CrowdStrike Next-Gen SIEM Onboarding

Dhruv Rawat

https://www.linkedin.com/in/dhruv-rawat-46a445205/

Index

Section 1: Install LogScale Collector

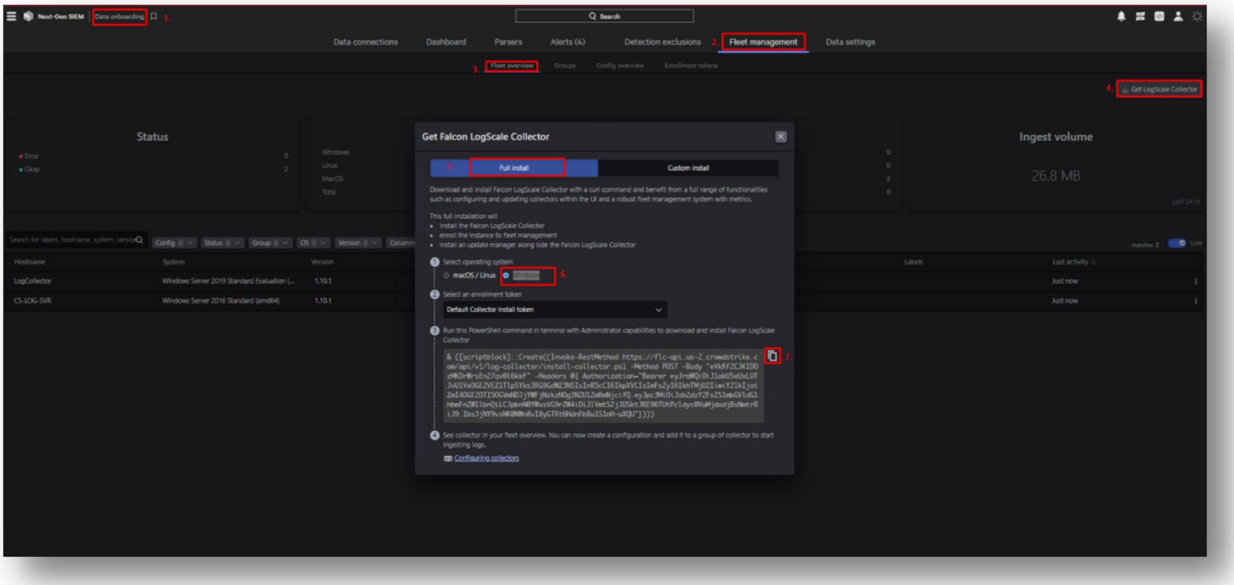
Fleet Management

Fleet Management lets you install and manage LogScale Collectors. We'll use the Full Install method so the Falcon LogScale collector can be configured and updated directly in the Falcon Console. Custom install requires local updates through a systems package manager.

Minimum System Requirements for Next-Gen SIEM Logscale Collector:-

- **OS**: Microsoft Windows server 2016, 2019 Standard and 2022 Standard
- **vCPU**: 2–4 CPUs
- **RAM**: 8 GB
- **Disk**: 100 GB
- **TLS**: above 1.2
- **Windows Firewall:** Allow inbound/outbound UDP 514,515

Step 1: Navigate to Data Onboarding → Fleet Management → Get LogScale Collector → Full Install, select Windows, and copy the script.



Hostname	System	Version	Labels	Last activity
LogCollector	Windows Server 2019 Standard Evaluation (...	1.10.1		Just now
CS-LOG-SVR	Windows Server 2016 Standard (amd64)	1.10.1		Just now

Get Falcon LogScale Collector

Full install | Custom install

Download and install Falcon LogScale Collector with a curl command and benefit from a full range of functionalities such as configuring and updating collectors within the UI and a robust fleet management system with metrics.

This full installation will

- install the Falcon LogScale Collector
- enroll the instance to fleet management
- install an update manager along side the Falcon LogScale Collector

1 Select operating system

○ macOS / Linux ● Windows

2 Select an enrollment token

Default Collector install token

3 Run this PowerShell command in terminal with Administrator capabilities to download and install Falcon LogScale Collector

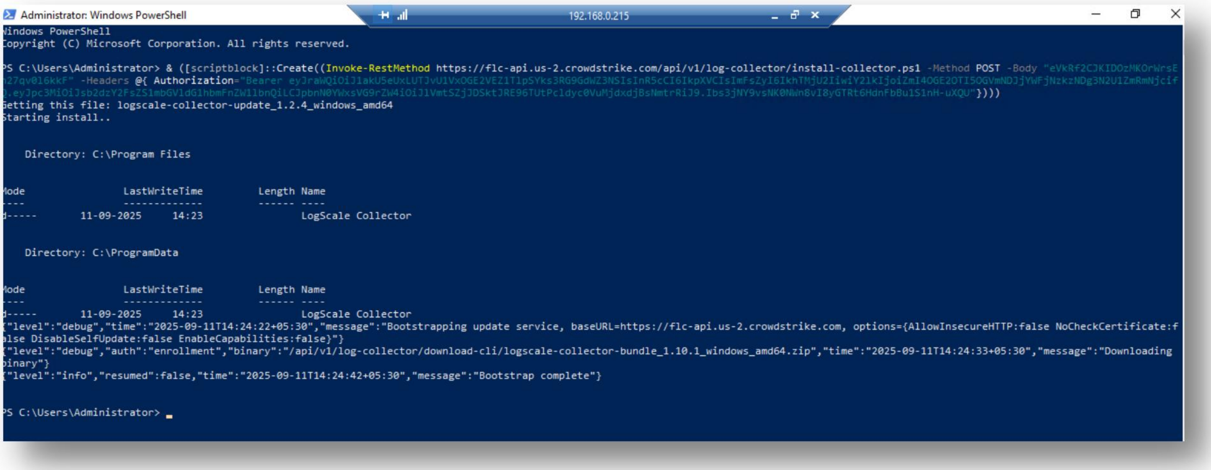
```
& ([scriptblock]::Create((Invoke-RestMethod https://flc-api.us-2.crowdstrike.c
om/api/v1/log-collector/install-collector.ps1 -Method POST -Body "eVkRf2CJKIDO
zMKOrWrsEn27qv0l6kkF" -Headers @{ Authorization="Bearer eyJraWQiOiJlakU5eUxLUT
JvU1VxOGEZVEZ1TlpSYks3RG9GdWZ3NSIsInR5cCI6IkpXVCIsImFsZyI6IkhTMjU2IiwiY2lkIjoi
ZmI4OGE2OTI5OGVmNDJjYWFjNzkzNDg3N2U1ZmRmNjcifQ.eyJpc3MiOiJsb2dzY2FsZS1mbGVldG1
hbmFnZW1lbnQiLCJpbnN0YW xsVG9rZW4iOiJlVmtSZjJDSktJRE96TUtPcldyc0VuMjdxdjBsNmtrR
iJ9.Ibs3jNY9vsNK0NWn8vI8yGTRt6HdnFbBu1S1nH-uXQU"})))
```

4 See collector in your fleet overview. You can now create a configuration and add it to a group of collector to start ingesting logs.

Configuring collectors

Step 2: Run Script on Windows Server: -

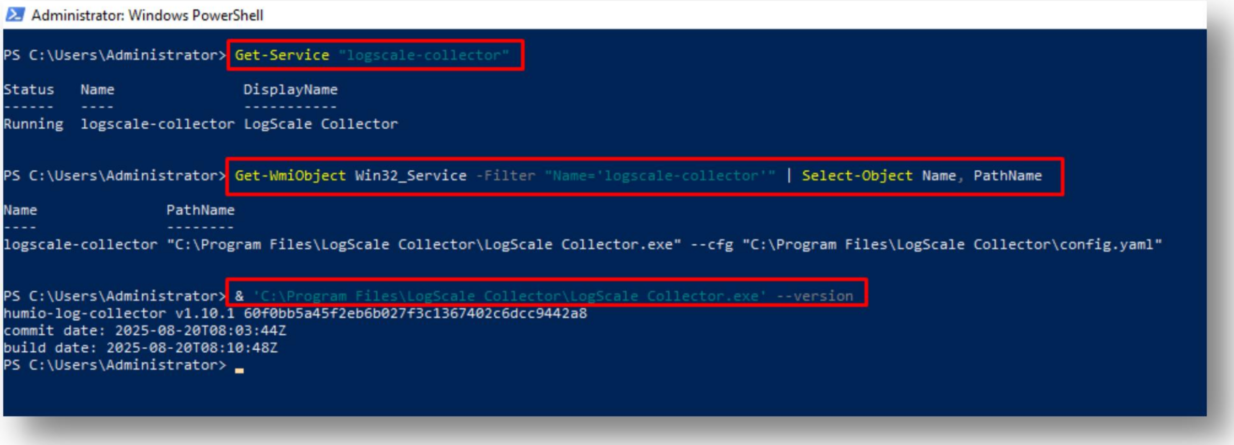
Open PowerShell (Admin) on your Windows Server 2019 and run the copied script.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> & ([scriptblock]::Create((Invoke-RestMethod https://flc-api.us-2.crowdstrike.com/api/v1/log-collector/install-collector.ps1 -Method POST -Body "eVkRf2CJKIDOzMKOrWrsE
n27qv016kkF" -Headers @{ Authorization="Bearer eyJraWQiOiJ1akU5eUxLUTJvU1VxOGE2VEZ1TlpSYks3RG9GdWZ3NSIsInR5cCI6IkpXVCIsImFsZyI6IkhTMjU2IiwiY2lkIjoiZmI4OGE2OTI5OGVmNDJjYWFjNzkzNDg3N2U1ZmRmNjcif
Q.eyJpc3MiOiJsb2dzY2FsZS1mbGVldG1hbmFnZW1lbnQiLCJpbnN0YWxsVG9rZW4iOiJ1VmtSZjJDSktJRE96TUtPcldyc0VuMjdxdjBsNmtrRiJ9.Ibs3jNY9vsNK0NWn8vI8yGTRt6HdnFbBu1S1nH-uXQU"})))
Getting this file: logscale-collector-update_1.2.4_windows_amd64
Starting install..


    Directory: C:\Program Files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11-09-2025     14:23                LogScale Collector


    Directory: C:\ProgramData


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        11-09-2025     14:23                LogScale Collector
{"level":"debug","time":"2025-09-11T14:24:22+05:30","message":"Bootstrapping update service, baseURL=https://flc-api.us-2.crowdstrike.com, options={AllowInsecureHTTP:false NoCheckCertificate:f
alse DisableSelfUpdate:false EnableCapabilities:false}"}
{"level":"debug","auth":"enrollment","binary":"/api/v1/log-collector/download-cli/logscale-collector-bundle_1.10.1_windows_amd64.zip","time":"2025-09-11T14:24:33+05:30","message":"Downloading
binary"}
{"level":"info","resumed":false,"time":"2025-09-11T14:24:42+05:30","message":"Bootstrap complete"}

PS C:\Users\Administrator> _
```

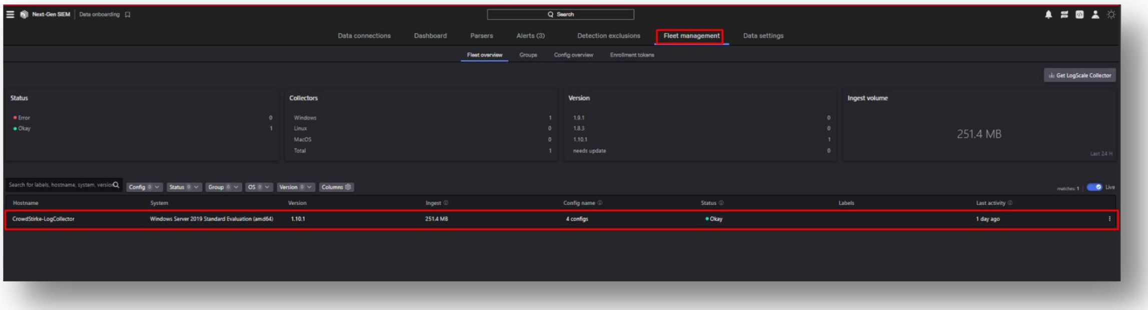
Step 3: Verify Collector is Running

Check that the collector is active using PowerShell commands. Confirm directory path and version.



```
PS C:\Users\Administrator> Get-Service "logscale-collector"

Status   Name               DisplayName
------   ----               -----------
Running  logscale-collector LogScale Collector

PS C:\Users\Administrator> Get-WmiObject Win32_Service -Filter "Name='logscale-collector'" | Select-Object Name, PathName

Name               PathName
----               --------
logscale-collector "C:\Program Files\LogScale Collector\LogScale Collector.exe" --cfg "C:\Program Files\LogScale Collector\config.yaml"

PS C:\Users\Administrator> & 'C:\Program Files\LogScale Collector\LogScale Collector.exe' --version
humio-log-collector v1.10.1 60f0bb5a45f2eb6b027f3c1367402c6dcc9442a8
commit date: 2025-08-20T08:03:44Z
build date: 2025-08-20T08:10:48Z
PS C:\Users\Administrator> _
```

Step 4: In Fleet overview, confirm your Falcon LogScale Collector is now available..



Status	
● Error	0
● Okay	1

Collectors	
Windows	1
Linux	0
MacOS	0
Total	1

Version	
1.9.1	0
1.8.3	0
1.10.1	1
needs update	0

Ingest volume

251.4 MB

Hostname	System	Version	Ingest	Config name	Status	Labels	Last activity
CrowdStirke-LogCollector	Windows Server 2019 Standard Evaluation (amd64)	1.10.1	251.4 MB	4 configs	● Okay		1 day ago

Section 2: Create Data Connector for Palo Alto & FortiGate

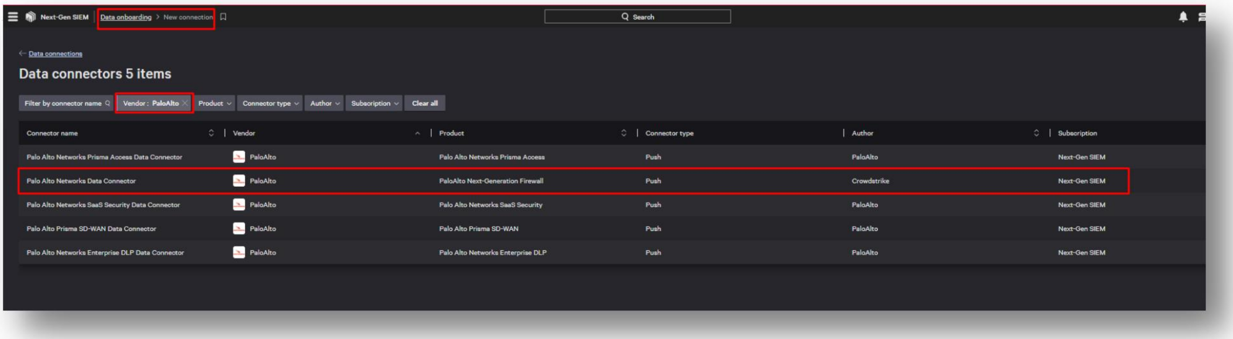
Data Connectors

Create data connectors in the Falcon console to automate and manage ingestion from third-party data sources.

We are using PaloAlto & FortiGate

Step 1: Add Connection

Data Connection → Add Connection → Choose Vendor Filter → Search Paloalto



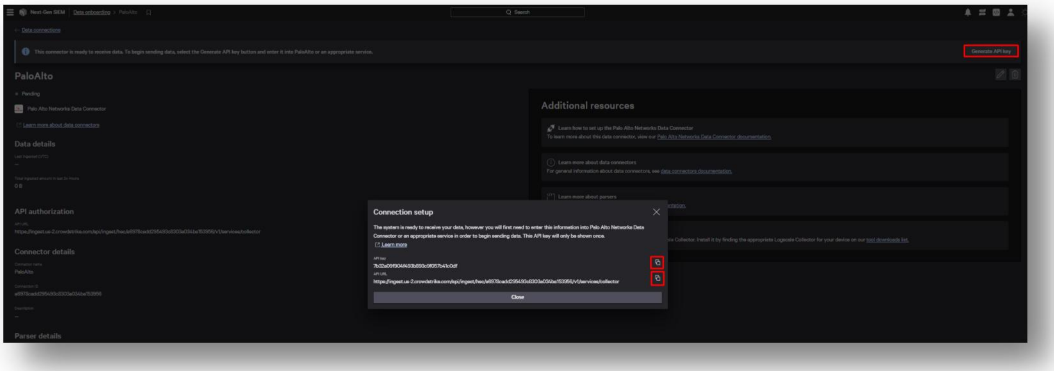
Data connectors 5 items

Vendor : PaloAlto

Connector name	Vendor	Product	Connector type	Author	Subscription
Palo Alto Networks Prisma Access Data Connector	PaloAlto	Palo Alto Networks Prisma Access	Push	PaloAlto	Next-Gen SIEM
Palo Alto Networks Data Connector	PaloAlto	PaloAlto Next-Generation Firewall	Push	Crowdstrike	Next-Gen SIEM
Palo Alto Networks SaaS Security Data Connector	PaloAlto	Palo Alto Networks SaaS Security	Push	PaloAlto	Next-Gen SIEM
Palo Alto Prisma SD-WAN Data Connector	PaloAlto	Palo Alto Prisma SD-WAN	Push	PaloAlto	Next-Gen SIEM
Palo Alto Networks Enterprise DLP Data Connector	PaloAlto	Palo Alto Networks Enterprise DLP	Push	PaloAlto	Next-Gen SIEM

Step 2: Configure Connection

Give it a name, enable parser, and create the connection. Save the generated **API key** and **URL** for later.



Connection setup

The system is ready to receive your data, however you will first need to enter this information into Palo Alto Networks Data Connector or an appropriate service in order to begin sending data. This API key will only be shown once.

Learn more

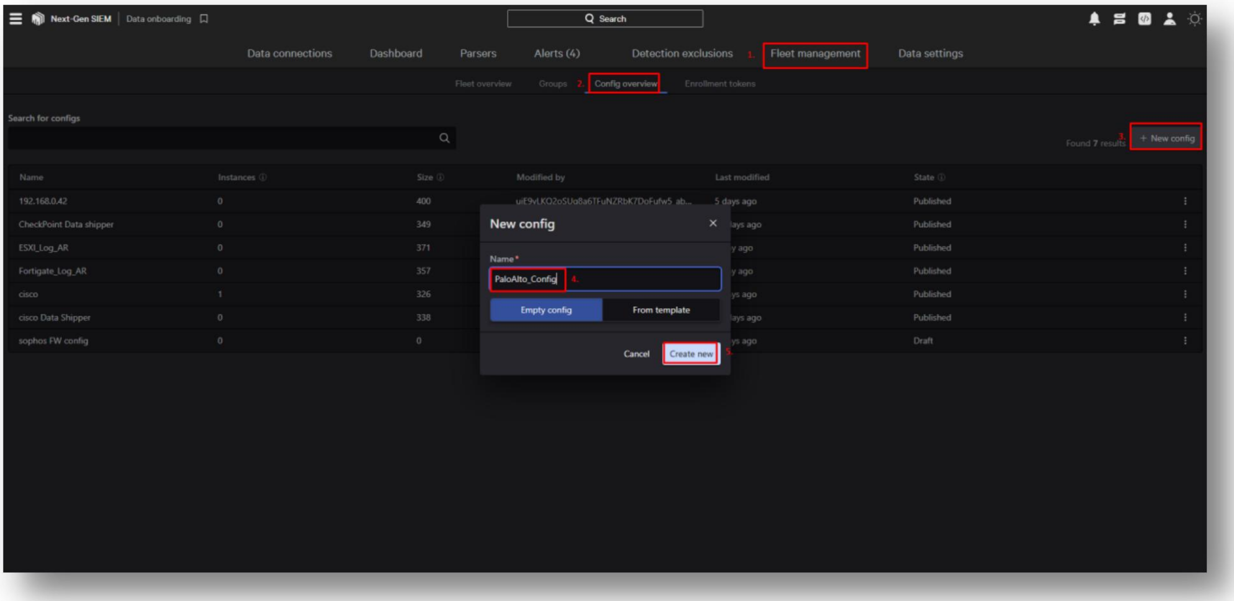
API key
7b32a09f904f493b893c9f057b41c0df

API URL
https://ingest.us-2.crowdstrike.com/api/ingest/hec/a6978cadd295493c8303a034ba153956/v1/services/collector

https://www.linkedin.com/in/dhruv-rawat-46a445205/

Step 3: Create Config

In **Fleet Management → Config Overview → +New Config**, create a new configuration.



Name	Instances	Size	Modified by	Last modified	State
192.168.0.42	0	400	uiE9vLKO2oSUa8a6TFuNZRbK7DoFufw5_ab...	5 days ago	Published
CheckPoint Data shipper	0	349		...ays ago	Published
ESXI_Log_AR	0	371		...y ago	Published
Fortigate_Log_AR	0	357		...y ago	Published
cisco	1	326		...ys ago	Published
cisco Data Shipper	0	338		...ays ago	Published
sophos FW config	0	0		...ys ago	Draft

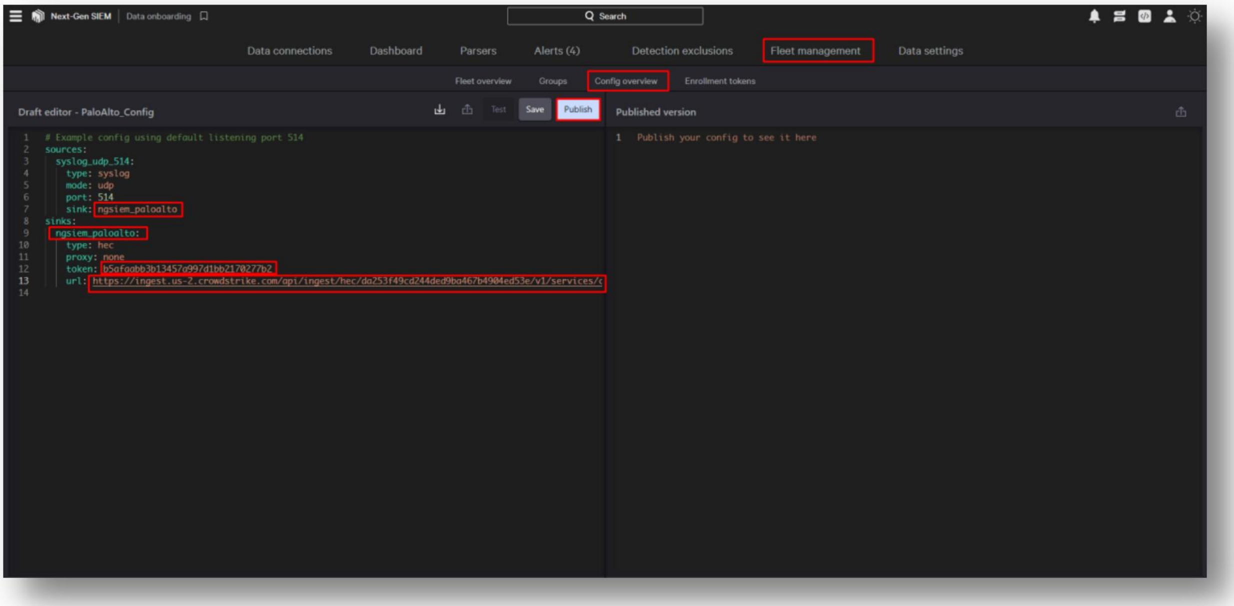
New config

Name*: PaloAlto_Config

Step 4: Edit Config.yaml

Set the syslog source for the collector. By default, it listens on **UDP 514** — ensure:

- No other service is already using port **514**.
- Each additional source uses a **unique port**.
- Windows Firewall allows the configured port, and the collector is in your allow list.



Draft editor - PaloAlto_Config

```yaml
# Example config using default listening port 514
sources:
  syslog_udp_514:
    type: syslog
    mode: udp
    port: 514
    sink: ngsiem_paloalto
sinks:
  ngsiem_paloalto:
    type: hec
    proxy: none
    token: b5afaabb3b13457a997d1bb2170277b2
    url: https://ingest.us-2.crowdstrike.com/api/ingest/hec/da253f49cd244ded9ba467b4904ed53e/v1/services/c
```

```
Publish your config to see it here
```

Step 6: Fortigate Connector

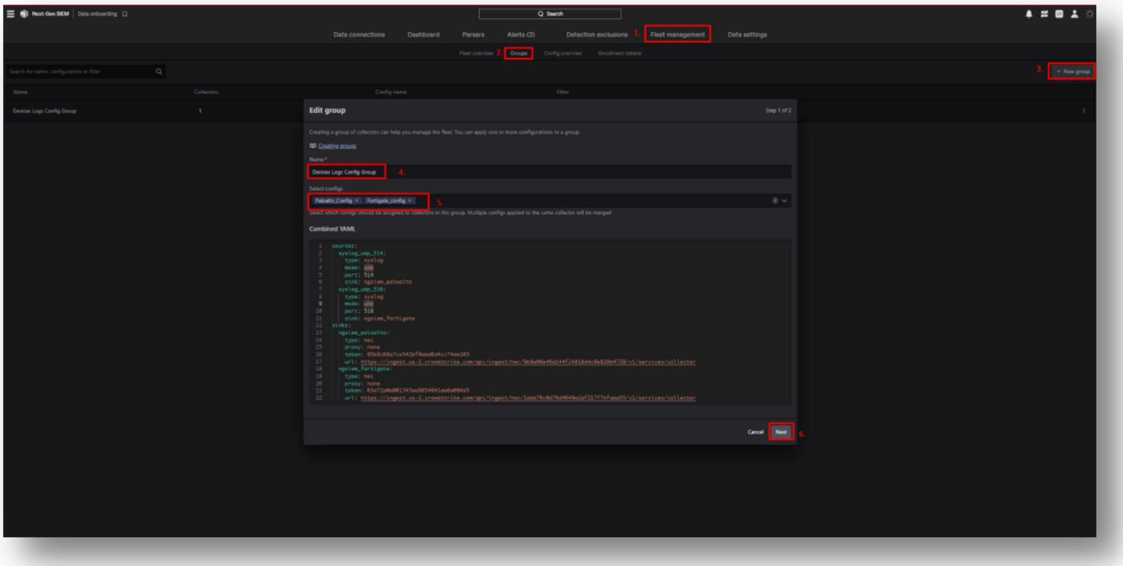
The process for Fortigate is almost identical to Palo Alto:

1. Go to **Data Connections → Add Connection → Fortigate**.
2. Configure the connector (name, enable parser).
3. Save the **API key and URL** for syslog forwarding.

💡 **Tip:** If Palo Alto is already sending logs on port 514, configure FortiGate to use **port 516** (or another free port) and add this port in the LogScale Collector config group.

Step 7: Create Group

Go to **Fleet Management → Groups → + New Group → Select configs (Palo Alto, FortiGate)**



Edit group — Step 1 of 2

Creating a group of collectors can help you manage the fleet. You can apply one or more configurations to a group.

Creating groups

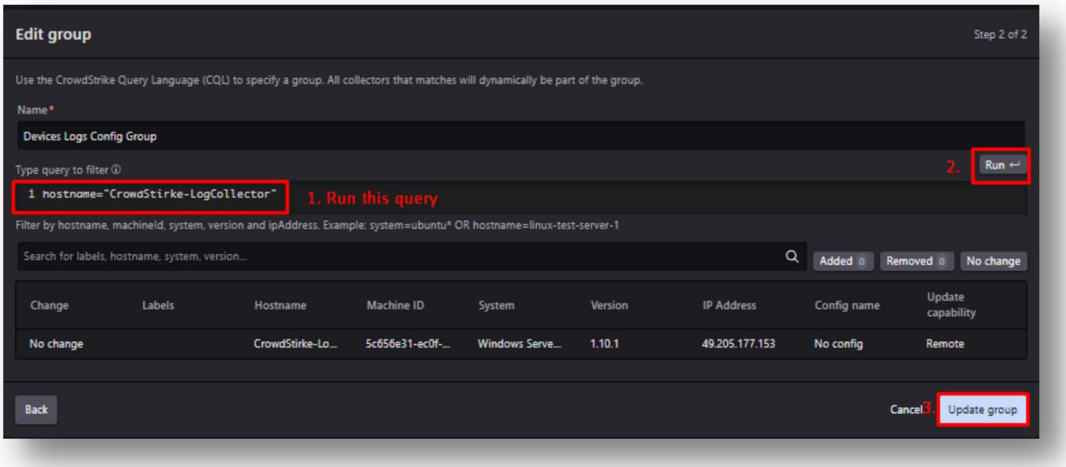
Name*: Devices Logs Config Group

Select configs: Paloalto_Config × Fortigate_config ×

Select which configs should be assigned to collectors in this group. Multiple configs applied to the same collector will be merged

Combined YAML

```yaml
sources:
  syslog_udp_514:
    type: syslog
    mode: udp
    port: 514
    sink: ngsiem_paloalto
  syslog_udp_516:
    type: syslog
    mode: udp
    port: 516
    sink: ngsiem_fortigate
sinks:
  ngsiem_paloalto:
    type: hec
    proxy: none
    token: 95b8c68a7ca542bf9abd6d4cc74ae185
    url: https://ingest.us-2.crowdstrike.com/api/ingest/hec/9b8e00e46d144f24818d4c9e829b4729/v1/services/collector
  ngsiem_fortigate:
    type: hec
    proxy: none
    token: 65a72a0a001545aa9854941aa8d094a5
    url: https://ingest.us-2.crowdstrike.com/api/ingest/hec/1abb76c8d76d4649a2df217f7bfaaa55/v1/services/collector
```



Edit group — Step 2 of 2

Use the CrowdStrike Query Language (CQL) to specify a group. All collectors that matches will dynamically be part of the group.

Name*: Devices Logs Config Group

Type query to filter ⓘ

```
hostname="CrowdStirke-LogCollector"
```

Filter by hostname, machineId, system, version and ipAddress. Example: system=ubuntu* OR hostname=linux-test-server-1

Search for labels, hostname, system, version...

Change	Labels	Hostname	Machine ID	System	Version	IP Address	Config name	Update capability
No change		CrowdStirke-Lo...	5c656e31-ec0f-...	Windows Serve...	1.10.1	49.205.177.153	No config	Remote

https://www.linkedin.com/in/dhruv-rawat-46a445205/

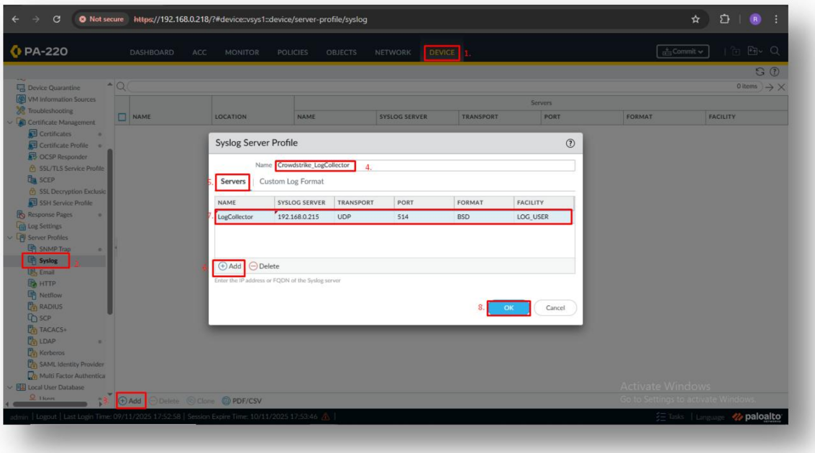
Section 3: Configure Palo Alto Firewall

These steps are performed in the administration interface for your instance of Palo Alto Firewall console.

1. Create Syslog Server Profile

In Palo Alto console, go to **Device → Server Profiles → Syslog**, Create a new profile with:

- Transport: UDP
- Port: 514
- Format: BSD
- Facility: LOG_USER.



Name: Crowdstrike_LogCollector

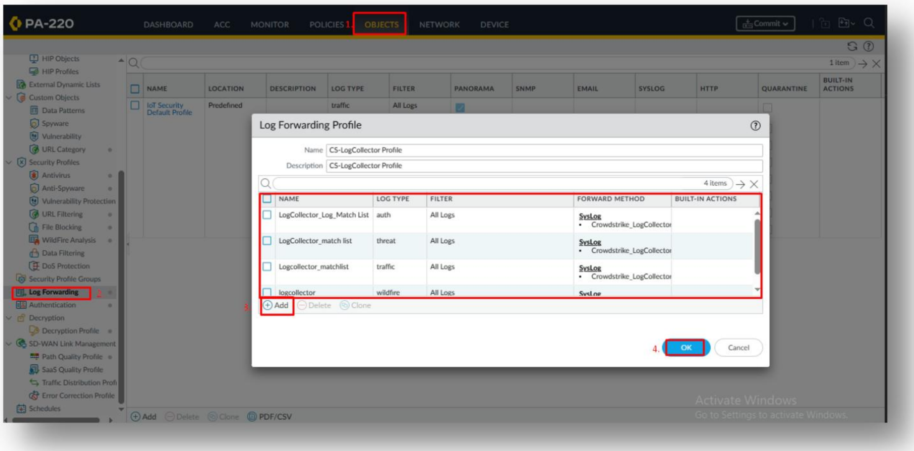
Servers | Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
LogCollector	192.168.0.215	UDP	514	BSD	LOG_USER

Enter the IP address or FQDN of the Syslog server

2. Log Forwarding Profile

Under **Objects → Log Forwarding**, add a new profile, select log types (auth, traffic, threat, etc.), and link the syslog server profile.



Log Forwarding Profile

Name: CS-LogCollector Profile

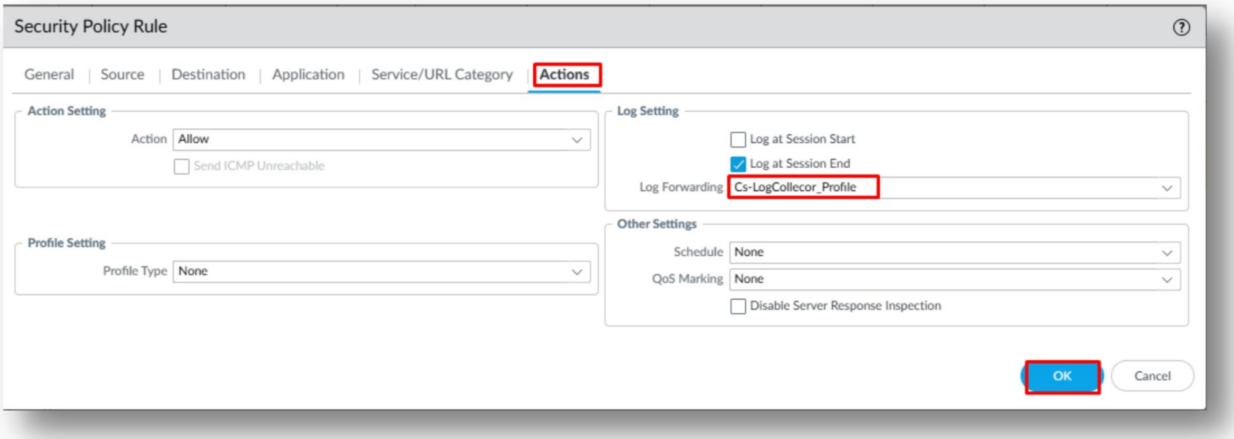
Description: CS-LogCollector Profile

4 items

NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
LogCollector_Log_Match List	auth	All Logs	SysLog • Crowdstrike_LogCollector	
LogCollector_match list	threat	All Logs	SysLog • Crowdstrike_LogCollector	
Logcollector_matchlist	traffic	All Logs	SysLog • Crowdstrike_LogCollector	
logcollector	wildfire	All Logs	SysLog	

https://www.linkedin.com/in/dhruv-rawat-46a445205/

3. **Apply to Security Policy**
   Go to **Policies → Security**, edit your rule, and attach the log forwarding profile under **Actions**.



Action: Allow

□ Send ICMP Unreachable

Profile Type: None

□ Log at Session Start

☑ Log at Session End

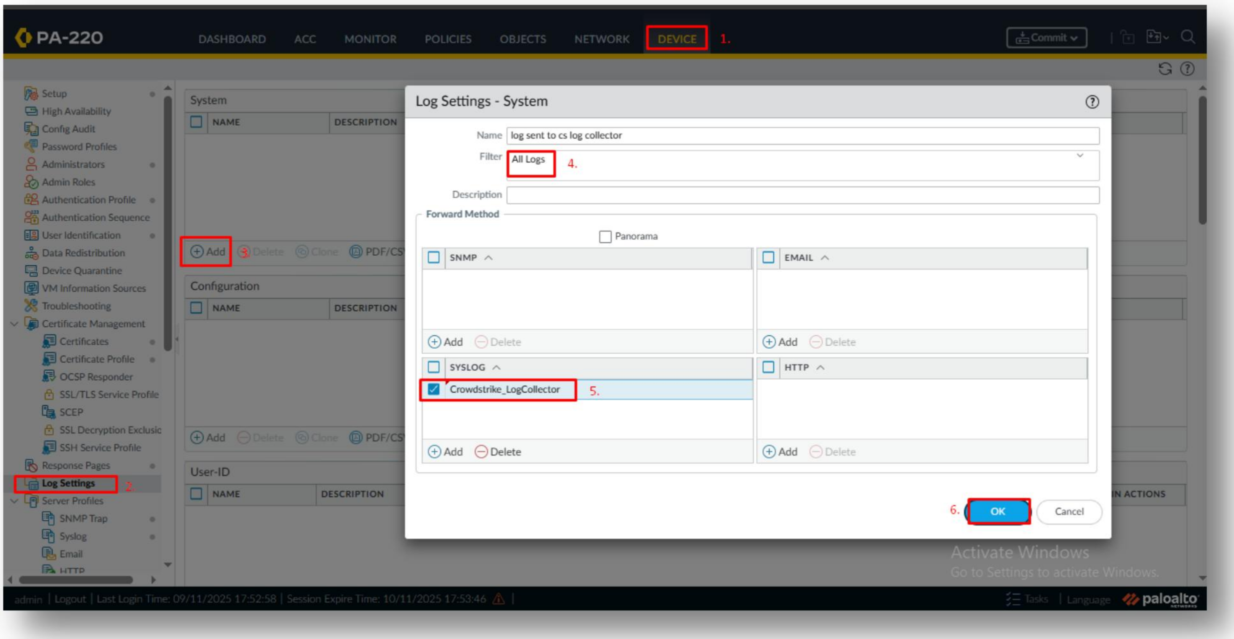
Log Forwarding: Cs-LogCollecor_Profile

Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

4. **Additional Logs**
   Configure forwarding for system, config, User-ID, HIP Match, Global Protect, and IP-Tag logs under **Device → Log Settings**.



Name: log sent to cs log collector

Filter: All Logs 4.

Description:

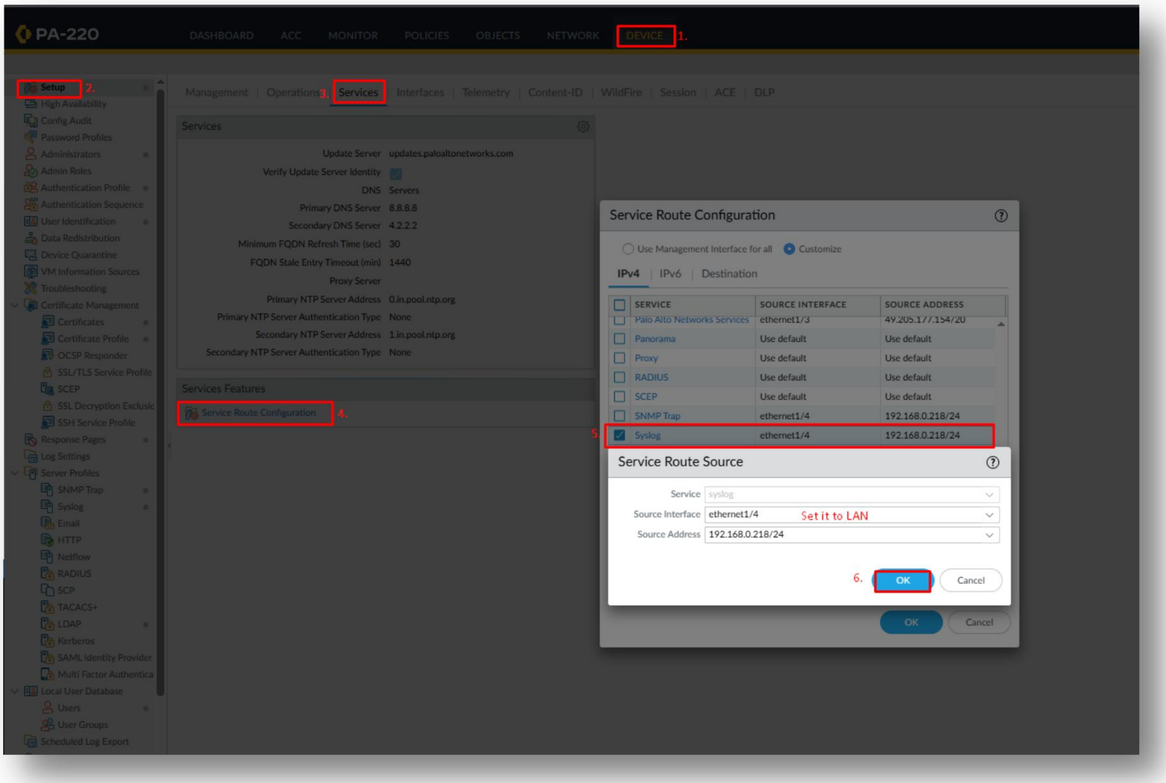
□ Panorama

SYSLOG: ☑ Crowdstrike_LogCollector 5.

https://www.linkedin.com/in/dhruv-rawat-46a445205/

5. Service Route Configuration

Ensure service routes are set so firewall logs can reach the LogScale Collector.



Services

Update Server	updates.paloaltonetworks.com
Verify Update Server Identity	☑
DNS	Servers
Primary DNS Server	8.8.8.8
Secondary DNS Server	4.2.2.2
Minimum FQDN Refresh Time (sec)	30
FQDN Stale Entry Timeout (min)	1440
Proxy Server	
Primary NTP Server Address	0.in.pool.ntp.org
Primary NTP Server Authentication Type	None
Secondary NTP Server Address	1.in.pool.ntp.org
Secondary NTP Server Authentication Type	None

Services Features

Service Route Configuration

Service Route Configuration

○ Use Management Interface for all ● Customize

IPv4 | IPv6 | Destination

	SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
□	Palo Alto Networks Services	ethernet1/3	49.205.177.154/20
□	Panorama	Use default	Use default
□	Proxy	Use default	Use default
□	RADIUS	Use default	Use default
□	SCEP	Use default	Use default
□	SNMP Trap	ethernet1/4	192.168.0.218/24
☑	Syslog	ethernet1/4	192.168.0.218/24

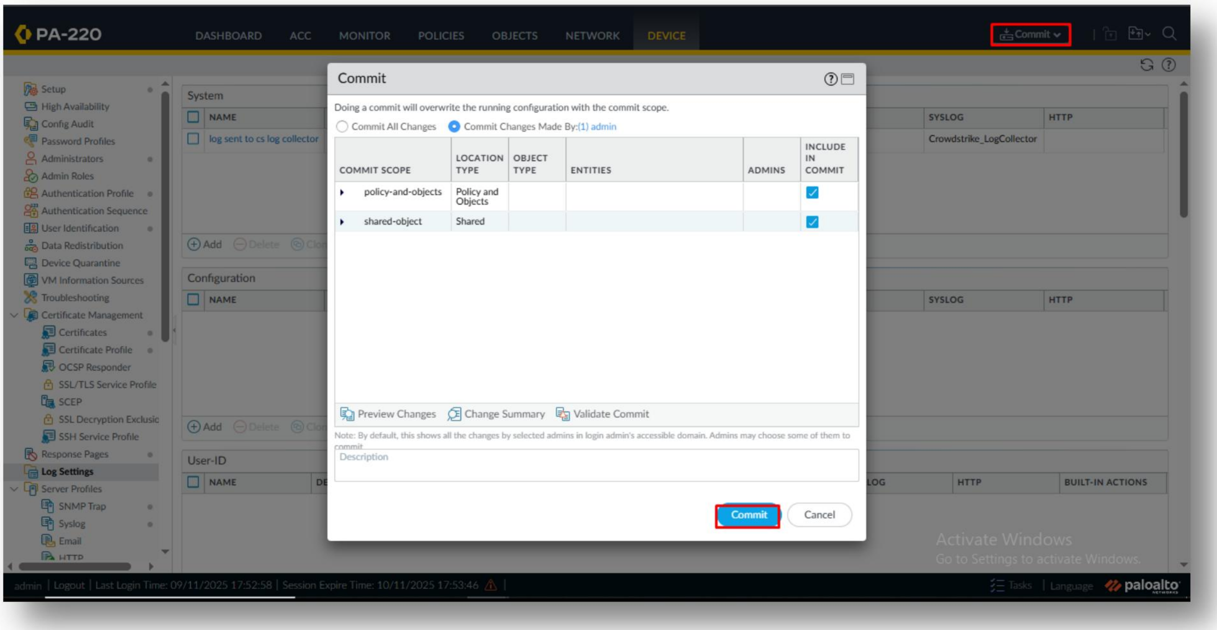
Service Route Source

Service	syslog
Source Interface	ethernet1/4
Source Address	192.168.0.218/24

OK Cancel

6. Commit Changes

Click Commit, select scope, and confirm.



Commit

Doing a commit will overwrite the running configuration with the commit scope.

○ Commit All Changes ● Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE	OBJECT TYPE	ENTITIES	ADMINS	INCLUDE IN COMMIT
policy-and-objects	Policy and Objects				☑
shared-object	Shared				☑

Note: By default, this shows all the changes by selected admins in login admin's accessible domain. Admins may choose some of them to commit

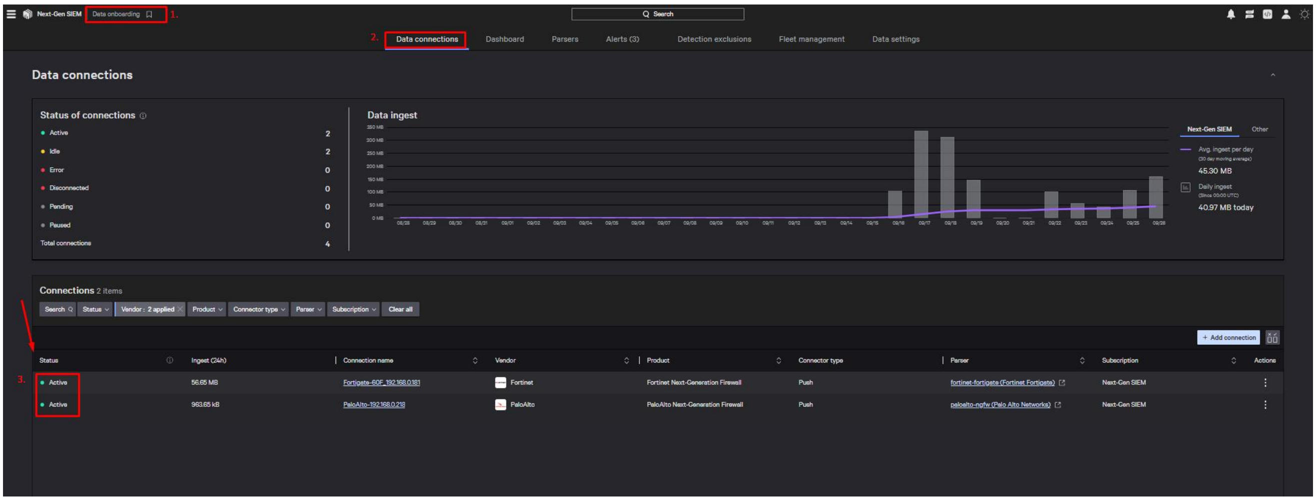
admin | Logout | Last Login Time: 09/11/2025 17:52:58 | Session Expire Time: 10/11/2025 17:53:46

https://www.linkedin.com/in/dhruv-rawat-46a445205/

Section 4: Verify Ingestion

Verify in Falcon Console

In Falcon Console → Data Onboarding → Data Connections, check that Palo Alto & Fortigate connection status is Active.



Data connections

Status of connections

● Active	2
● Idle	2
● Error	0
● Disconnected	0
● Pending	0
● Paused	0
Total connections	4

Avg. ingest per day (30 day moving average) 45.30 MB

Daily ingest (Since 00:00 UTC) 40.97 MB today

Connections 2 items

Status	Ingest (24h)	Connection name	Vendor	Product	Connector type	Parser	Subscription	Actions
● Active	56.65 MB	Fortigate-60F_192.168.0.181	Fortinet	Fortinet Next-Generation Firewall	Push	fortinet-fortigate (Fortinet Fortigate)	Next-Gen SIEM	⋮
● Active	963.65 kB	PaloAlto-192.168.0.218	PaloAlto	PaloAlto Next-Generation Firewall	Push	paloalto-ngfw (Palo Alto Networks)	Next-Gen SIEM	⋮

https://www.linkedin.com/in/dhruv-rawat-46a445205/