NOTE: You have to download the PDF to access the hyperlinks.

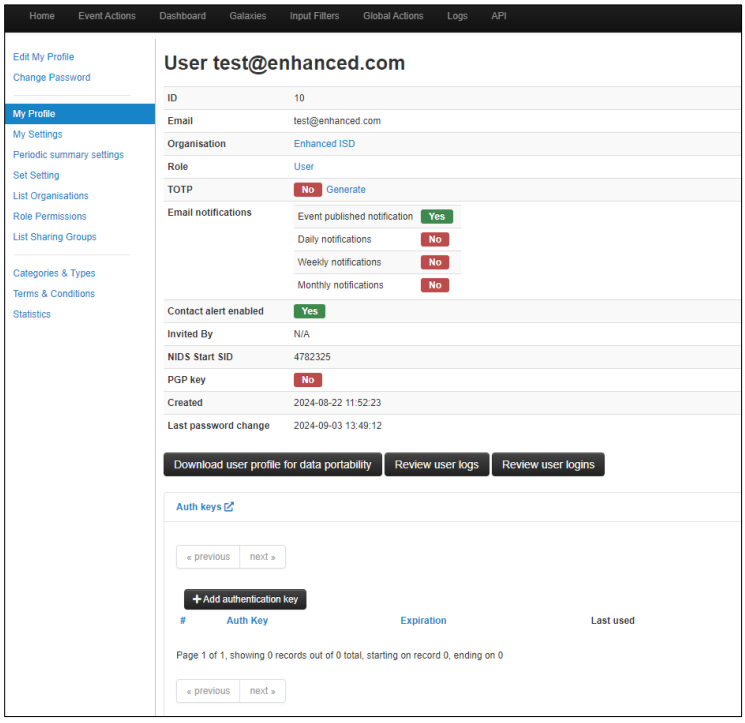
1. Generate Fortigate API token
   Follow this guide to generate the API token

   The accprofile will need UTM webfilter read-write permissions

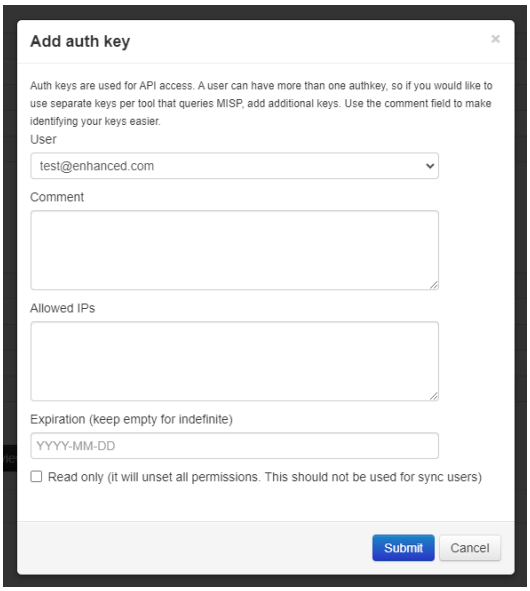
```
edit "Web and Email Override"
    set scope global
    set comments "Allow web and email override"
    set utmgrp custom
    set system-diagnostics disable
    config utmgrp-permission
        set webfilter read-write
        set emailfilter read-write
    end
```

2. Generate MISP API token
   Log into MISP and navigate to your profile:
   https://threatengine2.esc20.net/users/view/me

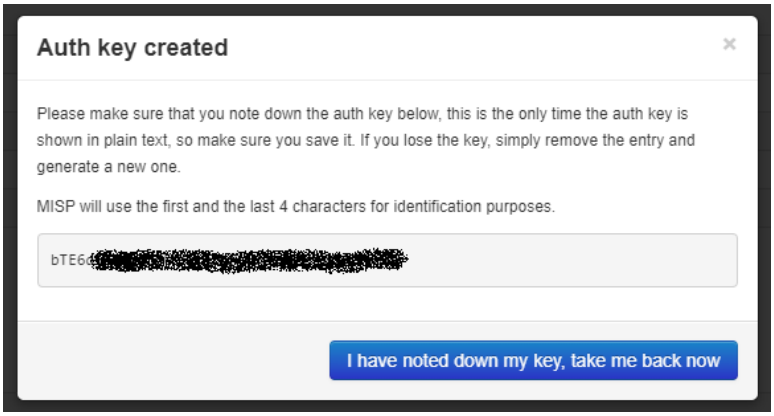
   Under Auth Keys, select + Add authentication key



   Fill out the optional forum fields and submit



Make sure you copy the API token



3. Install integration script
   The integration can be installed on any Windows device, but we recommend installing it on a server or desktop that is always online. The device will need to have IP connectivity to both the MISP webserver and Fortigate appliance.

   Start by choosing a location anywhere in the directory and create a folder (the folder name and location can be anything you choose). From that folder open a PowerShell window **with administrator privileges** and run these commands:
   # Invoke-WebRequest -Uri "https://raw.githubusercontent.com/secops-esc20/Threat-Engine-Integrations/refs/heads/main/Fortinet%20Web/install.ps1" -OutFile "install.ps1"
   # .\install.ps1

   During installation you will be prompted to enter the management URL for your Fortigate, the VDOM name, and the API tokens. For more information regarding the installation script, run:
   # .\install.ps1 -help

4. Verify
   In task scheduler you should see the following tasks:
   - "MISP-Fortigate-Sync"
   - "MISP-Fortigate-Integration-Updater"

   Every time the MISP-Fortigate-Sync task runs it should generate log files. The logs can be found in the folder you created during step 3 in a subfolder called logs\. The first time the integration script is run it will create the logs folder and generate the first log file.

   You can manually trigger the sync by either running the task or by running integration.py