access requested. Your admin will receive an email of the request. You will receive an email once the request is approved or denied.

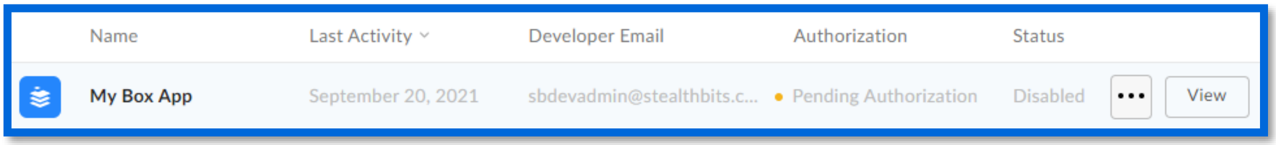
You must re-submit your app if any changes are made after submission

Step 9 – In the left sidebar, click **Back to My Account** and then navigate to the **Admin Console**.

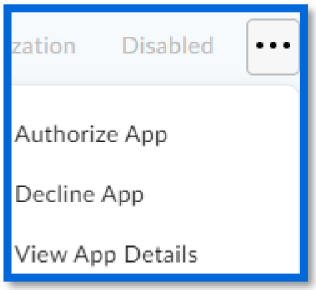


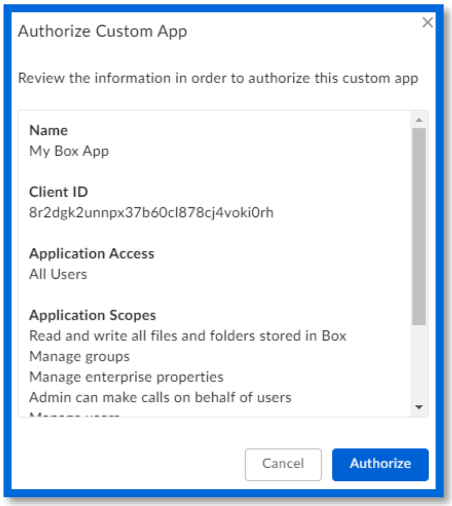
Step 10 – In the **Admin Console**, navigate to **Apps** in the left sidebar. Click on the **Custom Apps** tab.

Step 11 – Locate the app you created in the previous steps, hover over it to reveal the ellipsis (…) button, click the ellipsis, click **Authorize App**, and then click **Authorize**.



Name	Last Activity ⌄	Developer Email	Authorization	Status		
My Box App	September 20, 2021	sbdevadmin@stealthbits.c...	● Pending Authorization	Disabled	•••	View





Authorize Custom App

Review the information in order to authorize this custom app

Name
My Box App

Client ID
8r2dgk2unnpx37b60cl878cj4voki0rh

Application Access
All Users

Application Scopes
Read and write all files and folders stored in Box
Manage groups
Manage enterprise properties
Admin can make calls on behalf of users

Step 12 – After authorizing the app, click the app's ellipsis (…) button again. This time, enable the app rather than authorizing it.

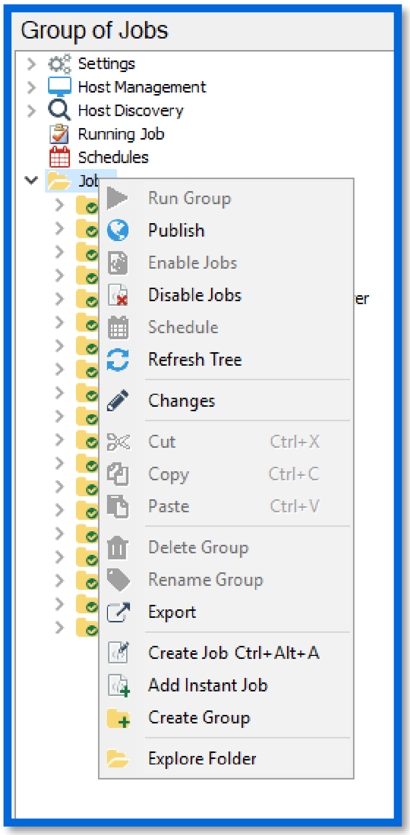
Step 13 – Navigate to **Account & Billing** in the left sidebar, and note your **Enterprise ID**.

Implementation

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

Extracting the Downloaded AnyData_Box 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_Box



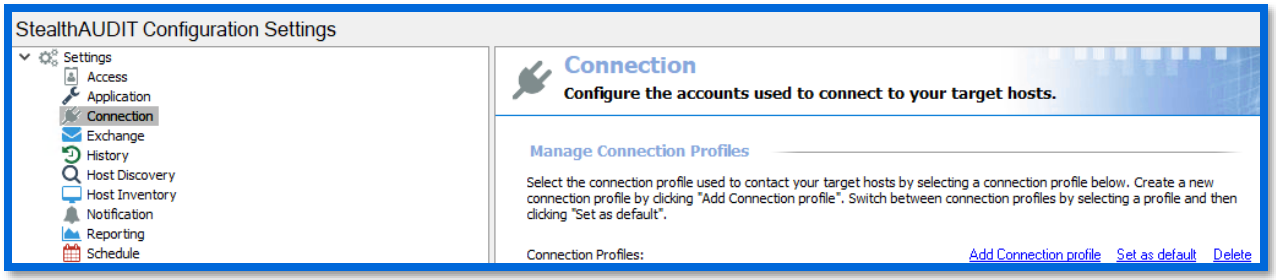
Step 2 – Right-click on the new Group and click **Explore Folder**. The directory that opens is where the AnyData_Box job that has been downloaded will be placed. Extract the job to this location and make sure any files in the job folder marked as read-only have that RO flag removed.

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

Configuring the AnyData_Box Job

Now that the downloaded job has been imported to StealthAUDIT, you can configure it to scan for sensitive data in a Box.com account.

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



Connection

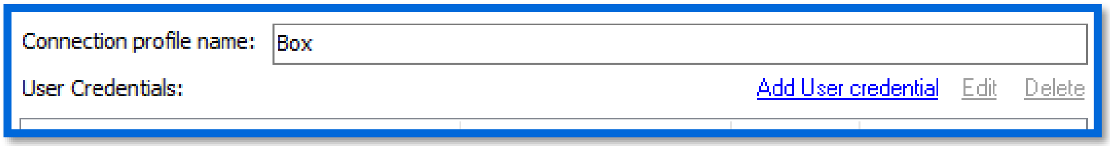
Configure the accounts used to connect to your target hosts.

Manage Connection Profiles

Select the connection profile used to contact your target hosts by selecting a connection profile below. Create a new connection profile by clicking "Add Connection profile". Switch between connection profiles by selecting a profile and then clicking "Set as default".

Connection Profiles:

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



Connection profile name: Box

User Credentials:

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.

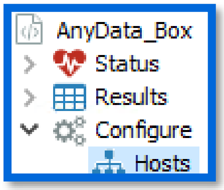
IMPORTANT: The **Active Directory Account** needs to be the first credential in the list for this Connection Profile. If it's not, use the **Move Up** button to adjust this credential's position.

Step 4 – Click **Add User Credential** again. For this credential's Account Type, select **StealthAUDIT Task (Local)**. The User Name is the previously noted **Enterprise ID** and **Client ID** separated by an "@" symbol.

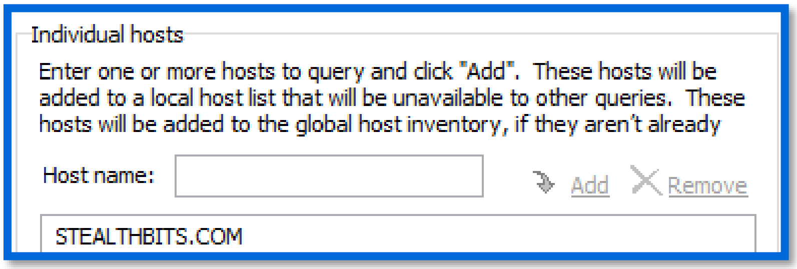
```
<enterprise_id>@<client_id>
```

The Password is the previously noted **Client Secret**. Click **OK** when finished.

Step 5 – Navigate back to the AnyData_Box 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 primary domain associated with your Box.com account for the Host Name, and click **Add** then **Save**. If there's no domain associated with your Box.com account, then this value can be anything you'd like (for example, "Box.com").



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

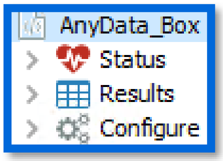
Host name:

STEALTHBITS.COM

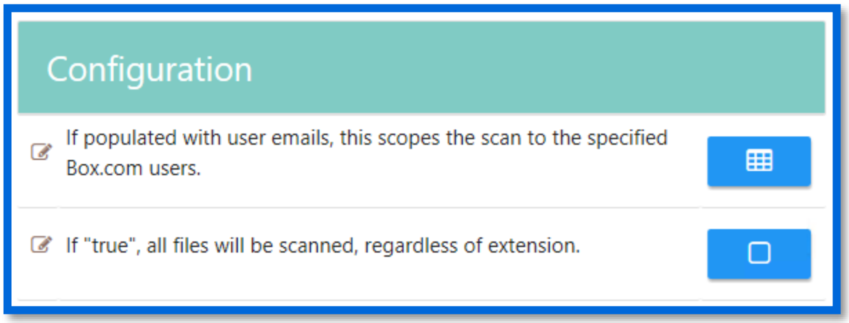
Step 6 – The following parameters can also be configured for the job:

Scan All File Types	If set to "true" all file types will be scanned, regardless of extension.
User Login Scoping	If populated with user emails, this scopes the scan to the specified Box.com users.

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.



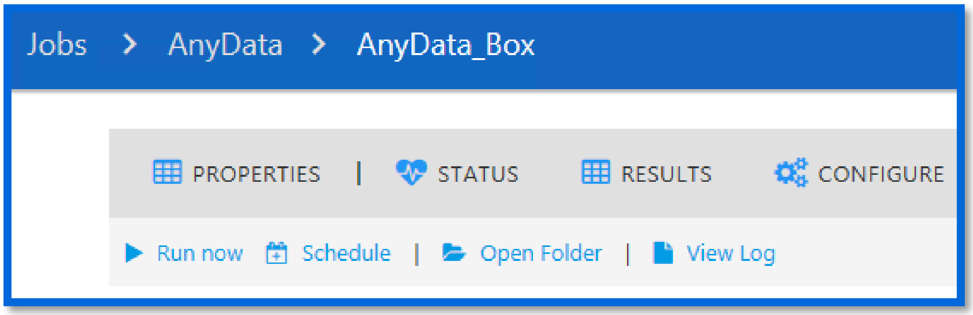
Configuration

If populated with user emails, this scopes the scan to the specified Box.com users.

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

Execution

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

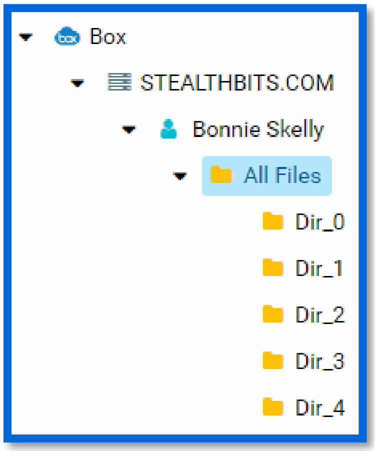

Jobs > AnyData > AnyData_Box
PROPERTIES | STATUS
RESULTS
CONFIGURE
Run now
Schedule | Open Folder | View Log

View Results

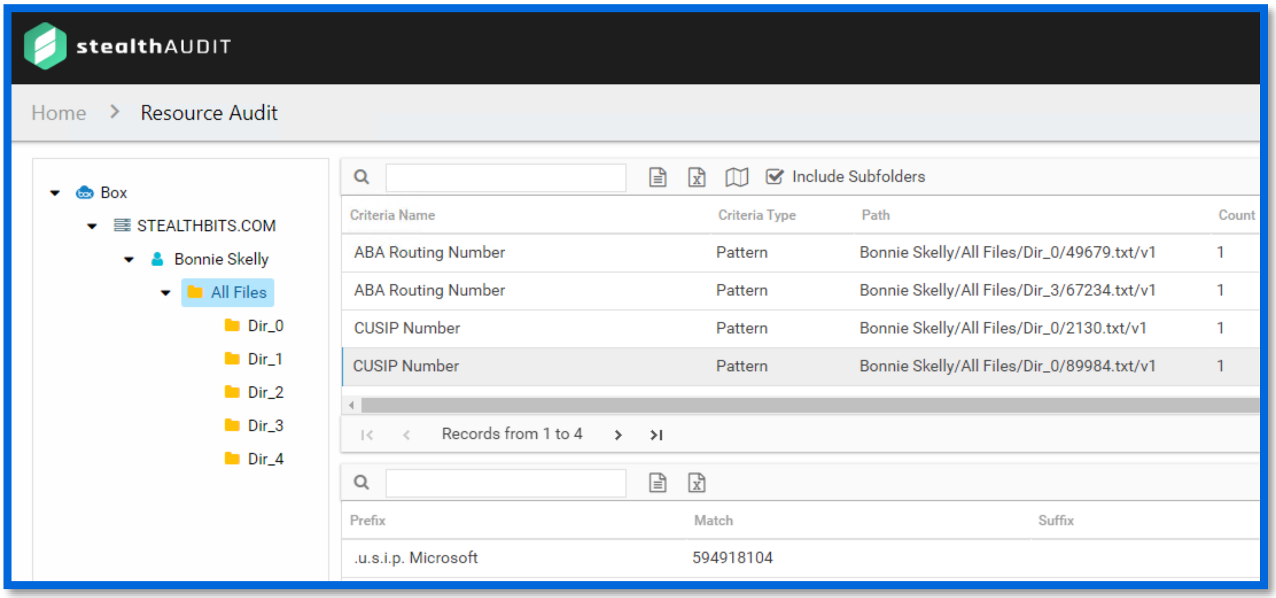
Sensitive data scan results from the AnyData_Box job will be output to the Access Information Center (AIC).

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



Information is broken down in a hierarchical view by Box user, folders, and files. 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.



☑ Include Subfolders

Criteria Name	Criteria Type	Path	Count
ABA Routing Number	Pattern	Bonnie Skelly/All Files/Dir_0/49679.txt/v1	1
ABA Routing Number	Pattern	Bonnie Skelly/All Files/Dir_3/67234.txt/v1	1
CUSIP Number	Pattern	Bonnie Skelly/All Files/Dir_0/2130.txt/v1	1
CUSIP Number	Pattern	Bonnie Skelly/All Files/Dir_0/89984.txt/v1	1

Records from 1 to 4

Prefix	Match	Suffix
.u.s.i.p. Microsoft	594918104	