FORCEPOINT

Forcepoint CASB and Okta

Integration Guide

Dlo Bagari
Mattia Maggioli
14 September 2020
Public

Version	Date	Author	Notes
0.1	07 January 2020	Dlo Bagari	First draft
0.2	13 January 2020	Mattia Maggioli	Review
0.3	15 January 2020	Dlo Bagari	Added auto active session termination
0.4	20 January 2020	Dlo Bagari	Updated package name
0.5	04 February 2020	Dlo Bagari	Updated mapping logic for risk score ranges
0.6	06 March 2020	Mattia Maggioli	Updated supported OS and Okta API
0.7	23 March 2020	Neelima Rai	Added troubleshooting chapter
0.8	14 September 2020	Mattia Maggioli	Minor updates

Summary

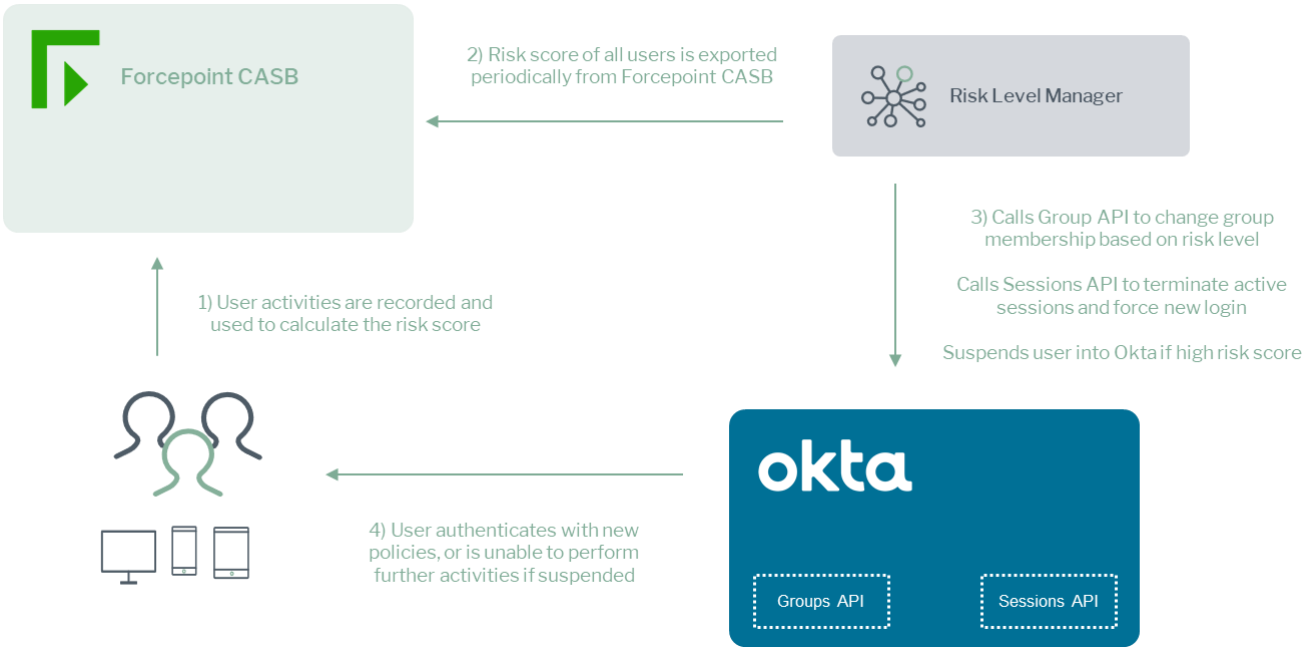
This guide provides step by step instructions to configure Forcepoint CASB and Okta to pass risk scores and to adjust authentication policies accordingly.

The code and instructions provided enable system administrators to automatically:

- Provide the risk level calculated by Forcepoint CASB for each user managed by Okta
- Adjust authentication policies applied by Okta to users based on their risk level
- Terminate active sessions in order to force re-authentication upon increase of risk score
- Terminate active sessions and suspend account of Okta users whose risk score reached a given threshold, to prevent any further action

This interoperability enables risk-adaptive authentication policies for Okta users based on the intelligence provided by Forcepoint CASB.

A description of the workflow between the components involved in this POC is depicted in this diagram:



Caveats

These implementation instructions are tested with the following product versions:

- Forcepoint CASB – 2019 R2
- Okta 2020.03.0

This interoperability uses the “Risk Score” of Forcepoint CASB for Okta users in order to change the login policies for the Okta users.

The following activities are out of the scope of this document and therefore left to the system administrator, as part of ordinary maintenance procedures to be put in place within the existing infrastructure:

- configuration of appropriate hygiene procedures to handle logs produced during any step of the solution workflow
- monitoring of the scripts, services and applications involved in the solution

Implementation

The solution described in this chapter requires the following files available at this link: https://frcpnt.com/casb-okta-latest

- fp-casb-exporter-okta-v1.tar.gz

The **fp-casb-exporter-okta-v1.tar.gz** contains all files necessary to setup and run all the services used by the Risk Level Manager to accomplish the interoperability between Forcepoint CASB and Okta:

- **Okta CASB Service**: extracts risk score from Forcepoint CASB for all users. Finds maximum risk score of each user across multiple accounts and orchestrates change of group membership for all accounts managed by Okta, so that risk-adaptive authentication polices are applied by Okta.
- **Okta CASB Timer Service**: monitors **Okta CASB Service** and runs it on a scheduled basis

We suggest deploying the **Risk Level Manager** on a CentOS 7.x or 8.x machine with at least 2 GB RAM and 20 GB of storage, the instructions provided in this document are based on this operating system and the following packages

- Python 3
- Python modules: requests, PyYAML

- The software packages and related dependencies are automatically installed by the **okta-casb-installer.sh** script provided inside the **fp-casb-exporter-okta-v1.tar.gz** file, which will execute the following commands as part of the deployment script of the Risk Level Manager:

```
sudo yum install -y https://centos7.iuscommunity.org/ius-release.rpm
sudo yum install -y python36u python36u-libs python36u-devel python36u-pip
sudo pip3 install PyYAML
sudo pip3 install requests
```

The machine hosting the Risk Level Manager will be referenced in the rest of this document with the name "**RLM-host**".

Step 1 – Create an API token in Okta

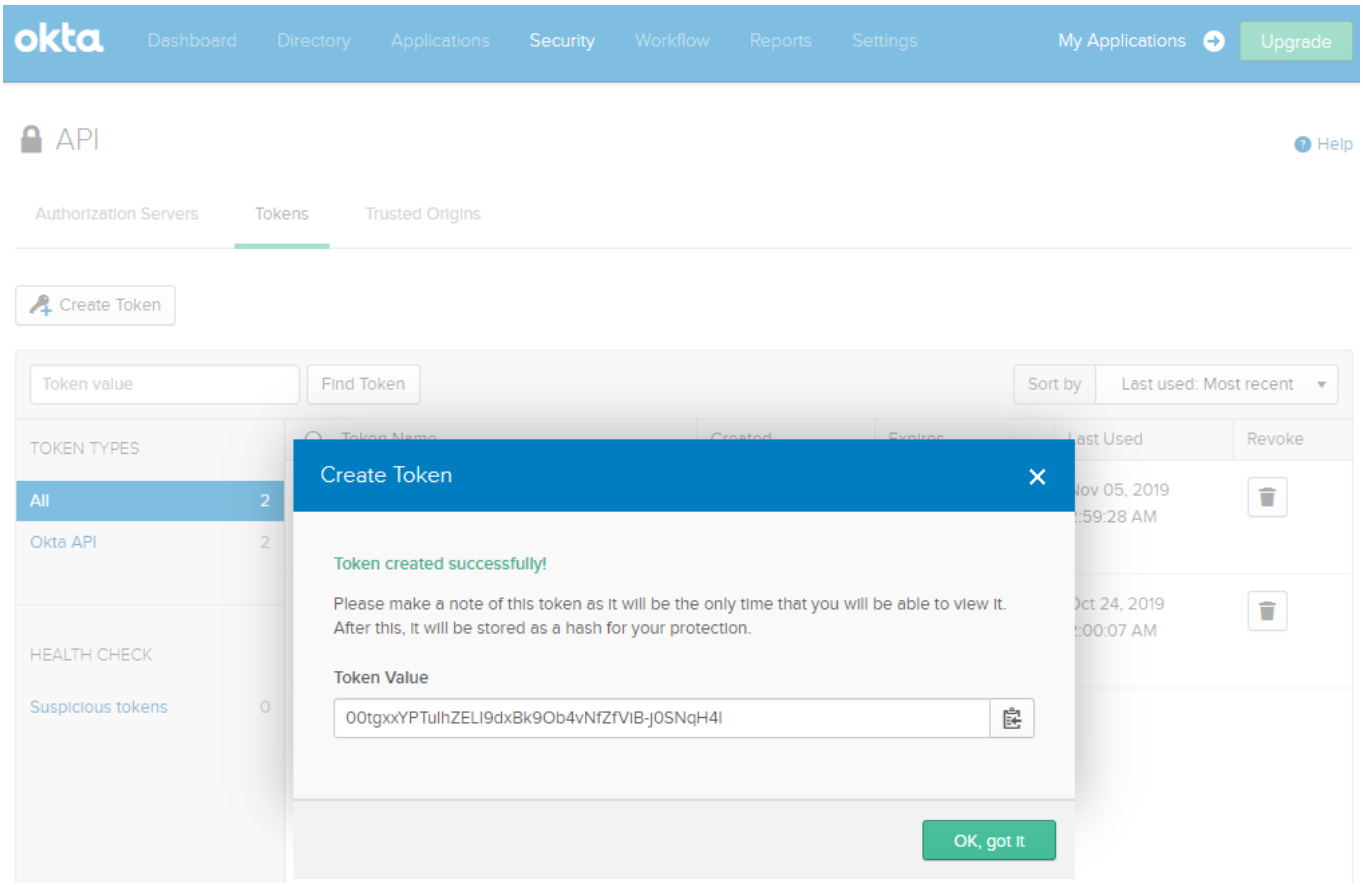
In order to connect and perform operations inside Okta, the Risk Level Manager requires a valid token. API tokens have the same permissions of the user who creates them, and the Risk Level Manager requires administrative access in order to perform its tasks.

It is recommended to create a new user with the minimum roles necessary to issue tokens and to perform the operations of the Risk Level Manager. Only the following **Administrator Roles** are necessary:

- **Read Only Administrator**
- **API Access Management Administrator**

Once a user is created, follow these steps to issue a new token under that user:

1. Sign into your Okta organization using the newly created administrator
2. Make sure you are using the **Classic UI**: you can check this setting in the top left corner of the Okta page, right above the Okta logo
3. Go to **Security > API** and click on the **Tokens** tab
4. Click **Create Token**, name your token and click **Create Token**
5. Save this **Token Value** in a secure location, as this is the only time it can be viewed.



Step 2 – Groups into Okta

Authentication steps applied to users authenticating through Okta are defined as **Sign On rules** configured into **Groups**, for example:

- Source IP of the user authenticating
- Okta Verify (either code or push notification)
- SMS authentication
- Voice Call Authentication
- External MFA apps
- Security question

A user authenticating through Okta will be challenged according to the policies configured via the user's group membership. To do this, create user groups to map the desired risk level policies to users.

A typical risk score mapping, group and policy configuration are as follows:

- Users with risk score in range 100 to 250 are mapped to **risk_level _1** group with standard

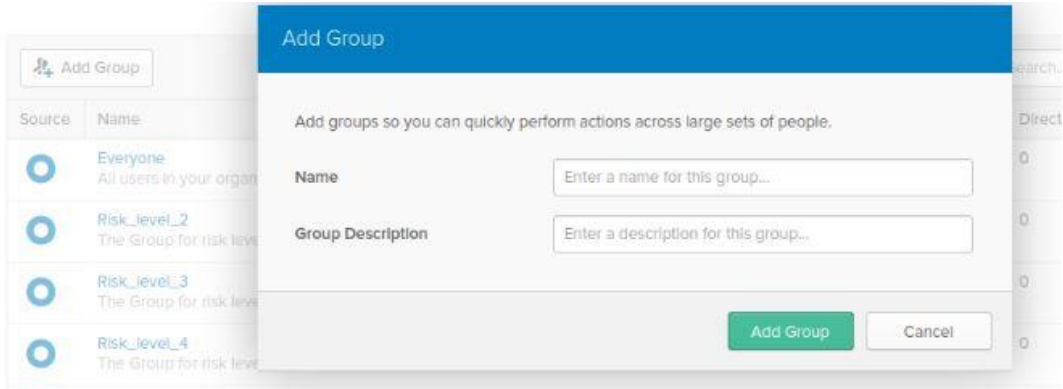
authentication policies (e.g. push notification)

- Users with risk score in range 251 to 500 are mapped to **risk_level 2** group which has more complex authentication policies (e.g. push notification and SMS authentication)
- Users with risk score equal and greater than 501 are mapped to **suspend** policy (it is a predefined policy in **Risk Level Manager**). Suspend users can't log in to Okta. Their group and app assignments are retained.

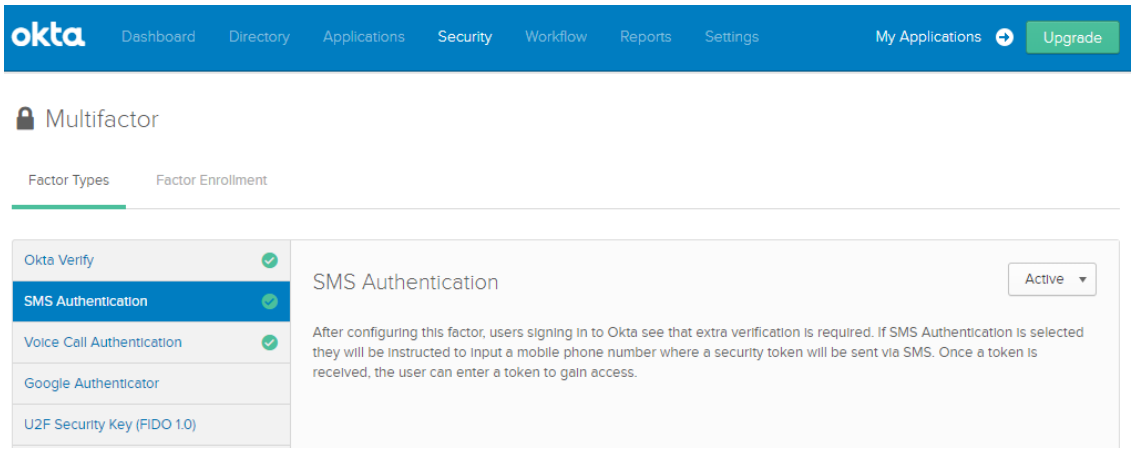
If multiple user groups with existing policies are already configured into Okta, then skip this part and go to **Step 3**.

In the following example, we create a new user group and assign a multifactor policy based on **SMS Authentication**:

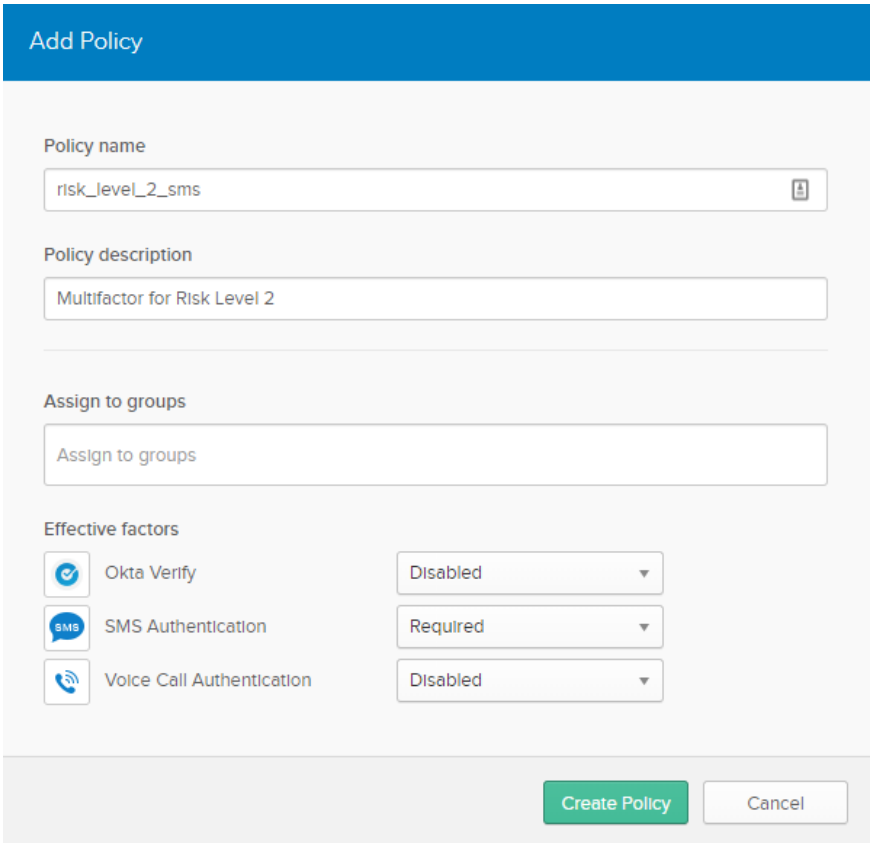
1. Go to **Directory > Groups**, click on **Add Group**
2. Name the new group and add a description, then click **Add Group** to create it



3. Go to **Security > Multifactor**, click **SMS Authentication** and then the drop-down menu so that the new factor is set to **Active**



4. Switch to the **Factor Enrollment** tab and click **Add Multifactor Policy**
5. Name your policy and enter a description, assign it to the group created for this risk level
6. Set the "**SMS Authentication**" to **Required** using the drop-down menu, set to **Disabled** any other factor not assigned to this policy. Once done click **Create Policy**.



7. Now click on the newly created policy and click **Add Rule**
8. Name the rule and set the conditions for the multi-factor enrollment

Multi-factor challenges must be enrolled in order to be applied to any further authentication attempt. It is recommended for all users to be pre-enrolled for any authentication method that may be required.

Alternatively, steps 7 and 8 above can also be used to configure multi-factor enrollment when the user is challenged for the first time. In this case it is suggested to configure the rule to only allow first time enrollment if the user is connecting from trusted networks (e.g. configure a network **Zone** in **Networks** so that trusted corporate IP ranges are known to Okta, and use the trusted **Zone** in a rule which allows multi-factor enrollment only when users authenticate from the corporate networks).

Repeat the steps above to create additional groups with the desired authentication policies to be mapped to a risk score range provided by Forcepoint CASB.

Step 3 – Configure the Risk Level Manager

All parameters required by the Risk Level Manager to operate its services are stored in a single file called **settings.yml**:

```
okta_token: <OKTA TOKEN>
okta_organization_url: <ORGANIZATION URL>
casb_login_password: <FORCEPOINT CASB PASSWORD>
casb_login_name: <FORCEPOINT CASB LOGIN NAME>
casb_ligin_form_action_url: https://my.skyfence.com/cm/j_spring_security_check
casb_users_csv_url: https://my.skyfence.com/cm/rs/0/human_risk/accounts/reports/csv?search=%2Brisk
application_directory: /var/okta_casb
logs_locations: /var/okta_casb/logs
database_path: /var/okta_casb/database.db

# Map each risk score range to one okta group or to a predefined policy.
# Predefined policies are:suspend
# suspend: suspended users Can't log in to Okta. Their group and app assignments are retained

risk_score_map:
  # from 100  to 250. mapped to the okta group Risk_level_1
  100-250: Risk_level_1
  # from 251 up to 500. mapped to the okta group Risk_level_2
  251-500: Risk_level_2
  # for 501 and above. Mapped to the 'suspend' predefined policy
  501+: suspend
terminate_user_session_after_policy_change: true
# Download the risk score from Forcepoint CASB every 'interval-time' minutes
interval_time: 10
```

The following table provides a description of every parameter in the **settings.yml** file:

Parameter	Description	Requires to be changed
okta_token	API token created in Okta as described in step 1 of this document	YES
okta_organization_url	Organization URL for Okta, used for authenticating users and for API calls by the Risk Level Manager and its services	YES
casb_login_password	Forcepoint CASB instance password	YES
casb_login_name	Forcepoint CASB instance login name	YES
casb_ligin_form_action_url	The callback function used by CASB UI for processing login credentials against the backend services of CASB	NO
casb_users_csv_url	The URL which allows users to download a .CSV file with the list of users and their risk score	NO
application_directory	Directory where the Risk Level Manager is stored, by default /var/okta_casb	NO

logs_locations	Directory where the Risk Level Manager logs are stored, by default /var/okta_casb/logs	NO
database_path	Directory where the Risk Level Manager database is stored, by default /var/okta_casb	NO
risk_score_map	Maps risk score ranges to Okta groups. e.g. To map the risk score from 100 to 150 to an Okta group named "Risk_level_1" 100-150: Risk_level_1 To consider all scores above a given value use the + sign e.g. To assign risk scores equal and greater than 500 to the predefined policy suspend use 500+: suspend	YES
terminate_user_session_after_policy_change	If set to true, terminates the user's active sessions upon change of risk score range, so that user is forced to log in again according to the authentication policies assigned to the new risk score range / Okta group.	NO
interval_time	To control how frequently risk score is downloaded from CASB and processed. Time is expressed in minutes.	NO

Step 4 – Installing Risk Level Manager

To set up the Risk Level Manager, proceed as follows:

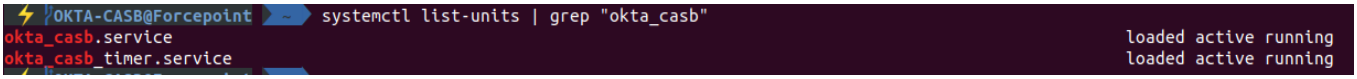
1. Login via SSH to the **RLM-host** and copy the **fp-casb-exporter-okta-v1.tar.gz** file into **/root** folder of the machine that will host the Risk Level Manager
2. Decompress the file using the command **tar -zxvf fp-casb-exporter-okta-v1.tar.gz**
3. Go into the **/root/ fp-casb-exporter-okta-v1** folder and edit **settings.yml** to update the value of the required parameters, change only the entries that are required to be changed according to the table in step 3
4. Make sure **installer.sh** is executable using the command **sudo chmod a+x okta-casb-installer.sh**
5. Install the Risk Level Manager using the command **sudo ./okta-casb-installer.sh**

   The installer script will read **settings.yml**, move the services to the **application_directory** and create two systemd services. The file **setings.yml** will then be moved to

application_directory: do not change the location of the file.

6. Once the installation is completed, reboot the machine
7. After reboot is completed, log into the machine and verify two services of the Risk Level Manager are running with the command

   systemctl list-units | grep okta_casb



If all services are running, the Risk Level Manager is operating normally and the interoperability between Forcepoint CASB and Okta is completed: the Risk Level Manager will automatically download users risk score from Forcepoint CASB and group memberships into Okta will be adjusted dynamically as soon as the risk score changes into a different range.

Troubleshooting

Follow these steps to identify issues impacting the normal operation of the integration described in this document.

Validate the prerequisites

Make sure the prerequisites described in the Summary chapter are all satisfied:

- Check the versions of Forcepoint CASB and Okta in use are listed as compatible

  Forcepoint CASB – 2019 R2
  Okta 2020.03.0

- Verify the integration component correctly operates on a clean CentOS 7.x or CentOS 8.x machine (**server version** only) with at least 2 GB RAM and 20 GB of storage
- User must be root to run the **okta-casb-installer.sh**
- Check the user can download the file with the below commands:

  yum install wget
  wget --content-disposition https://frcpnt.com/casb-okta-latest

Check network connectivity

Make sure firewalls or other security appliances are not impacting the network connectivity necessary for the operation of all components involved into this integration:

- Check Risk Level Manager has network connectivity to CASB: execute the following command on the **RLM-host** machine:

ping -c 2 example-casb.url

replacing the example URL/IP address with the current one used. Once done check the result is similar to below:

PING example-casb.url (10.10.120.12) 56(84) bytes of data.
64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=179 ms
64 bytes from 10.10.120.12 (10.10.120.12): icmp_seq=1 ttl=128 time=181 ms

Check dependencies are installed

Make sure the software dependencies needed by the components involved into this integration are installed:

- Check all dependencies are installed: execute the following command on **RLM-host**:

  python3 --version; pip3 --version; pip3 list 2> /dev/null | grep -e requests -e PyYAML

```
[root@localhost okta_casb]# python3 --version; pip3 --version; pip3 list 2> /dev/null | grep -e requests -e PyYAML
Python 3.6.8
pip 9.0.3 from /usr/lib/python3.6/site-packages (python 3.6)
PyYAML (5.3)
requests (2.23.0)
```

  Note: The software versions may change depending on latest upgrades.

- Check the last few lines after installation completion are similar to below:

```
Requirement already satisfied: requests in /usr/local/lib/python3.6/site-packages
Requirement already satisfied: idna<3,>=2.5 in /usr/local/lib/python3.6/site-packages (from requests)
Requirement already satisfied: urllib3!=1.25.0,!=1.25.1,<1.26,>=1.21.1 in /usr/local/lib/python3.6/site-packages
 (from requests)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.6/site-packages (from requests)
Requirement already satisfied: chardet<4,>=3.0.2 in /usr/local/lib/python3.6/site-packages (from requests)
Created symlink from /etc/systemd/system/multi-user.target.wants/okta_casb.service to /etc/systemd/system/okta_c
asb.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/okta_casb_timer.service to /etc/systemd/system/
okta_casb_timer.service.
```

Check all components are configured and running properly

Make sure the products and services involved into this integration are configured as expected and they are running:

- Check all components are configured and running as expected: Execute the below command:

  systemctl list-units | grep okta_casb

  and check the result is similar to below:

```
[root@localhost ~]# systemctl list-units | grep okta_casb
okta_casb.service
     loaded activating auto-restart read risk score from Forcepoint CASB and change okt
a login polices
okta_casb_timer.service
     loaded active     running      run timer service for okta_casb.service
```