

**ArcSight Manual Blacklist entries on Active list.**

Micro Focus

2018

Contents

**Chapter 1: Blacklisted Sources…………………………………………………………………….3**

**1.1 Active List**

**1.2 Automated way to populate Active list**

**1.3 Manual way to populate Active list.**

## Chapter 2:Report and Query…………………………………………………………………………..6 2.1 Creating a report.

**Chapter 3: Importing the CSV File 10**

**3.1Advantages and Disadvantages**.

# ArcSight Manual Blacklist entries on Active list.

IP address blacklisting is a method of protecting Web and other Internet servers from malicious attacks. So in order to detect the system reaching out to the blacklisted IP, ArcSight has a standard approach.

* Collecting the Blacklisted IP’s from standard blacklisted sources.
* Writing appropriate rule to detect the system reaching out to the blacklisted IP.

Chapter 1: Blacklisted sources

In order to collect the blacklisted IP’s, we searched for the blacklisted sources. We found the below source links from where we can download the blacklisted IP addresses.

<https://ransomwaretracker.abuse.ch/blocklist/>

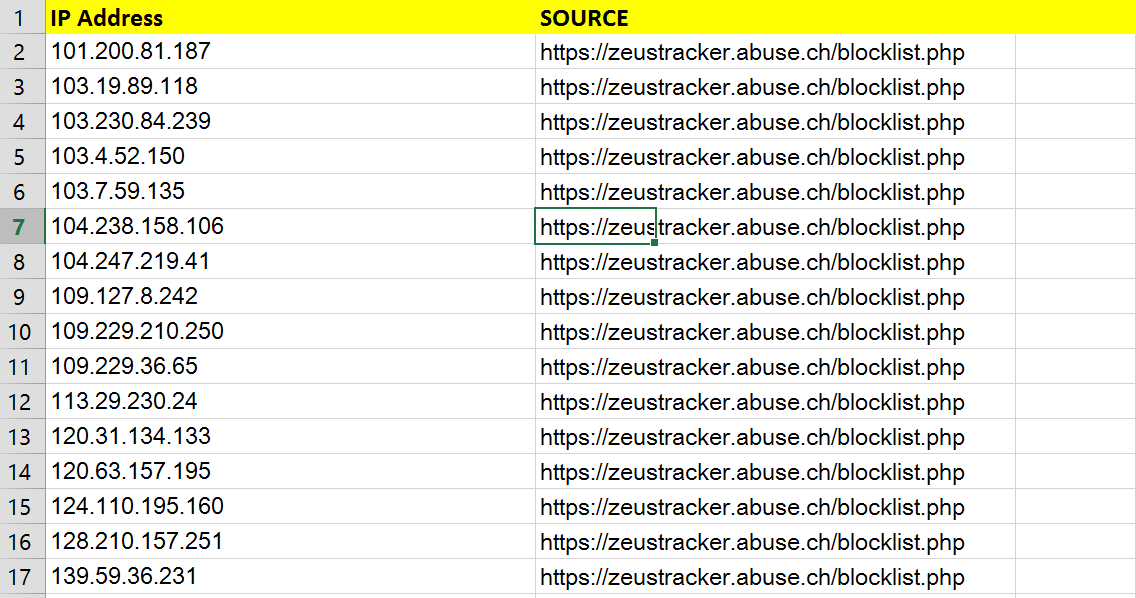
<https://sslbl.abuse.ch/blacklist/>

<https://zeustracker.abuse.ch/blocklist.php>

<https://myip.ms/browse/blacklist/Blacklist_IP_Blacklist_IP_Addresses_Live_Database_Real-time>

<https://feodotracker.abuse.ch/blocklist>

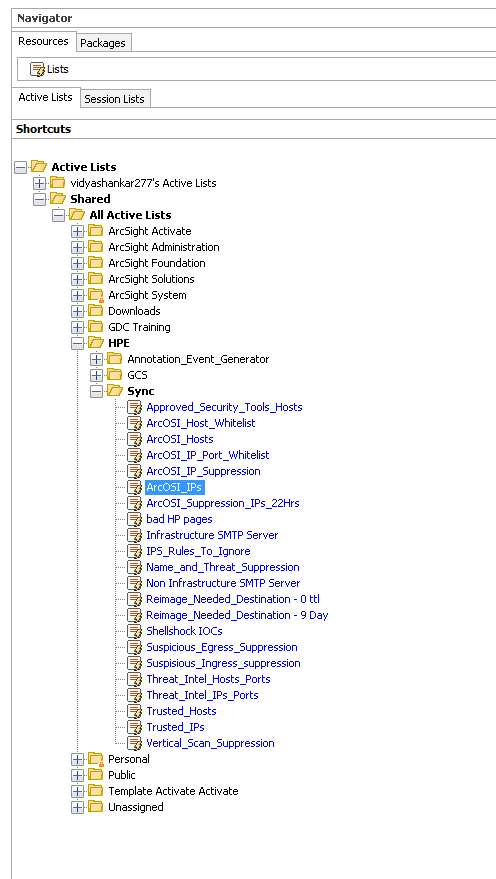
We downloaded the blacklisted IP’s from all the above source and consolidated into one single list.



**1.1 Active List**

To keep track of all blacklisted IP’s and to detect the system reaching out to the blacklisted sources an Active list which can store the blacklisted IP’s. The Active list ArcOSI IP’s has been created to store the blacklisted IP’s.

Path: **All Active Lists/HPE/Sync/ArcOSI\_IPs (PFB)**



**Fig: Active List ArcOSI\_IP’s**

There are 2 ways to populate this Active list with blacklisted IP’s:

* Automated.
* Manual.

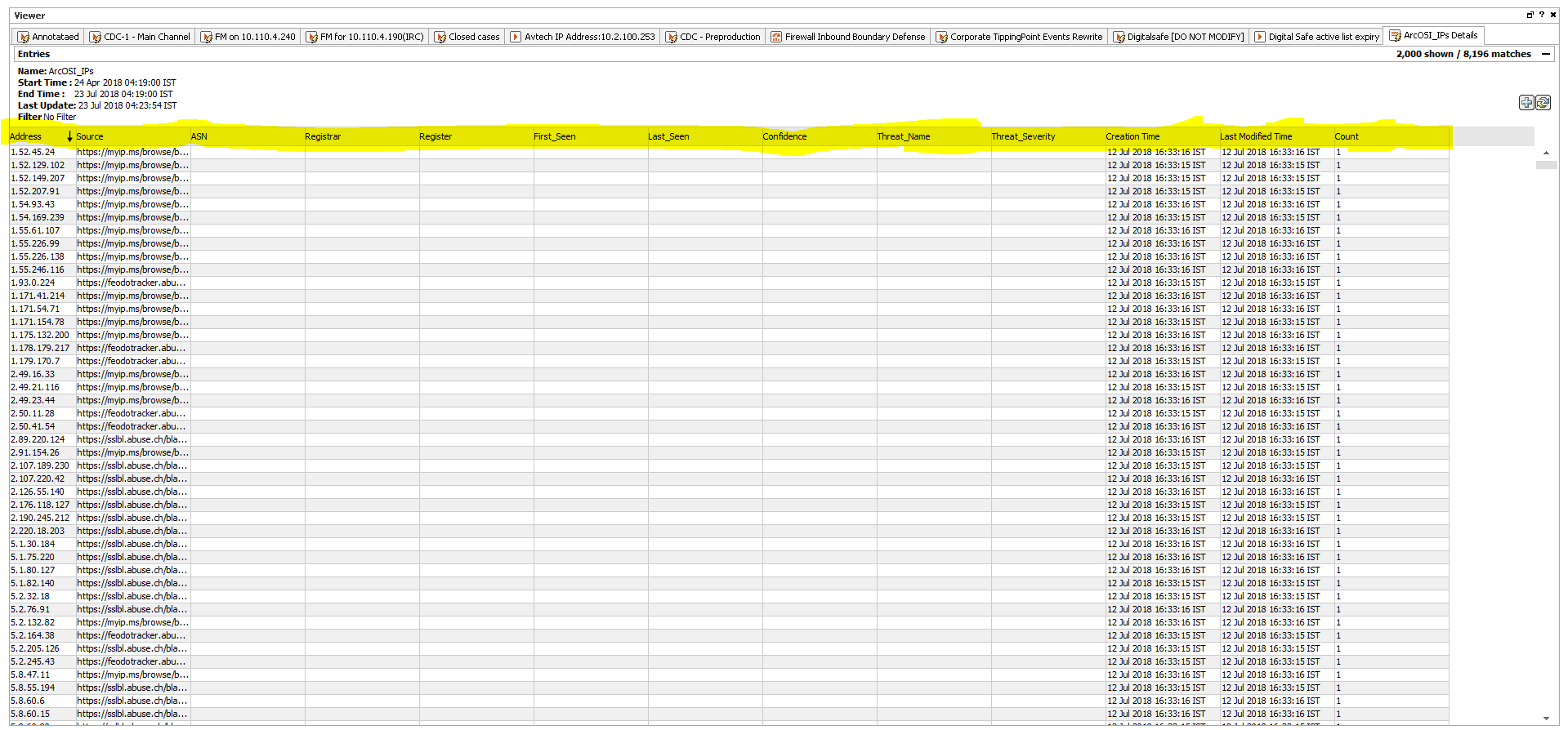
**1.2 Automated way to populate Active list**

Automated way is a more convient way to populate the Active list as the blacklist of IP should updated regularly.

In this documnet we will focus on Manual way to populate Active list.

**1.3 Manual way to populate Active list.**

Now we are having the consolidated list of blacklisted IP’s from different blacklist sources. We now need to update the consolidated list of blacklisted IP’s to the Active list (ArcOSI IP’s). In order to import the consolidated list of blacklisted IP’s to the Active list we need to match the fields of the Active list ArcOSI IP’s (PFB).



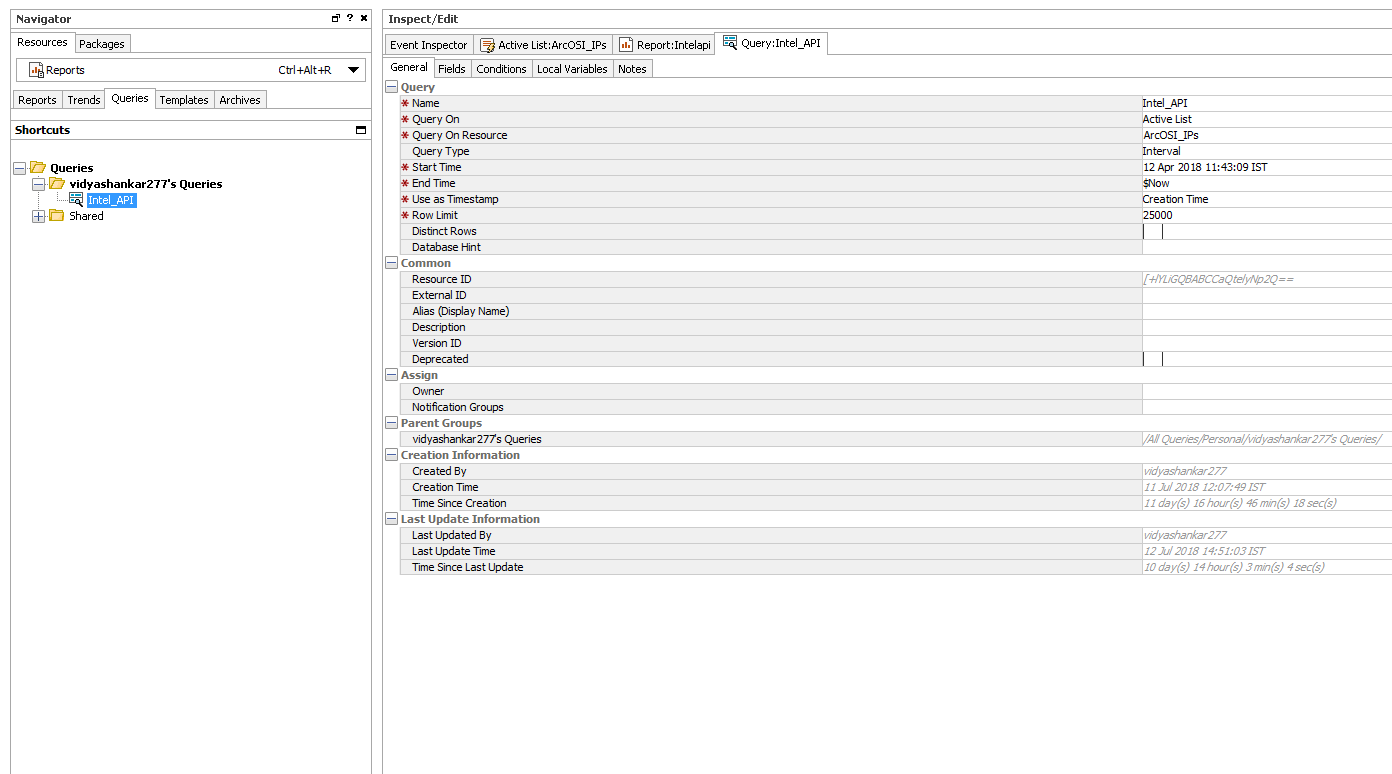
**Fig: Entries in Active list.**

To get the Active list ArcOSI IP’s with all the Field’s we need to create a report with appropriate query condition.

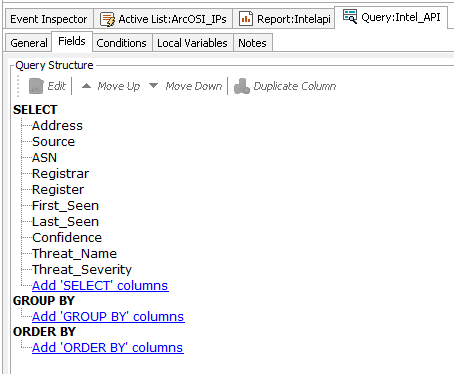
Chapter 2: Report and Query

## 2.1 Creating a report.

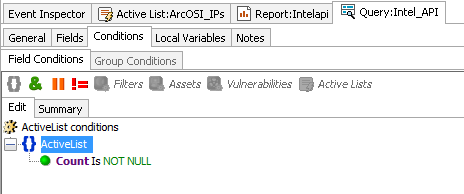
**Step1:** Go to the report resource in ArcSight and create a query with the appropriate query Field’s and Condition’s (PFB).



**Fig: General Attribute to create the Query**

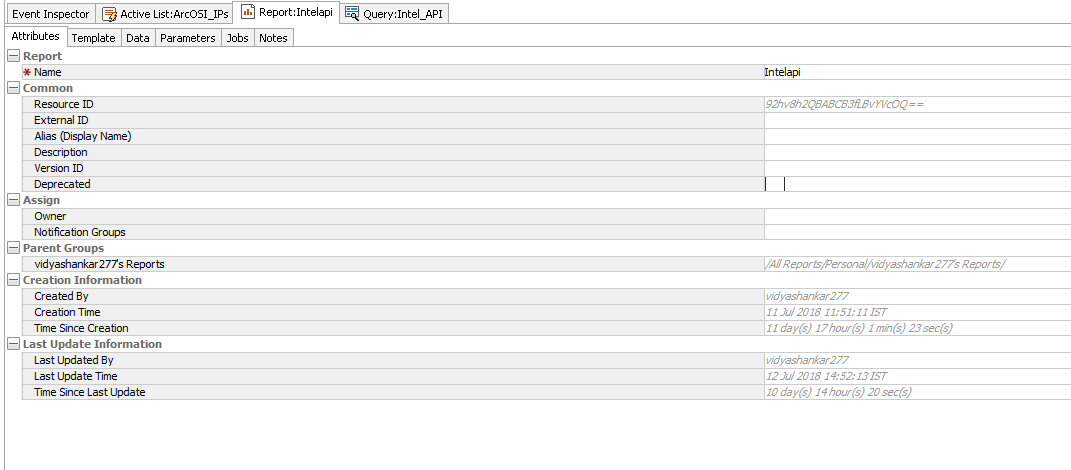


**Fig Appropriate Fields**

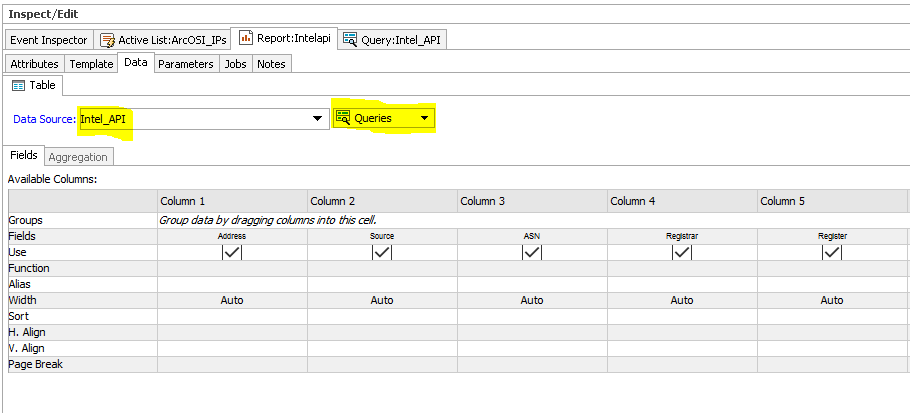


**Fig Appropriate Condition**

**Step2:** Then create a report and map the Data with this query.

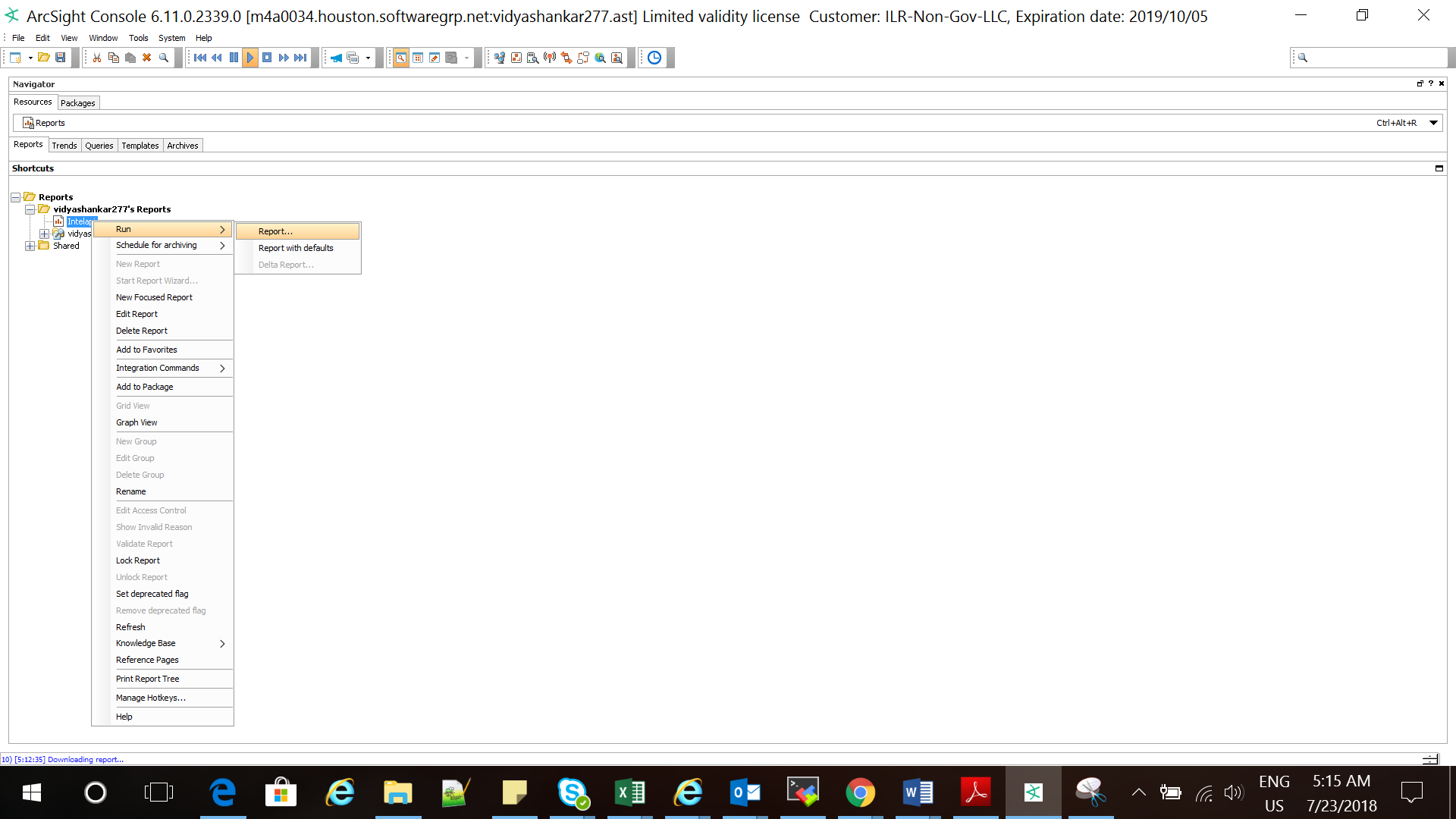


**Fig: General Attribute to create a report.**

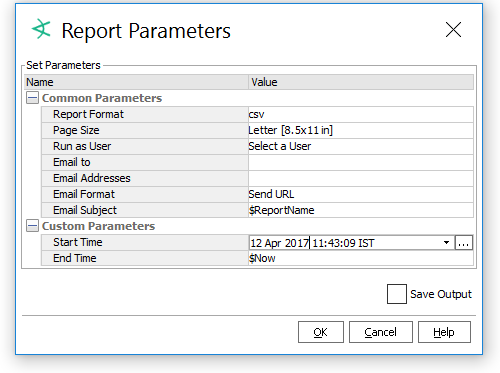


**Fig: Selecting the Data source.**

**Step3:** Run the report with below start time.

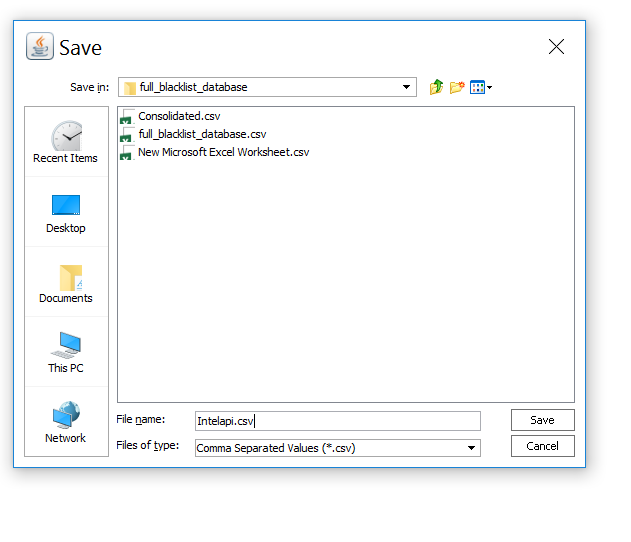


**Fig: Running the report.**



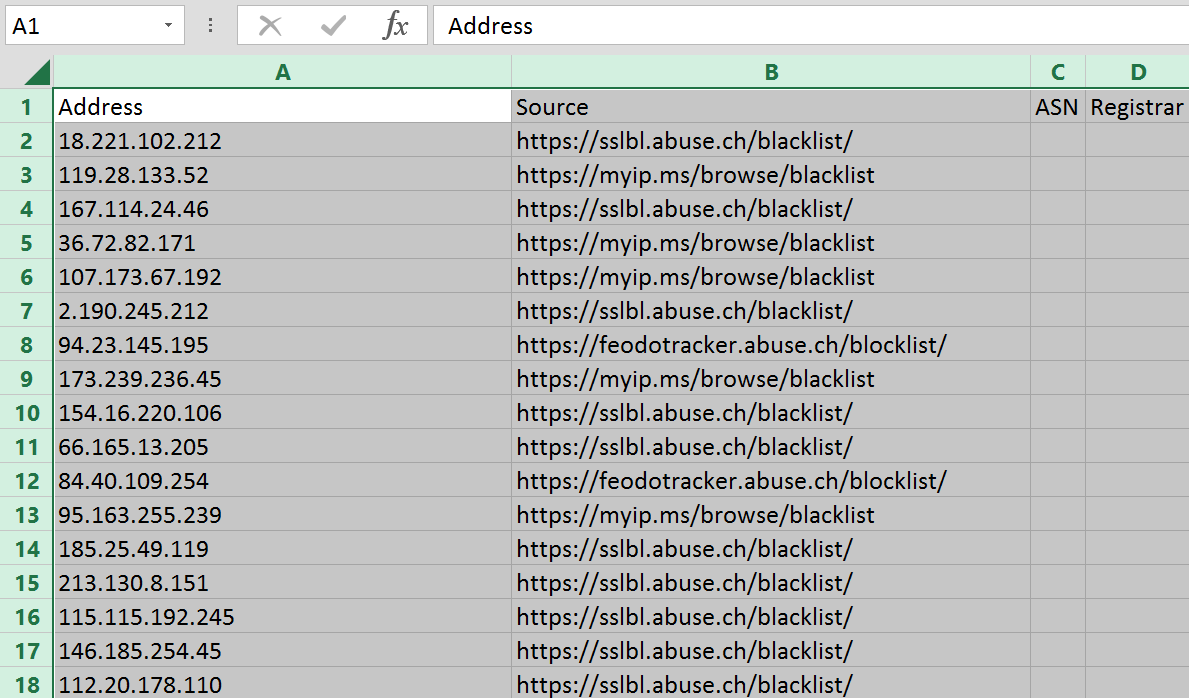
**Fig: Report Parameter.**

**Step4:** Save the report.



**Fig: Saving the report.**

Open the file and paste the consolidated IP’s and source that you have consolidated (consolidated list) to it.:

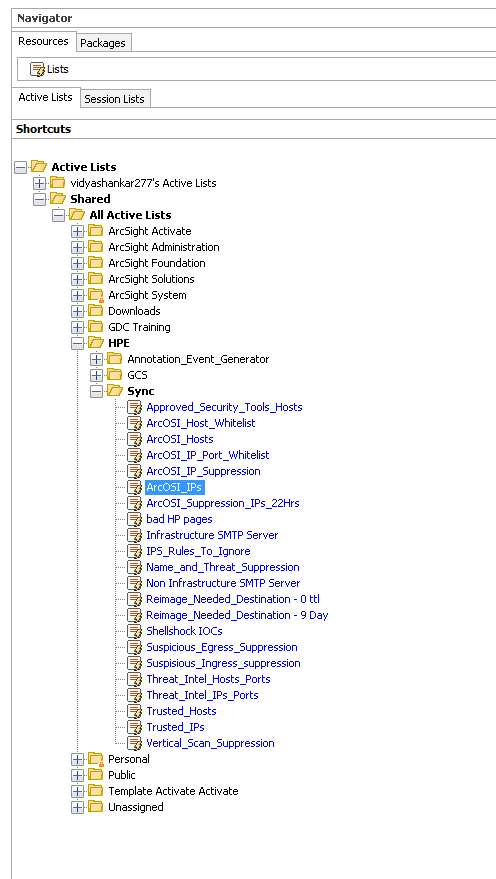


**Fig: File with consolidated blacklisted IP’s and Source.**

Save the file in .CSV format. Now we have consolidated list with the appropriate fields we just need to import this list to the Active list (ArcOSI IP’s).

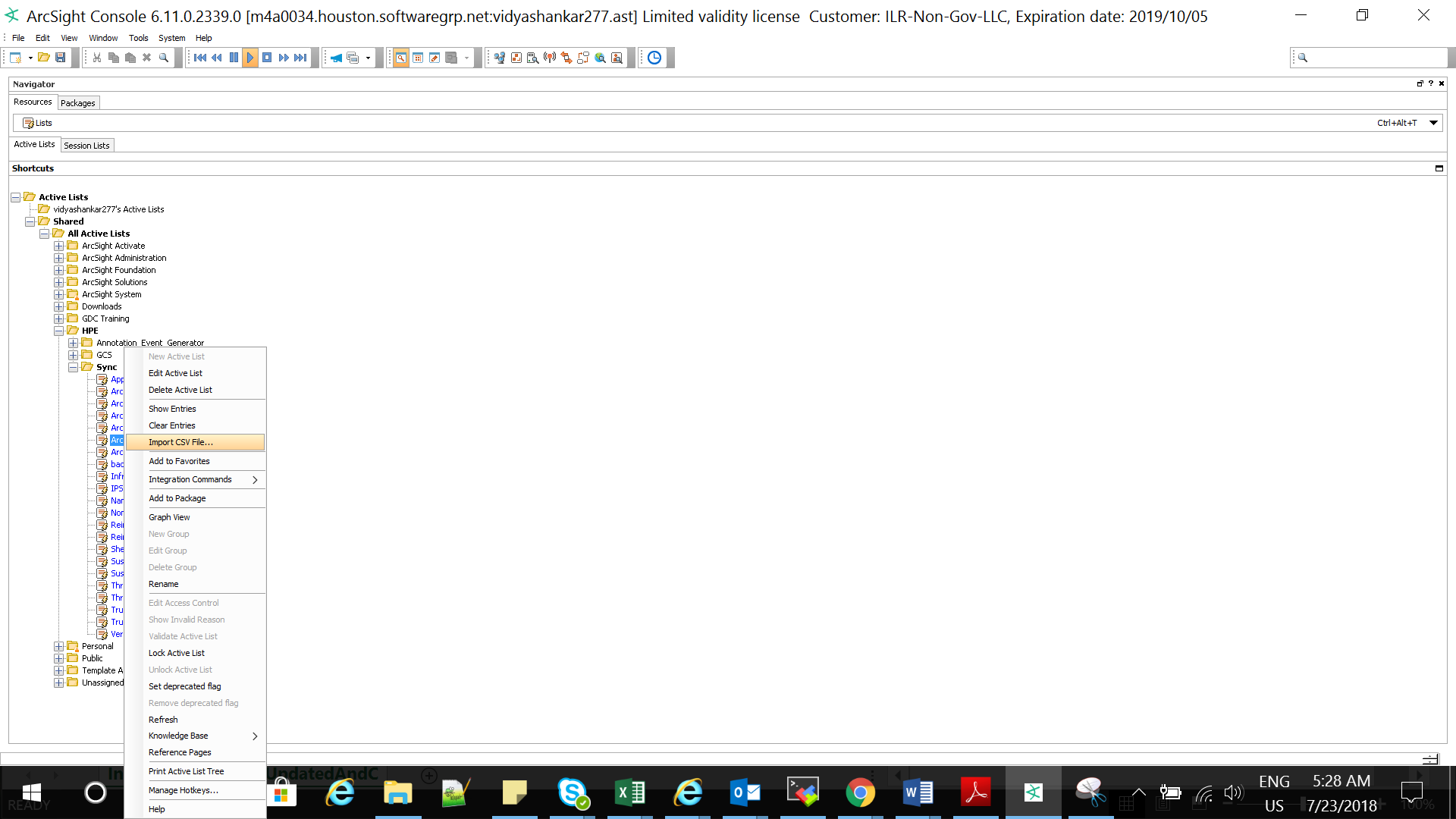
Chapter3: Importing CSV

**Step1:** Go to the Active list.



**Fig: ArcOSI IP’s Active list**

**Step2:** Right click on the Active list and import the Saved .csv file



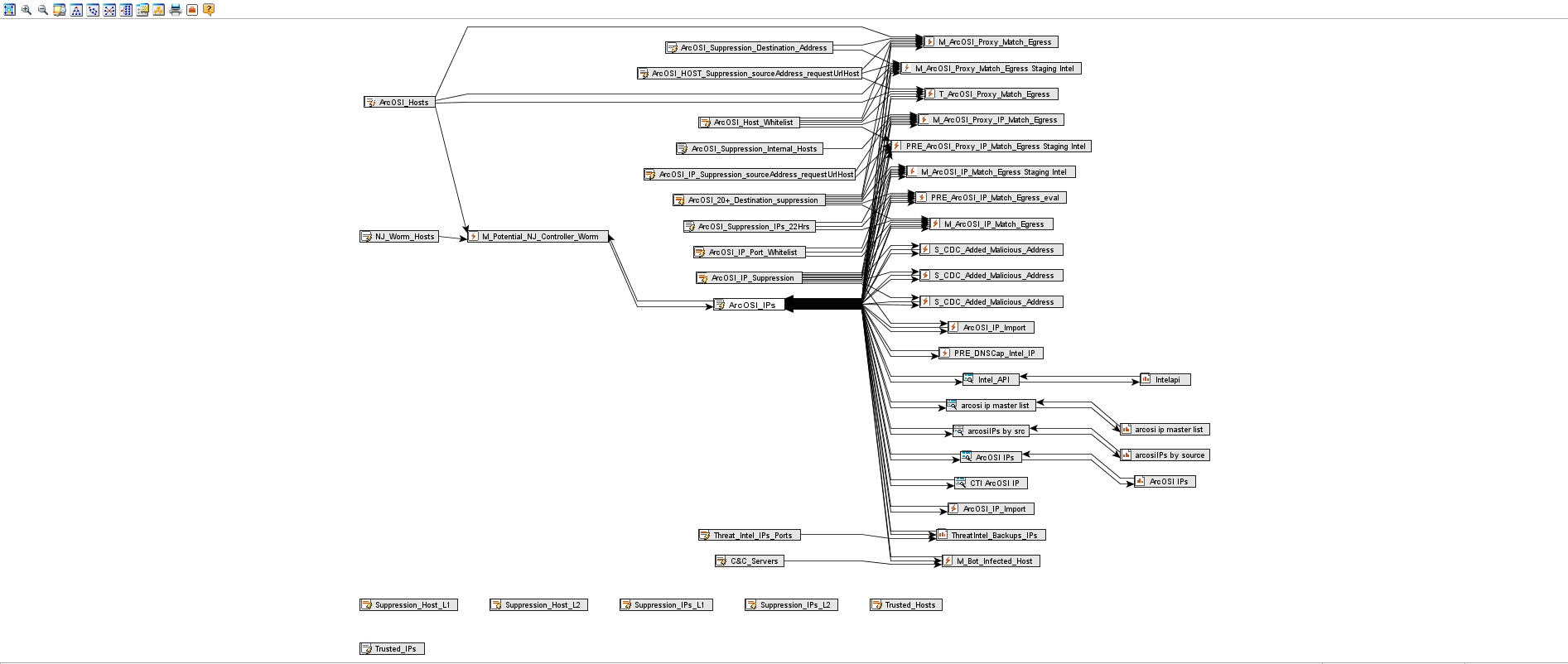
**Fig: Importing CSV File to Active list.**

Now we have the updated Active list of blacklisted IP’s.



**Fig: Populated Active list.**

This Active list has been included in the rule which detects when a system reach out to blacklisted IP that is present in the list.



**Fig: Graph view of Activelist ArcOSI IP’s.**

**3.1Advantages and Disadvantages**.

**Advantages:**

* Provides the mechanism to detect the system reaching out to the blacklisted IP’s.

**Disadvantages:**

* Consumes time to download, consolidate and update the Active list.

To overcome the Disadvantage we need to go for Automated way to populate the Active list.