# Exporting data to CSV file using API script

Quick guide

# Table of Contents

## Overview

This document details how to use a Proofpoint Meta API script for exporting data to a CSV file.

## Before you begin

Verify that you have the following:

- Shell environment for running scripts.
- Installed jq JSON processor.
- Proofpoint Meta account with an administrator account.

## Using the script

Follow these steps to use the Proofpoint Meta API script for data export:

1. Generate an API key and API ID.
2. Create a file with the generated API secret.
3. Create a file with the generated API ID.
4. If using Managed Security Service Provider (MSSP) mode, create a file with the required organization name.

***Note**: The files can be saved in a TXT or CSV formats, the script will process only the first line of the file to looking for the required data.*

### Generating API key and ID

1. Log into Meta Console as administrator.
2. Navigate to **Administration > API Keys**.
3. At the top right-hand corner, click on the Plus (+) sign to add a new key.
4. Enter the key name and description.
5. Enable the relevant Read (read-only) and Write (read/write) privileges for the key. The Org Write privilege allows the user to create sub-organizations. This option is grayed-out by default. To enable it, contact your Proofpoint Meta sales engineer.
6. At the top right-hand corner, click **Save** to finish.

   The API key information is displayed. It includes API ID and API secret.
7. Copy and store the API ID and secret for use in the next steps.

### Creating the files

Create the TXT or CSV files to be used by the Proofpoint Meta API script

1. Create a file with the generated API secret (API_KEY).
2. Create a file with the generated API ID (API_ID).

3. If using Managed Security Service Provider (MSSP) mode, create a file with the required organization name (Sub_ORG).

## Editing the script

1. Open the script file.
2. Edit the path for the API_KEY, API_ID and for SUB_ORG (if exists) in lines 3 to 7 and paste the path to the previously-created files. See the script sample below:

```
#Please fill the path to the API before running the script (only csv or txt file)
API_KEY="Path/to/the/API/Key/file"
API_ID="Path/to/the/API/ID/file"
#Sub_ORG is optional, mandatory for MSSP
Sub_ORG="Path/to/the/Sub/ORG/file"
```

## Running the script

1. Run the script, and use the following menu options to export the required data:

   1. Active users last 30 days – Minimum, Average, Maximum

   2. Roles – ID, Name, Role

   3. MetaPorts – ID, Name, Enabled, Mapped elements

   4. Mapped subnets – ID, Name, CIDR, DNS suffix:Enterprise DNS (true\false), Host name

   5. Mapped service – ID, Name, IP\Hostname, DNS suffix

   6. Policies – ID, Name, Created at, Description, Enabled, Modified at, Sources, Target, Protocols

   7. Egress – ID, Name, Source, Target, Via

   8. Routing groups – ID, Name, Mapped elements, Sources

   9. EasyLinks – ID, Name, Mapped elements, Domain name, IP/Hostname (null= probably it is a subnet), Port, Protocol, Viewers

   10. Split tunnel configuration – ID, Name, All org, Members

   11. IDPS – ID, Name, Created at, Modified at, SAML, SCIM key (if defined)

   12. Log streaming – ID, Name, SIEM configuration (URL:Port:Protocol)

   100. All data above

   0. Exit