



Netskope Security Cloud Adoption & Activation

Lab Guide

NETSKOPE CONFIDENTIAL

Version 23.11

Disclaimer

The contents of this course and each of the lessons and related materials, including handouts to participants, are subject to Netskope Copyright 2022.

This instructional program, including all materials provided herein, is provided without any guarantees from Netskope.

Netskope assumes no liability or legal action arising from the use or misuse of content or details contained herein.

This content may not be reproduced without the permission of Netskope.

Table of Contents

<i>Before you begin</i>	5
<i>Lab resources diagram.....</i>	5
<i>Lab Scenario</i>	6
<i>Lab A: Configure Cloud Exchange for log shipping</i>	7
Part 1 – Deploy Cloud Exchange	7
Part 2 – Set up log shipping	14
<i>Lab B: Installing Netskope Client in Identity Provider mode.....</i>	27
Part 1 – Install Netskope Client in identity provider mode	27
Part 2 – Verify the Netskope Client is tunneling traffic	29
<i>Lab C: Automating fingerprint uploading using a Netskope Virtual Appliance.....</i>	32
Part 1 – Register your on-premises virtual appliance.....	32
Part 2 – Create an empty fingerprint	34
Part 3 – Upload the fingerprint with a script	35
Part 4 – Configure a policy to block documents matching the fingerprint.....	38
Part 5 – Verify that the fingerprint-based policy is working.....	42
<i>Lab D: Browser-based Netskope Private Access (NPA).....</i>	45
Part 1 – Create NPA Publisher on the Netskope tenant	45
Part 2 – Review remote user authentication settings	49
Part 3 – Grant browser-based access to a private application	50
<i>Lab E: Cloud Explicit Proxy (CEP)</i>	56
Part 1 – Preparation	56
Part 2 – Review the tenant-side CEP configuration	58
Part 3 – Prepare a PAC file	60
Part 4 – Configure proxy settings using a PAC file	64
Part 5 – CEP validation	68
<i>Lab F: PAC file troubleshooting</i>	70

Part 1 – Detect coding errors in the PAC file	70
Part 2 – Add troubleshooting messages to the PAC file	72
Part 3 – Add context information to the troubleshooting message.....	73
Part 4 – Disable troubleshooting messages.....	75
<i>Lab G: Investigating with Netskope Advanced Analytics.....</i>	<i>76</i>
Part 1 – Review the user’s activities using Advanced Analytics.....	76
Part 2 – What other identities are being used in the environment by the same user?	80
Part 3 – What applications is the user accessing?	82
Part 4 – Which instances of the application is the user accessing?.....	84
Part 5 – Which activities is the user performing in these applications?.....	85
Part 6 – Create a filter for high-risk activities	86
Part 7 – What security actions were implemented to control this user’s activities?	87
Part 8 – Save the report as a widget.....	88

Before you begin

To participate in the Netskope Cloud Security Adoption and Activation Lab, you will need to:

- Obtain the NSCAA onboarding email with credentials and IP addresses.
- Download and install the Amazon WorkSpaces thick client on your computer

Note: If you are using a Windows computer, you can download either the 32-bit or 64-bit version.

- Test your Amazon WorkSpace credentials.
- Test your Netskope tenant credentials (which will be provided to you the day of the lab).

If you have an issue with those credentials, please send an email to: training@netskope.com

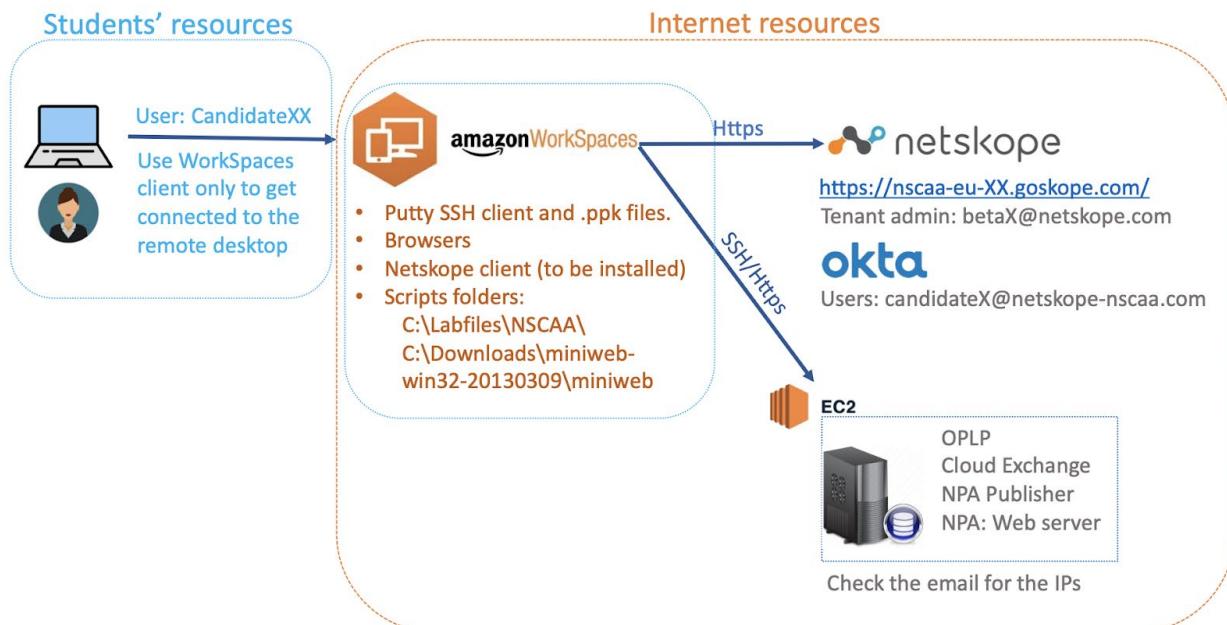
Note: Your Amazon WorkSpaces account will be of the form candidate{X}, where {X} is your student number. You will enter your student number to name different entities during the lab. For example, if you see the instruction to name your policy Policy{X}, and your student number is 4, you should name your policy Policy4.

During the lab, your Amazon WorkSpace will provide you with connectivity to all required elements to complete the lab.

The PuTTY SSH client will be used to connect from the WorkSpace to the Cloud Exchange server and Netskope virtual appliance (NS-VA, also often referred to as On-Premises Log Parser or OPLP, which is the most used role of the NS-VA).

During the lab, you will be asked to use specific browsers. These browsers have been made available in your Amazon WorkSpace.

Lab resources diagram



Lab Scenario

The Super Duper Cars and Trucks Company has recently installed Netskope as their security solution. Super Duper sells new and used cars and trucks and has just purchased Acme Loan Company so they can also offer to finance loans to their customers. With this recent addition, Super Duper now has access to and stores not only PII data but also financial data of their customers. Acme Loan Company runs a third-party endpoint protection product that conflicts with the Netskope client. They need an interim solution for the Acme Loan employees to connect to until their systems can be migrated to Netskope. Super Duper also shares cloud applications such as Salesforce with their partners and suppliers for their built-in collaboration and sharing capabilities. The company has some security concerns they need to address.

They need to:

- Centralize all logs to a SIEM server, including security logs collected from CrowdStrike.
- Install and authenticate all client deployments to their employees.
- Create marketing surveys in near real time, requiring new domains to host the surveys and landing pages.
- Deploy an OPLP virtual appliance to do fingerprinting locally because the CISO is reluctant to upload the company's most sensitive documents to Netskope.
- Implement a solution to provide external access to internal resources; suppliers for the company need to access certain internal company apps and resources, using their own devices to connect.
- Provide internet access to the Acme Loan employees who will not have the Netskope client installed on their computers for the interim; the CIO wants to use the Cloud Explicit Proxy access method until they can migrate the Acme Loan employees' systems to Netskope.
- Continually investigate any exposure or loss of customers' payment card data and other sensitive information.

Lab A: Configure Cloud Exchange for log shipping

The SOC team is centralizing all logs in a SIEM server. To include logs from the Netskope tenant, they need to deploy a Netskope Cloud Exchange server and set it up for log shipping.

During this lab, you will complete the following tasks:

- Deploy Cloud Exchange software containers.
- Configure the Cloud Log Shipper feature.

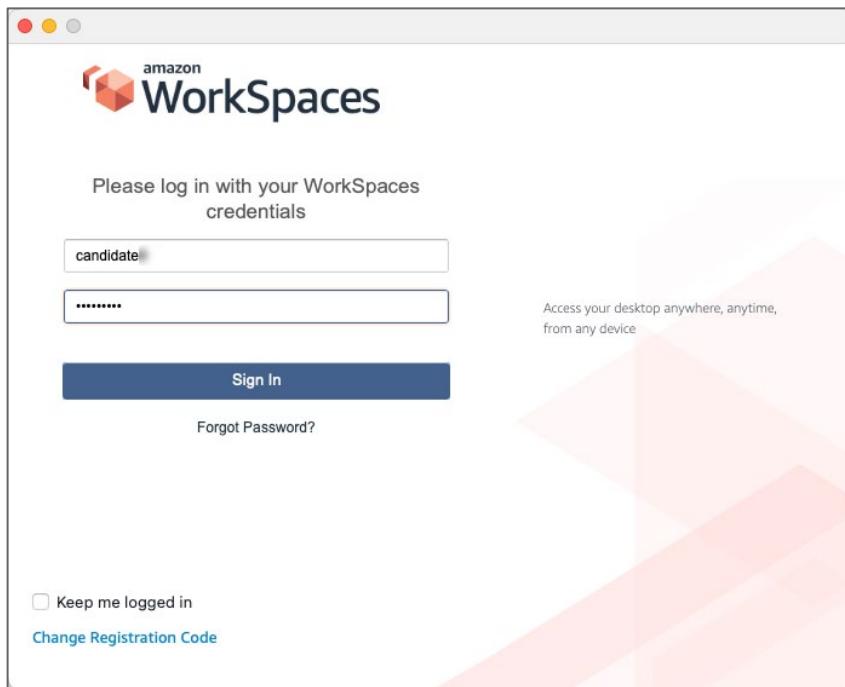
Your instructor has provisioned an EC2 instance with Ubuntu 18.04 on which you can install Netskope Cloud Exchange. You will also install the rsyslog server to act as a stand-in for a SIEM system.

Part 1 – Deploy Cloud Exchange

Task 1.1 – Check Availability of Docker

Netskope Cloud Exchange is provided as a set of containers that need **Docker** to run. The setup script uses Docker Compose (v1.x), a tool that simplifies deployment of multi-container applications. In this task, you will ensure that both Docker and Docker Compose are installed on the Ubuntu server.

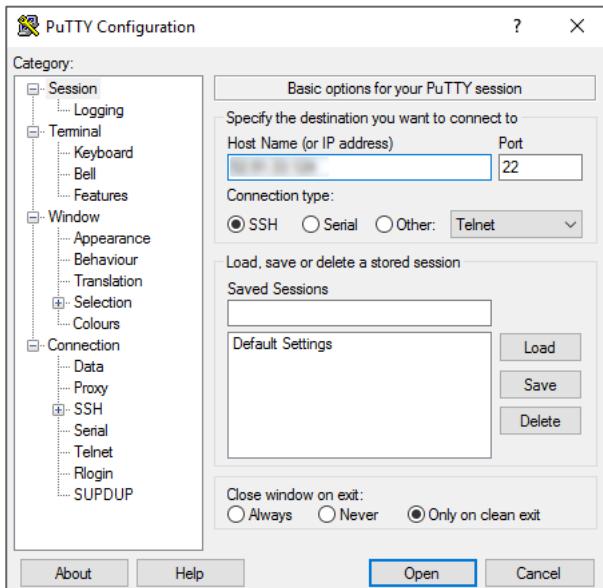
1. Open the Amazon WorkSpaces client and connect using the registration code, username, and password provided by your instructor.



Note: The first time you connect, the WorkSpace status will display as Resuming for a while.

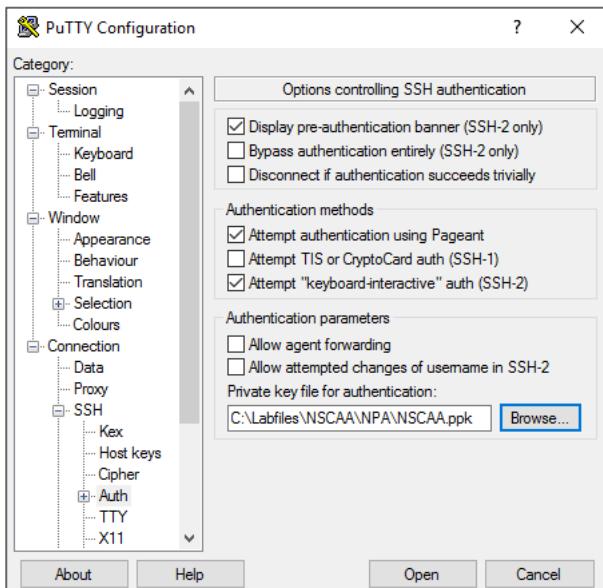
IMPORTANT: From this point on, perform all lab steps within your Amazon WorkSpace.

2. Run the PuTTY SSH client to connect to the virtual appliance.
3. In the **Host name (or IP address)** field enter the public IP address of the Cloud Exchange server provided by the instructor.



Note: The SSH server on this Ubuntu instance is configured to use public key authentication. To access the server, you will need to provide your private key, located in the lab files folder.

4. Select the private key to use for the SSH session:
 - a. In the side menu, navigate to **Connection > SSH > Auth**.
 - b. Click **Browse** and open the private key file C:\Labfiles\NSCAA\NPA\NSCAA.ppk.



Hint: If the C: drive is not available, type C:\ in the path field.

5. Click **Open**, then in the **PuTTY Security Alert** window click **Accept**.
6. To log in, type the username:
ubuntu

```
ubuntu@ip-:~$  
[+] login as: ubuntu  
[+] Authenticating with public key "imported-openssh-key"  
Last login: Sat Oct 12 17:08:12 from 10.0.2.15  
ubuntu@ip-:~$
```

- To check if prerequisite software git, python3, docker, and docker-compose are installed, use the command:

```
which git python3 docker docker-compose
```

```
ubuntu@ip-:~$ which git python3 docker docker-compose  
/usr/bin/git  
/usr/bin/python3  
/usr/bin/docker  
ubuntu@ip-:~$
```

Note: If the which command returns a path, the software has been installed. Notice that the command did not return path for docker-compose. You will update the Ubuntu server first and then install Docker Compose.

- To update software packages on the Ubuntu server, use the following commands:

```
sudo apt update
```

```
ubuntu@ip-:~$ sudo apt update  
Hit:1 http://us-west-2.ec2.archive.ubuntu.com/ubuntu bionic InRelease  
Hit:2 http://us-west-2.ec2.archive.ubuntu.com/ubuntu bionic-updates InRelease  
Hit:3 http://us-west-2.ec2.archive.ubuntu.com/ubuntu bionic-backports InRelease  
Fetched 90.2 kB in 1s (121 kB/s)  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
2 packages can be upgraded. Run 'apt list --upgradable' to see them.  
ubuntu@ip-:~$
```

```
sudo apt upgrade -y
```

```
ubuntu@ip-:~$ sudo apt upgrade -y  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
Calculating upgrade... Done  
The following packages were automatically installed and are no longer required:  
 libaio1 librados2 librbd1  
Use 'sudo apt autoremove' to remove them.  
The following packages have been kept back:  
 aws-neuron-dkms nvidia-fabricmanager-510  
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.  
ubuntu@ip-:~$
```

Note: Although the Ubuntu software repositories contain a package for Docker Compose, you should not use it. The version of Docker Compose in Ubuntu 18.04 repositories is too old and not compatible with Netskope Cloud Exchange installation scripts. You will download a newer version of Docker Compose as a precompiled binary.

- Download the Docker Compose binary using the following command (as a continuous line without breaks):

```
sudo curl -L  
"https://github.com/docker/compose/releases/download/1.29.2/docker-  
compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
```

```
ubuntu@ip-      :~$ sudo curl -L "https://github.com/docker/compose/releases/download/1.29.2/docker-  
compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose  
% Total    % Received % Xferd  Average Speed   Time     Time     Current  
          Dload  Upload Total Spent   Left  Speed  
  0     0     0     0    0     0      0 --:--:-- --:--:-- --:--:-- 0  
100 12.1M 100 12.1M    0     0  29.6M      0 --:--:-- --:--:-- 29.6M  
ubuntu@ip-      :~$
```

10. To grant the downloaded binary execution permissions for all users, type:

```
sudo chmod +x /usr/local/bin/docker-compose
```

11. To verify the installation, enter the following command:

```
docker-compose --version
```

```
ubuntu@ip-      :~$ sudo chmod +x /usr/local/bin/docker-compose  
ubuntu@ip-      :~$  
ubuntu@ip-      :~$ docker-compose --version  
docker-compose version 1.29.2, build 5becea4c  
ubuntu@ip-      :~$
```

Task 1.2 – Install Netskope Cloud Exchange

Management scripts and other necessary files to run Netskope Cloud Exchange are publicly available in a Github repository. You will clone the repository and run the scripts to download and start the containers comprising Netskope Cloud Exchange.

More information about installing Netskope Cloud Exchange is available at the link
<https://docs.netskope.com/en/install-cloud-exchange.html>

1. Clone the netskopeoss/ta_cloud_exchange Github repository into a dedicated folder using the following commands:

```
cd /opt  
sudo mkdir -p netskope  
cd netskope  
sudo git clone https://github.com/netskopeoss/ta_cloud_exchange  
cd ta_cloud_exchange
```

```
ubuntu@ip-      :~$ cd /opt/  
ubuntu@ip-      :/opt$ sudo mkdir netskope  
ubuntu@ip-      :/opt$ cd netskope/  
ubuntu@ip-      :/opt/netskope$ sudo git clone https://github.com/netskopeoss/ta_cloud_exchange  
Cloning into 'ta_cloud_exchange'...  
remote: Enumerating objects: 330, done.  
remote: Counting objects: 100% (160/160), done.  
remote: Compressing objects: 100% (79/79), done.  
remote: Total 330 (delta 126), reused 83 (delta 81), pack-reused 170  
Receiving objects: 100% (330/330), 3.10 MiB | 11.25 MiB/s, done.  
Resolving deltas: 100% (179/179), done.  
ubuntu@ip-      :/opt/netskope$ cd ta_cloud_exchange/  
ubuntu@ip-      :/opt/netskope/ta_cloud_exchange$
```

2. Execute the setup script:

```
sudo python3 ./setup
```

3. At the prompt Select the version you want to install, enter:

1

Note: 1 should correspond to CE v4-latest

4. At the prompt Are you using HTTP(s) proxy for outbound traffic? enter:

n

- When prompted, enter the name of your Netskope tenant, making sure you do *not* include the .goskope.com part.

Are you using HTTP(s) proxy for outbound traffic? [y/n]

> n

> Please enter the Netskope Tenant Name (Exclude .goskope.com)
(e.g. Enter 'demo' if Netskope Tenant URL is https://demo.goskope.com)

Please Enter 'test' if you do not have any Netskope tenant: nscaa-eu-

- After the setup script checks the prerequisites, complete the installation by providing the following answers to the prompts:

- a. Do you want to access CE over HTTP or HTTPS (HTTPS is recommended)?

Enter: HTTP

- b. Do you still want to access CE over HTTP?

Enter: v

Note: We use HTTP due to the specifics of the lab environment. In a production setting you should use HTTPS, unless you have specific reasons not to.

- c. Enter the port on which you want to access the Netskope CE UI (Default: "80")
Press ENTER to accept the default UI port of 80 TCP

```

Do you want to access CE over HTTP, or HTTPS (HTTPS is recommended)? HTTP ←
Accessing CE over HTTP is not recommended
Do you still want to access CE over HTTP? (y/yes) y ←
> Enter the port on which you want to access the Netskope CE UI (Current: "80"): ←
[P] Port 80 is available.

```

- d. Enter a JWT secret which will be used for signing authentication tokens:
Enter: secret
- e. Enter maintenance password...
Enter and confirm: netskope
- f. Do you want to enable TLSv1.2... (Default: "No")
Press ENTER to opt out of using TLSv1.2 for the CE UI.
- g. Do you want to provide custom CA certs?
Enter: n
- h. Do you want to take backup of .env file?
Enter: n

```

> Enter a JWT Secret which will be used for signing the authentication tokens: ←
> Enter maintenance password that will be used for RabbitMQ and MongoDB services (This password can be set only once): ←
> Confirm maintenance password: ←
> Do you want to enable TLSv1.2 along with TLSv1.3 for CE UI (Default: "No"): ←
> Do you want to provide custom CA certs? (y/n): n ←
> Do you want to take backup of .env file? [y/n]: n ←
Setup completed successfully...
Execute this command to start CE:
> ./start
Please re-run the setup script to update any parameter.

```

7. Start the Cloud Exchange server using the command:

```
sudo ./start
```

```

ubuntu@ip-      :/opt/netskope/ta_cloud_exchange$ sudo ./start
docker-compose version 1.29.2, build 5becea4c
docker-py version: 5.0.0
CPython version: 3.7.10
OpenSSL version: OpenSSL 1.1.0l 10 Sep 2019
Pulling rabbitmq-stats ... done
Pulling mongodb-primary ... done
Pulling core ... done
Pulling ui ... done
Creating network "ta_cloud_exchange_default" with the default driver
Creating ta_cloud_exchange_rabbitmq-stats_1 ... done
Creating ta_cloud_exchange_mongodb-primary_1 ... done
Creating ta_cloud_exchange_core_1 ... done
Creating ta_cloud_exchange_ui_1 ... done
ubuntu@ip-      :/opt/netskope/ta_cloud_exchange$ █

```

When all downloads are complete, the status "done" is displayed for each container.

8. After the container deployment process is finished and you are returned to the command line prompt, open a web browser window and navigate to:

<http://{your assigned Cloud Exchange public IP Address}>

9. Log in to Cloud Exchange with the following credentials:

username: admin

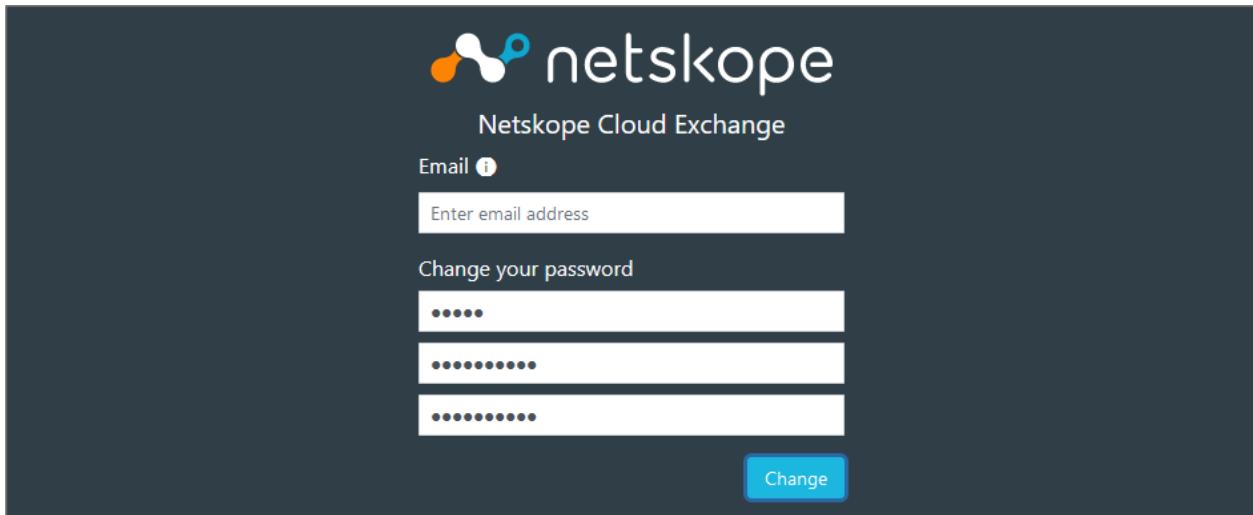
password: admin



10. When the license agreement is displayed, scroll to the bottom of the agreement and click **Accept**.

11. At the **Change your password** screen, perform the following:

- Leave the **Email** field blank
- Change the password from admin to **Password1!** (making sure to confirm the new password).
- Click **Change**.



12. In the **Confirm Action** window, click **Proceed**.

13. When the login screen is displayed again, log in with your new password:

username: admin

password: **Password1!**



Netskope Cloud Exchange is ready for use.

The image shows the "General Settings" page in the Netskope Cloud Exchange UI. On the left is a sidebar with "Settings" selected, showing options like General, Users, Plugins, Plugin Repository, and Netskope Tenants. The main area has tabs for General, Logs, Proxy, and Tasks Cleanup. Under General, there's a "Modules" section with toggle switches for Log Shipper, Ticket Orchestrator, Threat Exchange, User Risk Exchange, and Application Risk Exchange, all of which are turned off. There's also a "Software Version" section showing Core Version 4.1.0, UI Version 4.1.0, and Database Version 4.1.0. Finally, there's a "System Updates" section with a toggle switch for "Periodically check for updates" and a blue "Check For Update" button.

Part 2 – Set up log shipping

Task 2.1 – Install and configure a syslog server

You will deploy the rsyslog server on the same Ubuntu server to act as a stand-in for a SIEM platform. This is for simplicity and demo purposes. It is not recommended to install any additional software on the server acting as Netskope Cloud Exchange.

In a production environment the SIEM system is already provisioned, but you may need to set up a new connector to receive the incoming logs.

1. Go back to the SSH session established with the Netskope Cloud Exchange server.

2. To install rsyslog, type:

```
sudo apt install rsyslog -y
```

3. To edit the rsyslog configuration file, type:

```
sudo vim /etc/rsyslog.conf
```

```
ubuntu@ip-:~$ sudo apt install rsyslog -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
rsyslog is already the newest version (8.32.0-1ubuntu4.2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
ubuntu@ip-:~$ 
ubuntu@ip-:~$ sudo vim /etc/rsyslog.conf
```

4. Press the INSERT key on your keyboard to enter the editing mode.

5. To specify the protocol and port for incoming log messages:

- a. Remove # at the beginning of the line

```
module(load="imudp")
```

- b. Remove # at the beginning of the line

```
input(type="imudp" port "514")
```

6. Hit the ESC key, type

```
:wq
```

and press ENTER to save the configuration file.

```

# /etc/rsyslog.conf Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

;wa

```

You have configured rsyslog to receive log messages over UDP on port 514.

- For the new configuration to take effect, restart the rsyslog service with the command:

```
sudo systemctl restart rsyslog
```

```
ubuntu@ip- :~$ sudo systemctl restart rsyslog
ubuntu@ip- :~$
```

No output means that the service restarted without errors. If you see a warning or an error message, you may have made mistakes in the configuration file. Open the configuration again and check for typos or ask the instructor for assistance.

- To verify that the rsyslog server is listening on UDP port 514, type the command:

```
netstat -lnu
```

```
ubuntu@ip- :~$ netstat -lnu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
udp      0      0 127.0.0.53:53            0.0.0.0:*
udp      0      0 172.31.15.104:68          0.0.0.0:*
udp      0      0 0.0.0.0:111             0.0.0.0:*
udn      0      0 127.0.0.1:323            0.0.0.0:*
idp      0      0 0.0.0.0:514             0.0.0.0:*
udp      0      0 0.0.0.0:729             0.0.0.0:*
udp6     0      0 :::111                  :::*
udp6     0      0 :::1323                 :::*
udp6     0      0 :::514                  :::*
udp6     0      0 :::729                  :::*
ubuntu@ip- :~$
```

Syslog is now configured.

Task 2.2 – Configure the Cloud Exchange Log Shipper

- Open a web browser and navigate to the Netskope tenant assigned to you for this training.

2. Log in with the tenant credentials provided to you for this training.
3. Following the first login, change the initial password to Password1! and accept the Netskope Service Operation Policy.
4. On the Netskope tenant, click **Settings**, then navigate to **Tools > REST API v2**.
5. Ensure that **REST API Status** shows **Enabled**, then click **New Token**.

The screenshot shows the 'Tools > REST API v2' interface. On the left sidebar, 'REST API v2' is selected. In the main area, the 'REST API STATUS' section shows 'Enabled' with a green dot, 'GLOBAL RATE LIMIT' at '4 requests/second', and a link to 'API DOCUMENTATION'. Below this is a blue 'NEW TOKEN' button. Two orange arrows point to the 'Enabled' status and the 'NEW TOKEN' button respectively.

6. In the **Token name** field type, type CloudExchange{X}, where {X} is your student number.
7. In the **Expire in** field, type 12
8. Click **Add endpoint** and select `/api/v2/events/dataexport/events/alert`.

The screenshot shows the 'Create REST API Token' dialog. It has fields for 'TOKEN NAME' (CloudExchange) and 'EXPIRE IN' (12 Day(s)). Under 'SCOPE', there's a table with an 'ENDPOINT' column and a search bar above it. A modal window titled 'Search endpoints' is open, showing a list of endpoints with one selected: '/api/v2/events/dataexport/events/alert'.

9. Use the **Add endpoint** link to add all other endpoints containing dataexport:
 - `/api/v2/events/dataexport/events/application`
 - `/api/v2/events/dataexport/events/audit`
 - `/api/v2/events/dataexport/events/connection`
 - `/api/v2/events/dataexport/events/incident`

- /api/v2/events/dataexport/events/infrastructure
- /api/v2/events/dataexport/events/network
- /api/v2/events/dataexport/events/page
- /api/v2/events/dataexport/alerts/uba
- /api/v2/events/dataexport/alerts/securityassessment
- /api/v2/events/dataexport/alerts/quarantine
- /api/v2/events/dataexport/alerts/remediation
- /api/v2/events/dataexport/alerts/policy
- /api/v2/events/dataexport/alerts/malware
- /api/v2/events/dataexport/alerts/malsite
- /api/v2/events/dataexport/alerts/compromisedcredential
- /api/v2/events/dataexport/alerts/ctep
- /api/v2/events/dataexport/alerts/dlp
- /api/v2/events/dataexport/alerts/watchlist

Create REST API Token

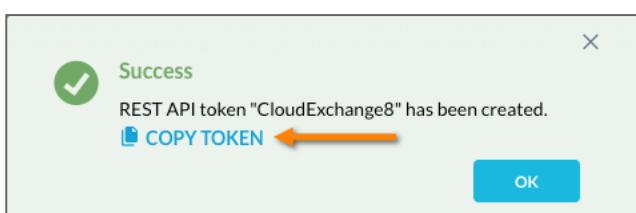
TOKEN NAME	EXPIRE IN	
CloudExchange	12 Day(s)	
SCOPE		
ADD ENDPOINT API DOCUMENTATION		
ENDPOINT	PRIVILEGE	
/api/v2/events/dataexport/events/alert	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/events/application	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/events/audit	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/events/connection	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/events/incident	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/events/infrastructure	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/events/network	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/events/page	<input checked="" type="radio"/> Read	
/api/v2/events/dataexport/alerts/uba	<input checked="" type="radio"/> Read	

[CANCEL](#) [SAVE](#)

10. Click **Save**.

*IMPORTANT: Make sure to click **COPY TOKEN** in the next step.*

11. In the **Success** message click **Copy token**.



12. Paste the copied token into a text editor.
13. Go back to your tenant and click **Ok** in the **Success** message.
14. Go back to the Netskope Cloud Exchange console and navigate to **Settings > General**.
15. Enable **Log Shipper**.

The screenshot shows the 'General Settings' page in the Netskope Cloud Exchange console. On the left, there's a sidebar with a logo and navigation links: 'Settings' (selected), 'General', 'Users', 'Log Shipper' (highlighted in blue), 'Plugins', 'Plugin Repository', and 'Netskope Tenants'. The main content area has a title 'General Settings' and a green banner at the top right stating 'Log Shipper module is Enabled' with a close button. Below the banner, there are tabs for 'General', 'Logs', 'Proxy', and 'Tasks Cleanup'. Under the 'General' tab, there's a section titled 'Modules' containing five toggle switches: 'Log Shipper' (which is orange and turned on), 'Ticket Orchestrator' (off), 'Threat Exchange' (off), 'User Risk Exchange' (off), and 'Application Risk Exchange' (off). The 'Log Shipper' switch is highlighted with an orange border.

16. Navigate to **Settings > Netskope Tenants**.
17. Click **Add Tenant** and enter the following parameters:

Name	Candidate{X}, where {X} is your student number
Tenant Name	Your Netskope tenant name without the .goskope.com part
V1 API Token	Leave blank
V2 API Token	Paste the V2 API token you created [CloudExchangeX]
Alerts Filter	Leave the default selection
Initial Range (in days)	7

Note: Initial Range defines the number of days required to pull data for the initial run.

Add Tenant

Name <small>i</small>	<input type="text" value="Candidate"/>
Tenant Name <small>i</small>	<input type="text" value="nscaa-eu-"/>
V1 API Token (Optional) <small>i</small>	<input type="text" value="XXXXXXXXXXXXXXXXXXXXXX"/>
V2 API Token <small>i</small>	<input type="text" value="XXXXXXXXXXXXXXXXXXXXXX"/>
Alerts Filter <small>i</small>	<input type="checkbox"/> Compromised Credential <small>x</small> <input type="checkbox"/> Policy <small>x</small> <input type="checkbox"/> Malsite <small>x</small> <input type="checkbox"/> Malware <small>x</small> <input type="checkbox"/> DLP <small>x</small> <input type="checkbox"/> Security Assessment <small>x</small> <input type="checkbox"/> Watchlist <small>x</small> <input type="checkbox"/> Quarantine <small>x</small> <input type="checkbox"/> Remediation <small>x</small> <input type="checkbox"/> UBA <small>x</small>
Initial Range (in days) <small>i</small>	<input type="text" value="7"/>
<input type="checkbox"/> Use System Proxy <small>i</small>	
<input type="button" value="Cancel"/>	<input type="button" value="Save"/>

18. Click **Save**.

19. Verify that the tenant is listed in the **Configured Netskope Tenants** section.

Configured Netskope Tenants				
Name	Tenant Name	Poll Interval	Initial Range (in days)	Action
Candidate	nscaa-eu-	30 Seconds	7	

20. Navigate to **Settings > Plugins**.

21. From the **Category** drop-down menu, select **CLS**.

*Note: Plugins marked as **CLS**, **CTO**, **CTE**, **URE**, and **ARE** correspond to the Log Shipper, Ticket Orchestrator, Threat Exchange, User Risk Exchange, and Application Risk Exchange features, respectively.*

22. Click the **Netskope v{x.y.z} (CLS)** plugin.

The screenshot shows the 'Plugins' section of a software interface. On the left is a sidebar with 'Settings' and 'Log Shipper' sections, and 'Plugins' is currently selected. The main area is titled 'Plugins' and contains three items:

- Syslog for CE v1.0.0 (CLS)
- Netskope WebTx v1.0.0 (CLS)
- Netskope v1.0.0 (CLS) - This item is highlighted with an orange box.

At the top, there are search and filter options. A dropdown menu labeled 'Category' is set to 'CLS', which is also highlighted with an orange box.

23. Configure the **Basic Information** using the following parameters:

Configuration Name	Candidate{X} NS, where {X} is your student number
Tenant	Candidate{X}

24. Click **Next**.

The screenshot shows the configuration dialog for the 'Netskope v1.0.0' plugin. The title bar says 'Netskope v1.0.0' with 'Cancel' and 'Save' buttons. Below it is a descriptive text: 'This plugin is used to fetch alerts and events from Netskope.' The main area is titled '1 Basic Information'.

Configuration Name: Candidate NS

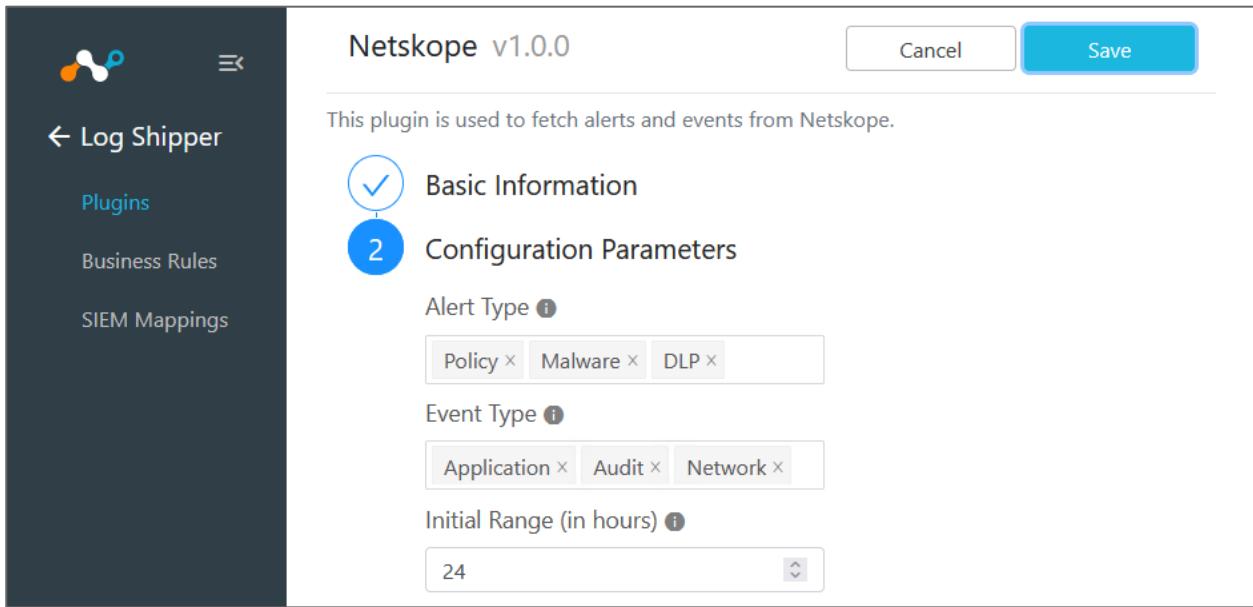
Tenant: Candidate

At the bottom is a 'Next' button.

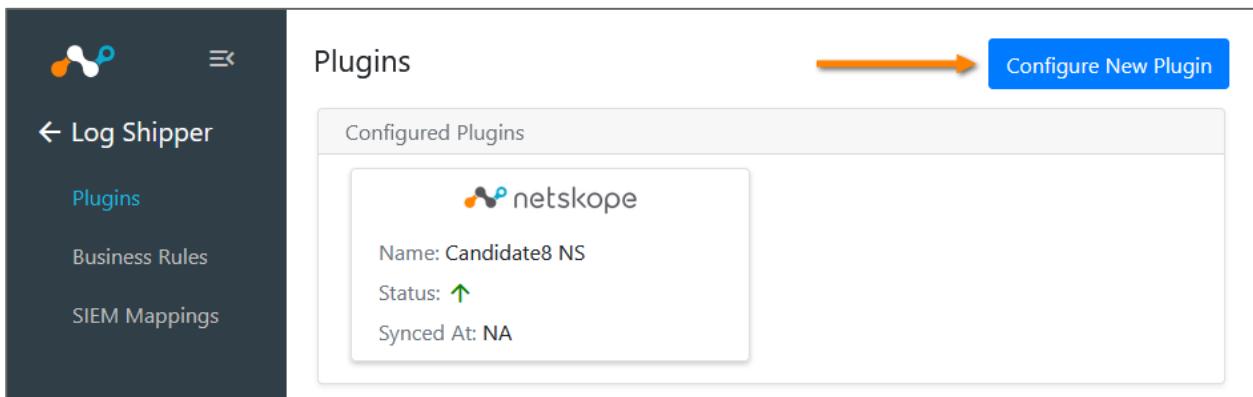
25. Configure records to be shipped from the Netskope tenant under **Configuration Parameters**:

Alert Type	Policy, Malware, DLP
Event Type	Application, Audit, Network
Initial Range (in hours)	24

26. Click **Save**.



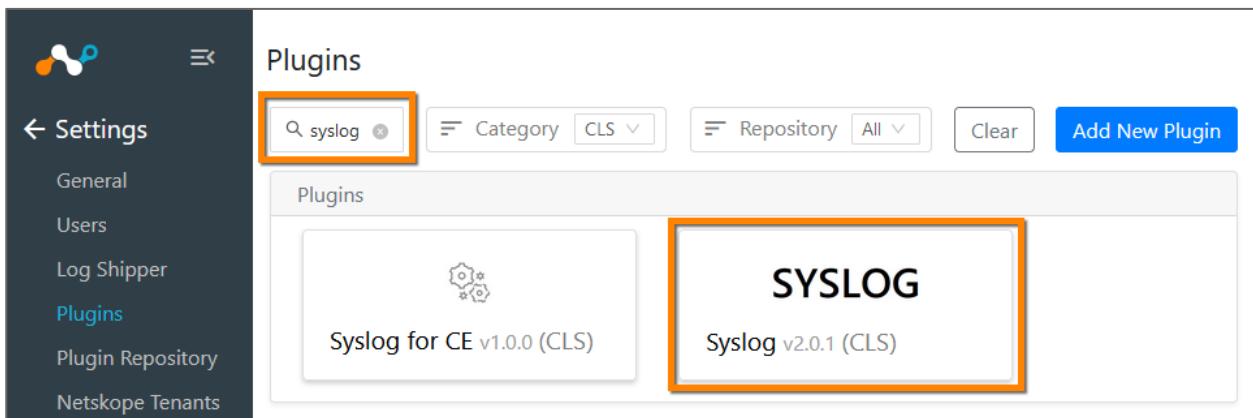
27. Verify that the plugin is listed in the **Configured Plugins** section and its **Status** is **Up**.



28. Click **Configure New Plugin**.

29. Find the **Syslog v{x.y.z} (CLS)** plugin and click it.

Hint: Type sysLog in the search field above the plugins to narrow down the list.



30. Enter the **Basic Information** using the following parameters:

Configuration Name	Candidate{X} Syslog, where {X} is your student number
Mapping	Syslog Default Mappings
Transform the raw logs	Enabled

The screenshot shows the 'Log Shipper' interface with the 'Syslog v2.0.1' configuration screen. On the left sidebar, there are links for 'Log Shipper', 'Plugins' (which is selected), 'Business Rules', and 'SIEM Mappings'. The main panel has a heading 'Basic Information' with a step indicator '1'. It contains fields for 'Configuration Name' (set to 'Candidate Syslog'), 'Mapping' (set to 'Syslog Default Mappings'), and two toggle switches: 'Transform the raw logs' (selected) and 'Use System Proxy' (disabled). A 'Next' button is at the bottom.

31. Click **Next**, then enter the **Configuration Parameters** using the following values:

Syslog Server	Cloud Exchange server public IP
Syslog Format	CEF
Syslog Protocol	UDP
Syslog Port	514
Syslog Certificate	Leave blank
Log Source Identifier	netskopece

32. Click **Save**.
33. Ensure both plugins are listed in the **Configured Plugins** section and their **Status** is **Up**.

Configured Plugins	
netskope Name: Candidate NS Status: Up Synced At: NA	SYSLOG Name: Candidate Syslog Status: Up Synced At: NA

34. In the left menu under **Log Shipper**, select **SIEM Mappings**.
35. Click **Add SIEM Mapping** and configure the mapping with the following parameters:

Source Configuration	Candidate{X} NS, where {X} is your student number
Destination Configuration	Candidate{X} Syslog, where {X} is your student number
Business Rule	All

Create SIEM Mapping

Source Configuration

Candidate NS

Destination Configuration

Candidate Syslog

Business Rule ⓘ

All

Save

Cancel

36. Click **Save** and verify that the mapping is listed in the **SIEM Mappings** section.

Rule	Folder Path	Source Configuration	Destination Configuration	Total Logs Sent	Total WebTx Sent	Actions
All	-	Candidate NS	Candidate Syslog	-	-	

Note: In the lab environment you can ignore the warning at the top of the page. In a production environment you should size your Cloud Exchange server to match the expected workload.

Task 2.3 – Validate Logs

1. Go back to the SSH session established to your Cloud Exchange server.
2. To verify that syslog messages are coming from the Netskope tenant, type:

```
grep Netskope /var/log/syslog | tail -n 3
```

Hint: Look for the Netskope name at the beginning of the messages.

```
ubuntu@ip-10-10-10-10:~$ grep Netskope /var/log/syslog | tail -n 3
netskopece CEF: 0|Netskope|nscaa.eu|NULL|audit|NULL|Medium|auditLogEvent=Logout Successful auditType=admin_audit_logs suser=candidate@nscaa-training.com timestamp= 569
netskopece CEF: 0|Netskope|nscaa.eu|NULL|audit|NULL|Medium|auditLogEvent=Login Successful auditType=admin_audit_logs suser=candidate@nscaa-training.com timestamp= 592
netskopece CEF: 0|Netskope|nscaa.eu|NULL|audit|NULL|Medium|auditLogEvent=Created REST API token auditType=admin_audit_logs suser=candidate@nscaa-training.com timestamp= 686
```

Note: At this point there are no traffic events or alerts in the tenant, but you should see audit events about your actions in the tenant: login, create token, etc. You can revisit this command after completing the next lab.

Lab Complete

Lab B: Installing Netskope Client in Identity Provider mode

This lab will showcase the installation of Netskope Client in Identity Provider (IdP) mode.

Scenario

Super Duper Cars and Trucks uses Okta as their identity provider. To ensure that the policies are applied correctly when the users' traffic is steered by the Netskope client, you will install the Netskope client in the Identity Provider mode.

Lab Tasks

During this lab, you will complete the following tasks:

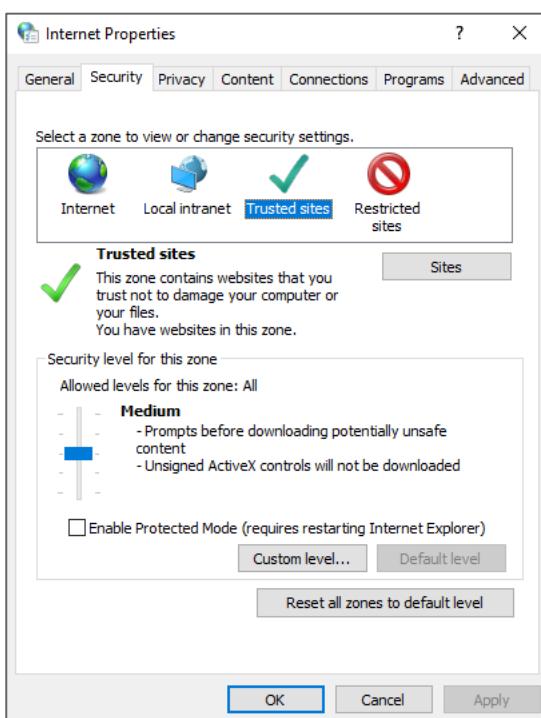
- Install the Netskope Client in Identity Provider mode.
- Verify installation.

Part 1 – Install Netskope Client in identity provider mode

To properly enroll your Netskope client with Okta as identity provider, you must allow JavaScript for the Okta domains as well as the Netskope tenant authentication URL. Too strict Internet security settings for these domains will prevent the enrollment of the client.

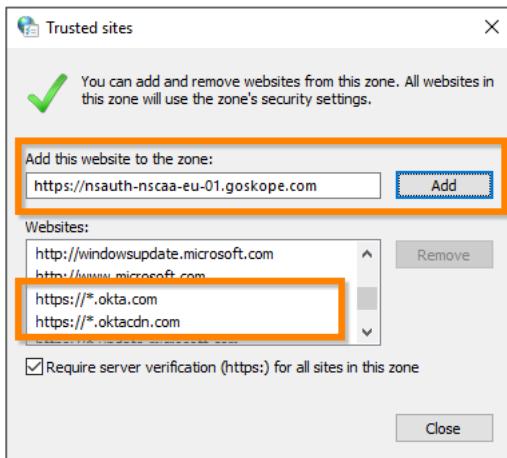
Task 1.1 – Add Okta to trusted sites

1. Click **Start**, type **internet** and choose **Internet Options**.
2. On the **Security** tab, select **Trusted sites** and click **Sites**.



3. Add the following URLs to the list of trusted websites:

- https://*.okta.com
- https://*.oktacdn.com
- <https://nsauth-{your tenant URL}>



- Click **Close** and then click **OK** to save the settings.

Task 1.2 – Install Netskope Client

- Open a web browser and download the Netskope client installer from your tenant by navigating to <https://download.goskope.com/dlr/win/get>
- Open a regular (non-admin) command prompt window and change to the Downloads folder by typing:

```
cd Downloads
```

- Install Netskope client with the following command (as one line without breaks):

```
msiexec /i NSClient.msi tenant={your tenant name} domain={your tenant domain} mode=peruserconfig installmode=idp
```

Hint: Your tenant name is the lowest level domain in your tenant URL, from the left to the first dot. The rest after the dot is your tenant domain.

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

D:\Users\student1>cd Downloads

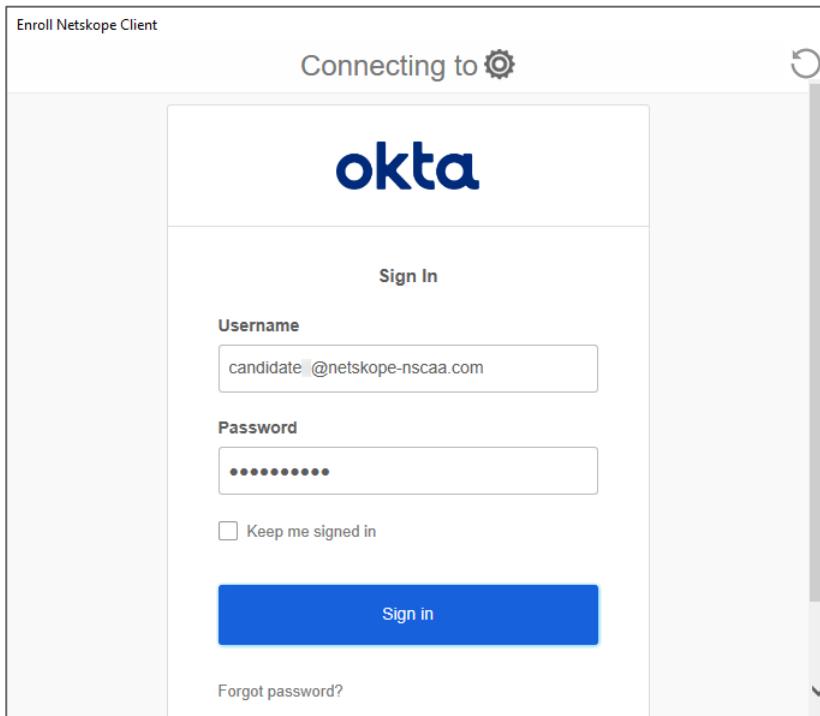
D:\Users\student1>msiexec /i NSClient.msi tenant=nscaa domain=goskope.com mode=peruserconfig installmode=idp
```

Note: When installing the Netskope Client on a VDI host, disable automatic updates with the parameter autoupdate=off. For non-VDI hosts, don't use autoupdate=off and manage updates with the client configuration settings in the tenant instead.

- When prompted, authenticate using your Okta credentials:

Username: candidate{X}@netskope-nscaa.com (where {X} is your student number)

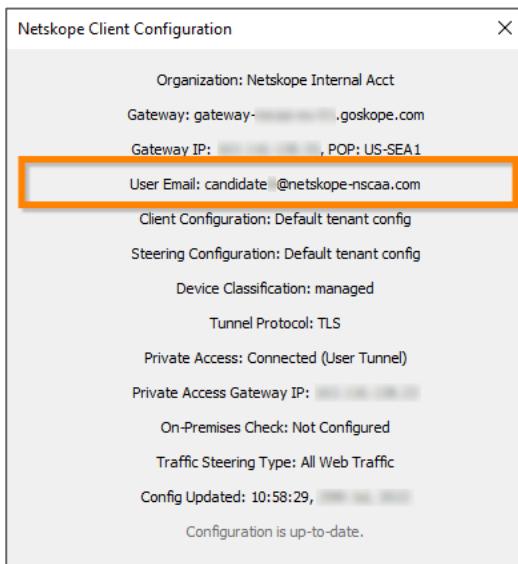
Password: Password1!



5. Wait for the Netskope client to display as enabled on the taskbar. Your Netskope client is installed in identity provider mode.

Part 2 – Verify the Netskope Client is tunneling traffic

1. Right-click the Netskope client icon and select **Configuration**.



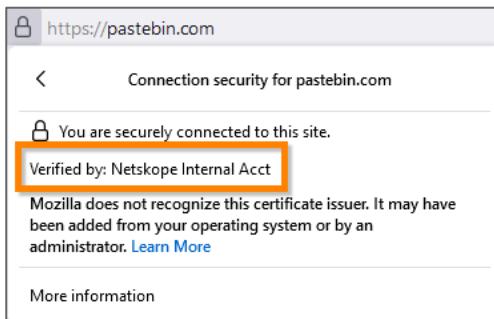
Note: The User Email in the identity provider mode is your Okta login, and not the Windows domain user.

2. If you see a link to update the configuration, please do so.

3. Open a browser window and navigate to <https://pastebin.com>
4. Click the padlock icon (in the address bar, then click **Connection secure** (or **Connection is secure**, depending on the web browser).



5. Ensure that the site certificate is verified by a Netskope certificate. This indicates Netskope has visibility into the SSL connection.



6. On the **pastebin.com** webpage, scroll down and click **Create New Paste**.

A screenshot of the 'Create New Paste' form on pastebin.com. The form includes fields for Syntax Highlighting (None), Paste Expiration (Never), Paste Exposure (Public), Folder (dropdown menu), Password (checkbox labeled 'Disabled'), and Burn after read (checkbox labeled 'Burn after read'). There is also a Paste Name / Title field and a large 'Create New Paste' button at the bottom, which is highlighted with a yellow box.

A block notification should display. This indicates that Netskope is intercepting browser traffic to the website.

Non-compliant action.

The current operation is blocked by your IT administrator.
Click 'OK' to continue.

This window will auto-close in **59 seconds**

OK

7. In the Netskope tenant, navigate to **Skope IT™ > Events > Application Events**.
8. Use the filter options to search for your identity (i.e., user like candidate{X}, where {X} is your student number).

The screenshot shows the Netskope Application Events interface. At the top, there is a search bar with the query "user like candidate". Below the search bar, the results are displayed under the heading "Application Events". The results table has columns: TIME, ACTIVITY, USER, APPLICATION, OBJECT, and WEBSITE. Two entries are listed:

TIME	ACTIVITY	USER	APPLICATION	OBJECT	WEBSITE
2:03:47 PM	Post	candidate @netskope-nscaa.com	Pastebin	PostForm[name]	Pastebin
2:02:40 PM	Post	candidate @netskope-nscaa.com	Pastebin	PostForm[name]	Pastebin

9. Click the magnifier icon (🔍) next to your event to review the details. The presence of events verifies that traffic to the Pastebin application is being steered through Netskope and events are being recorded.

Lab Complete

Lab C: Automating fingerprint uploading using a Netskope Virtual Appliance

Scenario

Super Duper Cars and Trucks has a set of documents that they want to be able to track using the DLP fingerprinting feature. However, for regulatory and privacy reasons, they are reluctant to upload the documents to the Netskope tenant for fingerprinting purposes. To allow for on-premises fingerprinting, a Netskope virtual appliance has already been provisioned. Your task is to register the appliance with the tenant and automate the workflow of uploading the documents to the appliance, requesting and uploading a fingerprint for the document, and deleting the document afterwards.

Lab Tasks

During this lab you will perform the following tasks:

- Create a new fingerprint object in the lab tenant.
- Automate the process of creating Fingerprint content for this object.
- Upload the file to a tenant using the on-premises virtual appliance.
- Verify the detection of a document using the fingerprint classification.

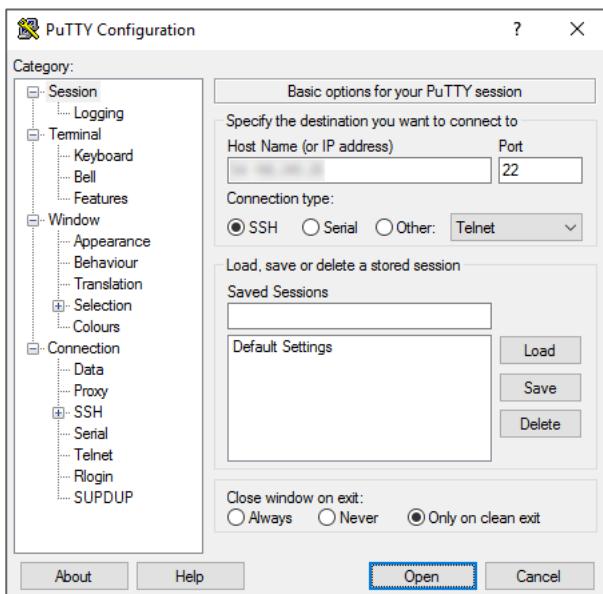
Part 1 – Register your on-premises virtual appliance

1. In your Netskope tenant console, navigate to **Settings > Security Cloud Platform > On-Premises Infrastructure**.
2. Copy the key in the **License Key** section.

License Key
 937D2375- XXXXXXXX-XXXX-XXXX-XXXX-XXXXXX -535498C2

3. Run PuTTY to connect to your assigned OPLP virtual appliance over SSH.

- In the Host Name (or IP address) field, enter your assigned OPLP public IP address and click Open.



- In the security alert dialog, click Accept to continue.

- Enter the following credentials:

username: nsadmin

password: nsappliance

```

[1] 14:166.245.28 - PuTTY
[1] login as: nsadmin
[1] nsadmin@14.166.245.28's password:
=====
Netskope Appliance (version 77.6.0.1150)
All contents Copyright (c) 2015 Netskope, Inc.
All rights reserved.
=====
nsappliance> 

```

- Enable configuration mode using the command

configure

- Provide a hostname for your OPLP using the command

set system hostname candidate{X}oplpx

where {X} is your student number

- License your OPLP using the following command. To enter the license key you copied earlier, right-click inside the PuTTY window.

set system licensekey <key>

- To save the configuration, type:

save

11. To exit configuration mode, type:

```
exit
```

```
nsappliance> configure
Entering configuration mode

nsappliance(config)# set system hostname candedate OPLP
nsappliance(config)#
nsappliance(config)# set system licensekey 937D2375-00520E84-0072E1889-4838388-98AC2A2A-00000CC-6E7363636
0-330452-00000001-535498C2
nsappliance(config)#
nsappliance(config)# save
Restarting lccloudsync-oplp container
Configuration saved

candedate OPLP(config)# exit
Exiting configuration mode

candedate OPLP>
```

When the appliance completes the registration process with the tenant, it will appear in **Settings > Security Cloud Platform > On-Premises > On-Premises Infrastructure**. This could take up to 20 minutes. While the appliance gets registered you should proceed to the next task.

Infrastructure								VIEW LOGS	CONFIGURE ALERTS
CONTENT	SF UPGRADE	SERIAL NUMBER	NAME	CONFIGURATION	STATUS	LAST STATUS...	LAST SEEN	VERSION	
	FF03	E8CD	candidate OPLP	Log Parser	OK	8/2/2023	77.6.0.11...	...	

Part 2 – Create an empty fingerprint

Before you can upload the fingerprint from the appliance, you will need to configure a fingerprint classification in the tenant.

1. Navigate to **Policies > Profiles > DLP**.
2. Click **Edit Rules** and choose **Fingerprint Classification**.
3. Switch to the **Fingerprints** tab.
4. Click **New Fingerprint**.
5. Name the fingerprint Candidate{X}, where {X} is your candidate number.

New Fingerprint

X

FINGERPRINT NAME:

Candidate

SAVE

6. Click **Save**, then **Apply Changes**, and then **Apply** to confirm.

Part 3 – Upload the fingerprint with a script

Task 3.1 – Obtain the SSH keys to the on-premises Virtual Appliance

1. In your Amazon WorkSpace, open a web browser and browse to <https://github.com/powershell/win32-openssh/releases>
2. Scroll down to the **Assets** section and download OpenSSH-Win64.zip.
3. After the zip file has completed downloading, right-click and extract all files.
4. Open a command prompt and change to the extracted files folder by typing:

D:

```
cd D:\Users\CandidateX\Downloads\OpenSSH-Win64\OpenSSH-Win64
```

```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

D:\Users\      >d:
D:\Users\      >cd Downloads\OpenSSH-Win64\OpenSSH-Win64
```

5. Type the command:

```
ssh nstransfer@[your assigned OPLP public IP address]
```

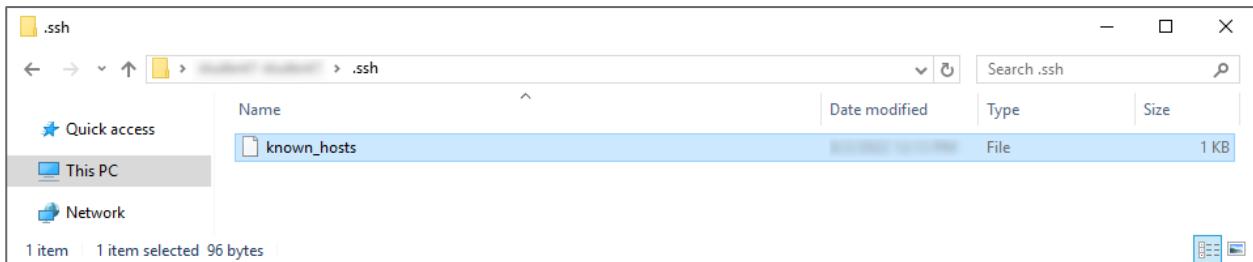
6. To the message to confirm that you want to continue connecting, enter:

```
yes
```

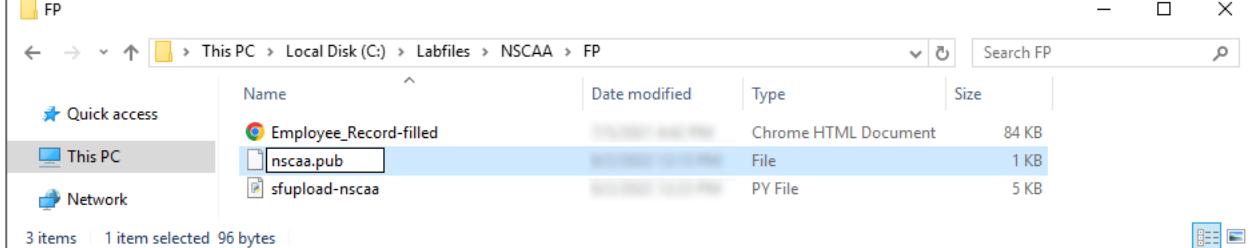
```
D:\Users\      \Downloads\OpenSSH-Win64\OpenSSH-Win64>ssh nstransfer@
The authenticity of host '...' (ED25519) can't be established.
ED25519 key fingerprint is SHA256:hnHo9oNQAU4VDlBIJ6FzDX/P9/YvZ0+cvyV5Q60qLOY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '...' (ED25519) to the list of known hosts.
nstransfer@...'s password:
```

The OPLP's public key has been added to the list of known hosts. You do not have to enter a password to finish the connection.

7. Open File Explorer and navigate to the folder D:\Users\Candidate{X}\.ssh.



8. Copy the known_hosts file to the C:\Labfiles\NSCAA\FP folder, which also contains the Python script. This step is required for the script to run.
9. Rename the known_hosts file to: nscaa.pub



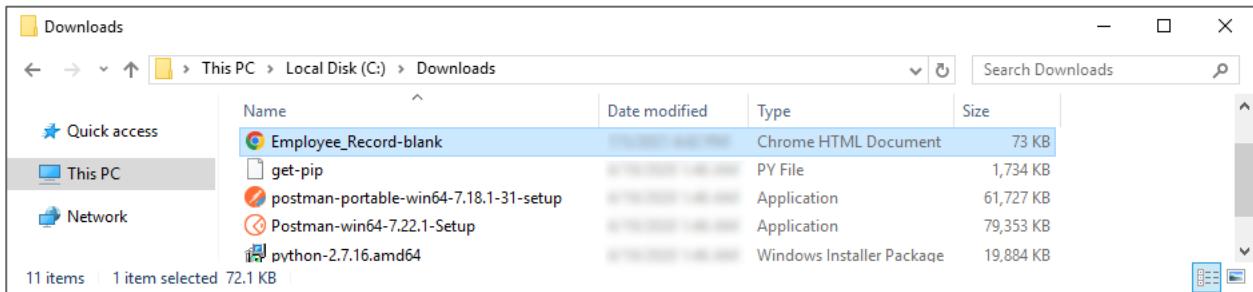
Task 3.2 – Run the script

1. In the Netskope tenant, navigate to **Settings > Security Cloud Platform > On-Premises > On-Premises Infrastructure** and confirm that the appliance registration has completed.

Infrastructure							VIEW LOGS	CONFIGURE ALERTS
CONTENT	SF UPGRADE	SERIAL NUMBER	NAME	CONFIGURATION	STATUS	LAST STATUS ...	LAST SEEN	VERSION
FF03	E8CD	candidate	OPLP	Log Parser	77.6.0.11...	8/3/20...	...	

Note: Do not proceed to the next step, until the appliance is registered.

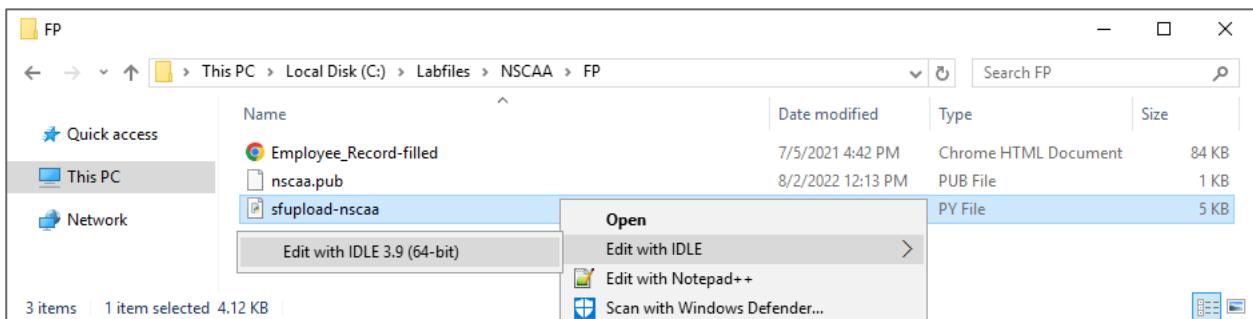
2. In your Amazon WorkSpace, ensure that the file named Employee_Record-blank.pdf is in C:\Downloads.



Note: The file may appear to be an html file; however, the file extension is .pdf.

3. Navigate back to the folder C:\Labfiles\NSCAA\FP.
4. Right-click the sftppupload-nscaa.py Python file and select **Edit with Idle > Edit with Idle 3.9 (64-bit)**.

Note: The script requires Python 3.x to run.



5. When the file opens, click **Run > Run Module** in the top menu.

```

sftppupload-nscaa.py - C:\Labfiles\NSCAA\FP\sftppupload-nscaa.py (3.9.13)
File Edit Format Run Options Window Help
Run Module F5 =====
Run... Customized Shift+F5 <print
Check Module Alt+X <is a POC script to upload/delete fingerprints on a VA
Python Shell Sinclair (EMEA Training)
'2022
=====
#version :1
#usage :Edit Variables and run
#notes :cnopts.hostkeys = None could allow MITM attacks and is not advised
#python_version :3
#changelog :Auto File Deletion feature
=====

-- hostkey of VA keyloc can be gained by downloading OpenSSH
-- 1. https://github.com/PowerShell/Win32-OpenSSH/releases/tag/V8.6.0.Opt-Beta
-- 2. connect to VA 'ssh nstransfer@ec2-18-134-129-180.eu-west-2.compute.amazonaws.com'
-- 3. edit known_hosts located in cd /d "%USERPROFILE%\ssh" for example C:\Users\sincl\ssh

import pysftp
from paramiko import SSHClient
import datetime
import os, sys, time

-- edit as required
vahost = input("Enter OPLP IP Address: ")
#keyloc = input("Enter nscaa.pub location: ")
fpname = input("Enter the name of your Fingerprint: ")
logfile = 'C:\\\\Downloads\\\\pysftp.log' #SFTP logfile

```

6. At the first prompt, enter your assigned OPLP public IP address.

- At the second prompt, type the name of your fingerprint classification, created in the tenant UI (i.e., Candidate{X}, where {X} is your student number).

```
===== RESTART: C:\Labfiles\NSCAA\FP\upload-nscaa.py =====
Enter OPLP IP Address:
Enter the name of your Fingerprint: Candidate
C:\Downloads\Employee_Record-blank.pdf uploaded

connected to VA via SSH

generating fingerprints

request dlpfingerprint generate classification Candidate9 path /var/ns/docker-mounts/lclw/mountpoint/nslogs/user/pdd_data
request dlpfingerprint status

=====
Netskope Appliance (version 77.6.0.1150)
All contents Copyright (c) 2015 Netskope, Inc.
All rights reserved.

=====
candidate9OPLP> request dlpfingerprint generate classification Candidate9 path /var/ns/docker-mounts/lclw/mountpoint/nslogs/user/pdd_data
Process for generating fingerprint has started (pid: 8603). Monitor the status using 'request dlpfingerprint status'

candidate9OPLP> request dlpfingerprint status
2022-08-02 13:54:54      Started Fingerprinting Files
2022-08-02 13:54:54      Finished Fingerprinting all FileTotal num of file sets: 1
Uploading Fingerprint Set (1/1)
Uploading files: /tmp/dlpgly_9g18.8246/1/1_journal.bin , /tmp/dlpgly_9g18.8246/1/1_md5_journal.bin, /tmp/dlpgly_9g18.8246/1/nsdlp_fingerprint_keys_journal.json

Skipping proxy: Proxy file not found: /opt/ns/cfg/proxy.json
Uploaded classification journal file
Uploaded md5 classification journal file
Uploaded fingerprint keys journal file
Fingerprint generation complete (1/1)

candidate9OPLP>
removed /home/nstransfer/pdd_data/Employee_Record-blank.pdf
====
```

Note: The script will generate the fingerprint and then display the status, using the commands:

```
request dlpfingerprint generate classification
request dlpfingerprint status
```

The script then waits 60 seconds and removes the uploaded file from the appliance.

Part 4 – Configure a policy to block documents matching the fingerprint

Task 4.1 – Create a DLP rule

- In the Netskope tenant, navigate to **Policies > Profiles > DLP**.
- Click **Edit Rules** and choose **Fingerprint Classification**.
- Click **New Fingerprint Rule**.
- Select your **Candidate{X}** fingerprint classification and click **Next**.

New Fingerprint Rule

SETTINGS THRESHOLD SET RULE

FINGERPRINTS [Clear Selection](#) + NEW FINGERPRINT

Candidate

OVERVIEW
 Settings Candidate
 Threshold 85%

NEXT

- In the **Threshold** section, move the slider to the **70%** position and click **Next**.

New Fingerprint Rule

SETTINGS THRESHOLD SET RULE

The Fingerprinting Rule Threshold allows you to configure the similarity of the fingerprint match. The recommended default value is 70%. A similarity level of 100% means identical to the fingerprinted document. Setting this too high may miss variances of the original document while a lower percentage may generate false positives.

70% 100% 70 %

OVERVIEW
 Settings Candidate
 Threshold 70%

PREVIOUS NEXT

- In the **Rule Name** field, type **FPCandidate{X}** (where {X} is your student number) and click **Save**.

New Fingerprint Rule

SETTINGS THRESHOLD SET RULE

RULE NAME:
 FPCandidate

OVERVIEW
 Settings Candidate
 Threshold 70%

PREVIOUS SAVE

- Click **Apply Changes**, then click **Apply** to confirm.

Policies > Profiles > DLP >

Fingerprint Rules

RULES **FINGERPRINTS**

Search keywords:

NEW FINGERPRINT RULE

APPLY CHANGES

Fingerprint Rules		
1 FOUND		
NAME	LAST EDIT	
FPCandidate	Created	M by .com

Task 4.2 – Create a DLP profile

Next, create a DLP profile for your rule.

1. Navigate again to **Policies > Profiles > DLP**.
2. Click **New Profile**.
3. On the **File Profiles** page, click **Next**.
4. On the **Rule | Classification** page, in the **Fingerprint Rule** field, select your rule **FPCandidate{X}**, then click **Next**.

New DLP Profile

FILE PROFILES RULE | CLASSIFICATION SET PROFILE

If it also matches any of the following conditions (optional): Advanced

DLP Rule = Select dlp rule to match

OR

Classifier = Select classifier rule to match

OR

Fingerprint Rule = FPCandidate

PREVIOUS NEXT

OVERVIEW

Rule | Classification
Fingerprint Rule = FPCandidate

- On the **Set Profile** page, in the **Profile Name** field, enter the same name as your rule: **FPCandidate{X}** (where {X} is your student number) and click **Save**.

New DLP Profile

FILE PROFILES ✓

RULE | CLASSIFICATION ✓

SET PROFILE

PROFILE NAME: FPCandidate

OVERVIEW

Rule | Classification
Fingerprint Rule = FPCandidate

PREVIOUS SAVE

- Click **Apply Changes**, then click **Apply** to confirm.

Policies > Profiles >

DLP

NEW PROFILE **EDIT RULES** **APPLY CHANGES**

Custom Profiles All Industries All Regions **Q** **X**

DLP Profiles
1 FOUND

NAME	TYPE	LAST EDIT	...
FPCandidate	custom	Created	M by ...@netskope-nascaaa.com

Task 4.3 – Create a real-time protection policy

- Navigate to **Policies > Real-time Protection**.
- Click **New Policy**, then select **DLP** from the dropdown menu.
- Configure the policy with the following information:

Source > User	Your Okta user candidate{X}@netskope-nascaaa.com
Destination > Category	Login Screens
Destination > Activity	Upload
Profile & Action > DLP Profile	FPCandidate{X} (custom)
Action	Block
Set Policy > Policy Name	FPCandidate{X}, where {X} is your student number

Real-time Protection Policy

Activities and actions available are dependent on the type of profile and applications you selected.

Source
User = candidate @netskope-nscaa.com

Destination
Category = Login Screens

ACTIVITIES & CONSTRAINTS
Activity = Upload

Profile & Action
DLP Profile = FPCandidate (custom)

Action: Block
Template: Default Template

Set action for each profile

+ ADD TRAFFIC ACTION

Set Policy
FPCandidate

+ POLICY DESCRIPTION
+ EMAIL NOTIFICATION

Status
 Enabled
+ POLICY SCHEDULE

CANCEL **SAVE**

4. Click **Save**, choose **To the top** and click **Save** again.
5. Click **Apply Changes**, then click **Apply** to confirm.

Policies >

Real-time Protection

APPLY CHANGES

NEW POLICY

Policy Name ~ **+ ADD FILTER**

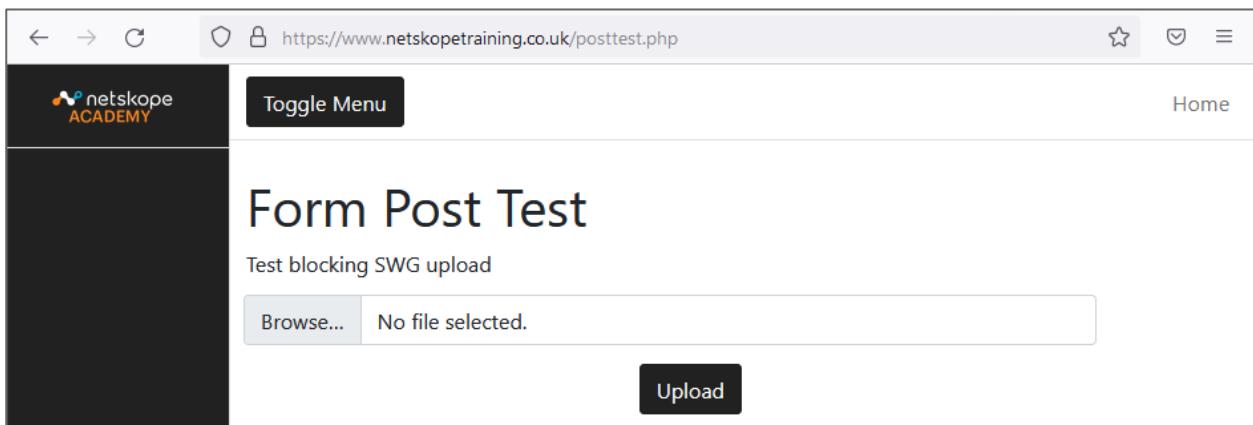
Policies
29 CREATED

	⚠	⌚	NAME	SOURCE ⓘ	DESTINATION	PROFILE	ACTION	# ALERTS ⓘ	...
1	FPCandidate	⌚	candidate @netskope-nscaa.com	Login Screens	FPCandidate	Block	Default ...	6	...

Part 5 – Verify that the fingerprint-based policy is working

1. Ensure that your Netskope client is active, and that the icon is displaying in blue and orange in the system tray.

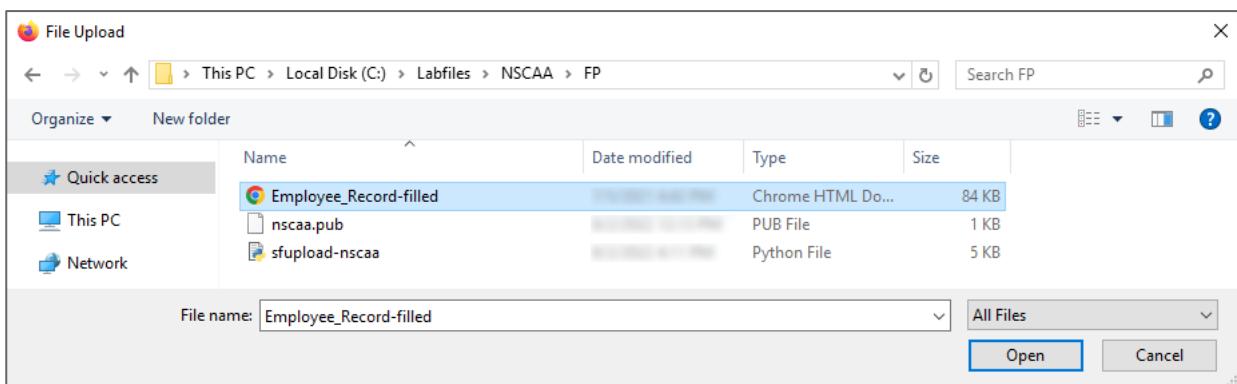
2. In a browser window, navigate to <https://www.netskopetraining.co.uk/posttest.php>



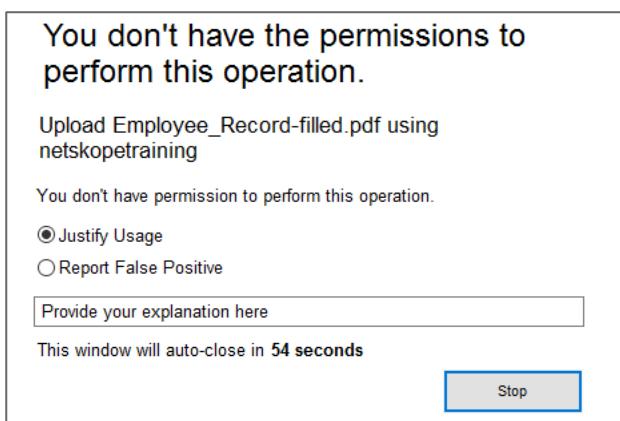
The screenshot shows a web browser window with the URL <https://www.netskopetraining.co.uk/posttest.php>. The page has a dark header with the 'netskope ACADEMY' logo and a 'Toggle Menu' button. The main content area has a light background. It features a large heading 'Form Post Test' and a sub-section titled 'Test blocking SWG upload'. Below this is a file input field with the placeholder text 'No file selected.' and a 'Browse...' button to its left. At the bottom center is a large, prominent black button labeled 'Upload'.

3. Attempt to upload the Employee_Record-filled.pdf file from C:\Labfiles\NSCAA\FP.

Note: This document is slightly different from the original document.



4. Ensure that the upload is blocked.



5. In the Netskope tenant, navigate to **Incidents > DLP** to find and review the DLP incident that was created.

Incidents							Sort by:	Timestamp	MARK STATUS AS	SEVERITY	ASSIGN	EXPORT
1 OBJECTS WITH INCIDENTS												
	TITLE	SITE	# VIOLATIONS	LAST ACTION	DLP PROFILE	TIMESTAMP					⚙️	
	Employee_Record-filled.pdf	netskopetraining	1	block	FPCandidate	2023-09-11T14:45:00Z						
◀	1	▶						Rows per page:		10	▼	

Lab Complete

Lab D: Browser-based Netskope Private Access (NPA)

This lab covers automating the process of registering the NPA publisher using APIs.

Scenario

Super Duper Cars and Trucks Company has 10 partners. Each partner is required to deploy and register an NPA publisher. However, the partners do not have access to the Netskope tenant because the tenant is managed and maintained by Super Duper. In this scenario, you will create a RestAPI token for the partners, allowing them to deploy a publisher and pull the registration token from your tenant. The partners can then register their publishers via the command menu.

In this lab, the NPA publisher appliance has already been deployed in AWS by your instructor.

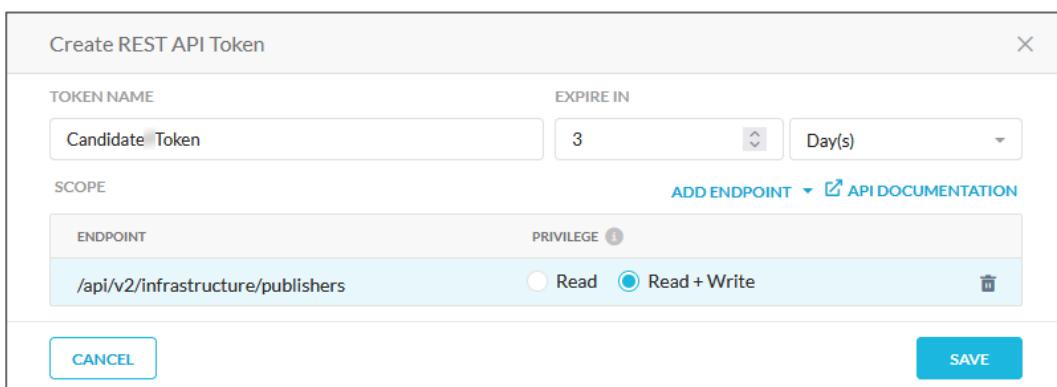
In this lab, you will complete the following tasks:

- Create a RestAPI registration token for deploying a publisher.
- Retrieve the registration token from the Netskope tenant.
- Register the publisher via the command line interface.
- Publish a private app and access it from a web browser.

Part 1 – Create NPA Publisher on the Netskope tenant

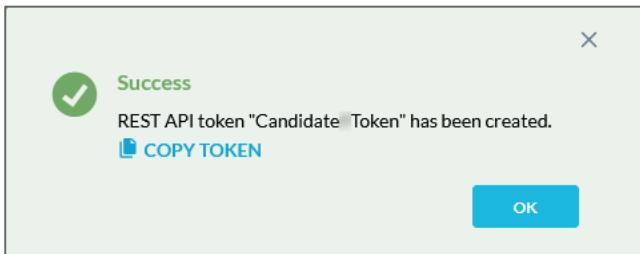
Task 1.1 – Create a REST API v2 token for publisher management

1. In your Netskope tenant, click **Settings** and navigate to **Tools > REST API v2**
2. Ensure that **Rest API Status** displays **Enabled**, then click **New Token**.
3. Enter a token name **Candidate{X}Token** and set the token expiration time to 3 days.
4. Click **Add Endpoint** to select the following endpoint to use with the token:
/api/v2/infrastructure/publishers
Hint: Type pub in the search field to narrow down the list of API endpoints.
5. Change the privilege for the endpoint to **Read + Write** and click **Save**.



The screenshot shows the 'Create REST API Token' dialog box. The token name is 'Candidate Token' and it expires in 3 days. The endpoint selected is '/api/v2/infrastructure/publishers' with a privilege of 'Read + Write'. The 'SAVE' button is visible at the bottom right.

6. In the **Success** message, click **Copy Token** to save it for later use in your API requests.

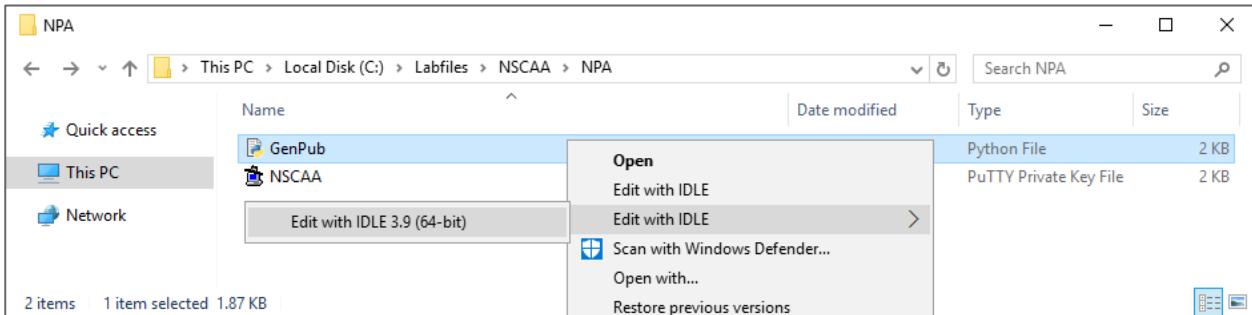


Hint: paste the copied token into a text file and save it within your WorkSpace.

7. When finished, click **OK**.

Task 1.2 – Register a new Publisher with a script

1. Open File Explorer and navigate to C:\LabFiles\NSCAA\NPA.
 2. Right-click the GenPub.py Python script file and select **Edit with Idle** > **Edit with Idle 3.9 (64-bit)** from the options displayed.



3. In the Idle Editor window, select **Run > Run Module**.



- Enter the following information to the successive prompts:

Publisher name	Candidate{X}, where {X} is your student number
Full tenant URL	Training Netskope tenant URL
RestAPI token	The REST API token copied from your tenant at a previous step

- Copy the publisher registration token value within the quotation marks from the script output.

```
===== RESTART: C:\Labfiles\NSCAA\NPA\GenPub.py =====
Enter Publisher Name: Candidate
Enter the full tenant url e.g. academy-emea.goskope.com: [REDACTED].goskope.com
Enter your RestAPI Token: f748 1f57
2
https://[REDACTED].goskope.com/api/v2/infrastructure/publishers/2/registration_token
{"data": {"token": "eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJuCY0xNTExOCS5ubC1hbTIubnBhLmdvc2tvOGUuY29tIiwic3ViIjoiZmRkYWMyOGExYTU5OWE3OSIsImV4cCI6MTY1OTYzMjM1MywianRpIjoiYjE2Y2YwYTktZjEyZS00YjZjLTg5MTgtNjUzOTAxZmIzMjDU4In0.mILNr7nMQ7HwBRz7AcPQj-bcE4cUq2QWYGbF2JAoQ-TIAFLhOfjDtxG7m9d2UU0F3vFQXBftYgZZOU2qF5D-T1107s9gksSTk-BkwI8yR8jByFP4-JXvN7BTcpLBXdoYJ8tEu7Sp3pbb-mzYRE7jwqErq6cKUL7WqGrm18x8Aghxh1rtUIwGYeeecOZvD4ykqWKIIMc8SgLbob0RE1-EMOJ_VtLTXk4KBsDZ17RZov7nqcu-U6wd0kW2vc1cEqfVEw64eU19BBv-nC4CyaMYwk-Qh-Bne9JtLmXcqaR662JdK-nSHWrmzc-kZmrtKuH9QQ0ahhN8wDNnhKoGVuQ"}, "status": "success"}
>>>
```

- In the Netskope tenant settings navigate to **Security Cloud Platform > Traffic Steering > Publishers**. Verify that your NPA Publisher has been created but not registered.

Security Cloud Platform > Traffic Steering > Publishers

Publishers

Publishers are Netskope software components which are deployed in your virtual network at your public cloud provider (e.g. AWS VPC) or internal network in your private datacenter. Publishers make your private applications available to authorized users and devices.

Netskope Publishers are supported on AWS, Azure, GCP, VMware ESXi, Hyper-V, or any Ubuntu based Linux systems. For AWS based publishers, registration can be expedited by entering the provided token into the User Data field during EC2 Instance launch configuration.

[View more instructions.](#)

AWS: PUBLISHER AMI VMware ESXi: PUBLISHER OVA Hyper-V: PUBLISHER VHDX

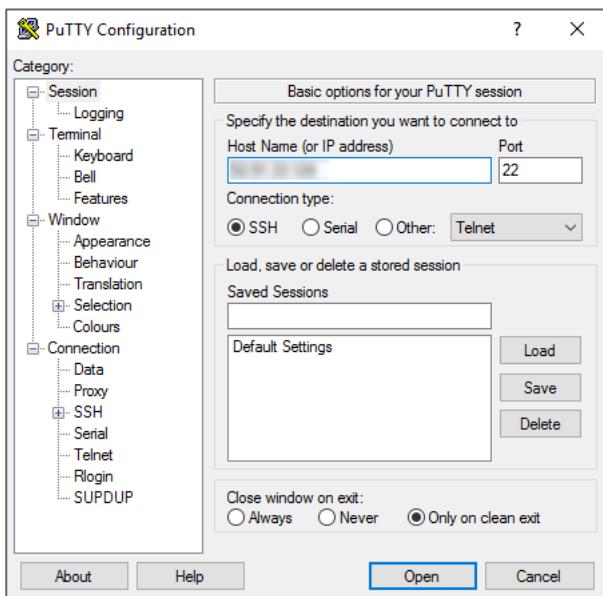
Publishers					Sort by: Publisher
1 CREATED					
PUBLISHER	STATUS	VERSION	CN	CONNECTED APPS	
Candidate	Not registered		fdda 9a79	0	

Rows per page: 10

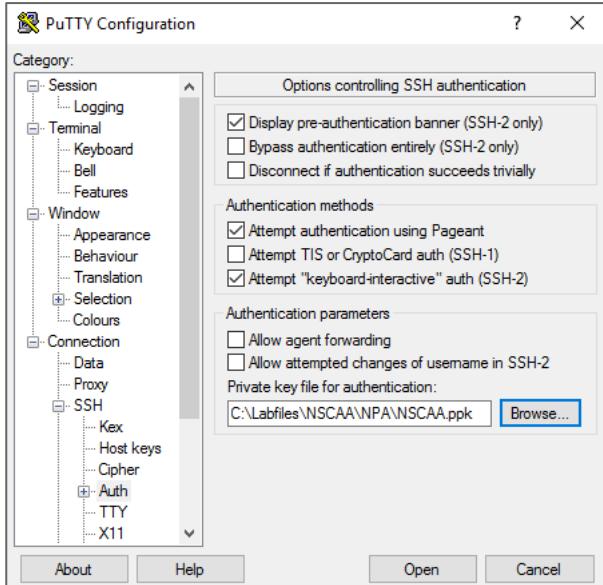
Task 1.3 – NPA Publisher registration

- From your Amazon WorkSpace, open a PuTTY window.

2. In the **Host Name (or IP address)** field, enter your assigned publisher public IP address.



3. In the side menu, navigate to **Connection > SSH > Auth**.
4. Click **Browse** and open the private key C:\LabFiles\NSCAA\NPA\NSCAA.ppk



5. Click **Open** and answer **Accept** in the security alert window.
6. In the command line interface, enter **centos** in the login as prompt.



7. To register your publisher, at the **Configuration menu** prompt, type: 1

- Paste the publisher registration token copied from the Python script output and press ENTER.

```
Configuration menu:
1. Register
2. Upgrade
3. Network settings
4. Syslog settings
5. Troubleshooter
6. Log settings
7. Exit
1
Please enter the Netskope Private Access Publisher registration token:
eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJucy0xNTEzOC5ubC1hbTIubnBhLmdvc2tvcGUuY29tIiwic3ViIjoiYWFlZTJhZjE1ZmU5Y2E5MSIsImV4cCI6MTY1OTYzNDczOSwianRpIjoiMDAzZjY0MTktNWY2Yy00Y2M4LTk0MTAtMTF1MzIxNmJkOWI5In0.g0XLHEH77AHGLqy-nL_YbBuwoQvzE27Yf0I17fuLRLJQzJPPs6v_2gpb9YshFfcC1BSo8Yfrigd0vYYBN8g2zbsav5NuC7xyvRGuvpZYm1EhEB31Kbcd9H1QKrpPk2WhzGfNL6hDuyerumCtbrRUWQHAMyKtQIT0tm04v_fIpXxe3YyoIcc3C9h0ln3MXdv_3Z9BOXCFnPnCsjrrXiWBj9AkfZluwqWG_ABDE4WzkIAmPrKK-LBmp1FKfgDWYKJjQnigAc5GQJTgrU2xTqBookdcnYOUnsquoFJ7W5KLvqY0dw3ezumtjuzUbR2SapYmdCjEBw0580Twj3-nCxAhA
```

- Verify that the publisher has been registered successfully.

```
Please enter the Netskope Private Access Publisher registration token:
eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJucy0xNTEzOC5ubC1hbTIubnBhLmdvc2tvcGUuY29tIiwic3ViIjoiYWFlZTJhZjE1ZmU5Y2E5MSIsImV4cCI6MTY1OTYzNDczOSwianRpIjoiMDAzZjY0MTktNWY2Yy00Y2M4LTk0MTAtMTF1MzIxNmJkOWI5In0.g0XLHEH77AHGLqy-nL_YbBuwoQvzE27Yf0I17fuLRLJQzJPPs6v_2gpb9YshFfcC1BSo8Yfrigd0vYYBN8g2zbsav5NuC7xyvRGuvpZYm1EhEB31Kbcd9H1QKrpPk2WhzGfNL6hDuyerumCtbrRUWQHAMyKtQIT0tm04v_fIpXxe3YyoIcc3C9h0ln3MXdv_3Z9BOXCFnPnCsjrrXiWBj9AkfZluwqWG_ABDE4WzkIAmPrKK-LBmp1FKfgDWYKJjQnigAc5GQJTgrU2xTqBookdcnYOUnsquoFJ7W5KLvqY0dw3ezumtjuzUbR2SapYmdCjEBw0580Twj3-nCxAhA

Registering with your Netskope address: ns-15138.nl-am2.npa.goskope.com
Publisher certificate CN: aeee2af15fe9ca91
Attempt 1 to register publisher.
Publisher registered successfully.

Verifying connectivity to the Netskope Dataplane...
Connectivity to the Netskope Dataplane was successfully verified.
```

- In the Netskope tenant settings navigate to **Security Cloud Platform > Traffic Steering > Publishers**.

- Ensure that the status of your publisher has changed to **Connected**.

Publishers					Sort by:	Publisher	
1 CREATED							
PUBLISHER	STATUS	VERSION	CN	CONNECTED APPS			
Candidate	Connected		aeee ca91	0			
1					Rows per page:	10	

Note: Status update can take up to a minute. Refresh the page as necessary.

Part 2 – Review remote user authentication settings

Private app access, whether browser-based or client-based, assumes user authentication. Since browser-based private app access is based on the reverse proxy technology, the authentication comes from an identity provider which must be set up in the Netskope tenant reverse proxy settings.

You will not set up authentication in this lab, but you will review the settings configured for your Netskope tenant by the instructor.

1. In the Netskope tenant settings, navigate to **Security Cloud Platform > Reverse Proxy > SAML**.
2. Ensure that there is a SAML account for integrating with an identity provider to authenticate users accessing private apps.

Note: In this lab the identity provider is Okta.

NAME	APPLICATION	ACS URL	BYPASS
NPA	Netskope Settings Private Apps	N/A	N/A

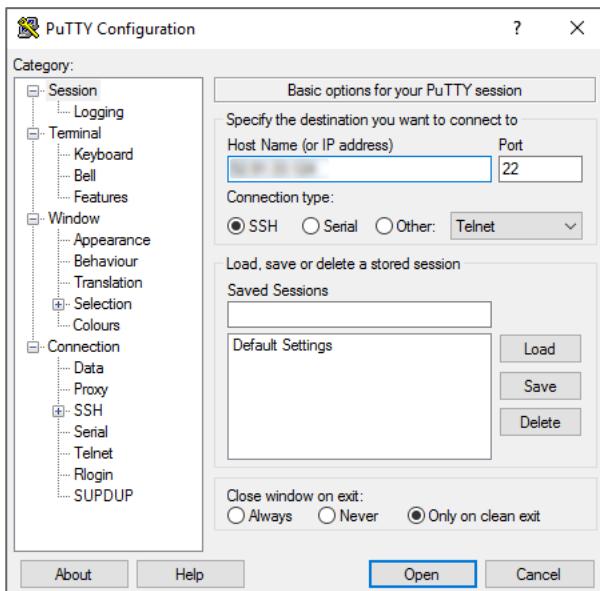
Note: In a production environment you will have to create this configuration. Read more at the link: <https://docs.netskope.com/en/configure-browser-access-for-private-apps.html>

Part 3 – Grant browser-based access to a private application

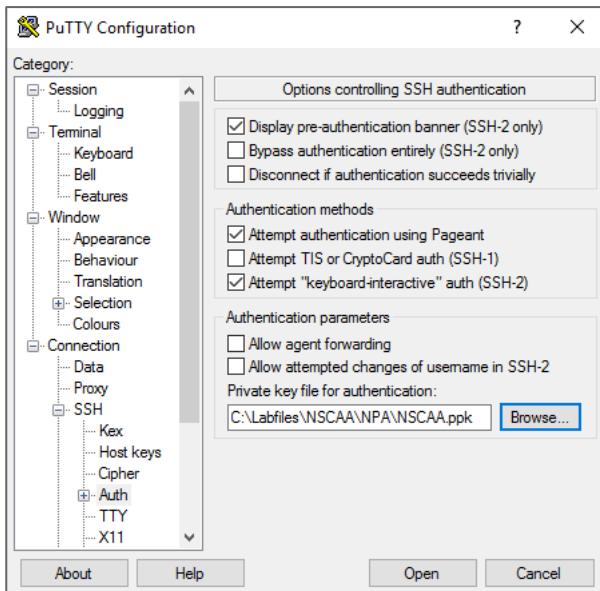
Task 3.1 – Publish the private app for browser access

Next, a private application needs to be created in the Netskope tenant. You will use your Cloud Exchange web UI as the private application.

1. Run PuTTY.
2. In the **Host name (or IP address)** field enter the public IP address of the Cloud Exchange server provided by the instructor.



3. Select the private key to use for the SSH session:
 - a. In the side menu, navigate to **Connection > SSH > Auth**.
 - b. Click **Browse** and open the private key file C:\Labfiles\NSCAA\NPA\NSCAA.ppk.



4. Click **Open**.
 5. To log in, type the username:
ubuntu
 6. To determine the local address of the Cloud Exchange server, run the command:
`ip -br a`
- ```
ubuntu@ip-172-31-34-33:~$ ip -br a
lo UNKNOWN 127.0.0.1/8 ::1/128
ens5 UP 172.31.34.33/20 fe80::ce9:8aff:fe11:facf/64
docker0 DOWN 172.17.0.1/16
br-fba3862e3979 UP 172.18.0.1/16 fe80::42:21ff:fe55:53a8/64
vethd2199da@if5 UP fe80::7004:33ff:fee3:662/64
veth197f7dd@if7 UP fe80::dc68:82ff:fe40:d724/64
veth163dd4a@if9 UP fe80::240d:f5ff:fe6a:85f4/64
vethc9c4125@if11 UP fe80::c7:7bff:fe7b:27e6/64
ubuntu@ip-172-31-34-33:~$
```
7. Copy the address of the **ens5** interface and save it for future use.
  8. In the Netskope tenant settings, navigate to **Security Cloud Platform > Traffic Steering > App Definition**.

9. On the **App Definition** page, switch to the **Private Apps** tab and click **New Private App**.

10. Create a new private app using the following information:

|                             |                                                |
|-----------------------------|------------------------------------------------|
| <b>Application Name</b>     | Candidate{X}, where {X} is your student number |
| <b>Allow Browser Access</b> | Enabled                                        |
| <b>Host</b>                 | Cloud Exchange local IP address copied earlier |
| <b>TCP Port</b>             | 80                                             |
| <b>HTTP/HTTPS</b>           | HTTP                                           |
| <b>Publisher</b>            | Your publisher Candidate{X}                    |

New Private App

Private apps are blocked by default. Policies are required to log events and enable access.

APPLICATION NAME  
Candidate

BROWSER ACCESS ⓘ  
 Allow Browser Access

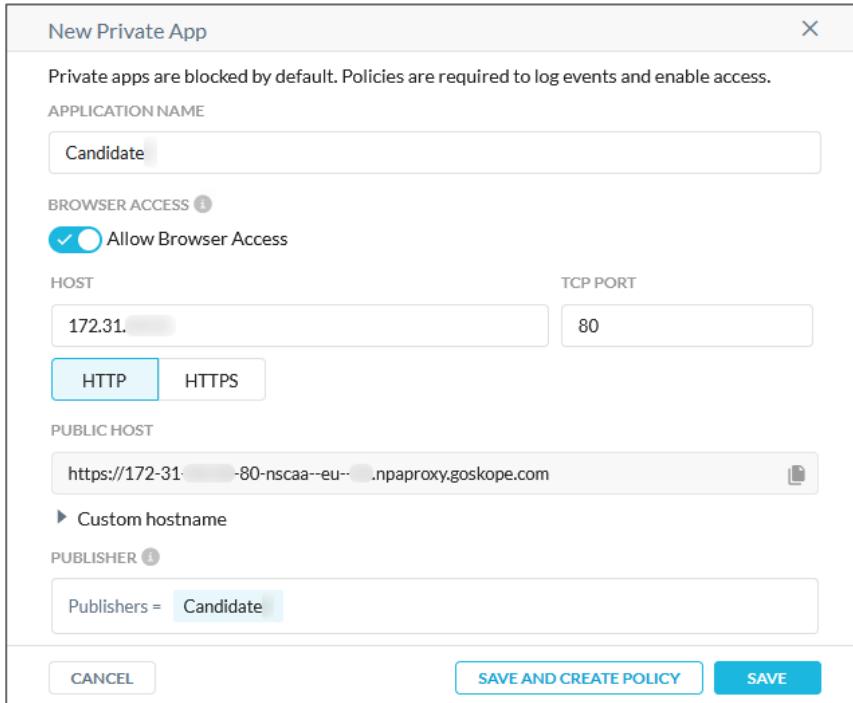
HOST  
172.31. [ ] TCP PORT  
80

HTTP  HTTPS

PUBLIC HOST  
https://172-31- -80-nscaa--eu-- .npaproxy.goskope.com

▶ Custom hostname

PUBLISHER ⓘ  
Publishers = Candidate



11. Click **Save**.

### Task 3.2 – Create a policy to grant access to the published app

1. In the Netskope tenant, navigate to **Policies > Real-time Protection**.

2. Click **New Policy > Private App Access**.

3. Configure a new policy using the following information:

|                                         |                                                   |
|-----------------------------------------|---------------------------------------------------|
| <b>Source &gt; User</b>                 | Your Okta user candidate{X}@netskope-nscaa.com    |
| <b>Source &gt; Access Methods</b>       | Browser Access                                    |
| <b>Destination &gt; Private App</b>     | [Candidate{X}]                                    |
| <b>Profile &amp; Action &gt; Action</b> | Allow                                             |
| <b>Set Policy &gt; Policy Name</b>      | NPACandidate{X}, where {X} is your student number |

Real-time Protection Policy

CANCEL SAVE

Activities and actions available are dependent on the type of profile and applications you selected.

**Source**

User = candidate@netskope-nscaa.com

Access Methods = Browser Access

**Destination**

Private App

Private App = [Candidate]

**Profile & Action**

Action: Allow

**Set Policy**

NPACandidate

+ POLICY DESCRIPTION  
+ EMAIL NOTIFICATION

4. Click **Save** and choose **To the top**, then click **Save**.
5. Click **Apply Changes** and click **Apply** to confirm.

| Policies  |              |                                                |             |         |        |          |
|-----------|--------------|------------------------------------------------|-------------|---------|--------|----------|
| 3 CREATED |              |                                                |             |         |        |          |
|           | NAME         | SOURCE                                         | DESTINATION | PROFILE | ACTION | # ALERTS |
| 1         | NPACandidate | candidate@netskope-nscaa.com<br>Browser Access | [Candidate] | None    | Allow  | 0        |

### Task 3.3 – Verify Access

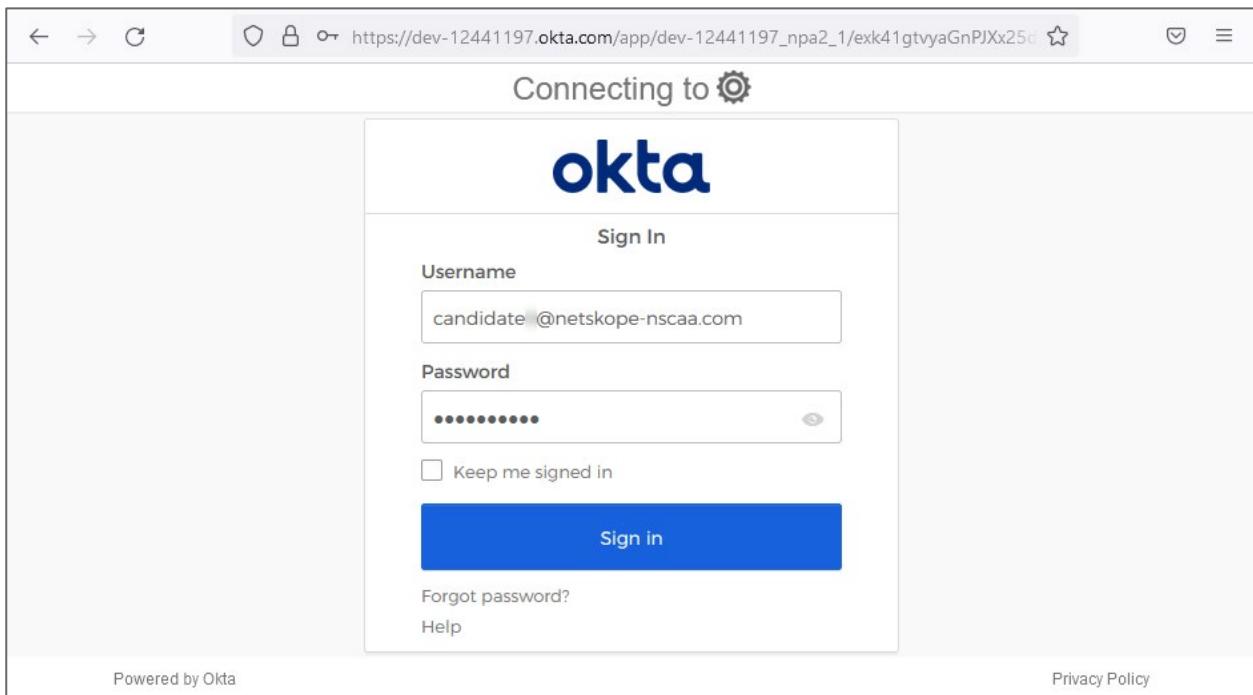
1. Open Netskope tenant settings and navigate to **Security Cloud Platform > App Definition > Private Apps**.
2. Click the name of your private app **[Candidate{X}]**, where {X} is your student number.

- Copy the URL displayed in the **Public Host** field, then click **Cancel**.

The screenshot shows the 'Edit Private App' dialog box. Key fields include:

- APPLICATION NAME:** [Candidate]
- BROWSER ACCESS:** Allow Browser Access (checked)
- HOST:** 172.31. (input field)
- TCP PORT:** 80 (input field)
- PUBLIC HOST:** https://172-31- -80-nscaa--eu-- .npaproxy.goskope.com (copy icon highlighted)
- PUBLISHER:** Publishers = Candidate
- Buttons:** CANCEL, SAVE

- Ensure that the Netskope client in your Amazon WorkSpace is disabled.
- Open a new browser window and browse to the copied URL of the private app.
- Sign in with your Okta username candidate{X}@netskope-nscaa.com, where {X} is your student number, and the Password1! password.



*Note: Browser-based private app access requires users to authenticate with an identity provider.*

7. Ensure that the Netskope Cloud Exchange UI is displayed.



**Lab Complete**

## Lab E: Cloud Explicit Proxy (CEP)

### Scenario

The newly acquired Acme Loan company employees need an interim solution to connect to company resources since they cannot install the Netskope client on their systems. To ensure visibility and control of their activity, the security team has decided to implement a Cloud Explicit Proxy (CEP) deployment.

In this lab, you will implement the final part of this deployment — direct user's traffic to your tenant's Cloud Explicit Proxy using a proxy auto-configuration (PAC) file.

### Lab Tasks

During this lab, you will complete the following tasks:

- Review the tenant-side CEP configuration.
- Download the sample.pac file from the tenant and adapt it to your environment.
- Set up proxy server settings using the PAC file.
- Verify conditional redirection to the Cloud Explicit Proxy.

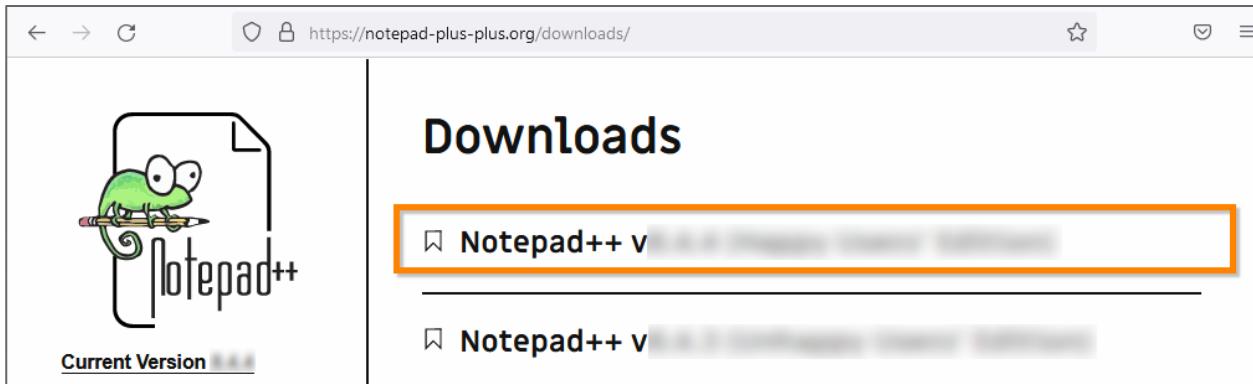
### Part 1 – Preparation

#### Task 1.1 – Install Notepad++

1. In your Amazon WorkSpace, open a web browser and navigate to:

<https://notepad-plus-plus.org/downloads>

2. Click the newest version.



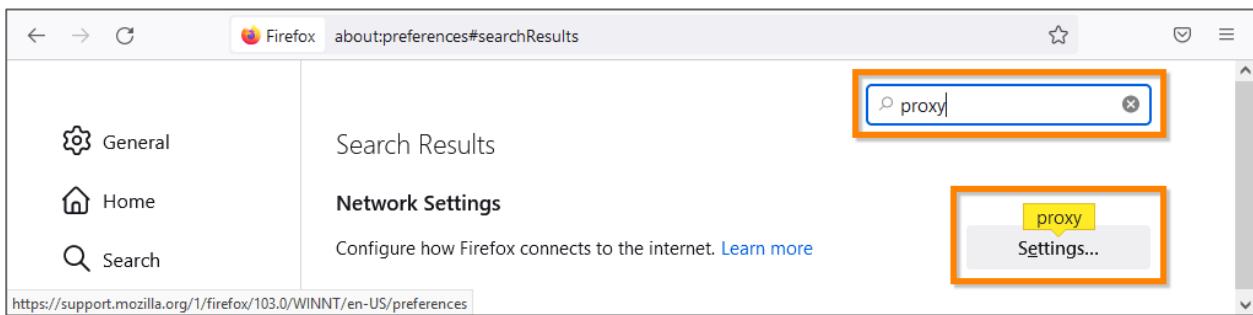
3. Download the installer and install it within your Amazon WorkSpace with the default installation settings.

#### Task 1.2 – Set up Firefox to use system proxy and certificates

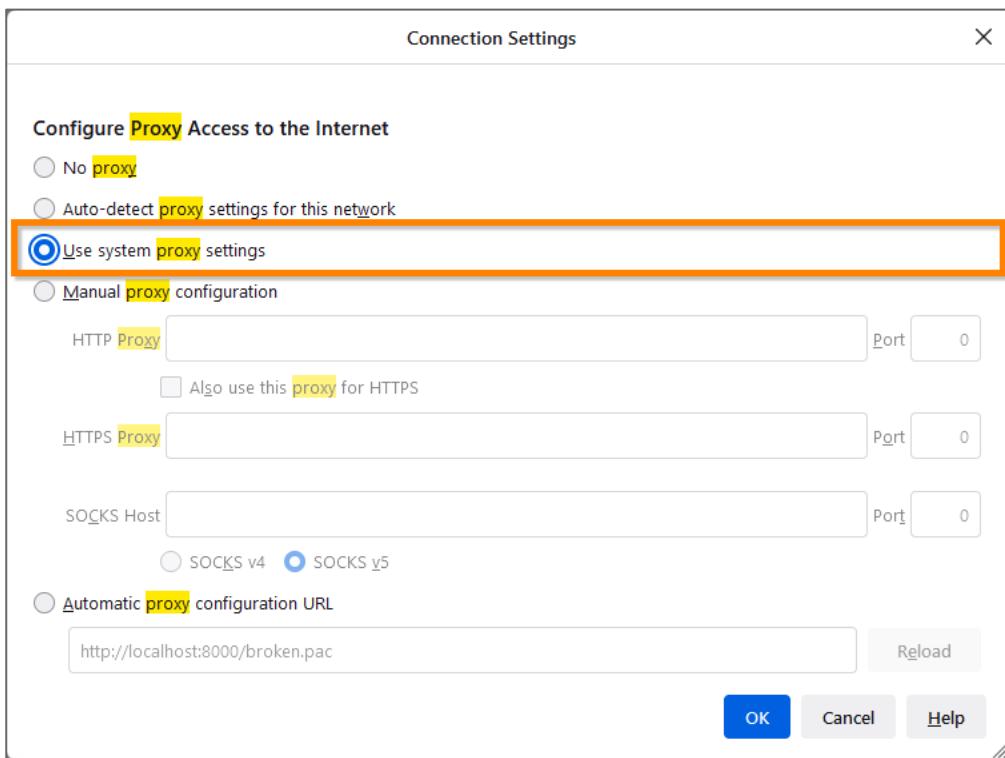
To ensure this lab works for Firefox as well as for Chrome, you will configure Firefox to use system proxy configuration and system certificates.

1. Open a Firefox browser window.
2. Open the Application menu (≡) and click **Settings**.

3. Type proxy in the search field and then click **Settings** in the **Network Settings** section.



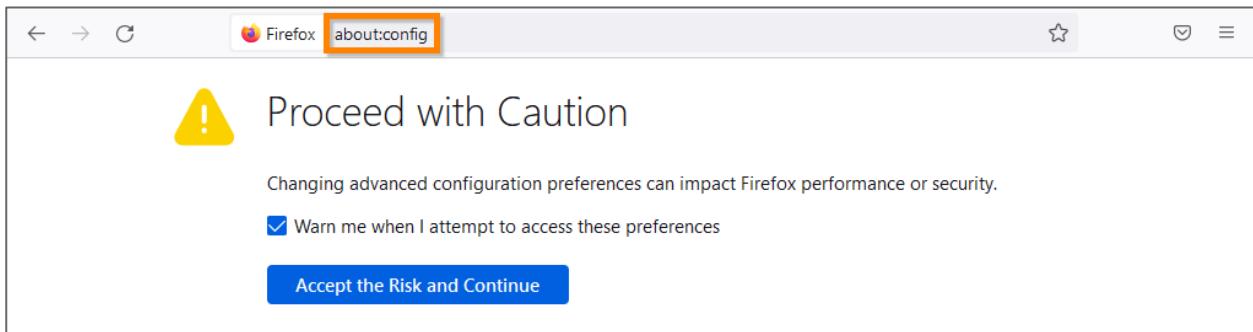
4. Choose **Use system proxy settings** and click **OK**.



5. In the Firefox address bar, enter:

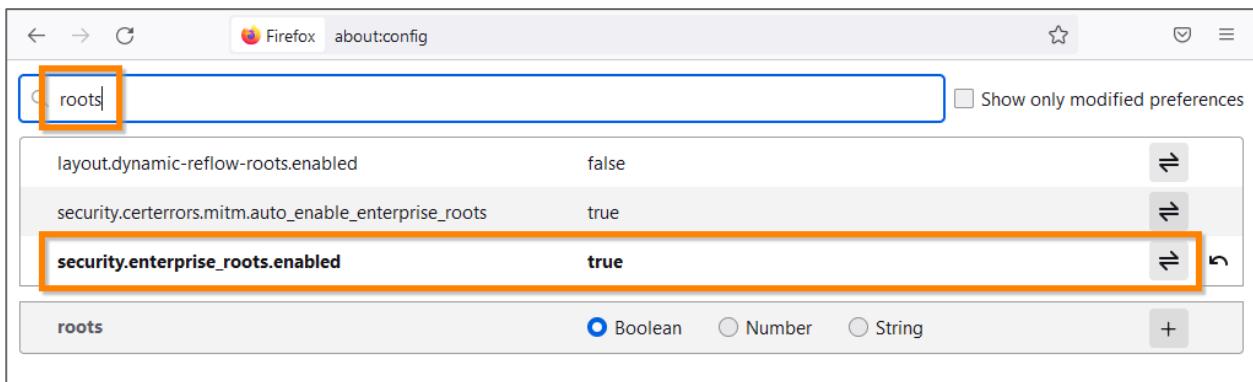
`about:config`

6. Click **Accept the Risk and Continue**.



7. In the search field, type roots

8. Click the toggle icon (⟲) to set the **security.enterprise\_roots.enabled** parameter to true.



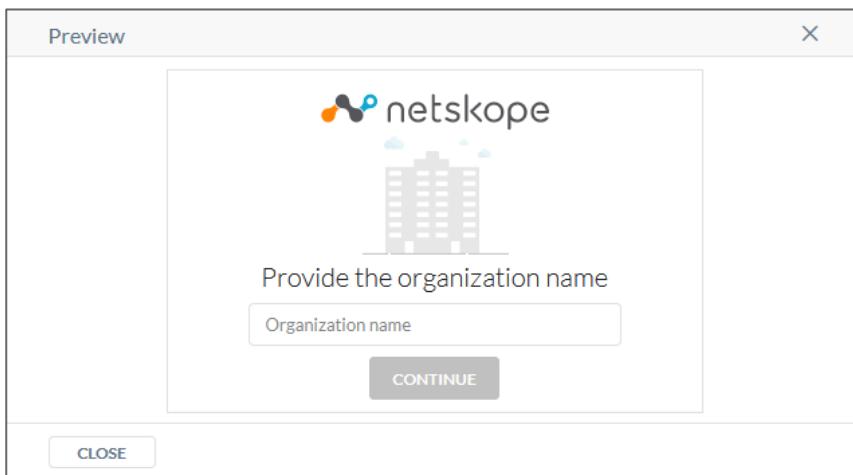
## Part 2 – Review the tenant-side CEP configuration

Tenant-side configuration steps are not included in this lab because students are sharing the same tenant. You will review the configuration prepared by the instructor.

1. In the Netskope tenant, click **Settings** and navigate to **Security Cloud Platform > Traffic Steering > Explicit Proxy**.
2. Examine the **Explicit Proxy Destination URL**. This is the address of your tenant's Cloud Explicit Proxy that you will use in the proxy auto-configuration (PAC) file later in the lab.

A screenshot of the 'Explicit Proxy Destination' section of the Netskope Tenant Settings. It shows a text input field with the placeholder 'Explicit Proxy Destination: eproxy-nscaa-...goskope.com:8081'. Below the input field is a link 'DOWNLOAD ROOT CERTIFICATE (REMOTE USERS)'.

3. In the **Tenant Lookup Service** section, click **Preview**.



*Note: Remote users will use the Netskope tenant name as their organization name.*

4. Click **Close** and note the tenant name.

The screenshot shows the "Tenant Lookup Service" settings page. It includes a descriptive text about the service, a "Tenant Name" input field containing "nscaa-eu-01" which is highlighted with an orange border, and a "PREVIEW" button.

*Note: In a production environment, you will need to communicate the tenant name to your remote users.*

5. Examine the **IP Address Allowlist & User Identity** settings.

The screenshot shows the "IP Address Allowlist & User Identity" settings page. It has sections for "Unauthenticated Traffic" (Allow), "IP Address Allowlist" (0 IP ADDRESSES), and a note "No IP Address Allowlist" with a small icon of a document with a smiley face.

*Note: There are no addresses in the allowlist. All remote users will require authentication via an identity provider.*

6. Navigate to **Security Cloud Platform > Forward Proxy > Authentication**.
7. Ensure that **Authentication** is **enabled** and a **SAML Authentication** configuration is used.

The screenshot shows the 'Authentication' section of the Netskope Forward Proxy settings. It displays the status 'Authentication: Enabled' and the type 'SAML Authentication: Nscaa-...-Client\_idp'. Below this is a blue 'ENABLE AUTHENTICATION' button.

8. Navigate to **Security Cloud Platform > Forward Proxy > SAML**.
9. Ensure that the **SAML authentication** configuration uses Okta as an identity provider.

The screenshot shows the 'Netskope SAML Config' page. It displays the SAML Entity ID (<https://nsauth-nscaa-...-goskope.com/pv9MyPD4sKN3jX4SxD8>) and SAML ACS URL (<https://nsauth-nscaa-...-goskope.com/nsauth/saml2/http-post/pv9MyPD4sKN3jX4SxD8/acs>). There is a 'DOWNLOAD SAML CERTIFICATE' link and a 'NEW ACCOUNT' button. Below is a table with one row:

| NAME                 | IDP URL                                                                                                                                                           | ... |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Nscaa-...-Client_idp | <a href="https://dev-...-okta.com/app/dev-..._nscaa..._clientidp_1/exk415tkaw1H...">https://dev-...-okta.com/app/dev-..._nscaa..._clientidp_1/exk415tkaw1H...</a> | ... |

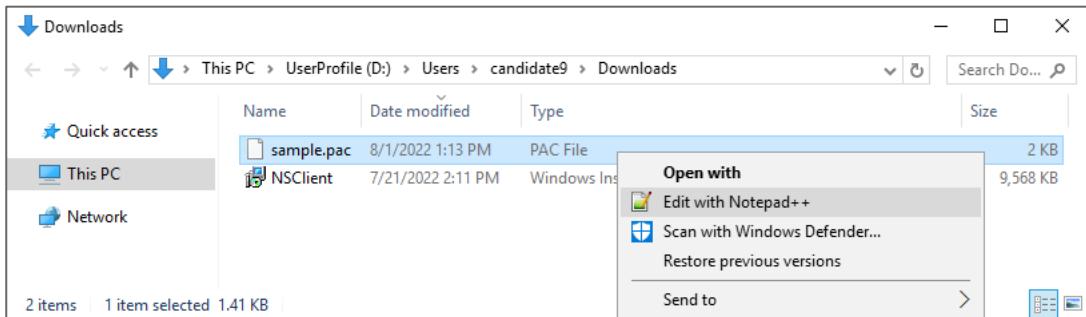
*Note: In a production environment, forward proxy authentication via a SAML-supporting identity provider must be configured for remote users to authenticate themselves at the Netskope Cloud Explicit Proxy. Read more at the link: <https://docs.netskope.com/en/saml-forward-proxy.html>*

### Part 3 – Prepare a PAC file

You will download a sample PAC file from your Netskope tenant and modify it to suit your environment.

#### Task 3.1 – Inspect the sample PAC file

1. In your Amazon WorkSpace, ensure that the Netskope client is disabled.
2. In the Netskope tenant settings, navigate back to **Security Cloud Platform > Traffic Steering > Explicit Proxy**.
3. In the top right corner, click **Download Sample PAC File** and save it to the default Downloads folder.
4. Open File Explorer and navigate to D:\Users\{Candidate}\Downloads\
5. Right-click the sample.pac file and select **Edit with Notepad++**.



6. To make the code more readable, select **Language > J > JavaScript** in the top menu.

```

1 function FindProxyForURL(url, host) {
2 /* Normalize the URL for pattern matching */
3 url = url.toLowerCase();
4 host = host.toLowerCase();
5 /* Don't proxy local hostNames */
6 if (isPlainHostName(host)) {
7 return 'DIRECT';
8 }
9
10 /* Don't send non-routable addresses (aka internal networks) to Netskope */
11 var hostIP = dnsResolve(host);
12 if (
13 isInNet(hostIP, '0.0.0.0', '255.0.0.0') ||
14 isInNet(hostIP, '10.0.0.0', '255.0.0.0') ||
15 isInNet(hostIP, '127.0.0.0', '255.0.0.0') ||
16 isInNet(hostIP, '169.254.0.0', '255.255.0.0') ||
17 isInNet(hostIP, '172.16.0.0', '255.240.0.0') ||
18 isInNet(hostIP, '192.0.2.0', '255.255.255.0') ||
19 isInNet(hostIP, '192.88.99.0', '255.255.255.0') ||
20 isInNet(hostIP, '192.168.0.0', '255.255.0.0') ||
21 isInNet(hostIP, '198.18.0.0', '255.254.0.0') ||
22 isInNet(hostIP, '224.0.0.0', '240.0.0.0') ||
23 isInNet(hostIP, '240.0.0.0', '240.0.0.0')
24) {
25 return 'DIRECT';
26 }
27
28 /* Don't proxy IDP servers. */
29 /*
30 if ((dnsDomainIs(host, '.idp.com')) {
31 return 'DIRECT'
32 }
33 */
34
35 /* Don't proxy for domains. */
36 /*
37 if ((dnsDomainIs(host, '.domain-example1.com')) ||
38 (dnsDomainIs(host, '.domain-example2.com'))) {
39 return 'DIRECT'
40 }
41 */
42
43 if (
44 url.substring(0, 5) === 'http:' ||
45 url.substring(0, 6) === 'https:'
46) {
47 return 'PROXY eproxy-<tenant-name>.gskope.com:8081';
48 }
49 return 'DIRECT';
50 }

```

JavaScript file length: 1,518 lines: 50 Ln:23 Col: 50 Pos: 975 Unix (LF) UTF-8 INS

*Note: A PAC file contains a JavaScript function which the browser executes for every URL it accesses. If the function returns 'DIRECT' the browser tries to access the URL directly. If the function returns 'PROXY' followed by a proxy address and port, the browser tries to access the original URL via the proxy.*

*This sample.pac file is incomplete and cannot be used as it is. You will modify it before usage.*

7. Review the distinct sections of the file from top to bottom.

```
1 function FindProxyForURL(url, host) {
2 /* Normalize the URL for pattern matching */
3 url = url.toLowerCase();
4 host = host.toLowerCase();
```

The browser passes the URL and the host part of the URL to the function as parameters. To make further comparisons easier, this PAC file normalizes both the URL and the host to lowercase.

```
6 if (isPlainHostName(host)) {
7 return 'DIRECT';
8 }
```

If the host name does not contain dots and is meant to be resolved in the local network, the PAC file instructs the browser to access such hosts directly.

```
10 /* Don't send non-routable addresses (aka internal networks) to Netskope */
11 var hostIP = dnsResolve(host);
12 if (
13 isInNet(hostIP, '0.0.0.0', '255.0.0.0') ||
14 isInNet(hostIP, '10.0.0.0', '255.0.0.0') ||
15 isInNet(hostIP, '127.0.0.0', '255.0.0.0') ||
16 isInNet(hostIP, '169.254.0.0', '255.255.0.0') ||
17 isInNet(hostIP, '172.16.0.0', '255.240.0.0') ||
18 isInNet(hostIP, '192.0.2.0', '255.255.255.0') ||
19 isInNet(hostIP, '192.88.99.0', '255.255.255.0') ||
20 isInNet(hostIP, '192.168.0.0', '255.255.0.0') ||
21 isInNet(hostIP, '198.18.0.0', '255.254.0.0') ||
22 isInNet(hostIP, '224.0.0.0', '240.0.0.0') ||
23 isInNet(hostIP, '240.0.0.0', '240.0.0.0')
24) {
25 return 'DIRECT';
26 }
```

Likewise, if the host resolves into a private/non-routable IP address, it is to be accessed directly.

```
25 /* Don't proxy IDP servers. */
26 /*
27 if ((dnsDomainIs(host, '.idp.com'))
28 {
29 return 'DIRECT'
30 }
31 */
```

This is a placeholder for identity provider exclusions. Netskope Cloud Explicit Proxy redirects users to an identity provider for authentication; therefore, the identity provider domains should be excluded to avoid a redirection loop.

```
33 /* Don't proxy for domains. */
34 /*
35 if ((dnsDomainIs(host, '.domain-example1.com')) ||
36 (dnsDomainIs(host, '.domain-example2.com')))
37 {
38 return 'DIRECT'
39 }
40 */
```

Then follows another placeholder for any other exclusions.

```

41 if (url.substring(0, 5) == 'http:' || url.substring(0, 6) == 'https:') {
42 return 'PROXY eproxy-<tenant name>.goskope.com:8081';
43 }
44
45 return 'DIRECT';

```

Finally, any URL or host that starts with http or https (web traffic) and doesn't match the above exclusions is to be redirected to the Netskope Cloud Explicit Proxy. Remaining URLs and hosts that do not match any of the conditions are to be accessed directly.

### Task 3.2 – Configure proxy URL and exclusions

- To redirect web traffic to your tenant Cloud Explicit Proxy, replace <tenant-name> with your tenant name in the line:

```
return 'PROXY eproxy-<tenant-name>.goskope.com:8081';
```

```

43 if (
44 url.substring(0, 5) == 'http:' ||
45 url.substring(0, 6) == 'https:'
46) {
47 return 'PROXY eproxy-nscaa-eu-.goskope.com:8081';
48 }
49 return 'DIRECT';
50 }

```

- To directly access your tenant's configured identity provider, replace .idp.com with .okta.com and remove comments around the condition.

```

28 /* Don't proxy IDP servers. */
29 if ((dnsDomainIs(host, '.okta.com')) {
30 return 'DIRECT'
31 }
32
33 /* Don't proxy for domains. */

```

*Note: Okta uses another domain for authentication: .oktacdn.com. Exclude it too.*

- To add an exclusion for the .octacdn.com domain, replace the condition

```
if ((dnsDomainIs(host, '.okta.com'))
```

with

```
if (dnsDomainIs(host, '.okta.com') || dnsDomainIs(host, '.oktacdn.com'))
```

```

28 /* Don't proxy IDP servers. */
29 if (dnsDomainIs(host, '.okta.com') || dnsDomainIs(host, '.oktacdn.com')) {
30 return 'DIRECT'
31 }
32
33 /* Don't proxy for domains. */

```

*IMPORTANT: Make sure to keep the opening curly bracket after the closing parenthesis of the condition.*

- To ensure direct access to the tenant itself, exclude .goskope.com

To do this, uncomment the code under /\* Don't proxy for domains. \*/ and replace the condition

```
if ((dnsDomainIs(host, '.domain-example1.com')) ||
(dnsDomainIs(host, '.domain-example2.com')))
```

with

```

28 /* Don't proxy IDP servers. */
29 if (dnsDomainIs(host, '.okta.com') || dnsDomainIs(host, '.oktacdn.com')) {
30 return 'DIRECT';
31 }
32 /* Don't proxy for domains. */
33 if (dnsDomainIs(host, '.goskope.com')) {
34 return 'DIRECT';
35 }
36
37 if (
38 url.substring(0, 5) === 'http:' ||
39 url.substring(0, 6) === 'https:'
40) {
41 return 'PROXY eproxy-nscaa-eu-01.goskope.com:8081';
42 }
43 return 'DIRECT';
44 }
45

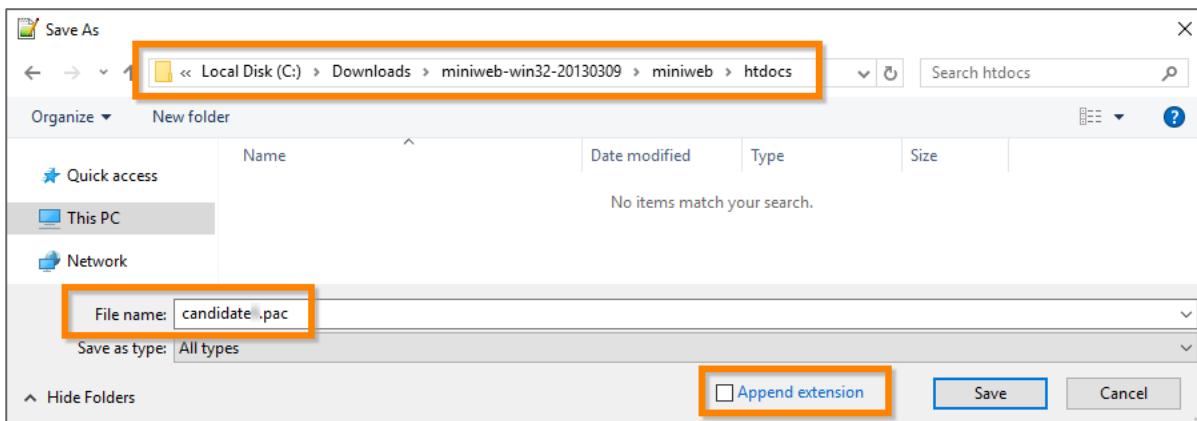
```

#### Part 4 – Configure proxy settings using a PAC file

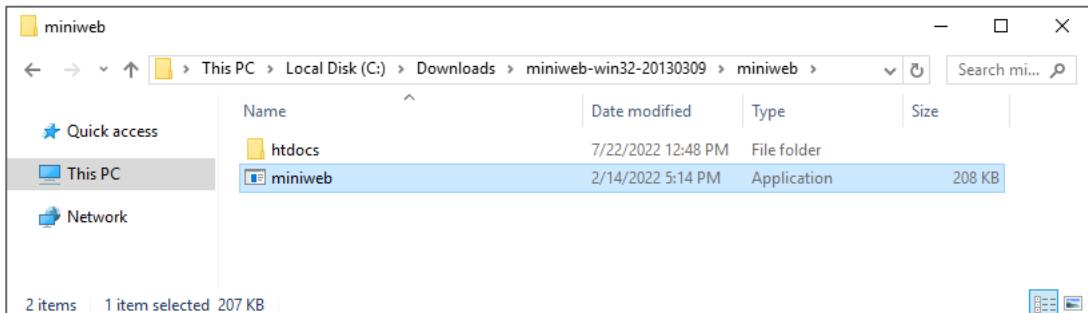
##### Task 4.1 – Publish the PAC file on a web server

This lab uses a simple web server running locally from your Amazon WorkSpace.

1. In Notepad++, click **File > Save As**, then navigate to C:\Downloads\miniweb-win32-20130309\miniweb\htdocs
2. Deselect the **Append extension** checkbox and save the file as candidate{X}.pac, where {X} is your student number.



3. Run File Explorer and navigate to C:\Downloads\miniweb-win32-20130309\miniweb
4. Run miniweb.exe.



- Do not close the command line window.

```
C:\Downloads\miniweb-win32-20130309\miniweb\miniweb.exe
MiniWeb (build 300, built on Feb 28 2013)
(C)2005-2013 Written by Stanley Huang <stanleyhuangyc@gmail.com>

Host: 172.16.0.64:8000
Web root: C:\Downloads\miniweb-win32-20130309\miniweb\htdocs
Max clients (per IP): 32 (16)
URL handlers: 2
Dir listing enabled
```

- To test that your web server is functioning, open a browser window and navigate to:

localhost:8000



## Task 4.2 – Import Netskope certificates into the local stores

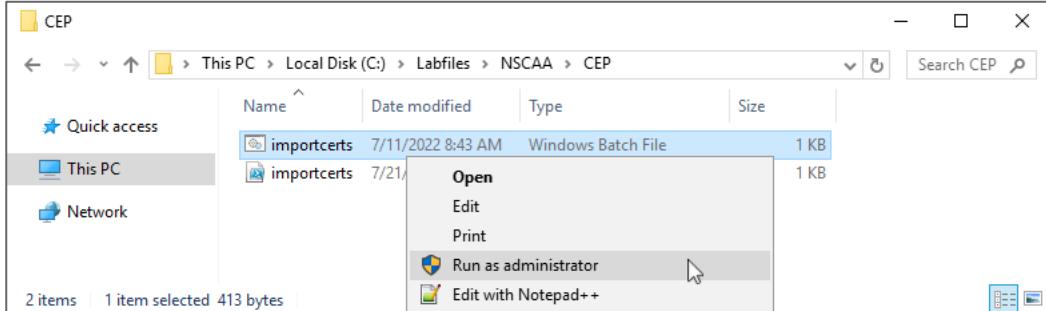
In this task you will download and import your tenant certificates into the local certificate stores to ensure that browsers trust site certificates that are signed by Netskope. In a production environment, you would distribute certificates via GPO or another management tool, depending on what kind of devices you are managing (e.g., Android, iPhone, Windows, etc.).

- In the Netskope tenant settings, navigate to **Manage > Certificates**.
- Switch to the **Signing CA** tab and download the three certificates to the default Downloads folder D:\Users\{Candidate{X}\Downloads.

The screenshot shows the Netskope Management interface. On the left, there's a sidebar with a key icon and a 'Manage' button. Below it are several options: Device Classification, External DLP Integrations, IRM Integration, Forward to Proxy Integration, Application Feature Support, and Certificates (which is highlighted in blue). The main content area has a title 'Certificates' and a subtitle 'Manage >'. It shows three tabs: TRUSTED CA, SIGNING CA (which is selected and underlined), and PRIVATE APP CERT. Below the tabs, there's a note: 'Download the Netskope root and intermediate certificates to setup trust from the devices.' followed by three download links: 'DOWNLOAD NETSKOPE ROOT CERTIFICATE', 'DOWNLOAD NETSKOPE INTERMEDIATE CERTIFICATE', and 'DOWNLOAD NETSKOPE ROOT CERTIFICATE (REMOTE USERS)'.

3. Open File Explorer and navigate to C:\Labfiles\NSCAA\CEP.
4. Run the batch file importcerts.bat as administrator.

*IMPORTANT: Do not run the PowerShell script by the same name.*



5. In the command prompt, type your student number.



6. Double-click the cert.log file to review the results.

```

cert - Notepad
File Edit Format View Help
You are candidate
The Cert path is D:\Users\candidate\Downloads
Importing Certs

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\Root
Thumbprint Subject

EE10C86887882C01E90ADAD00669FC8C7CA574D E=certadmin@netskope.com, CN=certadmin, OU=certadmin, O=Netskope Inc., L=S.
964BBF16DA82275E54A45A8D886C8E8200D835C9 E=certadmin@netskope.com, CN=eproxy.caadmin.netskope.com, OU=Cert Manageme.

PSParentPath: Microsoft.PowerShell.Security\Certificate::CurrentUser\My
Thumbprint Subject

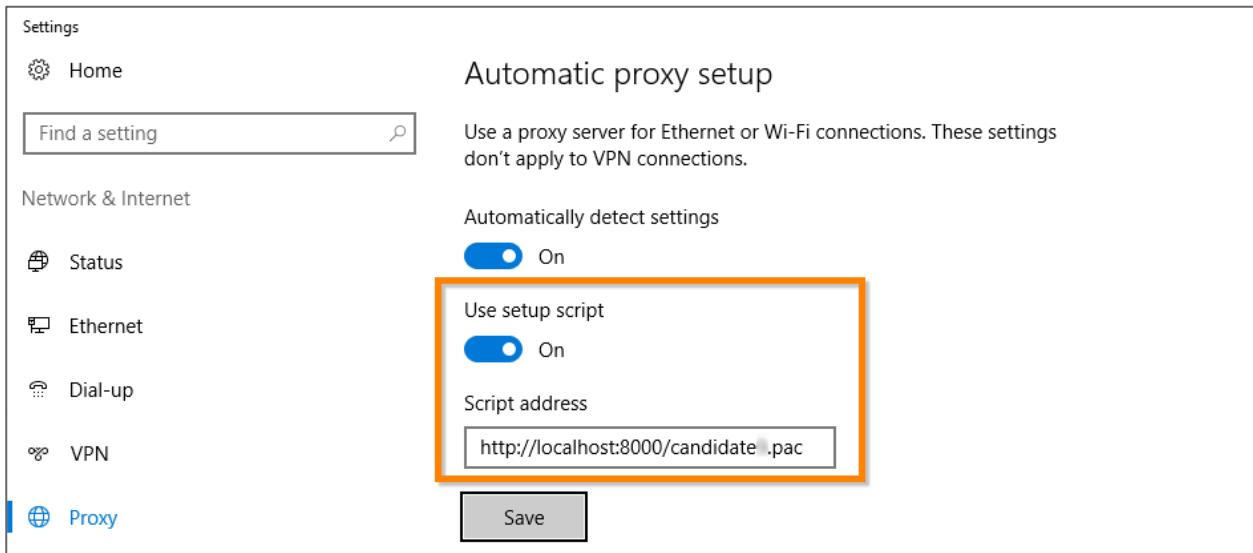
08A96BB228F0EF0FCEACA9B9AD3DFFEA58613C4 E=certadmin@netskope.com, CN=ca.nscaa-[REDACTED].gskope.com, OU=23a025b39050ad.

```

*Note: The script imports two of the certificates into the computer's root store and one into the user's personal store. If there are any errors, use the log to assist with troubleshooting.*

#### Task 4.3 – Set up system proxy settings to use the PAC file

1. Open system proxy settings (click **Start** > (settings) and navigate to **Network & Internet > Proxy**).
2. Set **Use setup script** to **On**.
3. In the **Script address** field, type the URL to your PAC file:  
`http://localhost:8000/candidate{X}.pac`
4. Click **Save**.

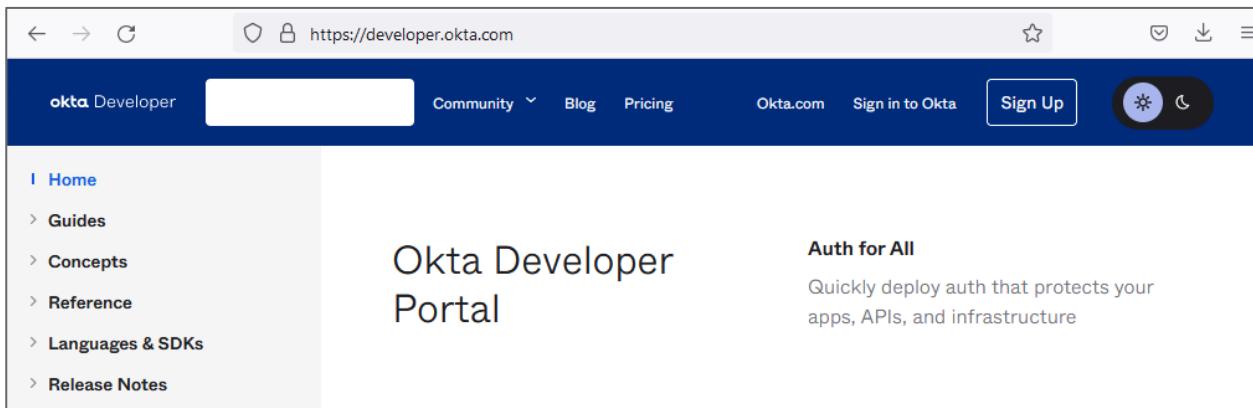


*Note: In a production environment, you can distribute proxy server settings via a GPO or another third-party tool, depending on the kind of devices you are managing.*

## Part 5 – CEP validation

### Task 5.1 – Validate direct connection to Okta developer website

1. Restart your browser, then open a new private/incognito browser window.
2. Navigate to developer.okta.com



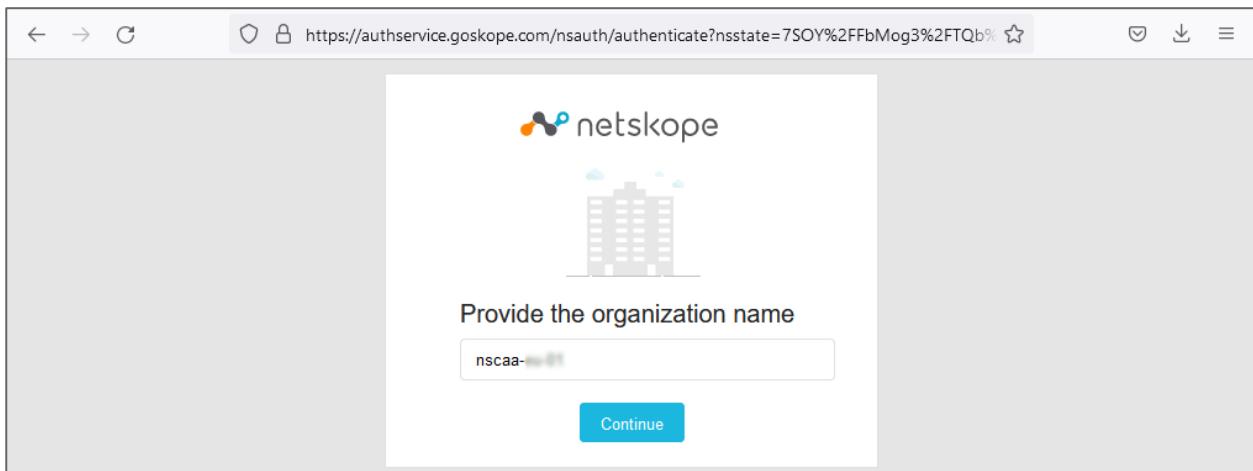
The website opens without any redirect.

### Task 5.2 – Validate redirection to Netskope Cloud Explicit Proxy

1. Navigate to www.cnn.com

*Note: The connection is redirected to the Netskope Cloud Explicit Proxy, which requires users to authenticate.*

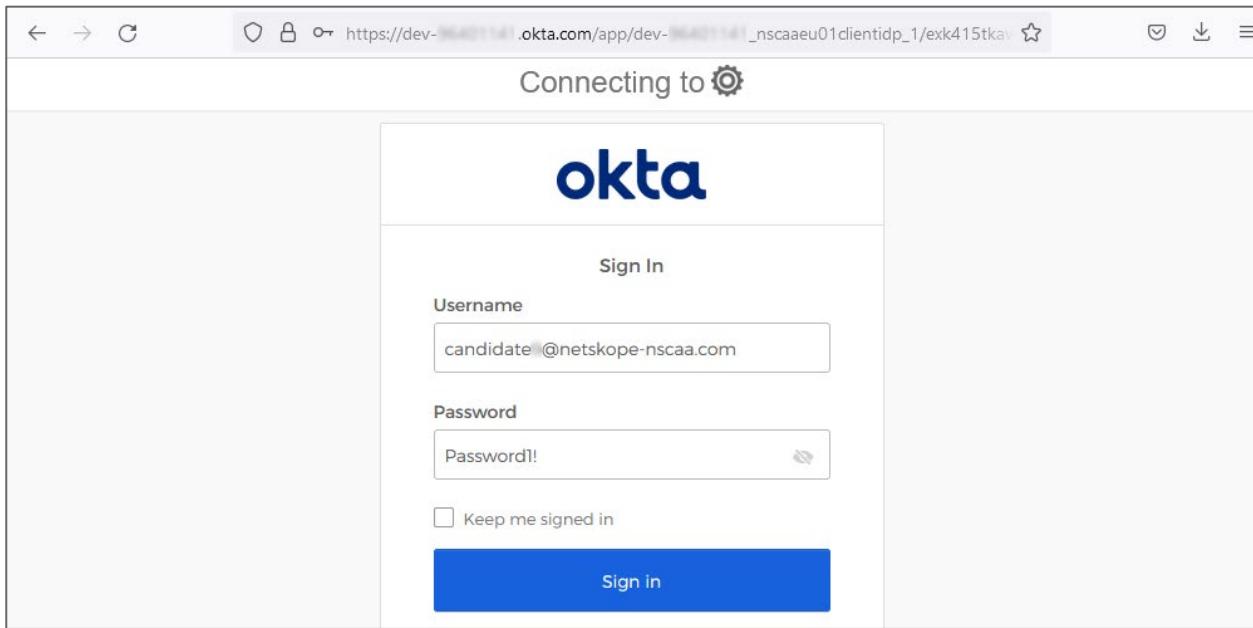
2. In the **Organization name** field, enter your Netskope tenant name without the domain name and click **Continue**.



3. On the Okta login page, authenticate with your Okta credentials:

Username: candidate{X}@netskope-nscaa.com

Password: Password1!



The browser will redirect you to the website.

4. In the Netskope tenant, navigate to **Skope IT™ > Page Events**.
5. Locate the event and click the magnifying glass icon (🔍) to review the **Page Event Details** pane.
6. Add the **Access Method** column and the **URL** column to the table. The Access Method is displayed as Explicit Proxy and the User is displayed as candidate{X}@netskope-nscaa.com.

| TIME | ACCESS METHOD  | USER                         | URL          |
|------|----------------|------------------------------|--------------|
| [@]  | Explicit Proxy | candidate@netskope-nscaa.com | www.cnn.com/ |

*Note: It may take a minute or two before the events appear. Refresh the page as necessary.*

**Lab Complete**

## Lab F: PAC file troubleshooting

You will practice how to troubleshoot a PAC file.

### Lab Tasks

During this lab, you will complete the following tasks:

- Create a broken PAC file and fix it.
- Add troubleshooting messages to the PAC file code.

### Part 1 – Detect coding errors in the PAC file

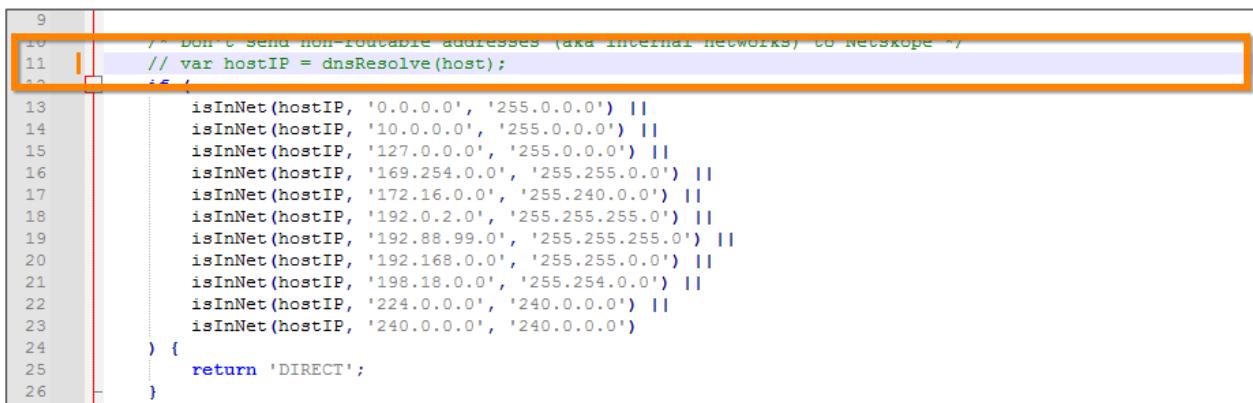
#### Task 1.1 – Modify the PAC file to add broken code

1. Open your PAC file in Notepad++:

C:\Downloads\miniweb-win32-20130309\miniweb\htdocs\candidate{X}.pac

2. Comment out the declaration of the hostIP variable by adding two forward slashes at the beginning of the line:

```
// var hostIP = dnsResolve(host);
```



```
9 /* DON't SEND NON-ROUTABLE addresses (aka internal networks) TO Netskope */
10 // var hostIP = dnsResolve(host);
11 if (
12 isInNet(hostIP, '0.0.0.0', '255.0.0.0') ||
13 isInNet(hostIP, '10.0.0.0', '255.0.0.0') ||
14 isInNet(hostIP, '127.0.0.0', '255.0.0.0') ||
15 isInNet(hostIP, '169.254.0.0', '255.255.0.0') ||
16 isInNet(hostIP, '172.16.0.0', '255.240.0.0') ||
17 isInNet(hostIP, '192.0.2.0', '255.255.255.0') ||
18 isInNet(hostIP, '192.88.99.0', '255.255.255.0') ||
19 isInNet(hostIP, '192.168.0.0', '255.255.0.0') ||
20 isInNet(hostIP, '198.18.0.0', '255.254.0.0') ||
21 isInNet(hostIP, '224.0.0.0', '240.0.0.0') ||
22 isInNet(hostIP, '240.0.0.0', '240.0.0.0')
23) {
24 return 'DIRECT';
25 }
26 }
```

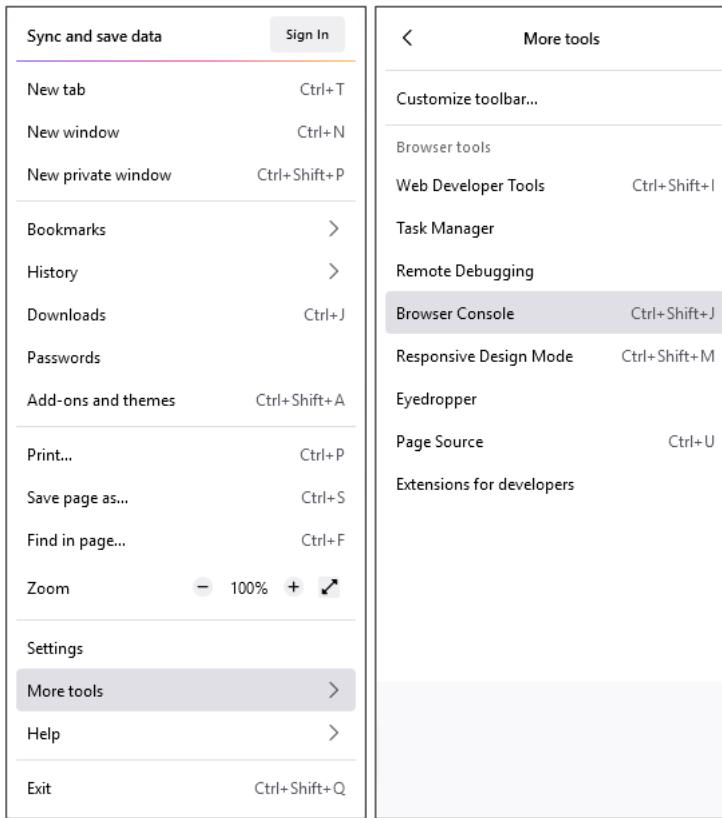
Now the code contains an error, as the variable **hostIP** is used by never declared.

3. Click **File > Save** in the top menu of Notepad++.

#### Task 1.2 – Locate the error in the PAC code

You will use Firefox throughout this lab because it provides much easier access to the PAC-related messages.

1. Restart your Firefox browser.
2. In a Firefox window, open the menu (≡) and navigate to **More tools > Browser Console**.



*Note: This is a different console from the more familiar web developer console accessible with the F12 keyboard shortcut.*

3. Ensure that Browser Console displays the source of the PAC file and an error processing the broken PAC file: hostIP is not defined.

The screenshot shows the Firefox Browser Console window. The 'Errors (3)' tab is selected, highlighted with an orange box. The console output shows several errors related to a PAC file named 'candidate9.pac' installed from 'http://localhost:8000/candidate9.pac'. The errors are: 'PAC Execution Error: hostIP is not defined []', repeated multiple times. The 'Logs' tab is also visible in the header.

```

1659618506603 addons.xpi WARN Checking C:\Program Files\Mozilla Firefox\distribution\extensions for addons
PAC file installed from http://localhost:8000/candidate9.pac
PAC Execution Error: hostIP is not defined []

```

*Note: Several unrelated issues might be reported that are usually related to issues with browser extensions. These can be safely ignored. To hide them, click the Errors label.*

### Task 1.3 – Fix the error in the PAC file

1. Open your PAC file with Notepad++.
2. Remove the two forward slashes before the declaration of the **hostIP** variable.

```

9
10 /* Don't send non routable addresses (aka internal networks) to Netskope */
11 var hostIP = dnsResolve(host);
12 if (
13 isInNet(hostIP, '0.0.0.0', '255.0.0.0') ||
14 isInNet(hostIP, '10.0.0.0', '255.0.0.0') ||
15 isInNet(hostIP, '127.0.0.0', '255.0.0.0') ||
16 isInNet(hostIP, '169.254.0.0', '255.255.0.0') ||
17 isInNet(hostIP, '172.16.0.0', '255.240.0.0') ||
18 isInNet(hostIP, '192.0.2.0', '255.255.255.0') ||
19 isInNet(hostIP, '192.88.99.0', '255.255.255.0') ||
20 isInNet(hostIP, '192.168.0.0', '255.255.0.0') ||
21 isInNet(hostIP, '198.18.0.0', '255.254.0.0') ||
22 isInNet(hostIP, '224.0.0.0', '240.0.0.0') ||
23 isInNet(hostIP, '240.0.0.0', '240.0.0.0')
24) {
25 return 'DIRECT';
26 }

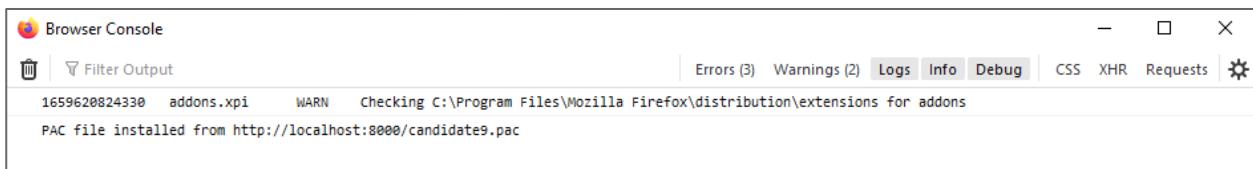
```

*Note: The function `isInNet` automatically resolves hostnames into IP addresses to check if the host belongs to a subnet.*

- To save your PAC file, click **File > Save**.

#### Task 1.4 – Verify the code

- Close all Firefox windows, including the Browser Console.
- Start Firefox and open the Browser Console: > More tools > Browser Console.
- Ensure that the PAC file has been loaded without errors.



## Part 2 – Add troubleshooting messages to the PAC file

#### Task 2.1 – Print a message about proxy decision

- Open your PAC file with Notepad++.
- Add the following lines right below the function definition:

```

var debugMode = true;
var debugMsg = "";

```

```

1 function FindProxyForURL(url, host) {
2 var debugMode = true;
3 var debugMsg = "";

```

*Note: The script will print or suppress troubleshooting messages depending on the value of the `debugMode` variable.*

- Add the following lines inside the condition for identity provider domains, right above the return statement:

```
debugMsg += "Proxy bypass for IDP servers";
```

```
if (debugMode) alert(debugMsg);
```

```
30 /* Don't proxy IDP servers. */
31 if (dnsDomainIs(host, '.okta.com') || dnsDomainIs(host, '.oktacdn.com')) {
32 debugMsg += "Proxy bypass for IDP servers";
33 if (debugMode) alert(debugMsg);
34 return 'DIRECT'
35 }
```

4. Add the lines to print another message above the line that redirects web traffic to proxy:

```
debugMsg += "Redirect to proxy for web traffic";
if (debugMode) alert(debugMsg);
```

```
42 if (
43 url.substring(0, 5) === 'http:' ||
44 url.substring(0, 6) === 'https:'
45) {
46 debugMsg += "Redirect to proxy for web traffic";
47 if (debugMode) alert(debugMsg);
48 return 'PROXY eproxy-nscaa-eu-goskope.com:8081';
49 }
```

*Note: In a production environment, you would want to print the PAC decision before every return statement. To save time, you won't be doing this step as part of this lab.*

5. To save the file, click **File > Save**.

### Task 2.2 – Verify the new PAC code

1. Close all Firefox windows, including the Browser Console.
2. Start Firefox and open the Browser Console: > More tools > Browser Console.
3. Open a new private Firefox window and navigate to developer.okta.com
4. Ensure that in the Browser Console there are messages about bypassing proxy for IdP servers as well as about redirecting web traffic to proxy.



The messages don't tell us which URL is being accessed. You will fix this in the next task.

### Part 3 – Add context information to the troubleshooting message

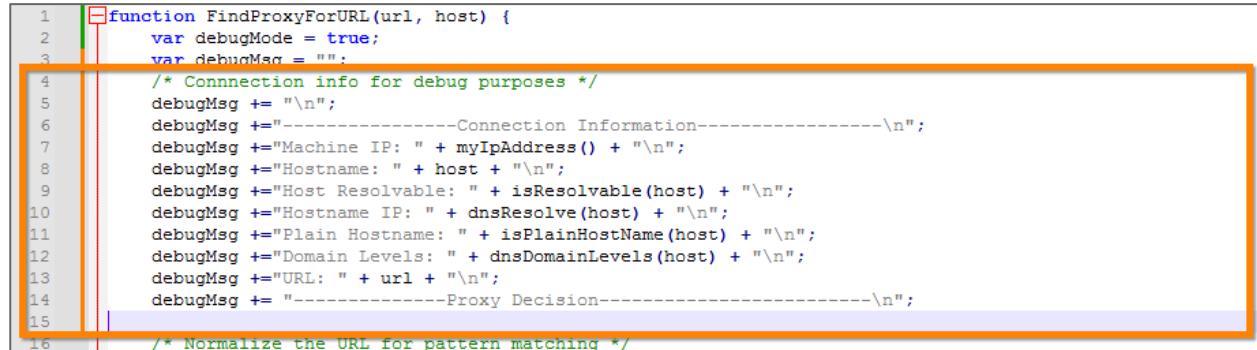
#### Task 3.1 – Print information about the requested URL

1. Open your PAC file with Notepad++.
2. Add the following lines right below the initial var debugMsg = ""; statement:  
/\* Connection info for debug purposes \*/

```

debugMsg += "\n";
debugMsg += "-----Connection Information-----\n";
debugMsg += "Machine IP: " + myIpAddress() + "\n";
debugMsg += "Hostname: " + host + "\n";
debugMsg += "Host Resolvable: " + isResolvable(host) + "\n";
debugMsg += "Hostname IP: " + dnsResolve(host) + "\n";
debugMsg += "Plain Hostname: " + isPlainHostName(host) + "\n";
debugMsg += "Domain Levels: " + dnsDomainLevels(host) + "\n";
debugMsg += "URL: " + url + "\n";
debugMsg += "-----Proxy Decision-----\n";

```



```

1 function FindProxyForURL(url, host) {
2 var debugMode = true;
3 var debugMsg = "";
4 /* Connection info for debug purposes */
5 debugMsg += "\n";
6 debugMsg += "-----Connection Information-----\n";
7 debugMsg += "Machine IP: " + myIpAddress() + "\n";
8 debugMsg += "Hostname: " + host + "\n";
9 debugMsg += "Host Resolvable: " + isResolvable(host) + "\n";
10 debugMsg += "Hostname IP: " + dnsResolve(host) + "\n";
11 debugMsg += "Plain Hostname: " + isPlainHostName(host) + "\n";
12 debugMsg += "Domain Levels: " + dnsDomainLevels(host) + "\n";
13 debugMsg += "URL: " + url + "\n";
14 debugMsg += "-----Proxy Decision-----\n";
15
16 /* Normalize the URL for pattern matching */

```

- To save the file, click **File > Save**.

### Task 3.2 – Verify the new PAC code

- Close all Firefox windows, including the Browser Console.
- Start Firefox and open the Browser Console:  > More tools > Browser Console.
- Notice that there are already messages about the traffic generated by the browser itself even before you typed any URL.



- Open a new private Firefox window and navigate to developer.okta.com

5. Ensure that in the Browser Console the messages include detailed connection info.



```
PAC-alert:
-----Connection Information-----
Machine IP: 172.31.17.9
Hostname: developer.okta.com
Host Resolvable: true
Hostname IP: 54.192.76.52
Plain Hostname: false
Domain Levels: 2
URL: https://developer.okta.com/
-----Proxy Decision-----
Proxy bypass for IDP servers
PAC-alert:
```

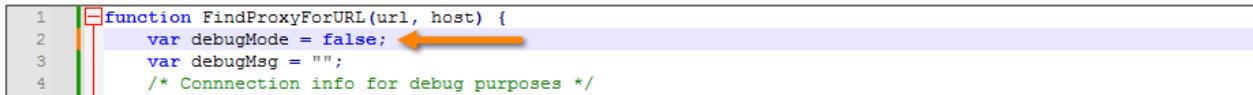
## Part 4 – Disable troubleshooting messages

### Task 4.1 – Set debugMode to false

1. Open your PAC file with Notepad++.

2. Change the statement

```
var debugMode = true;
to
var debugMode = false;
```



```
1 function FindProxyForURL(url, host) {
2 var debugMode = false; ←
3 var debugMsg = "";
4 /* Connection info for debug purposes */
```

3. To save the file, click **File > Save**.

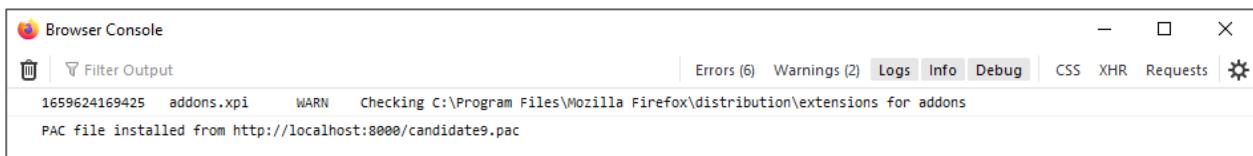
### Task 4.2 – Verify the new PAC code

1. Close all Firefox windows, including the Browser Console.

2. Start Firefox and open the Browser Console:  > More tools > Browser Console.

3. Open a new private Firefox window and navigate to developer.okta.com

4. Ensure that in the Browser Console there are no debugging messages.



```
Browser Console
Filter Output
Errors (6) Warnings (2) Logs Info Debug CSS XHR Requests
1659624169425 addons.xpi WARN Checking C:\Program Files\Mozilla Firefox\distribution\extensions for addons
PAC file installed from http://localhost:8000/candidate9.pac
```

**Lab Complete**

## Lab G: Investigating with Netskope Advanced Analytics

In this lab, you will examine how to investigate a user's suspicious activities using Netskope Advanced Analytics.

### Scenario

You have been informed of a possible insider threat. An employee (candidate1@netskope-nscaa.com) is acting suspiciously, and there is concern that this employee is exfiltrating data. In addition, the system has already generated a Behavior Analytics alert about a Bulk Download by this user.

The screenshot shows a detailed view of a Behavior Analytics alert. At the top, it says 'Incidents > Behavior Analytics >'. Below that is the title '← Bulk Download - Download via Client in Microsoft Office 365 OneDrive for Business'. Underneath the title, there is a summary bar with '20 Event' (represented by a calendar icon), 'User: [REDACTED]@netskope.com' (represented by a person icon), 'Score Impact: -50' (represented by a bar chart icon), and 'Status: Unacknowledged' (represented by a shield icon). A blue button labeled 'ACKNOWLEDGE ALERT' is visible. Below the summary bar, there are two tabs: 'SUMMARY' (which is underlined) and 'ALERT & EVENTS'. The 'SUMMARY' tab displays several details in boxes: 'Application' (Microsoft Office 365 OneDrive for Business), 'Instance' (empty), 'User' ([REDACTED]@netskope.com), and 'Device' (Windows Device).

You will investigate this user to understand if sensitive data has been exfiltrated and whether there are any gaps in the security policies. You will use Netskope Advanced Analytics and Sankey visualizations to answer the questions throughout this lab.

### Lab Tasks

During this lab, you will complete the following tasks:

- Investigate the suspicious user.
- Determine how this person has exfiltrated credit card information.

At the conclusion of the exercise, you will send a private message to the instructor with the app name and activity detected.

### Part 1 – Review the user's activities using Advanced Analytics

1. Log in to your Netskope tenant.
2. From the left navigation pane, select **Advanced Analytics > Explore**.

3. From the **Data Collection** dropdown menu at the top-right corner of the page, select **Application Events**.

The screenshot shows the Netskope Advanced Analytics interface. On the left, there's a sidebar with a logo, a back arrow, and the text "Advanced Analytics > Explore". Below this are sections for "Folders" (Personal, Group, Netskope Library) and "Explore". At the top right, there's a "Data Collection" dropdown menu with the following options: Alerts, Application Events (which is highlighted with a blue background and a cursor icon), Cloud Firewall Events, Network Events, and Page Events.

4. In the left menu of Advanced Analytics, expand the **Application Events > User** section.  
 5. Hover over the **User** dimension and click the **Filter by field** icon.

This screenshot shows the "Application Events" section under "User". A red arrow points to the "Filter by field" button, which is highlighted with a black border and a cursor icon.

6. Expand the **Filters** section.

This screenshot shows the "Filters" section expanded. It contains two filter rules:

- Application Events Event Date**: Set to "is in the past" for 7 days.
- Application Events User**: Set to "is equal to" (with a placeholder field).

A red box highlights the second filter rule.

- Under the **Application Events Event Date** filter and to the right of the dropdown menu (which should be set to **is in the past**), change the number to 120 days.
- Under the **Application Events Users** filter and to the right of the dropdown menu (which should currently be set to **is equal to**), enter the username `candidate1@netskope-nscaa.com`.

The screenshot shows the 'Application Events' search interface. On the left, there's a sidebar with fields like 'All Fields' (selected), 'In Use', 'To User Category', 'User', 'User Category', 'User Group', and 'User IP'. On the right, under 'Filters (2)', there are two entries: 'Application Events Event Date' with the condition 'is in the past' for 120 days, and 'Application Events User' with the condition 'is equal to' set to 'candidate1@netskope-nscaa.com'.

Next, you will add the Events measure.

- To the left of the **Filters** section, in the **Application Events** search field, type `#`
- Under **Application Events > Measures**, select `# Events`.

The screenshot shows the 'Explore' interface. In the 'Application Events' search field, the character '#' is typed. Below the search field, under the heading 'MEASURES', the option '# Events' is listed and highlighted with a blue selection bar. Other options include '# Applications', '# Blocked Events', '# Device Types', '# Instances', '# Objects', '# Sessions', '# Users', and '# Hostnames'.

11. Click **Run** at the top-right of the page.

The screenshot shows the Netskope Explore interface. On the left, there's a sidebar with 'Application Events' selected. Under 'All Fields', several metrics are listed: # Applications, # Blocked Events, # Device Types, # Events (which is highlighted), # Instances, # Objects, # Sessions, # Users, and # Hostnames. In the main area, there are two filters: 'Application Events Event' (Required) set to 'is in the past' for 120 days, and 'Application Events Use' set to 'is equal to' candidate1@netskope-nscaa.com. At the top right, there's a 'Run' button with an orange border, and a 'Custom Filter' checkbox. Below the filters, there's a 'Visualization' section with tabs for 'Data' (selected) and 'Results'. A 'Row Limit' dropdown is set to 500, and a 'Totals' checkbox is unchecked. The results table shows one row for 'Application Events # Events' with a value of 1 and a total of 68.

*Note: There are several access methods for importing data into the Netskope environment, so some of the same events are captured through multiple products, resulting in duplicate events. For example, an event captured by API Connector can also be captured by Next Generation Secure Web Gateway Inline (NG SWG/Inline). To ensure events are not duplicated, a filter needs to be added.*

12. In the **Application Events** search field, type: Access Method

13. From the results displayed, click the **Filter by field** icon (🔍) to the right of **Access Method**.

This screenshot shows the same Explore interface as above, but with a different search term in the 'Application Events' search bar: 'Access Method'. In the 'General' section of the sidebar, there are two items: 'Access Method' and 'Traffic Type'. To the right of 'Access Method', there is a 'Filter by field' icon (a magnifying glass with a minus sign). An orange arrow points to this icon, indicating where to click.

You should now see **Application Events Access Method** as an option in the **Filters** section.

14. Under the **Application Events Access Method** filter and to the right of the dropdown menu (which should currently be set to **is equal to**), enter: API Connector

The screenshot shows the 'Application Events' search interface. On the left, there's a sidebar with 'All Fields' and 'In Use'. Below it, under 'Application Events', there are 'DIMENSIONS' and 'General' sections. In the 'General' section, 'Access Method' is selected. On the right, there are three filters applied:

- Application Events Access Method:** Set to 'is not equal to' and 'API Connector'.
- Application Events Event Date:** Set to 'is in the past' with a value of '120' and 'days'.
- Application Events User:** Set to 'is equal to' and 'candidate1@netskope-nscaa.com'.

15. Click **Run**.

*Note: Adding a filter to exclude API Connector events removes any events generated by data at rest analysis and leaves the inline (i.e., data in motion) events.*

## Part 2 – What other identities are being used in the environment by the same user?

Is this user using other logins and accounts to exfiltrate sensitive company data? You will add the From User field to identify the identity/login used to access SaaS applications.

1. In the **Filters** section, click the gear icon (⚙️) next to **Application Events User** to add this field to the **Data** table.

The screenshot shows the 'Application Events' search interface with the same three filters as before. The third filter, 'Application Events User', has its 'Add to table' button highlighted with an orange box. A hand cursor icon is shown over the button, indicating it can be clicked to add the user field to the data table.

2. In the **Application Events** search field, type: From User

3. Under **User**, click the **From User** dimension to add it to the Data section.

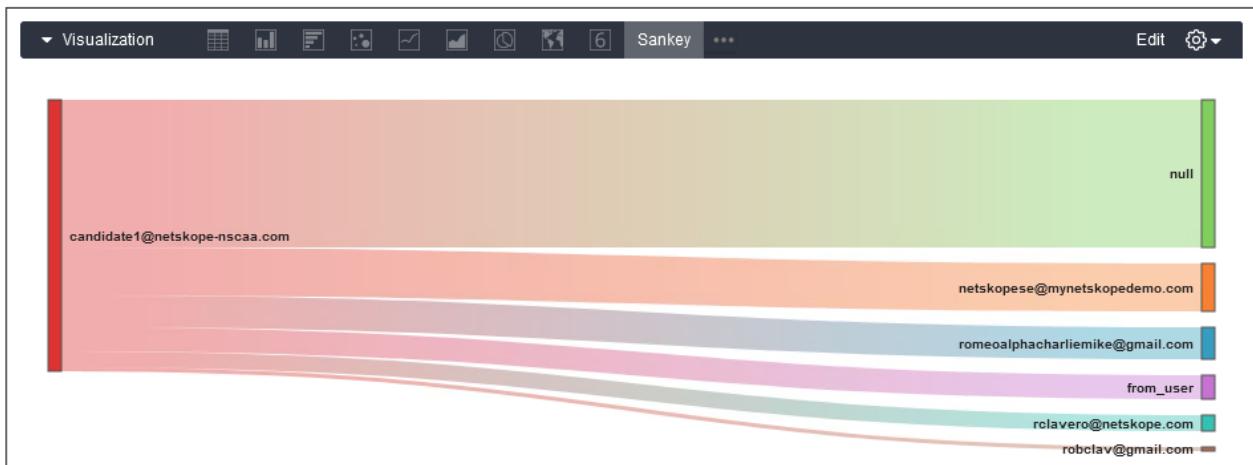
4. Click **Run**. In the **Data** section, you should see the **Application Events User** column as the left column and the **Application Events From User** column as the middle column. Next, you will select how the report is to be visualized.

| Application Events User         | Application Events From User   | Application Events # Events ↓ |
|---------------------------------|--------------------------------|-------------------------------|
| 1 candidate1@netskope-nscaa.com | ∅                              | 37                            |
| 2 candidate1@netskope-nscaa.com | netskopese@mynetskopedemo.com  | 12                            |
| 3 candidate1@netskope-nscaa.com | romeoalphcharliemike@gmail.com | 8                             |
| 4 candidate1@netskope-nscaa.com | from_user                      | 6                             |
| 5 candidate1@netskope-nscaa.com | rclavero@netskope.com          | 4                             |
| 6 candidate1@netskope-nscaa.com | robclav@gmail.com              | 1                             |

5. Expand the **Visualization** section, by clicking the arrow (▶) icon.



6. In the **Visualization** section, click the additional menu option icon (⋮⋮⋮) and select the **Sankey** option.



In the example screenshot above, the Sankey visualization shows the corporate identity `rclavero@netskope.com`. It also captured a personal identity

romeoalphacharliemlke@gmail.com. This second identity appears suspicious and warrants further investigation.

Your report might differ from the screenshot displayed in this guide. Review your report and determine the identities/accounts the user has been using to access cloud resources.

*Note: The null value in the identity column refers to any activity performed that did not require identity authentication (for example, browsing to a website such as the Wall Street Journal — <http://wsj.com>).*

### Part 3 – What applications is the user accessing?

Now that you have discovered the user's other identities, you need to investigate which applications these identities are using.

1. In the left menu of Advanced Analytics, clear the search field, then navigate to **Application Events > Application**
2. Click **Application** to add this dimension to the **Data** section.

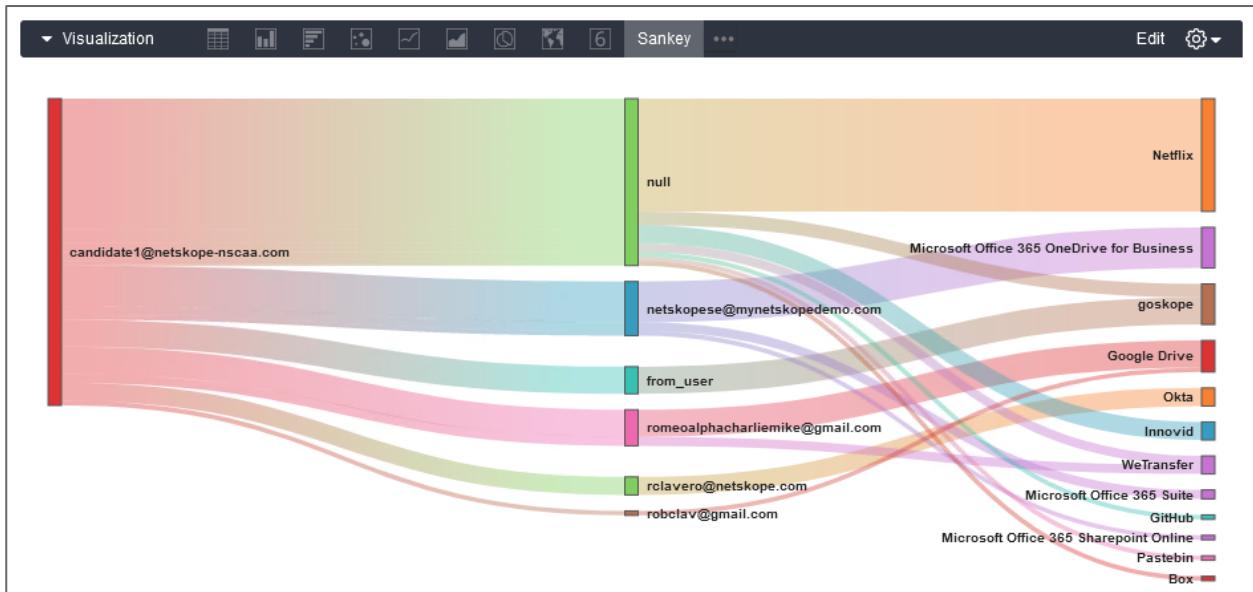
The screenshot shows the 'Application Events' interface. At the top, there is a search bar. Below it, two tabs are visible: 'All Fields' (which is selected) and 'In Use'. Under 'All Fields', there are sections for 'Custom Fields' and 'Application Events'. 'Application Events' has a count of 4. Below these are sections for 'FILTER-ONLY FIELDS' (containing 'IP Filters') and 'DIMENSIONS' (containing 'User', 'Alert', 'API Protection', and 'Application'). The 'Application' dimension is expanded, showing its fields: 'Application' and 'Application Instance ID'. A mouse cursor is hovering over the 'Application' field. The entire 'Application' section is highlighted with an orange box.

3. Click Run.

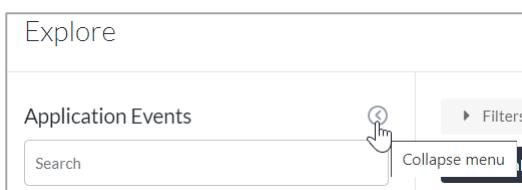
| Data |                               | Results                        |                              | Row Limit                                  | 500                           | <input type="checkbox"/> Totals | <input type="checkbox"/> Subtotals |
|------|-------------------------------|--------------------------------|------------------------------|--------------------------------------------|-------------------------------|---------------------------------|------------------------------------|
|      |                               | Application Events User        | Application Events From User | Application Events Application             | Application Events # Events ↓ |                                 |                                    |
| 1    | candidate1@netskope-nscaa.com | ∅                              |                              | Netflix                                    | 25                            |                                 |                                    |
| 2    | candidate1@netskope-nscaa.com | netskope@mynetskopedemo.com    |                              | Microsoft Office 365 OneDrive for Business | 9                             |                                 |                                    |
| 3    | candidate1@netskope-nscaa.com | from_user                      |                              | goskope                                    | 6                             |                                 |                                    |
| 4    | candidate1@netskope-nscaa.com | romealphacharliemike@gmail.com |                              | Google Drive                               | 6                             |                                 |                                    |
| 5    | candidate1@netskope-nscaa.com | rclavero@netskope.com          |                              | Okta                                       | 4                             |                                 |                                    |
| 6    | candidate1@netskope-nscaa.com | ∅                              |                              | Innovid                                    | 4                             |                                 |                                    |
| 7    | candidate1@netskope-nscaa.com | ∅                              |                              | goskope                                    | 3                             |                                 |                                    |
| 8    | candidate1@netskope-nscaa.com | romealphacharliemike@gmail.com |                              | WeTransfer                                 | 2                             |                                 |                                    |
| 9    | candidate1@netskope-nscaa.com | netskope@mynetskopedemo.com    |                              | Microsoft Office 365 Suite                 | 2                             |                                 |                                    |
| 10   | candidate1@netskope-nscaa.com | ∅                              |                              | WeTransfer                                 | 2                             |                                 |                                    |
| 11   | candidate1@netskope-nscaa.com | ∅                              |                              | Github                                     | 1                             |                                 |                                    |
| 12   | candidate1@netskope-nscaa.com | netskope@mynetskopedemo.com    |                              | Microsoft Office 365 Sharepoint Online     | 1                             |                                 |                                    |
| 13   | candidate1@netskope-nscaa.com | robclav@gmail.com              |                              | Google Drive                               | 1                             |                                 |                                    |
| 14   | candidate1@netskope-nscaa.com | ∅                              |                              | Pastebin                                   | 1                             |                                 |                                    |
| 15   | candidate1@netskope-nscaa.com | ∅                              |                              | Box                                        | 1                             |                                 |                                    |

4. Review the results in the Sankey visualization. You should observe the following:

- The user had been accessing risky applications such as WeTransfer and Pastebin.
- Google Drive was accessed using two different identities, neither of which appear to be the user's corporate identity.



*Hint: To see the full expanded view of the Visualization, minimize the Application Events/Search left menu pane using the arrow icon (<) to collapse the menu.*



#### Part 4 – Which instances of the application is the user accessing?

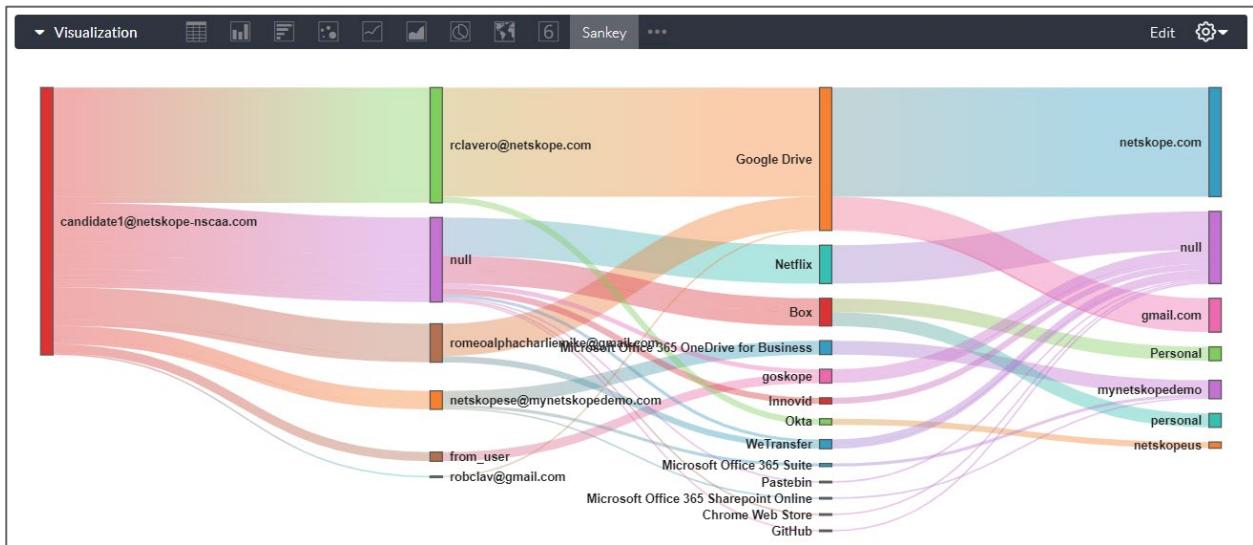
Next, you will investigate whether the user has been accessing instances of the applications using different identities by filtering for the application instance ID.

1. In the left menu of Advanced Analytics, navigate to **Application Events > Application**, then click **Application Instance ID** to add it to the **Data** section of the report.

The screenshot shows the 'Application Events' interface. At the top is a search bar. Below it are two tabs: 'All Fields' (which is selected) and 'In Use'. Under 'All Fields', there is a '+ Add' button. Below that is a section titled 'FILTER-ONLY FIELDS' which contains 'IP Filters' and 'DIMENSIONS'. Under 'DIMENSIONS', 'User' is selected. Under 'Application', 'Application' is selected. At the bottom of this list is 'Application Instance ID', which is highlighted with an orange box.

2. Click **Run**.

| Data                    |                               | Results                         |                                            |                                                                                  |                             |  |
|-------------------------|-------------------------------|---------------------------------|--------------------------------------------|----------------------------------------------------------------------------------|-----------------------------|--|
|                         |                               |                                 |                                            | Row Limit 500 <input type="checkbox"/> Totals <input type="checkbox"/> Subtotals |                             |  |
| Application Events User |                               | Application Events From User    | Application Events Application             | Application Events Application Instance ID                                       | Application Events # Events |  |
| 1                       | candidate1@netskope-nscaa.com | rclavero@netskope.com           | Google Drive                               | netskope.com                                                                     | 71                          |  |
| 2                       | candidate1@netskope-nscaa.com | Ø                               | Netflix                                    | Ø                                                                                | 25                          |  |
| 3                       | candidate1@netskope-nscaa.com | romeoalphacharliemike@gmail.com | Google Drive                               | gmail.com                                                                        | 21                          |  |
| 4                       | candidate1@netskope-nscaa.com | Ø                               | Box                                        | Personal                                                                         | 9                           |  |
| 5                       | candidate1@netskope-nscaa.com | netskope@mynetskopedemo.com     | Microsoft Office 365 OneDrive for Business | mynetskopedemo                                                                   | 9                           |  |
| 6                       | candidate1@netskope-nscaa.com | Ø                               | Box                                        | personal                                                                         | 9                           |  |
| 7                       | candidate1@netskope-nscaa.com | from_user                       | goskope                                    | Ø                                                                                | 6                           |  |
| 8                       | candidate1@netskope-nscaa.com | Ø                               | Innovid                                    | Ø                                                                                | 4                           |  |
| 9                       | candidate1@netskope-nscaa.com | rclavero@netskope.com           | Okta                                       | netskopeus                                                                       | 4                           |  |
| 10                      | candidate1@netskope-nscaa.com | romeoalphacharliemike@gmail.com | WeTransfer                                 | Ø                                                                                | 4                           |  |
| 11                      | candidate1@netskope-nscaa.com | Ø                               | goskope                                    | Ø                                                                                | 3                           |  |
| 12                      | candidate1@netskope-nscaa.com | Ø                               | WeTransfer                                 | Ø                                                                                | 2                           |  |
| 13                      | candidate1@netskope-nscaa.com | netskope@mynetskopedemo.com     | Microsoft Office 365 Suite                 | mynetskopedemo                                                                   | 2                           |  |
| 14                      | candidate1@netskope-nscaa.com | Ø                               | Pastebin                                   | Ø                                                                                | 1                           |  |
| 15                      | candidate1@netskope-nscaa.com | robclav@gmail.com               | Google Drive                               | gmail.com                                                                        | 1                           |  |

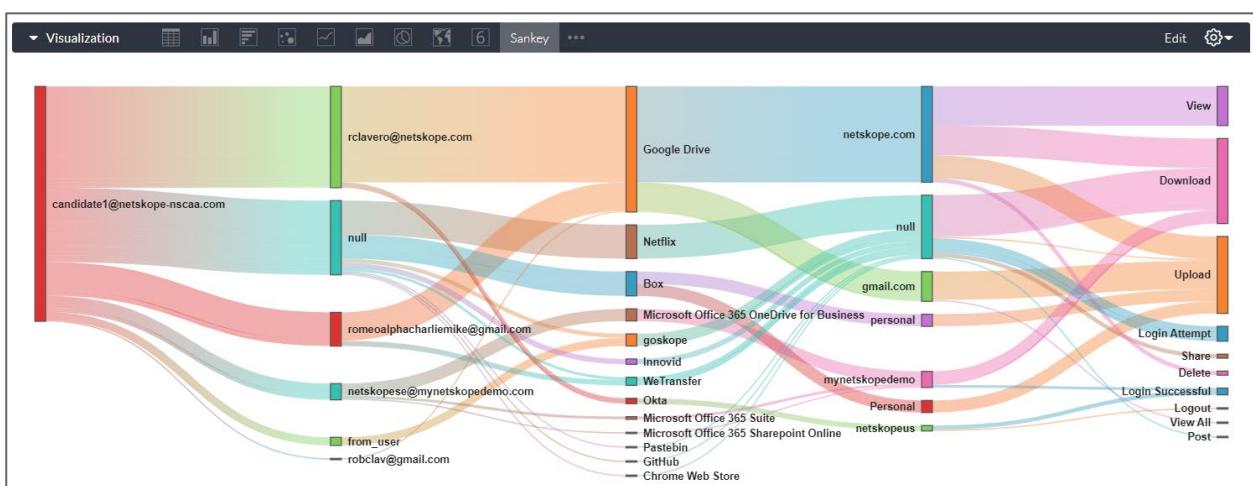


#### Part 5 – Which activities is the user performing in these applications?

You have now determined that candidate1 used personal identities to access Google Drive as well as some risky applications such as Pastebin and Wetransfer. To figure out if the user performed any suspicious activities in these applications and instances, you will include the Activity field in the Data table.

1. In the **Application Events** search field, type: **Activity**
2. Select **Activity** under **General** to add to the **Data** section.
3. Click **Run** to update the report.

*Note: The last column of the Sankey visualization displays the different activities performed by the user.*



## Part 6 – Create a filter for high-risk activities

You will create a filter for this user's activities, filtering for high-risk activities: Downloads, Uploads, Shares, and Posts.

1. Click the **In Use** tab in the left menu pane under the **Application Events search field** to apply a filter to an existing data field.

The screenshot shows the 'Application Events' search interface. At the top, there is a search bar and a 'Search' button. Below it, there are two tabs: 'All Fields' and 'In Use', with 'In Use' highlighted by an orange rectangle. Underneath these tabs is a section titled 'Application Events' with a minus sign icon. This section contains several data fields, each with a small filter icon to its right. The fields listed are: 'From User • User', 'User • User', 'Application • Application', 'Application Instance ID • Application', 'Access Method • General', 'Activity • General', 'Event Date • Time', and '# Events'. The '# Events' field is highlighted with an orange rectangle.

2. To create a filter for an existing data field, click the **Filter by field** icon ( ) for the **Activity • General** data field to add it to the **Filters** section.

The screenshot shows the same 'Application Events' search interface as the previous one, but with a different state. The 'In Use' tab is now highlighted with a blue underline. The 'Activity • General' field has a filter icon to its right, which is now highlighted with a black rectangle and a white cursor icon pointing at it. The other fields remain the same. At the bottom of the interface, there are two buttons: 'Clear all' and 'Clear fields, keep filters'.

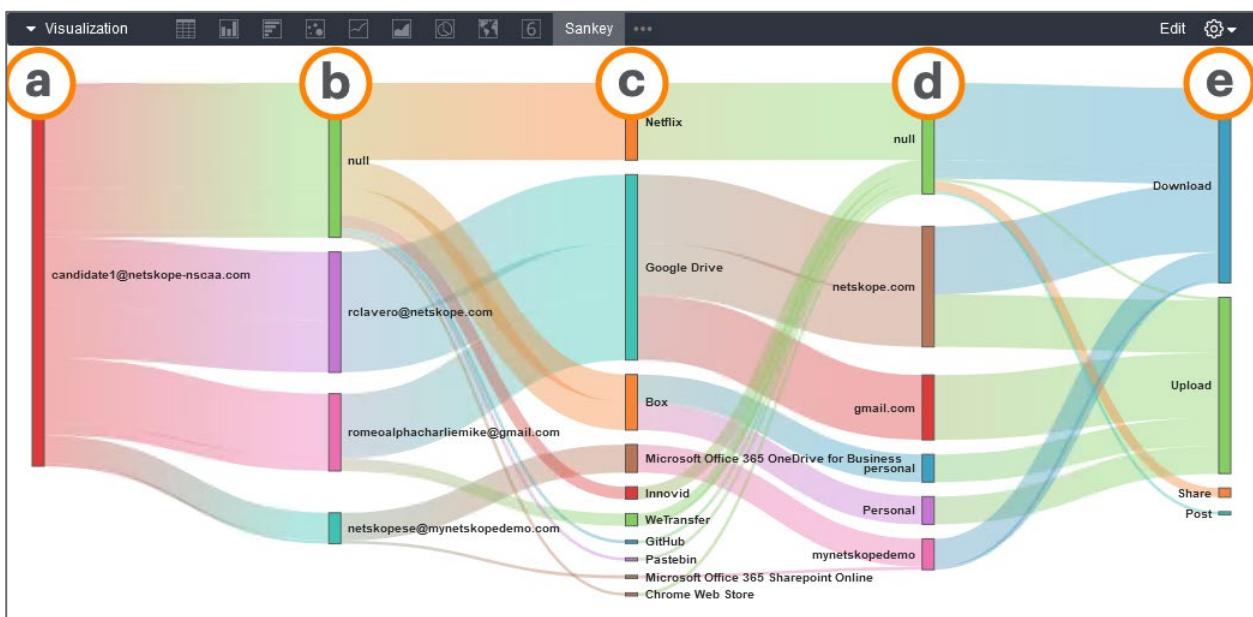
3. In the **Filters** section, under the **Application Events Activity** filter and in the field to the right of the dropdown menu (which should currently be set to **is equal to**), and select **Download, Post, Share, and Upload**.

4. Click **Run**.

5. Collapse the **Application Events** left menu pane and minimize the **Filters** and **Data** sections to fully view the Sankey visualization.

The report now shows Candidate1's data in the Sankey columns. From left to right, here is a summary of what you should see:

- The candidate's username (`candidate1@netskope-nscaa.com`)
- The identities associated with this user
- The list of applications accessed by the user
- The instances for each application
- Activities such as Uploads, Downloads, Shares, and Posts

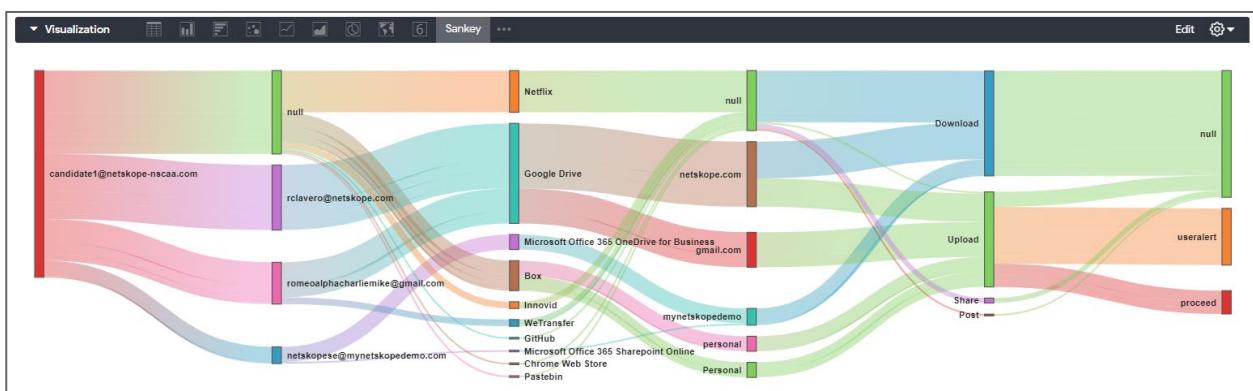


#### Part 7 – What security actions were implemented to control this user's activities?

You have observed that the user in question is uploading and posting to personal instances of Google Drive and to risky apps. However, these activities may not be an issue if there are policies in place to alert and block these activities. Next, you will check to see which policy actions occurred.

1. Expand the **Application Events** left menu pane by clicking the **arrow icon (↗)**.
2. In the **Application Events search field**, type: Action
3. Under **Policy**, click **Action** to add it to the **Data** section.

4. Click **Run**.

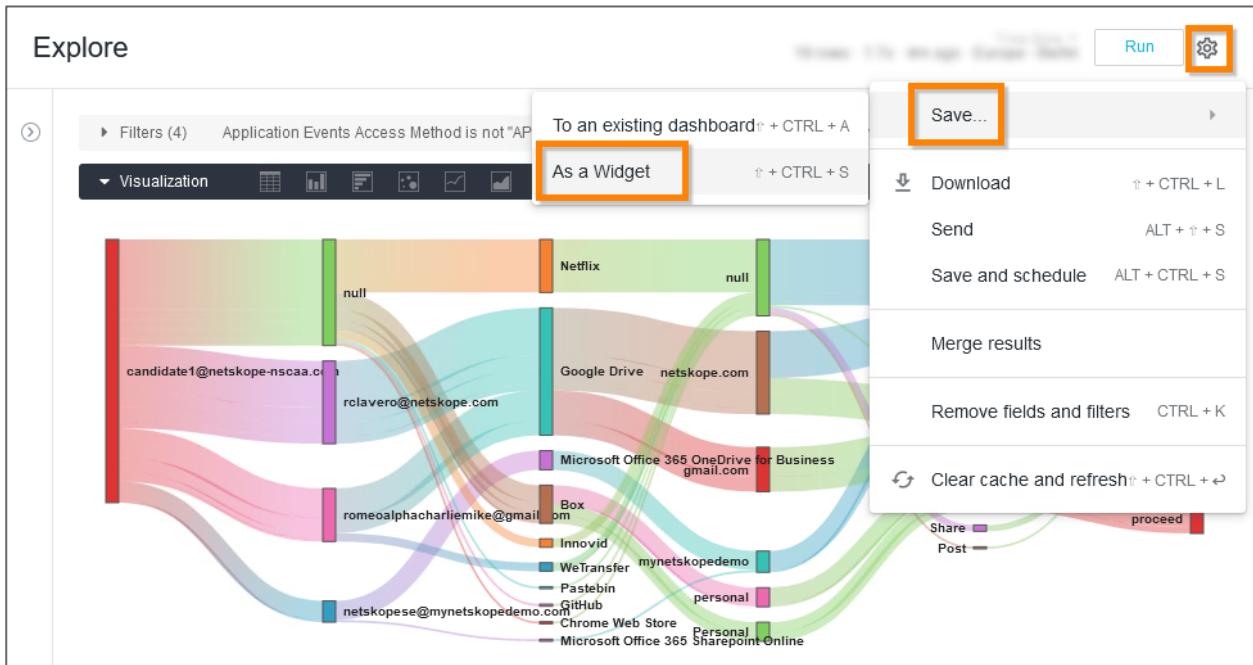


### Part 8 – Save the report as a widget

You have the option to save this investigation as a widget or add it to an existing dashboard.

1. Click the **settings gear icon** next to the **Run** button.

2. Click **Save > As a Widget**.



3. Enter Candidate{X}-AALAB (where {X} is your student number) as the title of the widget.

The screenshot shows the 'Save Widget' dialog box. The 'Title' field is filled with 'Candidate -AALAB'. The 'Folder' field is set to 'Personal'. At the bottom, there are 'Save & View Widget' and 'Save' buttons.

4. Click **Save & View Widget**.

**Lab Complete**