

**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

Home Event Actions Dashboard Galaxies Input Filters Global Actions Logs API

Edit My Profile  
Change Password

**My Profile**  
My Settings  
Periodic summary settings  
Set Setting  
List Organisations  
Role Permissions  
List Sharing Groups

Categories & Types  
Terms & Conditions  
Statistics

### User test@enhanced.com

ID	10
Email	test@enhanced.com
Organisation	Enhanced ISD
Role	User
TOTP	No <a href="#">Generate</a>
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
Last password change	2024-09-03 13:49:12

[Download user profile for data portability](#) [Review user logs](#) [Review user logins](#)

#### Auth keys [↗](#)

« previous next »

[+ Add authentication key](#)

#	Auth Key	Expiration	Last used
---	----------	------------	-----------

Page 1 of 1, showing 0 records out of 0 total, starting on record 0, ending on 0

« previous next »

Fill out the optional forum fields and submit

**Add auth key** ✕

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.

User  
test@enhanced.com

Comment

Allowed IPs

Expiration (keep empty for indefinite)  
YYYY-MM-DD

☐ Read only (it will unset all permissions. This should not be used for sync users)

**Submit** **Cancel**

Make sure you copy the API token

**Auth key created** ✕

Please make sure that you note down the auth key below, this is the only time the auth key is shown in plain text, so make sure you save it. If you lose the key, simply remove the entry and generate a new one.

MISP will use the first and the last 4 characters for identification purposes.

bTE6...

**I have noted down my key, take me back now**

### 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`