netskope

DATA SHEET

Netskope Cloud Log Shipper

High-performance Netskope log export

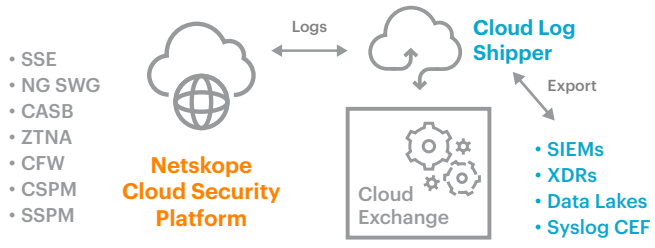
Cloud Log Shipper (CLS) is a Netskope high-performance integration module that sends all or a selected subset of customer tenant events and alerts logs to security information and event management (SIEM), data lakes, and extended detection and response (XDR) platforms.

WHY IS NETSKOPE THE BEST CHOICE?

The CLS module is included with Netskope Cloud Exchange, our free platform for integrating with third-party solutions. CLS regularly polls the Netskope REST API gateway to extract raw event and alert logs and quickly sends them in a customized, pre-selected format to your data receivers within minutes. Security operations centers gain extended visibility and context with support for CASB, SIEM, and XDR.

HIGH-PERFORMANCE LOG EXPORTER FOR MAJOR SIEM, XDR, AND DATA LAKE PLATFORMS

- **Small footprint.** CLS is simple and easy to implement where needed, providing customized, parser-ready output that popular XDR, SIEM, and data lake platforms can ingest.
- **Customize according to your logging needs.** Easily filter out fields that are not required and minimize API calls and connector rebuilds.
- **Fast delivery.** Platforms are notified within minutes after a user takes an action in an app, cloud service, or website, triggering the event log and related alerts.
- **Comprehensive support for Netskope data logs.** CLS works with all data logs from Netskope, including events, alerts, cloud firewall and web transaction logs, and more.



KEY BENEFITS AND CAPABILITIES

Log exporting simplified
Automatically pull all or specified tenant events and alerts logs and send them to SIEM, XDR, or data lake platforms.

Clean output
Eliminate the need to deal with raw API output and minimize API calls and connector rebuilds.

Customize and export logs
Easily filter fields you desire per destination.

Get requested logs during initial seeding and near real-time activities
CLS uses a sophisticated algorithm with a multi-threaded query engine, working within rate limits (4 queries/second), and handling error responses and datasets larger than its pagination limit.

Support for popular plug-ins
CLS supports many popular platforms, including AlienVault, Azure Sentinel, CrowdStrike Humio, Google Chronicle, AWS S3 buckets, and more.

One-click instantiation through container services
Get CLS through the AWS and GCP marketplaces or through the Netskope Support Portal.

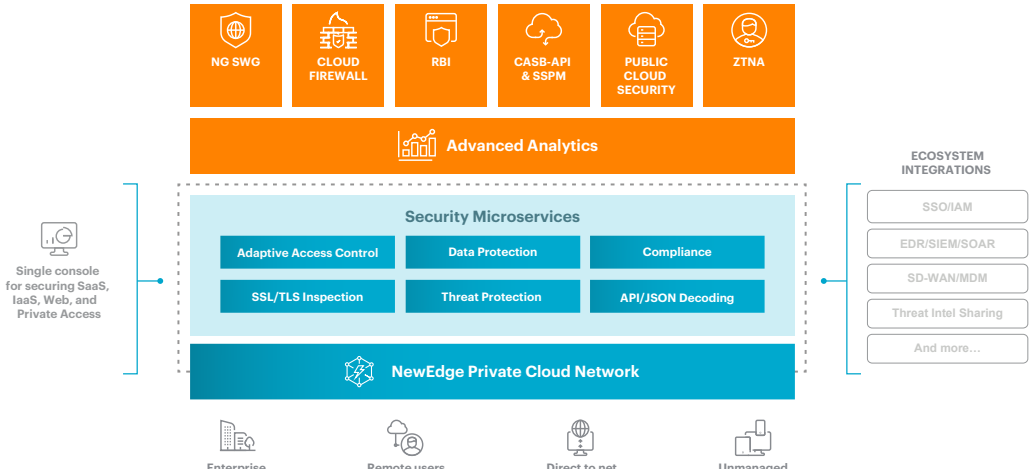
"Understanding the data content and context for apps, cloud services, and web user activity is the core of a single-pass SASE architecture for data and threat protection."

– CLOUD AND THREAT REPORT, FEBRUARY 2021

THE NETSKOPE DIFFERENCE

Fast everywhere, data-centric, and cloud-smart.

Using patented technology called Netskope Cloud XD™, the Netskope Security Cloud eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud (SaaS and IaaS) services and millions of websites. With full control from one cloud, our customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection, including targeted RBI for risky websites that stops elusive attacks.



YOUR NEEDS	THE NETSKOPE SOLUTION
Fast Netskope log export to preferred platforms	CLS regularly polls the Netskope REST API gateway to extract raw event and alert logs and sends them in a customized, pre-selected format to your data receivers within minutes.
Filter the logs desired to ingest in your SIEM, XDR, or data lake platform	Business rules make it easy to select just the data that your receiver requires.
Process events and alerts from one or more Netskope tenants for your SIEM platform	CLS offers mappings so that your SIEM platform can ingest events and alerts from multiple Netskope tenants.
Support for CASB, SIEM, and XDR plug-ins	Ready-to-use CLS plug-ins include: AlienVault, Azure Sentinel, CrowdStrike Humio, Google Chronicle, Google Cloud Security Command Center, IBM QRadar, LogRhythm, Micro Focus ArcSight, Microsoft Cloud Application Security, Rapid7, and generic (configurable) Syslog CEF.
Support for cloud storage plug-ins	CLS supports major cloud storage options, including AWS S3 buckets, Microsoft Azure Blob storage, and Google Cloud Platform storage.
Get requested logs during initial seeding and near real-time activities	CLS uses a sophisticated algorithm with a multi-threaded query engine, working within rate limits (4 queries/second), and handling error responses and datasets larger than its pagination limit.
Support for third-party log export tools	Netskope also has direct integrations with Exabeam, Securonix, Splunk, and Sumo Logic for log export.

netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.

©2021 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 11/21 DS-503-1