

1. Generate Fortigate API token
[Follow this guide to generate the API token](#)

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

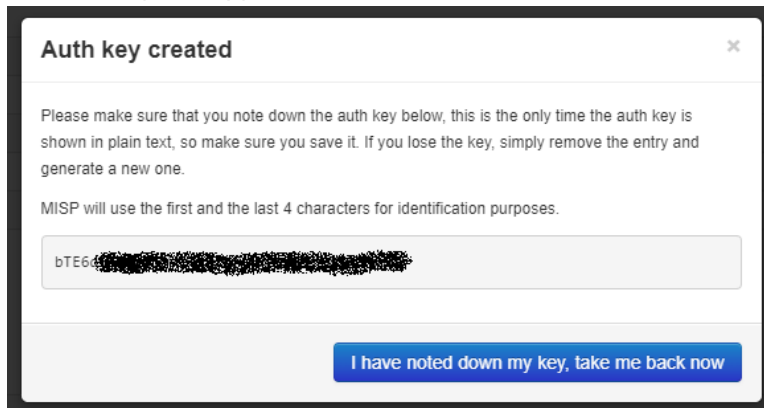
Under Auth Keys, select + Add authentication key

The screenshot shows the MISP user profile page for 'test@enhanced.com'. The page is divided into a left sidebar with navigation links and a main content area. The sidebar includes links for 'Edit My Profile', 'Change Password', 'My Profile' (selected), 'My Settings', 'Periodic summary settings', 'Set Setting', 'List Organisations', 'Role Permissions', 'List Sharing Groups', 'Categories & Types', 'Terms & Conditions', and 'Statistics'. The main content area displays user details: ID 10, Email test@enhanced.com, Organisation Enhanced ISD, Role User, TOTP No (with a 'Generate' link), Email notifications (Event published notification Yes, Daily notifications No, Weekly notifications No, Monthly notifications No), Contact alert enabled Yes, Invited By N/A, NIDS Start SID 4782325, PGP key No, Created 2024-08-22 11:52:23, and Last password change 2024-09-03 13:49:12. Below these details are three buttons: 'Download user profile for data portability', 'Review user logs', and 'Review user logins'. The 'Auth keys' section is visible at the bottom, showing a table with columns for '#', 'Auth Key', 'Expiration', and 'Last used'. The table is currently empty, and there is a '+ Add authentication key' button above it. The page footer indicates 'Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0'.

Fill out the optional forum fields and submit

The screenshot shows the 'Add auth key' form. It includes a title bar with a close button. The form contains a text area with instructions: 'Auth keys are used for API access. A user can have more than one authkey, so if you would like to use separate keys per tool that queries MISP, add additional keys. Use the comment field to make identifying your keys easier.' Below this is a 'User' dropdown menu with 'test@enhanced.com' selected. There is a 'Comment' text area, an 'Allowed IPs' text area, and an 'Expiration (keep empty for indefinite)' text area with a placeholder 'YYYY-MM-DD'. A checkbox labeled 'Read only (it will unset all permissions. This should not be used for sync users)' is present. At the bottom are 'Submit' and 'Cancel' buttons.

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/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, you can review the README.

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