

NG SIEM - Microsoft Defender ATP Logs

Prerequisite

Before starting, ensure you have the following ready:

Item	Details
OS	Windows 10 / Windows Server 2016 or later
Privileges	Local Administrator access on the machine
Network	Outbound HTTPS (port 443) to our Elastic endpoint

Step 1. Connect local Kibana to a Cloud instance

If you are running this Kibana instance against a hosted Elasticsearch instance, proceed with manual setup.

Save the **Elasticsearch** endpoint as `<es_url>` and the cluster **Password** as `<password>` for your records

Step 2. Download and install Filebeat

First time using Filebeat? See the [Quick Start](#).

1. Download the Filebeat Windows zip file from the [Download](#) page.
2. Extract the contents of the zip file into `C:\Program Files`.
3. Rename the `filebeat-9.2.0-windows` directory to `Filebeat`.
4. Open a PowerShell prompt as an Administrator (right-click the PowerShell icon and select **Run As Administrator**). If you are running Windows XP, you might need to download and install PowerShell.
5. From the PowerShell prompt, run the following commands to install Filebeat as a Windows service.

```
cd "C:\Program Files\Filebeat"
.\install-service-filebeat.ps1
```

Modify the settings under `output.elasticsearch` in the `C:\Program Files\Filebeat\filebeat.yml` file to point to your Elasticsearch installation.

Step 3. Edit the configuration

Modify `C:\Program Files\Filebeat\filebeat.yml` to set the connection information:

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
  # If using Elasticsearch's default certificate
  ssl.ca_trusted_fingerprint: "<es cert fingerprint>"
setup.kibana:
  host: "<kibana_url>"
```

Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana. To [configure SSL](#) with the default certificate generated by Elasticsearch, add its fingerprint in `<es cert fingerprint>`.

⚠ Important: Do not use the built-in `elastic` user to secure clients in a production environment. Instead set up authorized users or API keys, and do not expose passwords in configuration files. [Learn more](#).

Step 4. Enable and configure the microsoft module

From the `C:\Program Files\Filebeat` folder, run:

Modify the settings in the `modules.d/microsoft.yml` file. You must enable at least one fileset.

```
filebeat.exe modules enable microsoft
```

Step 5. Start Filebeat

The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
.\filebeat.exe setup
Start-Service filebeat
```

Step 6. Module status

We will check that data is received from the Filebeat `microsoft` module

Modules

These are the modules that will be ingested after integrating Microsoft Defender ATP Logs

```
microsoft.defender_atp : Module for ingesting Microsoft Defender ATP.
microsoft.defender_atp.lastUpdateTime: The date and time (in UTC) the alert was last updated.
(type: date)
microsoft.defender_atp.resolvedTime: The date and time in which the status of the alert was
changed to 'Resolved'. (type: date)
microsoft.defender_atp.incidentId: The Incident ID of the Alert. (type: keyword)
microsoft.defender_atp.investigationId: The Investigation ID related to the Alert. (type:
keyword)
microsoft.defender_atp.investigationState: The current state of the Investigation. (type:
keyword)
microsoft.defender_atp.assignedTo: Owner of the alert. (type: keyword)
microsoft.defender_atp.status: Specifies the current status of the alert. Possible values are:
'Unknown', 'New', 'InProgress' and 'Resolved'. (type: keyword)
microsoft.defender_atp.classification: Specification of the alert. Possible values are:
'Unknown', 'FalsePositive', 'TruePositive'. (type: keyword)
microsoft.defender_atp.determination: Specifies the determination of the alert. Possible
values are: 'NotAvailable', 'Apt', 'Malware', 'SecurityPersonnel', 'SecurityTesting',
'UnwantedSoftware', 'Other'. (type: keyword)
microsoft.defender_atp.threatFamilyName: Threat family. (type: keyword)
microsoft.defender_atp.rbacGroupName: User group related to the alert (type: keyword)
microsoft.defender_atp.evidence.domainName: Domain name related to the alert (type: keyword)
```

That's everything needed on your end. Once the Filebeat service is running, logs will automatically begin forwarding to our Elastic instance in real time — no ongoing maintenance is required on your side. If the service ever stops for any reason (e.g. after a Windows update or restart), it will resume automatically as it is installed as a Windows service. If you run into any issues during setup, just reach out and we'll walk you through it.

Revision #1

Created 5 March 2026 07:08:03

Updated 6 March 2026 06:19:39