LOGZILLA DOCUMENTATION

Netskope Security Cloud

Parses Netskope Security Cloud CEF logs forwarded by Cloud Exchange, with rules, dashboards, and alert triggers for CASB, SWG, Private Access, DLP, and threat events.

LogZilla App Store · Generated June 17, 2026 · logzilla.ai/docs/logzilla-appstore/netskope

Overview

Netskope Security Cloud is a Secure Access Service Edge (SASE) and Security Service Edge (SSE) platform providing inline CASB, Secure Web Gateway (SWG), Cloud Firewall, Private Access (NPA), Data Loss Prevention (DLP), and threat protection. Netskope Cloud Exchange forwards events and alerts to a SIEM in CEF format over syslog. Those CEF records are parsed and classified with the standard Event Class/Type taxonomy, MITRE ATT&CK techniques, and compliance framework tags.

App Function

- Parse Netskope CEF records and dispatch on the record type (CEF SignatureID): connection, application, page, network, clientstatus, policy, DLP, incident, malsite, malware, uba, anomaly, compromisedcredential, and audit
- Extract source/destination IPs, acting user, cloud application, app category, Cloud Confidence Level, activity, action, destination domain, and DLP details
- Classify web and cloud-app traffic, Private Access (NPA) and Cloud Firewall network events, endpoint client status, DLP and incident records, malicious site and malware detections, and user behavior anomalies
- Map data-loss, malware, and anomaly records to MITRE ATT&CK techniques and apply compliance framework tags by Event Type
- Provide dashboards for cloud/web activity, security threats, and DLP
- Alert on DLP violations, malware and malicious sites, behavior anomalies, compromised credentials, blocked uploads, and denied private-app access

Vendor Documentation

- Skope IT Events and Alerts (https://docs.netskope.com/en/about-events/)
- Network Events (https://docs.netskope.com/en/about-network-events/)
- Cloud Confidence Index and CCL (https://docs.netskope.com/en/cloud-confidence-index/)
- Behavior Analytics (UBA) (https://docs.netskope.com/en/behavior-analytics/)
- About Malicious Sites (https://docs.netskope.com/en/about-malicious-sites/)
- Cloud Exchange Log Shipper module (https://docs.netskope.com/en/log-shipper-module/)
- Syslog plugin for Log Shipper (https://docs.netskope.com/en/syslog-plugin-for-log-shipper/)
- REST API Events and Alerts field reference (https://docs.netskope.com/en/rest-api-events-and-alerts-response-descriptions/)

Device Configuration

Netskope delivers logs through Cloud Exchange (CE) using the Cloud Log Shipper (CLS) module. CE pulls alerts and events from the Netskope tenant and forwards them to a syslog destination. The records carry a vendor-unique `CEF:0|Netskope|` header and are recognized by content on the standard syslog listener.

On the Netskope side:

In Cloud Exchange, enable the **Log Shipper** module.
Add a **Syslog** business rule / mapping that forwards the desired event and alert types (connection, application, page, network, clientstatus, policy, DLP, incident, malsite, malware, uba) in **CEF** format.
Configure the syslog destination with the LogZilla server address, protocol UDP or TCP, and port 514.
Save and activate the configuration.
On the LogZilla side, point the Cloud Exchange destination at the standard syslog port. Events are identified automatically by the CEF vendor field.

Verification

Generate cloud-app activity or a DLP/policy event in the Netskope tenant, then confirm events appear in LogZilla with the `Vendor` tag set to `Netskope`.

Incoming Log Format

Netskope Cloud Exchange emits Common Event Format (CEF) records:

```
CEF:0|Netskope|OTG|NULL|<record_type>|<name>|<severity>|<key=value extensions>
```

- **record_type** (CEF SignatureID) is the log/alert category and drives classification: `connection`, `application`, `page` (web and cloud-app traffic), `network` (Private Access / Cloud Firewall), `clientstatus` (endpoint client health), `policy` (real-time protection alerts), `DLP` and `incident` (data loss prevention), `malsite` and `malware` (threats), `uba` and `anomaly` (user behavior analytics), `compromisedcredential`, and `audit`.
- **name** is the policy or signature name (left in the raw message).
- **severity** is the CEF band (`Unknown`, `Low`, `Medium`, `High`, `Very-High`), mapped to a syslog severity.
- **extensions** are space-separated `key=value` pairs; unset fields use the literal value `null`.

The CEF envelope (vendor, product, record type, severity) is removed from the stored message since those values are available as tags. The per-event `timestamp` and random correlation IDs are also stripped so that otherwise-identical events deduplicate; LogZilla records its own receive time.

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Netskope	Vendor name
Product	Netskope Security Cloud	Product name
Event Class	Web, Network, Security, Compliance, System	Cross-vendor classification
Event Type	Access Control, Policy Violation, Data Access, Threat, Audit	Event subtype
MitreId	T1567	MITRE ATT&CK technique ID
MITRE Tactic	Exfiltration	MITRE ATT&CK tactic
SrcIP	10.0.0.50	Source (client) IP address (HC)
DstIP	198.51.100.20	Destination IP address (HC)
DstPort	https	Destination port name, network events (translated)
Protocol	Http	Network/private-app protocol, network events
User	user1@example.com	Acting user (HC)
Domain	app.example.com	Destination host/domain (HC)
Application	Microsoft OneDrive for Business	Cloud app or service name (HC)
Action	block, alert, useralert, deny, anomaly_detection	Enforcement action
SrcMAC	00:00:5e:00:53:10	Endpoint MAC, clientstatus events (HC)
Netskope Record Type	connection, policy, dlp, malsite	CEF record type / log category

Tag Name	Example	Description
Netskope Name	Block Generative AI, Bulk Download	CEF Name field: policy, threat, or anomaly name (alert records)
Netskope Activity	Browse, Download, Upload	User activity
Netskope App Category	Generative AI, Cloud Storage	Cloud Confidence Index app category
Netskope Cloud Confidence	excellent, high, medium, low, poor, unknown	Cloud Confidence Level (CCL)
Netskope Traffic Type	PrivateApp	Network traffic classification (NPA / Cloud Firewall)
Netskope DLP Profile	GDPR	Matched DLP profile, DLP events
Netskope DLP Rule	EU-Name-Phone	Matched DLP rule, DLP events
Netskope Threat Category	Malicious Site	Malicious-site threat category
Compliance - <framework>	1	Applied per Event Type (data-privacy or security frameworks)

Log Examples

Connection event (web/cloud traffic)

```
CEF:0|Netskope|OTG|NULL|connection|NULL|Unknown|IncidentID=0 appcategory=Webmail browser=Chrome
ccl=high clientBytes=2048 device=Windows Device dst=198.51.100.20 os=Windows 11
page=updates.example.com requestClientApplication=Gmail serverBytes=4096 sourceServiceName=Gmail
src=10.0.0.50 suser=user1@example.com timestamp=1700000000 url=updates.example.com/mail
```

Application event (cloud-app activity)

```
CEF:0|Netskope|OTG|NULL|application|NULL|Unknown|act=Browse appcategory=Generative AI
applicationType=nspolicy browser=Edge ccl=medium device=Windows Device dst=198.51.100.30 os=Windows
11 requestClientApplication=ChatGPT sourceServiceName=ChatGPT src=10.0.0.51 suser=user2@example.com
timestamp=1700000001 url=chatgpt.com/api
```

Policy alert (real-time protection, block with user alert)

```
CEF:0|Netskope|OTG|NULL|policy|Block Generative AI|Low|accessMethod=Client act=Browse
action=useralert appcategory=Generative AI ccl=medium device=Windows Device dst=198.51.100.40
os=Windows 11 policy=Block Generative AI requestClientApplication=Langdock sourceServiceName=Langdock
src=10.0.0.52 suser=user3@example.com timestamp=1700000002 url=app.example.com/chat
```

Network event (Private Access / NPA)

```
CEF:0|Netskope|OTG|NULL|network|NULL|Unknown|action=allow ccl=unknown clientBytes=1302 dpt=443
dst=198.51.100.50 networkSessionId=10000001 policy=Default PrivateAccess proto=Http
requestMethod=Client serverBytes=5644 sourceServiceName=internal-app spt=51000 src=10.0.0.54
suser=user5@example.com timestamp=1700000004 trafficType=PrivateApp tunnelType=NPA
```

DLP event (data loss prevention)

```
CEF:0|Netskope|OTG|NULL|DLP|DLP GDPR Monitoring|Low|accessMethod=Client act=Download
appcategory=Collaboration ccl=excellent dlpFile=report.xlsx dlpProfile=GDPR dlpRule=EU-Name-Phone
dlpRuleCount=1 dst=198.51.100.60 fsize=60928 object=report.xlsx policy=DLP GDPR Monitoring
requestClientApplication=Sharepoint sourceServiceName=Microsoft Sharepoint src=10.0.0.56
suser=user8@example.com timestamp=1700000007 url=tenant1.example.com/download
```

Malicious site (threat protection block)

```
CEF:0|Netskope|OTG|NULL|malsite|phishing.example.com|Medium|accessMethod=Client action=block
appcategory=Business browser=Firefox dst=198.51.100.70 msCategory=['Malicious Site'] msMalicious=yes
msMatchField=domain os=Windows 11 policy=Block Security Risks sourceServiceName=Classifieds
src=10.0.0.57 suser=user10@example.com timestamp=1700000009 url=phishing.example.com/site.js
```

User behavior anomaly (bulk download)

```
CEF:0|Netskope|OTG|NULL|uba|Bulk Download|Unknown|accessMethod=Client act=Download
action=anomaly_detection appcategory=Collaboration ccl=excellent dst=198.51.100.80
event_type=sequence object=report.xlsx requestClientApplication=Sharepoint
sourceServiceName=Microsoft Sharepoint Sites src=10.0.0.58 suser=user11@example.com
timestamp=1700000010 url=tenant1.example.com/data
```

Dashboards

- **Netskope: Cloud & Web Overview** shows cloud/web event rate, top applications, app categories, Cloud Confidence distribution, activities, users, and domains
- **Netskope: Security & Threats** shows security event rate, MITRE techniques and tactics, threat record types and categories, affected users, and threat sources
- **Netskope: DLP & Compliance** shows DLP event rate, top DLP profiles and rules, app categories and applications with DLP hits, and top users and destinations

Triggers

Trigger	Description
`Netskope: MITRE ATT&CK Threat Detected`	Catch-all for MITRE-tagged events
`Netskope: DLP Violation`	DLP profile/rule match (data exfiltration)
`Netskope: Malware or Malicious Site`	Malware or malicious-site detection
`Netskope: User Behavior Anomaly`	UBA/UEBA anomaly (bulk transfer, anomaly)
`Netskope: Compromised Credential`	Compromised-credential alert
`Netskope: Blocked Upload to Cloud App`	Blocked upload (potential exfiltration)
`Netskope: Private App Access Denied`	Denied Private Access / Cloud Firewall connection