paloalto TECHDOCS

Strata Logging Service Administration

Administration

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 17, 2024

Table of Contents

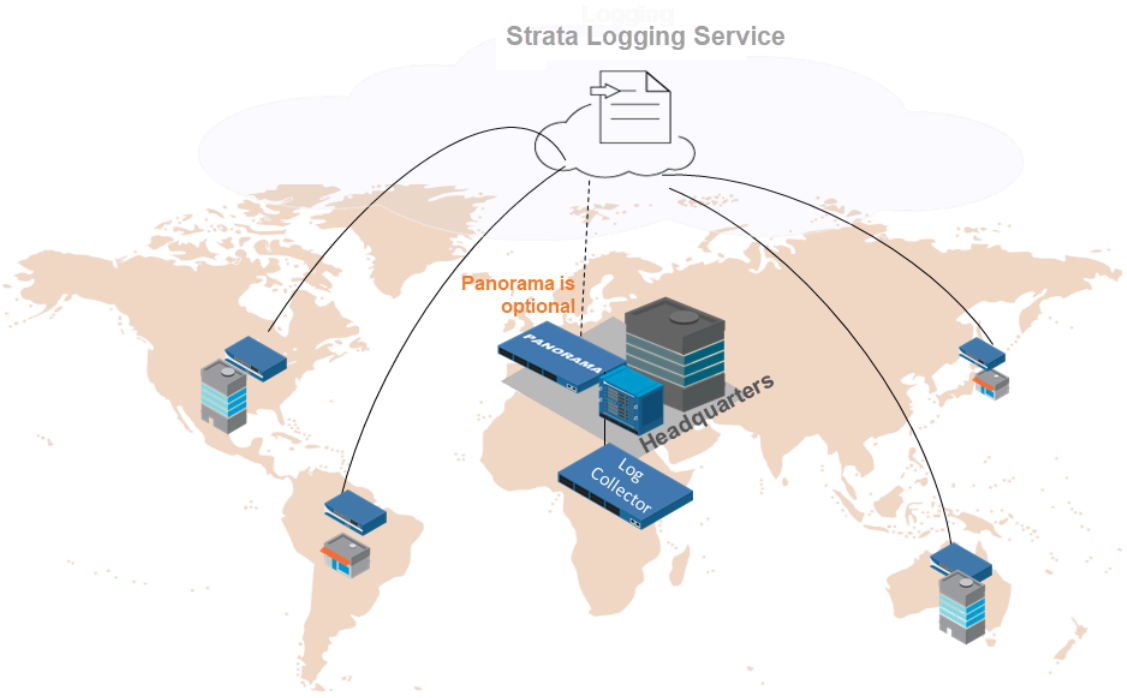
Introduction to Strata Logging Service

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access • Cortex Xpanse™ • Cortex XSOAR • Cortex XDR	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

Palo Alto Networks® Strata Logging Service provides cloud-based, centralized log storage and aggregation for your on premise, virtual (private cloud and public cloud) firewalls, for Prisma Access, and for cloud-delivered services such as Cortex XDR.

Strata Logging Service is secure, resilient, and fault-tolerant, and it ensures your logging data is up-to-date and available when you need it. It provides a scalable logging infrastructure that alleviates the need for you to plan and deploy Log Collectors to meet your log retention needs. If you already have on premise Log Collectors, the new Strata Logging Service can easily complement your existing setup. You can augment your existing log collection infrastructure with the cloud-based Strata Logging Service to expand operational capacity as your business grows, or to meet the capacity needs for new locations.

With this service, Palo Alto Networks takes care of the ongoing maintenance and monitoring of the logging infrastructure so that you can focus on your business.



Strata Logging Service interacts with several different products. Some products send logs to Strata Logging Service, while others use it to view and analyze the log data.

Features of Strata Logging Service

Use the Strata Logging Service to-

- Check the status of a Strata Logging Service instance
- View the devices and tenants onboarded to Strata Logging Service instance.
- Configure log storage quota
- Search, filter, and export log data
- Forward log data to a Syslog server, https server, or an email server for long-term storage, SOC, or internal audit.

Products that send logs to Strata Logging Service

Palo Alto Networks Firewalls	You can onboard individual firewalls directly to Strata Logging Service. Use the Strata Logging Service app to view all log records that the firewalls forward to Strata Logging Service.
Panorama-Managed Firewalls	If you're using Panorama, you can onboard firewalls to Strata Logging Service at scale, instead of onboarding each individual firewall. All Strata Logging Service logs are visible directly in Panorama.

Prisma Access	With Prisma Access, Palo Alto Networks deploys and manages the security infrastructure globally to secure your remote networks and mobile users. Prisma Access logs directly to Strata Logging Service. You can view the logs, ACC, and reports from Panorama for an aggregated view into your remote network and mobile user traffic. To enable logging for Prisma Access, you must purchase a Strata Logging Service license. Log traffic does not use the licensed bandwidth you purchased for Prisma Access.

Products that use logs stored in Strata Logging Service

AIOps for NGFW	AIOps for NGFW uses Strata Logging Service log data to assess the health of your firewalls and generate alerts. You can also view Strata Logging Service log data from within AIOps for NGFW.
Prisma Access (Cloud-Managed)	Cloud-managed Prisma Access enables you to view and filter your log data, and it can generate reports on your log data.
IoT Security	IoT Security is a cloud-based app that ingests the device data that next-generation firewalls collect from network traffic and send to Strata Logging Service. IoT Security then uses this data to discover the “things” on your network and identify normal device behavior and detect suspicious activity.
Panorama	Panorama displays logs stored in Strata Logging Service. The Panorama ACC and reports give you an aggregated view into your remote network traffic.
SaaS Security Inline	SaaS Security Inline uses Strata Logging Service logs to discover users and provide SaaS application usage data about those users.
Cortex XDR	If you extend your firewall security policy to mobile users and remote networks using Prisma Access or GlobalProtect, you can also forward related traffic logs to Strata Logging Service. The analytics engine can then analyze those logs and raise alerts on anomalous behavior.
Cortex XSOAR	In Cortex XSOAR Marketplace, install the Strata Logging Service Content Pack to run queries for critical threat logs, social applications, threat logs,

	etc. You can also Install the PAN-OS to Strata Logging Service Monitoring content pack to monitor the PAN-OS FW log in a recurring job.
Cortex Xpanse™	Cortex Xpanse™ consumes GlobalProtect login events on a daily basis to surface external exposures on employee networks.

Strata Logging Service Regions

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Strata Logging Service license

The region that you select when you activate Strata Logging Service determines the physical location in which your data is stored. If regulations require that your data remain within regional bounds, select the appropriate region to comply.

Strata Logging Service ensures data redundancy by storing your data in two different zones in the region you choose. Therefore, in case of an outage, Strata Logging Service will failover to the secondary zone in an attempt to prevent interruption of service.

If you want to use a third-party app to ingest your Strata Logging Service log data, ensure that the third-party app is supported in the same region as your Strata Logging Service instance. Otherwise, the third-party app will be unable to access your data. Third-party apps are currently supported in only the following regions:

- **United States - Americas**
- **United Kingdom**
- **Netherlands - Europe**
- **Japan**

These are the regions in which you can host Strata Logging Service. Each region has

- an address range that you must allow on your syslog or HTTPS server when forwarding logs from Strata Logging Service.
- FQDNs and ports that you must allow on any third-party firewalls you might have between your Palo Alto Networks firewalls and Strata Logging Service. Only Palo Alto Networks firewalls can generate logs for Strata Logging Service.

- *Products that use Strata Logging Service may support either all or some of the listed regions. To know which Strata Logging Service regions your product supports, refer to the respective product documentation. For instance, Prisma Access supports only a subset of Strata Logging Service regions.*
- *Strata Logging Service is unavailable in FedRAMP environments where Prisma Access is also not present.*

Region	Purpose	FQDN or IP Address	TCP Port
Australia	Source IP Addresses for Log Forwarding	35.244.108.240/28	N/A
	Firewall Log Ingestion	firewall-prd1.au1.se1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-au.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.au1.se1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-au.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.au1.se1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.au1.se1.cdl.paloaltonetworks.com	444
		cdl-prd1.au1.se1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-au.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Canada	Source IP Addresses for Log Forwarding	34.95.59.80/28	N/A
	Firewall Log Ingestion	firewall-prd1.ca1.ne1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-ca.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.ca1.ne1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-ca.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.ca1.ne1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.ca1.ne1.cdl.paloaltonetworks.com	444

Region	Purpose	FQDN or IP Address	TCP Port
		cdl-prd1.ca1.ne1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-ca.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
China	*Strata Logging Service in China has limitations. Review them here.*		
	Source IP Addresses for Log Forwarding	54.222.227.10, 54.223.157.221, 52.81.134.154	N/A
	Firewall Log Ingestion	firewall-prd1.cn1.no1.cdl.prismaaccess.cn	3978
		*.in2-lc-prod-cn.cdl.prismaaccess.cn	3978
	Enhanced Application Log Ingestion	fei-prd1.cn1.no1.cdl.prismaaccess.cn	443
		*.fei-lc-prod-cn.cdl.prismaaccess.cn	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.cn1.no1.cdl.prismaaccess.cn	443
		s3.cn-north-1.amazonaws.com.cn	443
	Log Access from Panorama	pcl-prd1.cn1.no1.cdl.prismaaccess.cn	444
		cdl-prd1.cn1.no1.cdl.prismaaccess.cn	443
		*.api2-lc-prod-cn.cdl.prismaaccess.cn	444
	License and Tenant Mapping Check	registry-prd1.cn1.no1.cdl.prismaaccess.cn	444
France	Source IP Addresses for Log Forwarding	34.155.98.0/28	N/A
	Firewall Log Ingestion	firewall-prd1.fr1.ew9.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-fr.gpcloudservice.com	3978

Region	Purpose	FQDN or IP Address	TCP Port
	Enhanced Application Log Ingestion	fei-prd1.fr1.ew9.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-fr.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.fr1.ew9.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.fr1.ew9.cdl.paloaltonetworks.com	444
		cdl-prd1.fr1.ew9.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-fr.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Germany	Source IP Addresses for Log Forwarding	35.246.195.240/28	N/A
	Firewall Log Ingestion	firewall-prd1.de1.ew3.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-de.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.de1.ew3.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-de.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.de1.ew3.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.de1.ew3.cdl.paloaltonetworks.com	444
		cdl-prd1.de1.ew3.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-de.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443

Region	Purpose	FQDN or IP Address	TCP Port
India	Source IP Addresses for Log Forwarding	35.244.35.240/28	N/A
	Firewall Log Ingestion	firewall-prd1.in1.as1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-in.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.in1.as1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-in.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.in1.as1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.in1.as1.cdl.paloaltonetworks.com	444
		cdl-prd1.in1.as1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-in.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Indonesia	Source IP Addresses for Log Forwarding	34.128.96.0/28	N/A
	Firewall Log Ingestion	firewall-prd1.id1.se2.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-id.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.id1.se2.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-id.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.id1.se2.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.id1.se2.cdl.paloaltonetworks.com	444

Region	Purpose	FQDN or IP Address	TCP Port
		cdl-prd1.id1.se2.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-id.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Israel - Tel Aviv	Source IP Addresses for Log Forwarding	34.165.82.208/28	N/A
	Firewall Log Ingestion	firewall-prd1.il1.mw1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-il.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.il1.mw1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-il.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.il1.mw1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.il1.mw1.cdl.paloaltonetworks.com	444
		cdl-prd1.il1.mw1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-il.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Italy	Source IP Addresses for Log Forwarding	34.154.10.144/28	N/A
	Firewall Log Ingestion	firewall-prd1.it1.ew8.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-it.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.it1.ew8.cdl.paloaltonetworks.com	443

Region	Purpose	FQDN or IP Address	TCP Port
		*.fei-lc-prod-it.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.it1.ew8.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.it1.ew8.cdl.paloaltonetworks.com	444
		cdl-prd1.it1.ew8.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-it.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Japan - Tokyo	Source IP Addresses for Log Forwarding	34.84.94.80/28	N/A
	Firewall Log Ingestion	firewall-prd1.jp1.ne1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-jp.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.jp1.ne1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-jp.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.jp1.ne1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.jp1.ne1.cdl.paloaltonetworks.com	444
		cdl-prd1.jp1.ne1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-jp.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443

Region	Purpose	FQDN or IP Address	TCP Port
Korea	Source IP Addresses for Log Forwarding	34.22.96.0/28	N/A
	Firewall Log Ingestion	firewall-prd1.kr1.ne3.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-kr.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.kr1.ne3.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-kr.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.kr1.ne3.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.kr1.ne3.cdl.paloaltonetworks.com	444
		cdl-prd1.kr1.ne3.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-kr.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Netherlands - Europe	Source IP Addresses for Log Forwarding	154.59.126.0/24, 34.90.138.80/28	N/A
	Firewall Log Ingestion	firewall-prd1.nl.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-eu.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.nl.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-eu.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.nl.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.nl.cdl.paloaltonetworks.com	444
		cortex-prd1.nl.cdl.paloaltonetworks.com	443

Region	Purpose	FQDN or IP Address	TCP Port
		*.api2-lc-prod-eu.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Poland - Warsaw	Source IP Addresses for Log Forwarding	34.118.66.32/28	N/A
	Firewall Log Ingestion	firewall-prd1.pl1.ec2.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-pl.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.pl1.ec2.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-pl.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.pl1.ec2.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.pl1.ec2.cdl.paloaltonetworks.com	444
		cdl-prd1.pl1.ec2.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-pl.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Qatar	Source IP Addresses for Log Forwarding	34.18.128.0/28	N/A
	Firewall Log Ingestion	firewall-prd1.qa1.mc1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-qa.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.qa1.mc1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-qa.gpcloudservice.com	444

Region	Purpose	FQDN or IP Address	TCP Port
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.qa1.mc1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.qa1.mc1.cdl.paloaltonetworks.com	444
		cdl-prd1.qa1.mc1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-qa.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Saudi Arabia	Source IP Addresses for Log Forwarding	34.166.52.80/28	N/A
	Firewall Log Ingestion	firewall-prd1.sa1.mc2.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-sa.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.sa1.mc2.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-sa.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.sa1.mc2.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.sa1.mc2.cdl.paloaltonetworks.com	444
		cdl-prd1.sa1.mc2.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-sa.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Singapore	Source IP Addresses for Log Forwarding	34.87.142.80/28	N/A

Region	Purpose	FQDN or IP Address	TCP Port
	Firewall Log Ingestion	firewall-prd1.sg1.se1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-sg.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.sg1.se1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-sg.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.sg1.se1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.sg1.se1.cdl.paloaltonetworks.com	444
		cdl-prd1.sg1.se1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-sg.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Spain	Source IP Addresses for Log Forwarding	34.175.10.160/28	N/A
	Firewall Log Ingestion	firewall-prd1.es1.sw1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-es.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.es1.sw1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-es.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.es1.sw1.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.es1.sw1.cdl.paloaltonetworks.com	444
		cdl-prd1.es1.sw1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-es.gpcloudservice.com	444

Region	Purpose	FQDN or IP Address	TCP Port
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Switzerland	Source IP Addresses for Log Forwarding	34.65.166.64/28	N/A
	Firewall Log Ingestion	firewall-prd1.ch1.ew6.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-ch.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.ch1.ew6.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-ch.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.ch1.ew6.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.ch1.ew6.cdl.paloaltonetworks.com	444
		cdl-prd1.ch1.ew6.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-ch.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
Taiwan	Source IP Addresses for Log Forwarding	34.81.162.32/28	N/A
	Firewall Log Ingestion	firewall-prd1.tw1.ae1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-tw.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.tw1.ae1.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-tw.gpcloudservice.com	444
	Telemetry and GlobalProtect	br-prd1.tw1.ae1.cdl.paloaltonetworks.com	443

Region	Purpose	FQDN or IP Address	TCP Port
	Troubleshooting Log Ingestion	storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.tw1.ae1.cdl.paloaltonetworks.com	444
		cdl-prd1.tw1.ae1.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-tw.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
United Kingdom	Source IP Addresses for Log Forwarding	35.246.51.240/28	N/A
	Firewall Log Ingestion	firewall-prd1.uk.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-uk.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.uk.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-uk.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.uk.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.uk.cdl.paloaltonetworks.com	444
		cortex-prd1.uk.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-uk.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
United States	Source IP Addresses for Log Forwarding	65.154.226.0/24, 34.67.106.64/28	N/A
	Firewall Log Ingestion	firewall-prd1.us.cdl.paloaltonetworks.com	3978

Region	Purpose	FQDN or IP Address	TCP Port
		firewall-prd1.us2.cent1.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-us.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-prd1.us.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-us.gpcloudservice.com	444
		eal-prd1.us2.cent1.cdl.paloaltonetworks.com	443
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-prd1.us.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-prd1.us.cdl.paloaltonetworks.com	444
		cortex-prd1.us.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-us.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
United States Government (High)	Source IP Addresses for Log Forwarding	34.132.154.128/28	N/A
	Firewall Log Ingestion	firewall-highgov.us1.cent1.highgov.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-highgov.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-highgov1.us1.cent1.highgov.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-highgov.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-highgov1.us1.cent1.highgov.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-highgov1.us1.cent1.highgov.cdl.paloaltonetworks.com	444

Region	Purpose	FQDN or IP Address	TCP Port
		cdl-highgov1.us1.cent1.highgov.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-highgov.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		registry.highgov.cdl.paloaltonetworks.com	443
United States Government (Moderate)	Source IP Addresses for Log Forwarding	34.67.50.64/28	N/A
	Firewall Log Ingestion	firewall-gov.gov.cdl.paloaltonetworks.com	3978
		*.in2-lc-prod-gov.gpcloudservice.com	3978
	Enhanced Application Log Ingestion	fei-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
		*.fei-lc-prod-gov.gpcloudservice.com	444
	Telemetry and GlobalProtect Troubleshooting Log Ingestion	br-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
		storage.googleapis.com	443
	Log Access from Panorama	pcl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443
		*.api2-lc-prod-gov.gpcloudservice.com	444
	License and Tenant Mapping Check	lic.lc.prod.us.cs.paloaltonetworks.com	444
		cdl-gov1.us1.cent1.gov.cdl.paloaltonetworks.com	443

If you plan to use Cortex XDR with Strata Logging Service deployed in the United Kingdom (UK), all Cortex XDR logs and data reside within the UK boundary, but Cortex XDR will send files that require analysis to the WildFire cloud for EU. If your compliance and privacy laws prohibit files from leaving the UK region, disable file uploads to WildFire in your Malware Security Profiles.

Limitations in Strata Logging Service China

The following Strata Logging Service features are unavailable or require you to take additional action to work for Strata Logging Service instances deployed in China:

- Exporting logs in Log Viewer/Explore is unavailable.
- Onboarding NGFW devices in Strata Logging Service app is unavailable.
- Dashboard view in Strata Logging Service app is unavailable.
- Enabling log forwarding from Strata Logging Service instance deployed in China to an external log server requires you to contact Palo Alto Networks team. Configuring log forwarding profiles to send logs to servers outside China can result in personally identifiable information leaving China.
- The Strata Cloud Manager app is unavailable to manage and monitor Strata Logging Service China instances, instead use the Strata Logging Service standalone app.

User Roles for Strata Logging Service

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Strata Logging Service license

The way that you assign roles for Strata Logging Service depends on the status of your transition to the Prisma™ SASE Platform.

Newly Activated	Transitioned to a Tenant Service Group	Pre-Transition
If you activated Strata Logging Service with Prisma Access or another product after August 2022, then you're using Identity & Access on the Prisma SASE Platform for license and role management. Rather than read this topic any further, go to Common Services: Identity & Access to see how to manage roles with Prisma SASE.	Was your Strata Logging Service instance recently transitioned to a tenant service group (TSG)? If so, there's a new way to manage administrator roles and access using Identity & Access. To learn more, see Common Services: Identity & Access	Did you activate Strata Logging Service before August 2022? You should have already received information about the transition of your Strata Logging Service instance. You'll receive an email when it's time for you to transition. Until your transition is complete, continue to manage roles using the information below.

Role-based access control (RBAC) enables you to assign privileges and access rights to administrative users through role assignment. You create user accounts in the Customer Support Portal (CSP), assign them roles in the hub, and limit the data and functionality they can access by site in the Strata Logging Service app.

Strata Logging Service supports the following user roles:

- App Administrator
- Instance Administrator
- Log Viewer Admin

The App Administrator and Instance Administrator are common roles that are available to every Palo Alto Networks app. To learn more about them, see Available Roles.

For Strata Logging Service instances that are transitioned to TSG, support the following user roles. Refer here for information about permissions for these user roles:

- Multitenant Superuser
- SOC Analyst
- Superuser
- View Only Administrator

The only user role specifically for Strata Logging Service is Log Viewer Admin. The permissions for this role is same as for the SOC Analyst user role.

Note that custom roles are not supported for Strata Logging Service.

User Role	Role Definition	Access Control
Log Viewer Admin	Same permissions as SOC Analyst. You can only view and export data in the **Explore** tab of the Strata Logging Service app or in the **Log Viewer** in Strata Cloud Manager.	• View the logs in **Explore** or **Log Viewer**. • Filter logs using queries. • Export log data - Ensure that Browser user role is not assigned along with this role. Browser role restricts you to export logs.

Launch Strata Logging Service

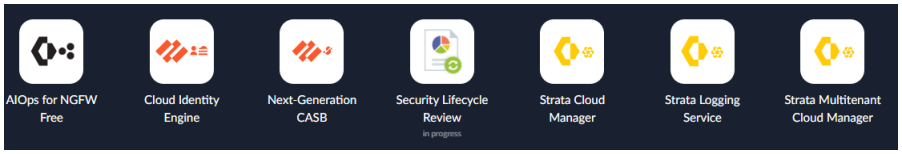
Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	You must have at least one of these licenses to use Strata Cloud Manager: • Prisma Access • AIOps for NGFW Premium • Prisma SD-WAN Strata Logging Service license

After you activate Strata Logging Service, you can access Strata Logging Service from Strata Cloud Manager app or the standalone Strata Logging Service app available on the Palo Alto Networks hub. Strata Cloud Manager is a unified management platform to manage your entire Palo Alto Networks Network Security infrastructure.

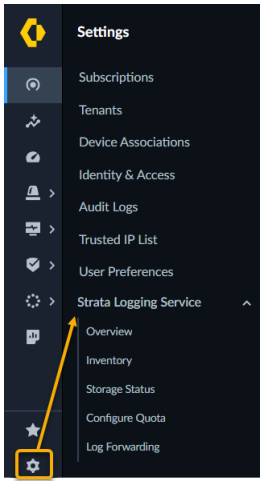
A Prisma Access license, AIOps for NGFW Premium license, or a Prisma SD-WAN license is a basic requirement for Strata Cloud Manager unified management and operations. If you have at least one of these licenses, you can access Strata Cloud Manager to gain visibility into or manage your product(s). Along with your product license, you must activate Strata Logging Service license to access and manage logging from Strata Cloud Manager.

Launch Strata Logging Service

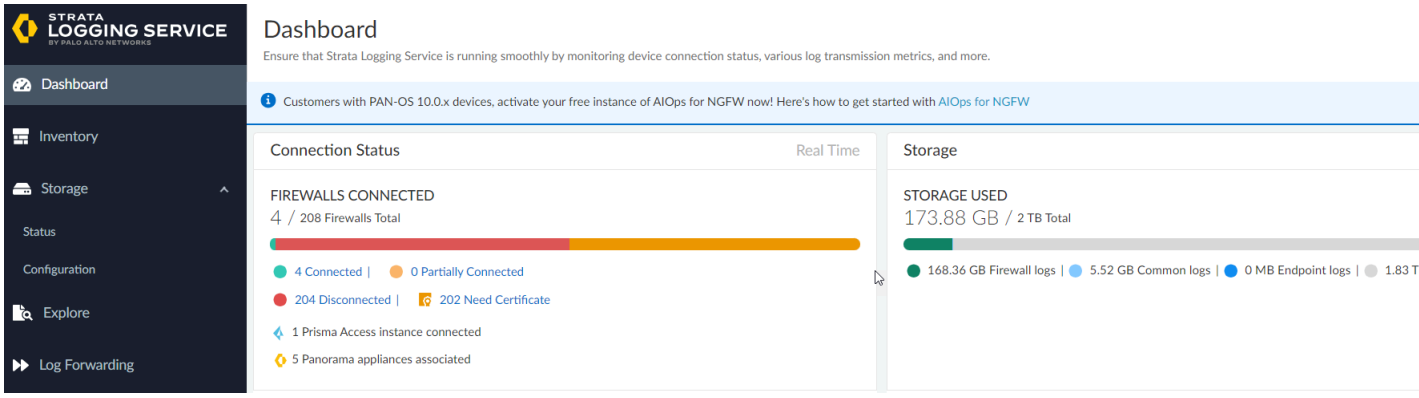
After you activate your product license and Strata Logging Service license, the Strata Cloud Manager app and standalone app will be available to you on the Palo Alto Networks hub. You can also access Strata Cloud Manager app directly at stratacloudmanager.paloaltonetworks.com.



To access Strata Logging Service from Strata Cloud Manager app, launch Strata Cloud Manager app and click **Settings** > **Strata Logging Service**.



To access Strata Logging Service from the standalone Strata Logging Service app, log in to the hub and launch the Strata Logging Service instance. If you have multiple instances of Strata Logging Service, you can choose which instance of the app you want to access.



Strata Logging Service Features in Strata Cloud Manager

The existing user of Strata Logging Service using standalone app have been or will be updated to Strata Cloud Manager. The update is seamless and does not impact your existing data and configuration in Strata Logging Service instances. If you've previously used the Strata Logging Service app, here's where you can find your features in Strata Cloud Manager.

If your Strata Logging Service instance is hosted in China or FedRAMP high regions, you can continue to use Strata Logging Service standalone app to manage your logs.

Features in Strata Logging Service App	Where to find the features in Strata Cloud Manager
Dashboard	**Settings > Strata Logging Service > Overview**
Inventory	**Settings > Strata Logging Service > Inventory**

Features in Strata Logging Service App	Where to find the features in Strata Cloud Manager
	Currently, you can Generate OTP, Generate PSK, and Add devices only in Standalone Strata Logging Service app. These options are also available in Strata Cloud Manager. When you select the options in Strata Cloud Manager, you will be automatically redirected to Strata Logging Service app.
Storage > Status	**Settings > Strata Logging Service > Storage Status**
Storage > Configuration	**Settings > Strata Logging Service > Configure Quota**
Explore	**Incidents & Alerts > Log Viewer**
Log Forwarding	**Settings > Strata Logging Service > Log Forwarding**

Monitor Strata Logging Service

Where Can I Use This?	What Do I Need?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Strata Logging Service

As a cloud-based logging service, Strata Logging Service requires a robust connection so that log records do not get lost and every network event is accounted for.

With the monitoring capabilities of the Strata Logging Service app, you can observe whether your devices are still sending logs to Strata Logging Service as well as view finer details about log transmission, such as storage, latency, ingestion, and log forwarding status. Closely monitoring this information can help you react faster to system outages and even anticipate their occurrence.

Every 5 minutes, the Strata Logging Service app collects a variety of metrics to give you a complete picture of your logging infrastructure. The metrics that the app collects include

- Incoming log rate per instance, firewall, and log type
- Incoming log bytes per instance, firewall, and log type
- Storage used per instance, firewall, and log type
- Forwarded logs per instance and destination
- Log latency between the firewall and Strata Logging Service
- Log latency between the firewall and log forwarding destinations

The app collects the following event data in real-time:

- Firewall connected or disconnected
- Service available or unavailable

If you are using cloud-managed Next-Generation Firewalls with AIOps for NGFW, you can view alerts about your Strata Logging Service instance to keep you aware of the latest issues affecting it and actions you can take to address them.

View Status of your Strata Logging Service Instance

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	Strata Logging Service

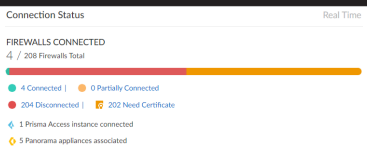
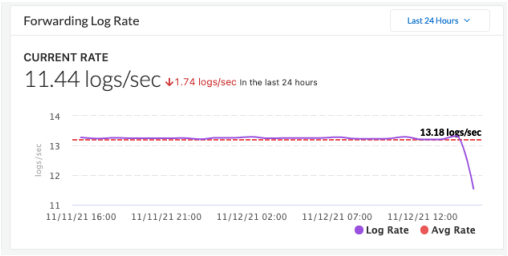
The view status dashboard does not apply to:

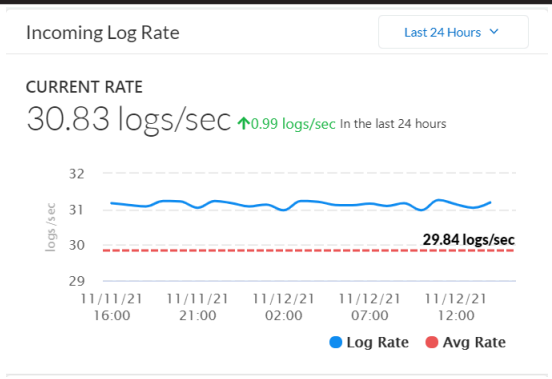
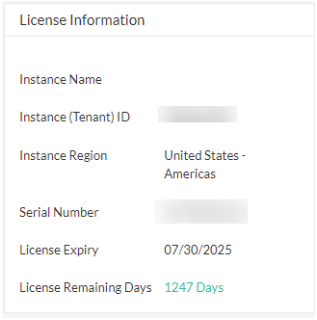
- *the qualifying users of Strata Logging Service using the new license that comes with one year log retention.*

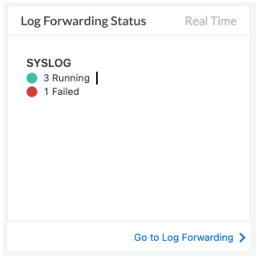
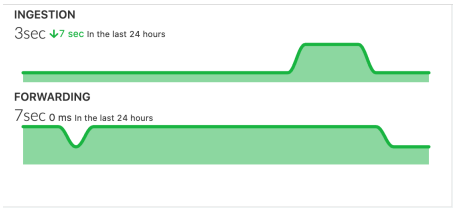
The Dashboard gives you the latest status of your Strata Logging Service instance. It displays several widgets that report on various metrics that you can use to assess the health of the instance.

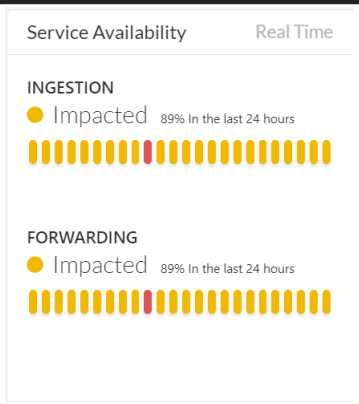
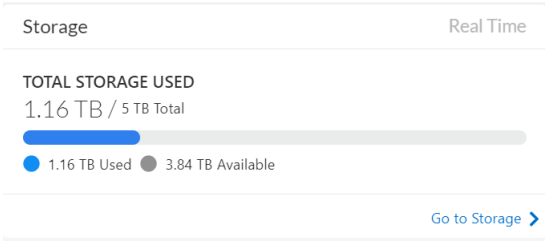
*If you are using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Overview** to check the status of your Strata Logging Service instance.*

Widget	Description
Connection Status	Displays the number of firewalls associated with your Strata Logging Service tenant and identifies them with each of the following statuses: • **Connected**—The firewall has an active channel through which it is sending session logs to Strata Logging Service. • **Partially Connected**—The firewall does not have an active channel through which it is sending session logs to Strata Logging Service. However, it is sending Enhanced Application logs on a session-less channel. • **Disconnected**—The firewall does not have an active channel through which to send sessions logs to Strata Logging Service, and it is not sending Enhanced Application Logs. • **Need Certificate**—The firewall does not have the certificate to connect to Strata Logging Service Click on any of these statuses to view the relevant firewalls on the **Inventory** page. Below the connection statuses, you can see whether a Panorama is associated with your Strata Logging Service instance. You can also see how many firewalls in your customer support account are available for onboarding. Clicking the text launches firewall onboarding.

Widget	Description
	
Forwarding Log Rate	Provides a graph of the logs that Strata Logging Service is forwarding to an external solution. The graph shows the current (avg over the last 5 mins) forwarding log rate for the tenant, how that rate varies from the average over time, and the trend of the log rate over time. You can choose a time period of 24 hours, 7 days, or 30 days. 
Forwarding Log Table	Displays the logs that Strata Logging Service is forwarding to external destinations, organized by destination. • Profile Type—The type of log forwarding profile that is forwarding logs to the destination. • Profile Name—The name of the log forwarding profile that is forwarding logs to the destination. • Log Types Forwarded—The types of logs that Strata Logging Service is forwarding to the destination. • Average Forwarding Rate—The average rate at which Strata Logging Service is forwarding logs to the destination. • Forwarding Log Count—The number of logs that Strata Logging Service is forwarding to the destination. • Retry Log Count—The number of logs that did not arrive at the destination in the first attempt but was sent to endpoint after retry. • Forwarding Log Size—The size of the logs that Strata Logging Service is forwarding to the destination.
Incoming Log Rate	Provides a graph of the logs that Strata Logging Service is ingesting. The graph shows the current (average over the last 5 minutes) incoming log rate for the tenant, how that rate varies from the average over time, and the trend of the log rate over time. You can choose a time period of 24 hours, 7 days, or 30 days. *If you have enabled enhanced application logging on any firewalls or Prisma Access, the incoming log rate will include that as well.*

Widget	Description
	
Incoming Log Table	Displays the logs that Strata Logging Service is receiving from connected devices, organized by log type. You can **Search** for specific information in the table as well as select a time range of **Last 24 Hours**, **Last 7 Days**, or **Last 30 Days**. • Actual Retention—The number of days that Strata Logging Service has stored the logs. • Target Retention—The number of days that you have set for Strata Logging Service to store logs. Logs older than this value are deleted. • Avg Incoming Log Rate—The average rate at which your devices are sending logs to Strata Logging Service. • Storage Used—The amount of storage used out of the storage you have allocated for the log type.
License Information	• Displays your license expiry date with a countdown from the current date to help you know when it's time to renew. • Shows instance details such as name, tenant ID, and serial number to quickly help Customer Support identify your instance if an issue arises. 
Log Forwarding Status	Provides the status of the different log forwarding profiles that you have configured to stream logs from Strata Logging Service to external sources like syslog servers or SIEMs. A log forwarding profile can have the following states: • Running—The log forwarding profile is ready to forward logs if the destination is reachable and ready to receive logs. • Failed—The log forwarding profile is not sending logs to the destination.

Widget	Description
	• Pending—Strata Logging Service is setting up your log forwarding profile. This is a temporary state when you create or modify a profile. 
Latency	Displays the latency both for ingestion and log forwarding. Ingestion latency is the time between when a log is generated on the firewall or Prisma Access to when it becomes available in Strata Logging Service for querying. Log Forwarding latency is the time between when the log is generated on the firewall or Prisma Access to when it becomes available in Strata Logging Service for log forwarding. The value presented here is the P50, which means that Strata Logging Service will receive 50% of the logs with a lower latency. This widget presents the real-time data for all logs received by Strata Logging Service in the last five minutes. This widget also provides a comparison of the real-time latency with the average of the past 24 hours. 
Service Availability	Provides the availability of the ingestion and log forwarding components within Strata Logging Service. This widget shows real-time availability as well as hourly availability over the last 24 hours. The components can have the following states: • Available: The ingestion or log forwarding components are working perfectly fine. • Impacted: The ingestion or log forwarding components are in a degraded state that is causing a processing delay for ingestion and log forwarding. You will not lose logs, but you might see a delay in log availability for querying and log forwarding. • Unavailable: The ingestion or log forwarding components are down and causing log loss.

Widget	Description
	
Storage	Shows the total storage purchased for your Strata Logging Service tenant and the amount currently used. This data is updated regularly. If you are using Strata Cloud Manager to view or configure storage quota, click **Settings** > **Strata Logging Service** > **Storage Status / Configure Quota**. *Due to the paused purging of data during the migration of Strata Logging Service to the new license tier, you may observe higher storage usage than your current subscription. This is a temporary measure and storage retention will return to normal once the migration is complete at the end of your contract term.* 

View Strata Logging Service Status

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	Strata Logging Service

This view does not apply to:

- *the qualifying users of Strata Logging Service using the new license that comes with one year log retention.*

The Strata Logging Service app in the hub allows you to confirm that your service is provisioned in the region you chose when you activated your auth code, and that the quota matches the storage quantity you purchased. The service status includes details on how you allocated log storage quota, the available storage space, and the number of days the logs are retained based on your incoming log rate.

STEP 1 | **Sign In** to the hub at https://apps.paloaltonetworks.com/.

STEP 2 | Select the Strata Logging Service instance for which you want to view status. If you have multiple Strata Logging Service instances, hover over the Strata Logging Service tile and then select from the list of available instances associated with your account.

To access Strata Logging Service in Strata Cloud Manager, click Strata Cloud Manager app from hub and select **Settings** > **Strata Logging Service**.

STEP 3 | In Strata Logging Service app, click **Storage** > **Status**.

To view Strata Logging Service service status in Strata Cloud Manager, click **Settings** > **Strata Logging Service** > **Storage Status**.

STEP 4 | Confirm the following **Status** details:

- Service status and the amount of storage used as a ratio of total storage you have purchased.
- The geographic region where your logs are stored.
- Verify your configuration on the different log types (sources) from which the Strata Logging Service is receiving logs, and the log storage space allocated for each log subtype.

Strata Logging Service Log Types

In the Strata Logging Service app, you can set how much of your overall log storage you want to allocate to the following log types:

Log Type	Description
config	Configuration logs—entries for changes to the firewall configuration.
system	System logs—entries for each system event on the firewall.
audit	Audit logs—entries for changes made to the service writing the logs.
auth	Authentication logs—information about authentication events that occur when end users try to access network resources for which access is controlled by Authentication Policy rules.
dns_security	**DNS Security Logs**—information from two sources: • DNS Security logs—a partial record of DNS requests that the firewall has deemed malicious based on Anti-Spyware policy rules. • (PAN-OS 10.0 or Later) DNS Security telemetry logs—supplemental information about DNS activity on your network. The DNS Security log data in Strata Logging Service represents only a subset of all DNS requests and responses detected in your network. To view all malicious DNS requests, check `threat` logs. Strata Logging Service does not store `dns_security` logs automatically. To begin storing them, you must set quota for `dns_security` to a value greater than 0. *The Strata Logging Service Estimator does not yet support DNS Security logs, so you must calculate log storage manually. The average size of a DNS Security log is approximately 833 bytes.*
extpcap	**Extended packet capture**—packet captures in a proprietary Palo Alto Networks format. The firewall only collects these if you enable extended capture in Vulnerability Protection or Anti-Spyware profiles.

Log Type	Description
file_data	Data filtering logs—entries for the security rules that help prevent sensitive information such as credit card numbers from leaving the area that the firewall protects.
globalprotect	• GlobalProtect system logs • LSVPN/satellite events • GlobalProtect portal and gateway logs • Clientless VPN logs
hipmatch	HIP Match logs—information about the security status of the end devices accessing your network.
iptag	IP-Tag logs—how and when a source IP address is registered or unregistered on the firewall and what tag the firewall applied to the address.
sctp	Stream Control Transmission Protol logs—events and associations based on logs generated by the firewall while it performs stateful inspection, protocol validation, and filtering of SCTP traffic.
threat	Threat logs—entries generated when traffic matches one of the Security Profiles attached to a security rule on the firewall.
traffic	Traffic logs—entries for the start and end of each session.
tunnel	Tunnel Inspection logs—entries of non-encrypted tunnel sessions.
url	URL Filtering logs—entries for traffic that matches the URL Filtering profile attached to a security policy rule.
userid	User-ID logs—information about IP address-to-username mappings and Authentication Timestamps, such as the sources of the mapping information and the times when users authenticated.
decryption	Decryption logs—information about sessions that match a Decryption policy to help you gain context about that traffic so you can accurately and easily diagnose and resolve decryption issues.
rbi	Remote Browser Isolation logs—display information about Remote Browser Isolation events.

Log Type	Description
gp_troubleshoot	GlobalProtect troubleshooting logs contains information about the GlobalProtect client and its host to help app users resolve issues.
agent	Prisma Access Agent logs contain information to help you troubleshoot any issue related to any activity or action performed by a user on the Prisma Access Agent.
epm	Management logs contain information to audit any activity or action performed by the user or Prisma Access Agent.
events	The event logs contain information that the Prisma Access Browser collects for investigating every activity within your Enterprise Browser deployment.
ai-firewall	The AI Security logs contain information to help you monitor and investigate threats found in your AI network traffic with AI Runtime Security.

Troubleshooting Firewall Connectivity

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

Find out what to do if one of the firewalls in your **Inventory** shows one of these issues:

- License Expired
- Needs Certificate
- Certificate Expired
- Connected but Logging Rate is Zero
- Failed to Fetch FQDN

License Expired

If a firewall is disconnected, check its license status by logging into the firewall CLI and entering the following:

`request license info`

Sample output:

```
Feature: Logging Service
    Description: Device Logging Service
    Expires: April 06, 2038
    Expired?: no
```

If you see `Expired?: yes`, follow the steps below to refresh the license on the firewall or on the Panorama managing the firewall.

Firewall	Panorama
For Panorama-managed firewalls, refresh the license from Panorama. For firewalls not managed by Panorama, manually refresh the license from Device > License in the firewall UI.	If the license on the Panorama managing the firewall is expired, refresh the license on Panorama.

If the above does not resolve the issue, enter the following command in the firewall CLI:

- If **Strata Logging Service Forwarding** is enabled, enter:**`request logging-service-forwarding status`**

- If **Duplicate Logging (Cloud and On-Premise)** is enabled, enter:**debug log-receiver log-forwarding-connections status**

Sample output:

```
Logging Service Licensed: Yes
    Logging Service forwarding enabled: No
    Duplicate logging enabled: No
    Enhanced application logging enabled: No

    Logging Service License Status:
    Status:

    Fetch:

    Install:
    Status: Success
    Msg: Successfully install fetched license
    Last Fetched: 2021/12/22 11:56:34

    Upgrade:



    Logging Service Certificate information:
    Info: Failed
    Status: failure
    Last fetched: Mon Dec 27 15:20:44 2021



    Logging Service Customer file information:
    Info: Failed to validate server certificate for endpoint
 api.paloaltonetworks.com
    Status: failure
    Last Fetched: 2021/12/27 15:24:24
```

If your output contains similar failures, this means that you upgraded a device from PAN-OS 10.0 or earlier to PAN-OS 10.1 or later, or you installed a device certificate on your 10.1 or later device. In that case, you should restart the **management-server** or restart the device. You can use the following CLI command to restart the **management-server**:

debug software restart process management-server

Needs Certificate

If the Certificate Status of a firewall indicates that the firewall Needs Certificate, this means that the firewall must be onboarded to Strata Logging Service.

Certificate Expired

To check the Certificate Status of a firewall, log into the firewall CLI and enter the following:

request logging-service-forwarding status

For Firewall running on 10.1 or earlier, enter:**request logging-service-forwarding certificate info**

For firewall running on 10.1 or later, enter:**show device-certificate infoshow device-certificate status**

If the output states that the certificate has expired, then follow the steps below for manually refreshing the certificate on the firewall.

If the output contains `Info: Error sending CSR signing request to Panorama`, then follow the steps for refreshing the certificate on Panorama.

Firewall	Panorama	Unm
In the firewall CLI, enter **request logging-service-forwarding certificate delete** **request logging-service-forwarding certificate fetch**	In the Panorama CLI, enter **request plugins cloud_services logging-service status** If the output contains `Logging service certificate expired`, then fetch a new certificate using the following command: `request plugins cloud_services panorama-certificate fetch otp <value>` where `value` is the one time password OTP needed to fetch the certificate from the customer support portal(CSP) server. If the command failed, check the plug-in log file with the following command: **less mp-log plugin_cloud_services.log** Otherwise, return to the CLI of the firewall you are troubleshooting and enter **request logging-service-forwarding certificate fetch**	In th **req cer sha** Here cust

After you've completed the above, check the certificate status in your Strata Logging Service **Inventory**.

Connected but Logging Rate is Zero

If the Connection Status of your firewall is Connected but the Ingestion Rate is zero, then verify that your log forwarding profiles are correctly configured.

Failed to Fetch FQDN

The firewall may be unable to connect because it is not successfully retrieving the ingest/query FQDN for Strata Logging Service. To find out if this is the case, log in to the firewall CLI and enter

request logging-service-forwarding status

or

request logging-service-forwarding customerinfo show

Sample output:

```
Logging Service Customer file information:
    Customer ID: xxxxxxx
    EAL Ingest FQDN: xxxxx.fei.lcaas-qa.us.paloaltonetworks.com.
    Ingest FQDN: xxxxxx.in2.lcaas-qa.us.paloaltonetworks.com
    Info: Failed to fetch ingest/query FQDN for customer (curl
 failed)
    Query FQDN: xxxxx.api2.lcaas-qa.us.paloaltonetworks.com:444
    Status: failure
    Last Fetched: 2020/07/22 19:01:06
```

If you see `Info: Failed to fetch ingest/query FQDN for customer (curl failed)` as in the above, then enter **request logging-service-forwarding customerinfo fetch**

to manually refresh the certificate. Then, check the Connection Status in your Strata Logging Service **Inventory** to see if the firewall is now connected.

View Logs in Strata Logging Service

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ❑ Strata Cloud Manager Pro ❑ Strata Logging Service

In most cases, you can view logs stored in Strata Logging Service locally on the product that is sending logs, or in Explore. The Explore app is free with Strata Logging Service, and you should see it as listed on the hub as one of your apps after you've activated Strata Logging Service. Explore provides an aggregated view of logs stored in Strata Logging Service, and you can use Explore to search, filter, and export log data. This app offers you critical visibility into your enterprise's network activities by allowing you to easily examine network log data.

Product or Service Sending Logs to Strata Logging Service	Where to see the logs stored in Strata Logging Service
Palo Alto Networks Firewalls (not managed by Panorama)	• Use the Explore tab to search, filter, and export firewall logs stored in Strata Logging Service.
Panorama-Managed Firewalls	• Use the Explore tab to search, filter, and export firewall logs stored in Strata Logging Service. • Use Panorama to view logs stored in Strata Logging Service. The Panorama ACC and reports give you an aggregated view into your remote network traffic.
Prisma Access	• Use the Explore tab to search, filter, and export firewall logs stored in Strata Logging Service. • Use Panorama to view Prisma Access logs stored in Strata Logging Service. The Panorama ACC and reports give you an aggregated view into your remote network and mobile user traffic.
Cortex XDR	Log in to Cortex XDR to view alerts (they are not visible in Explore).

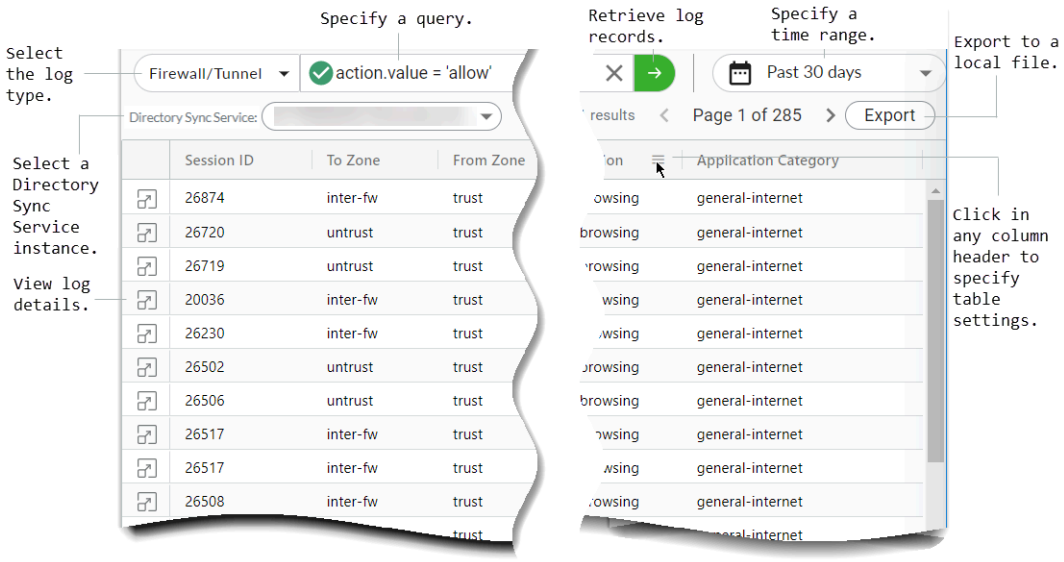
View Strata Logging Service Logs in Explore

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service ☐ A user role that has access to view logs ☐ A Customer Support Portal Account to view logs in **Explore**.

Use the **Explore** tab to view and interact with logs stored in your Strata Logging Service. The query builder along with time range preferences help you narrow down the specific logs that are of interest to you. You can view the log details and also export all log types to a compressed CSV file in GZ format.

You can view logs stored in your Strata Logging Service instance using both Standalone app or in Strata Cloud Manager.

- Log in to hub and launch Strata Logging Service and click **Explore**.
- Launch Strata Cloud Manager and click **Incidents and Alerts > Log Viewer**.



STEP 1 | Select the log type you want to view. For details on the exact log types you can retrieve and a definition of each of their log fields, see the Log Reference guide.

STEP 2 | Select a directory sync service instance for which you want to view logs.

STEP 3 | Define a query string in the query builder to filter the logs you want to view. If you do not provide a query string, the search returns every log record of the type you specify for the selected time range.

STEP 4 | Specify the time range for which you want to query the log records.

STEP 5 | Press enter in the query builder to view the log records and their details in the table. You can organize the columns in the log table based on what is relevant to you.

STEP 6 | (Optional) Save the preferred Explore settings you frequently use in your profile. You can save settings such as time range, log table view, saved queries, and the Directory Sync Service instance.

STEP 7 | (Optional) Export all log types to a compressed CSV file in GZ format. The exported logs will always display UTC, irrespective of the time zone you selected when you exported the logs.

Using Query Builder

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

Strata Logging Service helps you build queries by offering suggestions as to what you can specify next in your query. Queries are Boolean expressions that identify the log records Strata Logging Service will retrieve for the specified log record type. You use them as an addition to the log record type and time range information that you are always required to provide. Use queries to narrow the retrieval set to the exact records you want.

You can select field names, boolean operators, and equality and pattern matching operators as you build your query. You can also use type-down to specify field names and operators. Finally, you can left-click on a table cell to add that column and value, with an equality operator, to the query.

Query Syntax

Specify queries using match statements. These statements can be either an equality or pattern matching expression. You can optionally combine these statements using the Boolean operators: `AND` or `OR`.

```
<match_statement> [<boolean> <match_statement>] ...
```

For example:

```
source_user LIKE 'paloalto%' AND action.value = 'deny'
```

A query can be at most 4096 characters long. The actual field name that you use for your filters are not identical to the names shown in the column header. Also, the data displayed in the log table might not always be the identical value you want to use in your queries. For example, the

BYTES field shows values rounded to the nearest byte or kilobyte. To obtain the exact bytes_total value, use the add-to-search feature provided by the query builder.

The filter evaluates queries according to the standard order of precedence for logical operators. However, you can change the order of operations by grouping terms in parentheses.

It is an error to create a query with identical start and end times.

Expression Type	Definition
Numeric comparison	`<field_name> <equality_operator> <value>` Equality operators are described below.
String comparison	`<field_name> <equality_operator> '<value>'`
Pattern matching	`<field_name> LIKE '<string>%'` Pattern matching is supported only for fields that contain strings or IP addresses. For strings and IP addresses, **%** may be provided as a wild card character at any location in the value. A pattern matching expression that does not provide a wild card returns the identical log lines as an equality comparison.

You must use single quotes with your string values: '<value>'. Double quotes are illegal: "<value>".

Supported Operators

When building a query, you can choose from a set of operators. The following table describes when to use each operator and lists its compatible values.

Operator	When to Use it	Possible Values
=	Find logs that contain an exact value.	• Integer *bytes_total = 270* • String *action.value = 'allow'* • IP addresses Full: *src_ip.value = "192.1.1.10/32"* Subnet Range: *src_ip.value = "192.1.1.10/24"*

Operator	When to Use it	Possible Values
		• Timestamp *time_generated = '2022-03-29 12:57:14'*
!= or <>	Find logs that do not contain anexact value.	• Integer *bytes_total != 270* *bytes_total <> 270* • String *action.value != 'allow'* *action.value <> 'allow'* • IP addresses Full: *src_ip.value != "192.1.1.10/32"* Subnet range: *src_ip.value <> "192.1.1.10/24"* • Timestamp *time_generated != '2022-03-29 12:57:14'* *time_generated <> '2022-03-29 12:57:14'*
<	Find logs with data less than a value.	• Integer *bytes_total < 270* • Timestamp *time_generated < '2022-03-29 12:57:14'*
<=	Find logs with data less than or equal to a value.	• Integer *bytes_total <= 270* • Timestamp *time_generated <= '2022-03-29 12:57:14'*
>	Find logs with data greater than a value.	• Integer *bytes_total < 270* • Timestamp *time_generated > '2022-03-29 12:57:14'*

Operator	When to Use it	Possible Values
>=	Find logs with data greater than or equal to a value.	• Integer *bytes_total <= 270* • Timestamp *time_generated >= '2022-03-29 12:57:14'*
LIKE	Find logs with data that matches a string pattern. ***LIKE** is not supported for fields such as **action**, **tunnel**, or **proto** that have limited possible values.*	• String *source_user_info.name LIKE "usern_me"* *You can use either _ or % as wildcard characters.*
AND	Find logs that satisfy multiple search terms at once.	• Any *bytes_total = 270 AND source_user_info.name LIKE "usern_me" AND src_ip.value != "192.1.1.10/24"*
OR	Find logs that satisfy at least one of multiple search terms.	• Any *bytes_total = 270 OR source_user_info.name LIKE "usern_me" OR src_ip.value != "192.1.1.10/24"*
()	Specify the priority in which search terms are evaluated.	• Any *bytes_total = 270 AND (source_user_info.name LIKE "usern_me" OR src_ip.value != "192.1.1.10/24")*

Supported Characters

These are the characters that you can use when building a query using Query Builder.

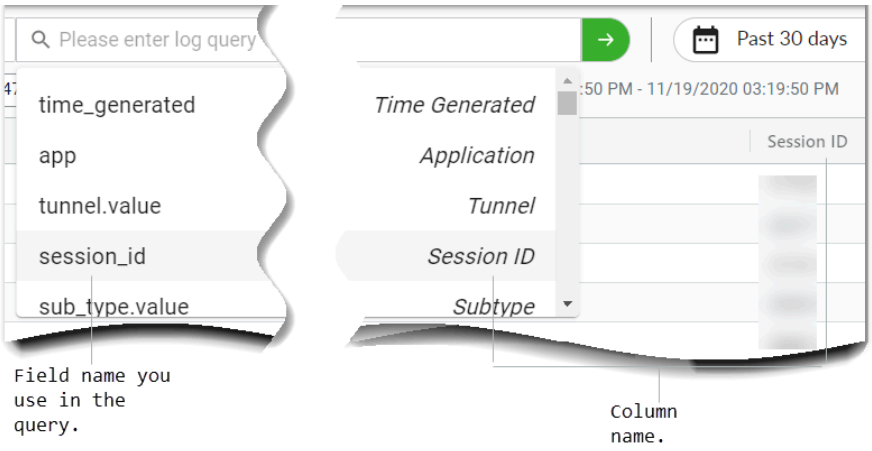
Alphanumeric characters	All letters, both uppercase and lowercase and numbers A-Z, a-z, 0-9
Special characters	underscore (_), black slash (\), forward slash (/) ampersand (&), at symbol (@), percent symbol (%), hash symbol (#), dollar symbol ($), tilde (~), asterisk (*), pipe (|), less than and

	greater than sign (< >), plus sign (+), comma (,), period (.), question mark (?), exclamation mark (!), colon (:), dash, or hyphen (-), equal (=)
White space characters	space

About Field Names

The field names that you use in your queries are sometimes, but not always, identical to the names shown in the log record column headers. The field name that you must use is the log record field name as it is stored in Strata Logging Service. There are two ways to obtain this field name:

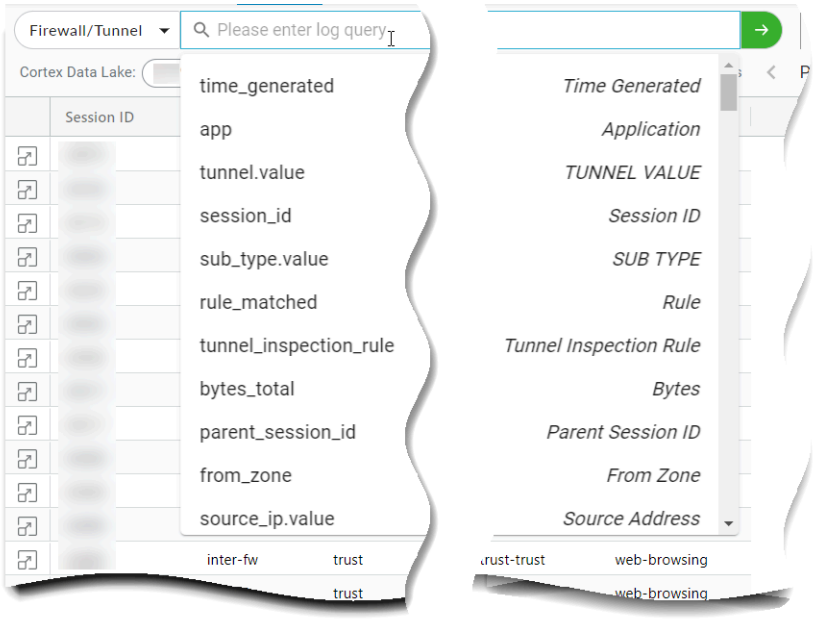
1. Click into the user interface query field to see a drop-down list of available field names for the selected log type. On the right-hand side of this drop-down list is the corresponding column name.



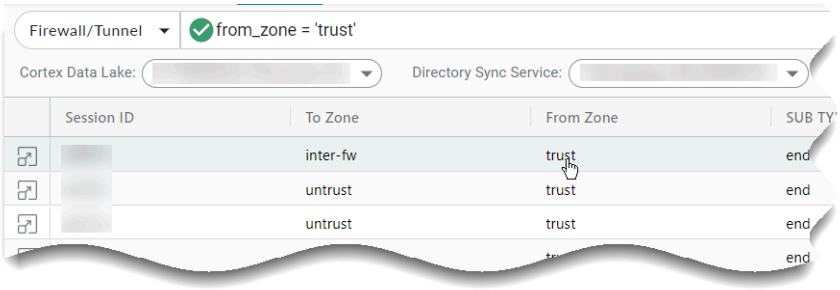
2. The Schema Reference guide provides a mapping of the log column name, as shown in the user interface, to the corresponding log record field name.

Build Queries

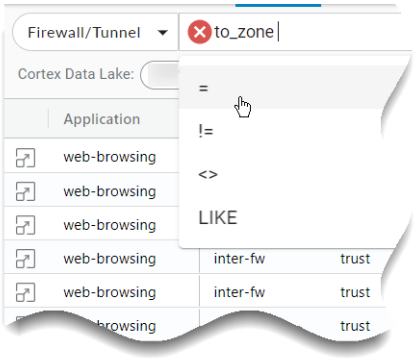
1. Do one of the following to build a query:
   - Click into the query field to see the list of available field names.



   - You can left-click on a table cell to add that column and value, with an equality operator, to the query.



2. Click to select the field that you want, or type down until you find the right field.
3. The user interface immediately displays the operators that are appropriate for the field's data type.



4. Continue this point-click-and-type activity until your query is complete. Click or press Enter to retrieve log records.

   You have the option to cancel a query you no longer want to run with the **Cancel** option

Interact with Query Results

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

After you create the filter to display the set of logs that you're interested in, you can choose to do the following:

- View log details from the log table.
- Configure the log table to show only the required fields.
- Save the filter to use later or to share with other users.
- Save the settings as preferences in profiles.
- Export the log details to a compressed CSV file in GZ format.

Save Filters

After you create the filter to display the set of logs that you're interested in, you can choose to save the filter to use later or to share with other users.

STEP 1 | Select and enter a query in the query field.

STEP 2 | (Optional) Name the filter.

The default name is `New Filter <date time>`.

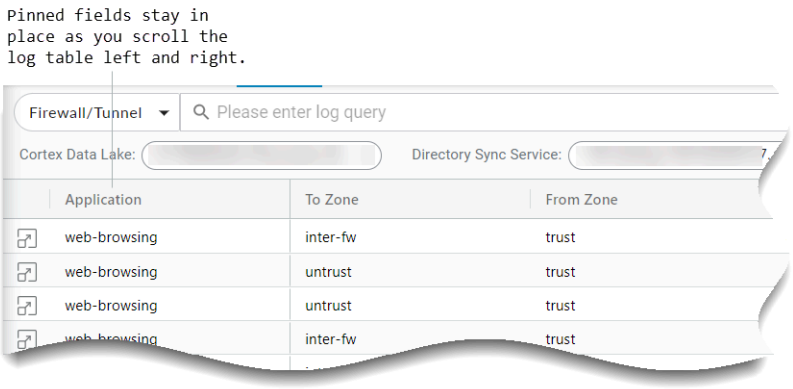
STEP 3 | **Save** the filter.

STEP 4 | After saving the query, click to view, execute, edit, delete, or share it (> **Share** > **Copy Link**) with other users.

The user must have access to the same Strata Logging Service tenant and the necessary permissions to view logs.

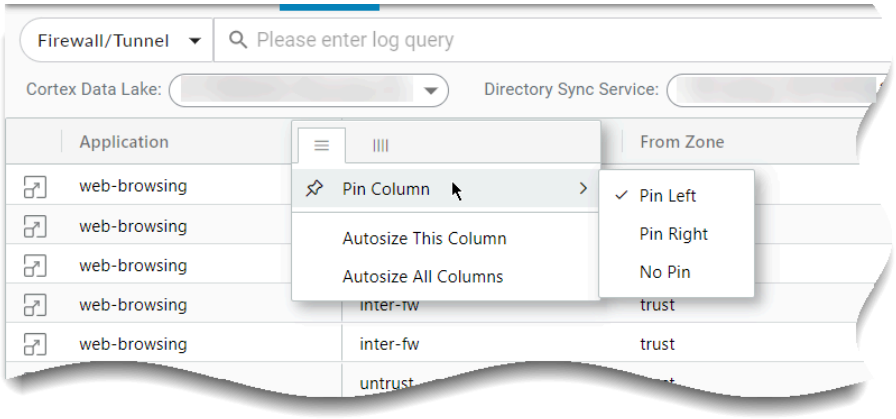
Configure Log Table

By default, the log table shows you a subset of the fields on the log record. These are shown in the order that they appear on the log record. The exception is the pinned field, which is shown as the first column in the table, and is by default the record's **Time Generated** field.

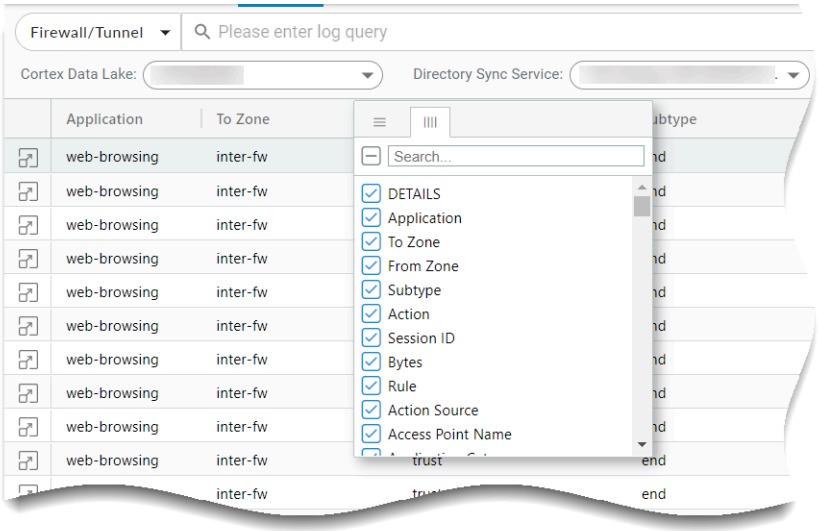


You can change the fields that are displayed in the log table, their order, and which fields are pinned.

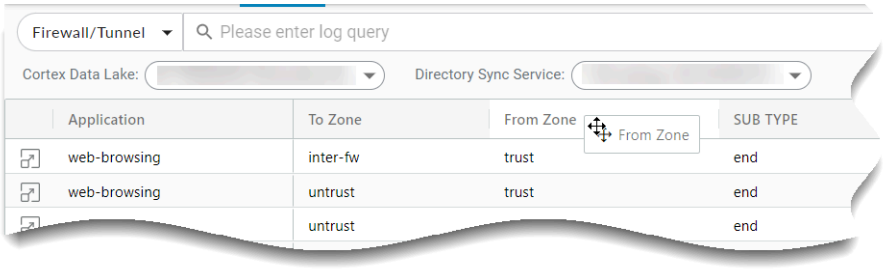
- To pin the column, click on the menu control in any table column header. In the resulting pop-up, you can configure your table settings. Use **Pin Column** to control whether the current column is pinned.



- Identify which fields appear in the log viewer table. Use the Search field to quickly find a specific field. Fields that are checked will appear in the log viewer table.



- Click and drag on any column header to reorder the table columns.



Save Preferences

You can configure preferences, such as time zone and Cloud Identity Engine (CIE) instance, and save these preferences in named profiles. Profiles also save the columns you've chosen to display in the order that you have arranged them, and they retain any queries you've saved.

STEP 1 | Select ⚙ > **+ New Profile**.

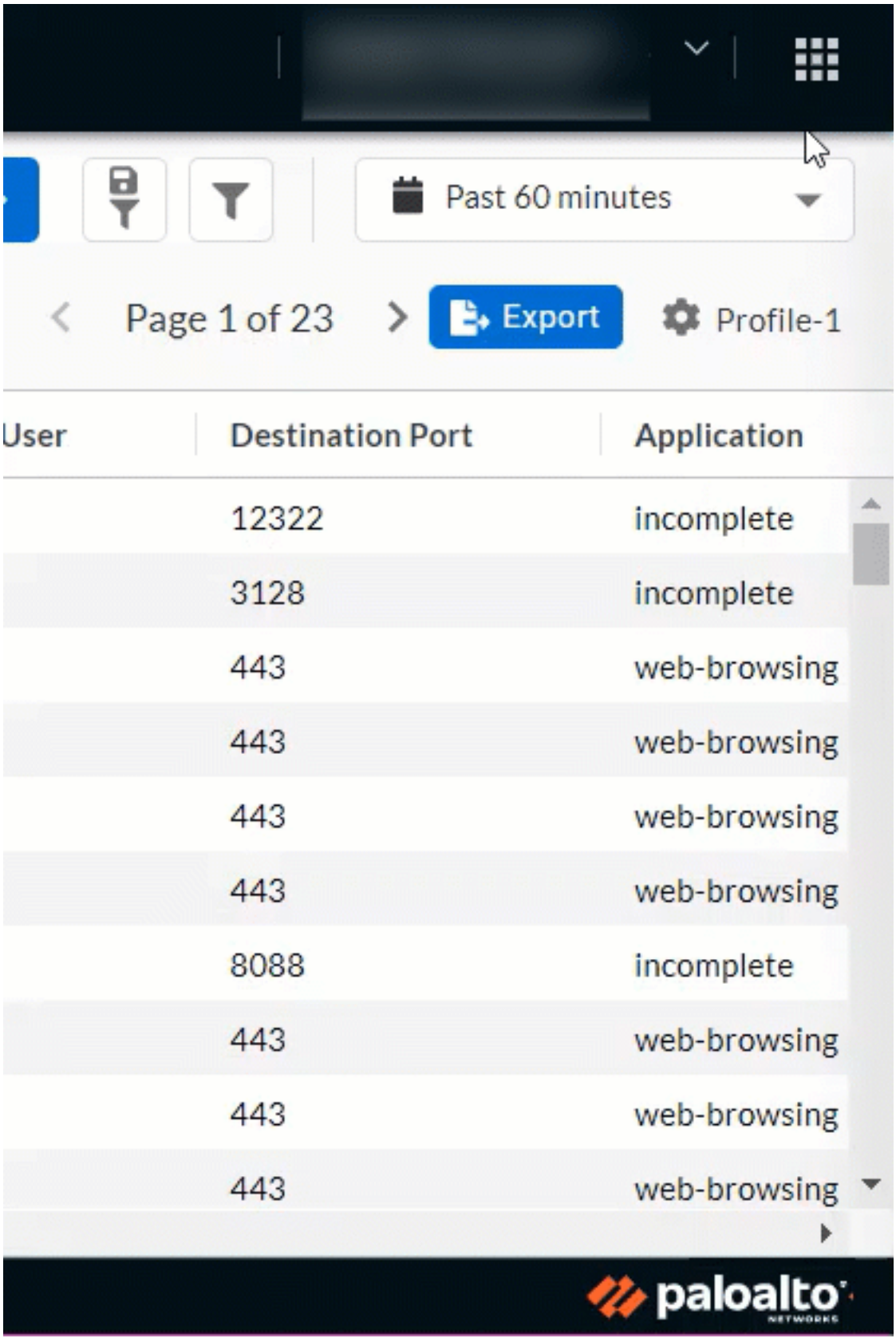
STEP 2 | Enter a profile name.

STEP 3 | Select an existing profile on which to base your new profile.

Selecting **Default** begins your profile with the preferences that were set when you first installed the app.

STEP 4 | **Save** the profile

Any preferences you change will automatically save to the currently selected profile.

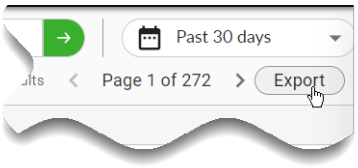


Export Log Records

Once you have retrieved log records, you can export them to a compressed CSV file in GZ format. No matter which time zone you selected, exported logs will always display UTC time.

Exports are limited to a maximum of 1.5 million rows of data as long as it does not exceed 1 GB of total data. If the export exceeds 1 GB, try refining your query to return fewer than 1.5 million rows.

Click **Export** to start exporting the log records. After a short period of time (which depends on how many records you are exporting), **Export** will turn into **Download**.

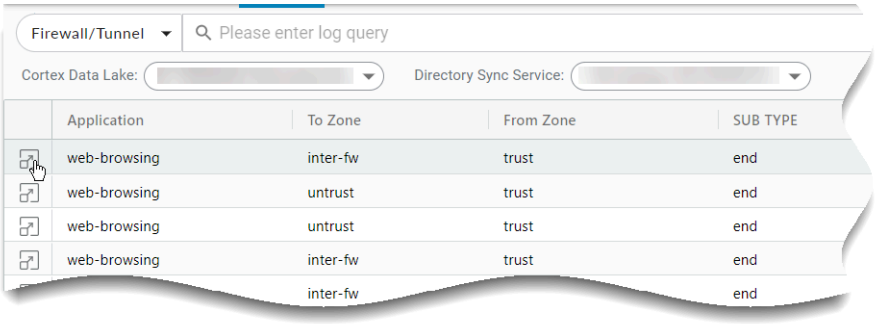


Click **Download** and the GZ file will appear in your downloads folder. Use file decompression software to extract the CSV file(s).

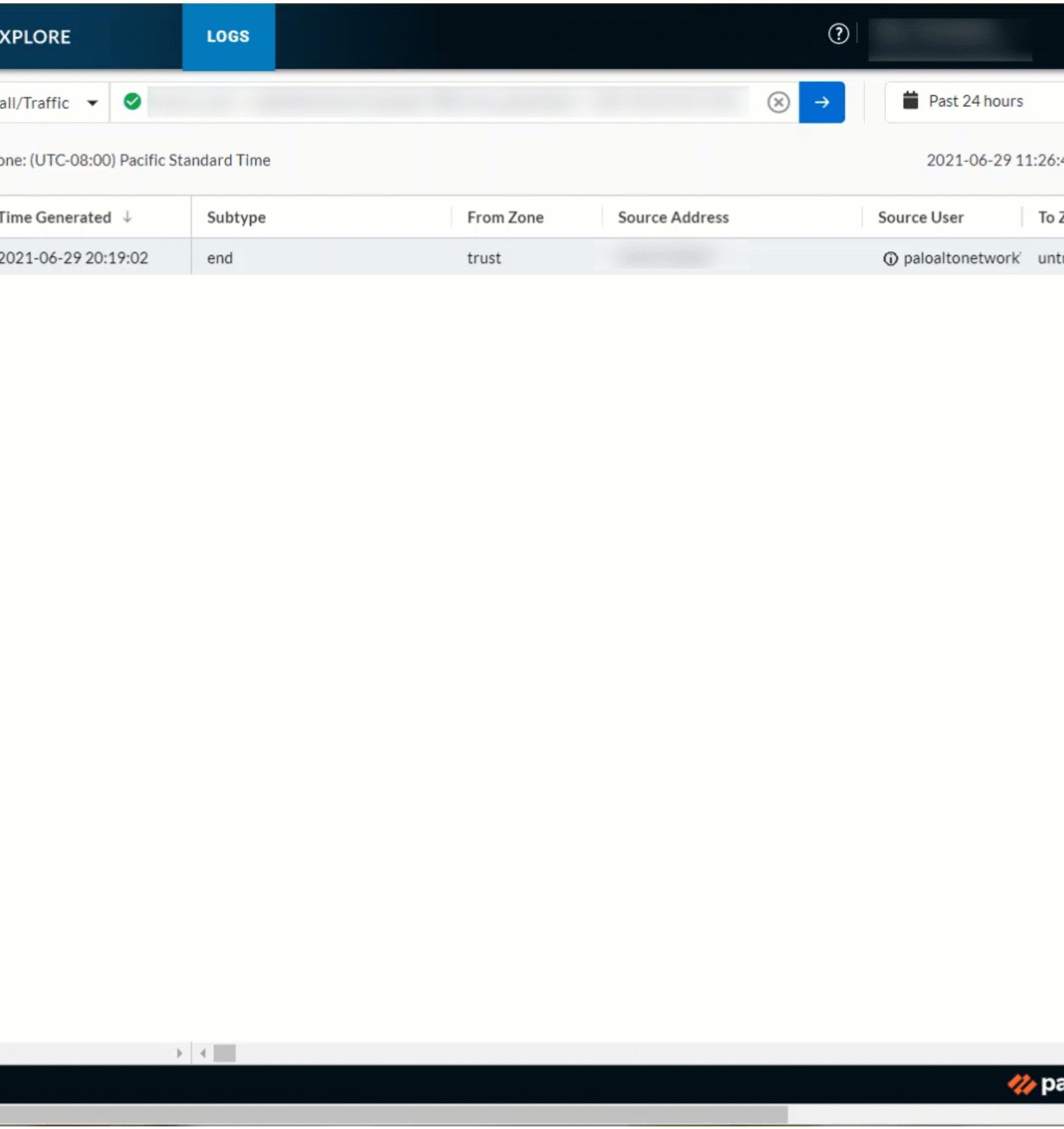
The columns in the CSV file are organized under the field names you use in queries, not the column headers in the Explore UI. For example, the `DESTINATION USER` column in the UI appears as `dest_user` in the CSV file.

View Log Details

It is possible for you to modify the log record summary table so that only some log fields are shown in it. If you want to see a log record in its entirety, click :



The **Log Details** window shows you the entire log record, with individual log fields placed into logical groupings. If the firewall generated other logs for the same session as the one you are viewing, you will see a list of those logs. Select one of the logs to view its details.



Forward Logs from Strata Logging Service

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ❑ Strata Cloud Manager Pro ❑ Strata Logging Service

To meet your organization's legal compliance requirements and operational needs, you can forward firewall logs stored in Strata Logging Service to external destinations. For example, you can forward logs using syslog to a SIEM for long term storage, SOC, or internal audit obligations, and forward email notifications for critical events to an email address. You can forward logs to the following SIEMs:

- Exabeam
- Google Chronicle
- Microsoft Sentinel
- Splunk HTTP Event Collector (HEC)

When forwarding logs, Strata Logging Service ensures accuracy by using unique identifiers and preserving long values, which are important for identifying log records.

If you use a third-party log streaming solution as an intermediary to forward logs from Strata Logging Service, the volume of received logs can vary depending on the log processing mechanism used by the third-party solution, including how the solution handles long identifiers. Strata Logging Service is tested and calibrated against the specific endpoints listed above. Therefore, we can't guarantee support for logs processed through unsupported intermediate streaming solutions. We recommend directly connecting to a supported endpoint or verifying compatibility when using an intermediary aggregator.

Strata Logging Service can forward logs in multiple formats: CSV, LEEF, CEF, JSON, or PARQUET. For each instance of Strata Logging Service, you can forward logs to up to 200 syslog destinations. Use the following table to find more information about supported log formats.

Log Format	Where to find more information about the logs:	IETF Standard	Default Field Delimiter
CSV	Log Forwarding Schema Reference	RFC 5425	,
LEEF	• Log Forwarding Schema Reference • IBM LEEF documentation	RFC 5425	<tab>

Log Format	Where to find more information about the logs:	IETF Standard	Default Field Delimiter
CEF	• Log Forwarding Schema Reference • Microfocus ArcSight documentation	RFC 5425	<space>

The Strata Logging Service ensures secure communication with log receivers through the following mechanisms:

- TLS 1.2 Encryption: All communications are encrypted using TLS 1.2, ensuring data security during transmission.
- Java 8 default cipher suites: The service uses Java 8 default cipher suites, with the exception of GCM ciphers, which are not currently supported.
- Certificate Validation: To establish a secure connection, the Strata Logging Service requires that the log receiver provides a valid certificate.
  - Trusted Certification: The receiver's certificate must be signed by a trusted root CA or a private CA.
  - Chain of Trust: The receiver must present all certificates in the chain of trust to successfully complete the TLS handshake and establish the connection.

Forward Logs to a Syslog Server

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

To meet your long-term storage, reporting and monitoring, or legal and compliance needs, you can configure Strata Logging Service to forward all logs or a subset of logs to a syslog receiver.

Strata Logging Service can forward logs in multiple formats: CSV, LEEF, or CEF. For each instance of Strata Logging Service, you can forward logs to up to 200 syslog destinations.

If you are using the Palo Alto Networks Splunk app, forward logs using HTTPS instead.

STEP 1 | (QRadar only) Add a log source in QRadar by using the TLS Syslog protocol.

For details about how to do this, see the IBM documentation.

STEP 2 | Enable communication between Strata Logging Service and your syslog receiver.

Ensure that your syslog receiver can connect to Strata Logging Service and can present a valid CA certificate to complete the connection request.

- ☐ Allow an inbound TLS feed to your syslog receiver from the IP address range that corresponds to your Strata Logging Service region.
- ☐ Obtain either a certificate from a well-known, public CA or a self-signed certificate and install it on your receiver. Please make sure that if you are using a certificate signed by a private CA, it contains CRL or OCSP information needed for certificate revocation checks.

  Because Strata Logging Service validates the server certificate to establish a connection, you must verify that the receiver is configured to properly send the TLS certificate chain to Strata Logging Service. If the app cannot verify that the certificate of the receiver and all CAs in the chain are trustworthy, the connection cannot be established. See the list of trusted certificates.

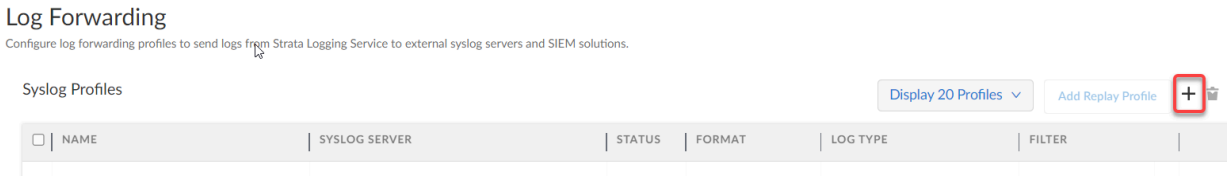
STEP 3 | **Sign In** to the hub.

STEP 4 | Select the Strata Logging Service instance that you want to configure for syslog forwarding.

If you have multiple Strata Logging Service instances, click the Strata Logging Service tile and select an instance from the list of those available.

*If you are using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Log Forwarding** to manage log forwarding from Strata Logging Service instance to an external server.*

STEP 5 | Select **Log Forwarding** > **Add** to add a new Syslog forwarding profile.



STEP 6 | Enter a descriptive `Name` for the profile.

STEP 7 | Enter the `Syslog Server` IPv4 address or FQDN.

Ensure that the value entered here matches the Subject Alternative Name (SAN) of the certificate installed on your syslog server.

STEP 8 | Enter the `Port` on which the syslog server is listening.

The default port for syslog messages over TLS is 6514.

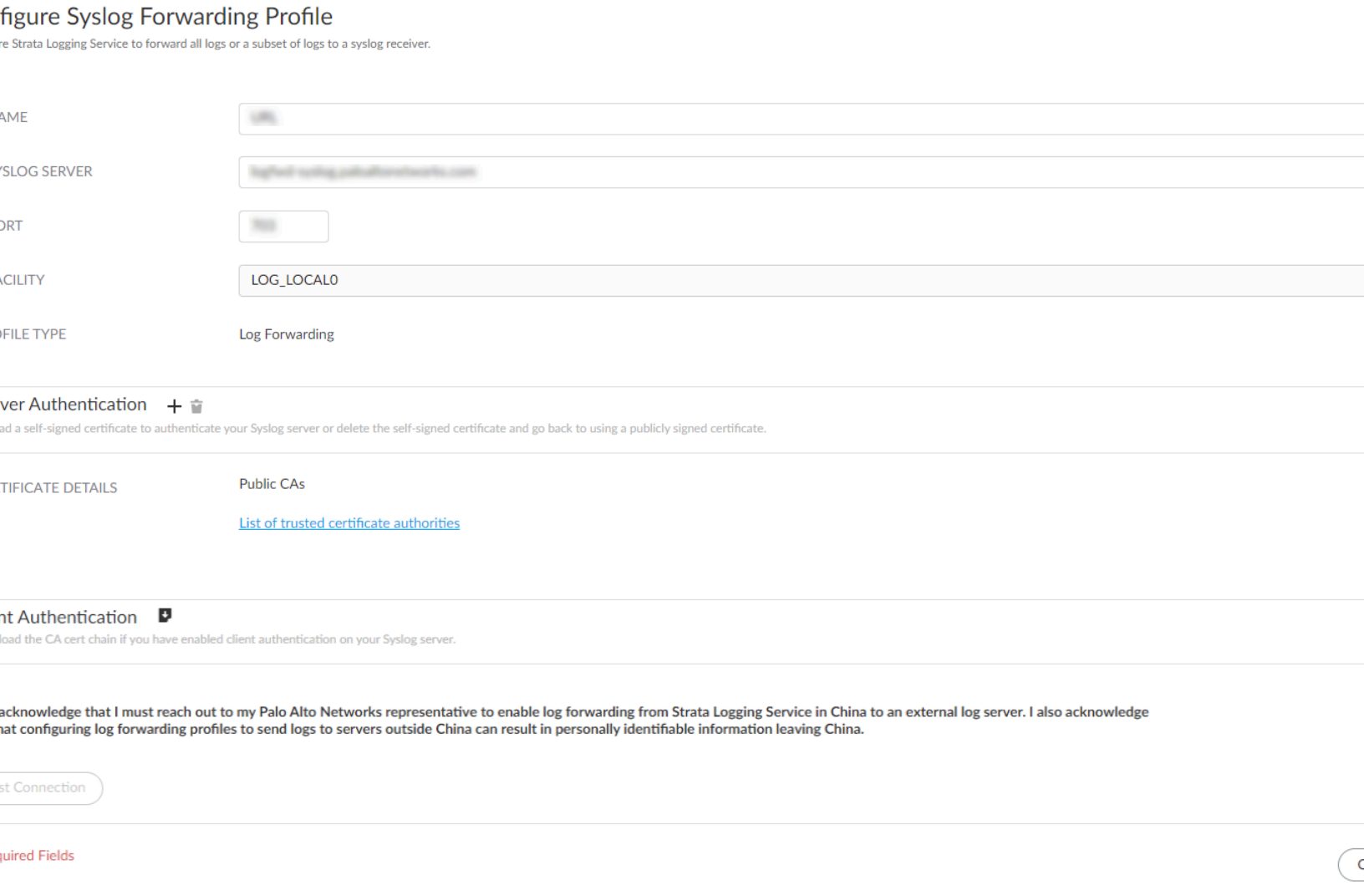
STEP 9 | Select the `Facility`.

Choose one of the syslog standard values. The value maps to how your syslog server uses the facility field to manage messages. For details on the facility field, see the IETF standard for the log format (CSV, LEEF, or CEF) that you will choose in the next step.

STEP 10 | (Optional) Authenticate your syslog server. Click **+** to upload certificate. You can upload:

- a self-signed certificate if you do not want to use a publicly signed certificate.
- the private Root CA and intermediate CAs (If an intermediate CA exists). Do not upload the certificate issued for the syslog server—only CA certificates are needed to verify the chain from the syslog server.

Only do this if you installed a private CA-signed, self-signed certificate on your receiver, or the public CA is not in the list of trusted CAs. The file containing the certificates must be in PEM format.



STEP 11 | (Optional) Enable client authentication.

Do this if company or regulatory policy requires client authentication when forwarding logs to your server.

1. **Download** the certificate chain.
2. Upload the certificate chain to your server.

   Refer to the documentation for your server management software to find out how to do this.

STEP 12 | **Acknowledge** to reach out to your Palo Alto Networks team to enable log forwarding from Strata Logging Service in China to an external log server. Be aware that configuring log forwarding profiles to send logs to servers outside China can result in personally identifiable information leaving China.

STEP 13 | **Test Connection** to ensure that Strata Logging Service can communicate with the receiver.

This checks TLS connectivity to verify that transmission is possible.

If the test fails, you can not proceed.

STEP 14 | Click **Next**.

STEP 15 | Specify the `Format` in which you would like to forward your logs.

The log format (CSV, LEEF, CEF, or JSON) that you should select depends on the destination of your log data.

STEP 16 | Specify the `Delimiter` that you would like to separate the fields in your log messages. This option is disabled if you select JSON log format.

STEP 17 | (Optional) To receive a `STATUS NOTIFICATION` when Strata Logging Service is unable to connect to the syslog server, enter the email address at which you'd like to receive the notification.

You will continue to receive these notifications at least once every 60 minutes until connectivity is restored. If the connectivity issue is addressed within 72 hours, no logs will be lost. However, any log older than 72 hours following the service disconnection could be lost.

STEP 18 | (Optional) Enter a `PROFILE TOKEN` to send logs to a cloud syslog receiver.

If you use a third-party cloud-based syslog service, you can enter a token that Strata Logging Service inserts into each syslog message so that the cloud syslog provider can identify the source of the logs.

1. Follow your cloud syslog provider's instructions for generating an identifying token.
2. Enter the `Profile Token`.

Tokens have a maximum length of 128 characters.

STEP 19 | (Optional) Create a log filter to forward only the logs that are most critical to you.

1. You can either write your own queries from scratch or use the query builder. You can also select the query field to choose from among a set of common predefined queries.

   Log filters function like queries in Explore, with the following differences:

   - No double quotes (“”).
   - No subnet masks. To return IP addresses with subnets, use the LIKE operator. Example: src_ip.value LIKE “192.1.1.%”.

   If you want to forward all logs of the type you selected, do not enter a query. Instead, proceed to the next step.
2. **Save** your changes.

STEP 20 | **Save** your changes.

STEP 21 | Verify that the `Status` of your Syslog forwarding profile is `Running` ( ).

STEP 22 | Verify that you can view logs on the syslog receiver.

For details about the log format, refer to the Syslog field descriptions (Select the PAN-OS Administrator’s Guide for your firewall version).

STEP 23 | (Optional) You can use the running Syslog forwarding profile to forward past logs spanning up to 3 days.

When configuring event source mapping in your SIEM, be aware that the hostname value can change in the hostname field of the syslog message sent from Strata Logging Service.

For example,

```
Oct  8 15:26:51 stream-logfwd20-602226222-10061338-i2hh-
harness-r9kt logforwarder LEEF:2.0|Palo Alto Networks|Next
 Generation
```

might change to

```
Oct  8 15:26:51 stream-logfwd20-602226222-10061338-i2hh-
harness-a7b1 logforwarder LEEF:2.0|Palo Alto Networks|Next
 Generation
```

A change to your log forwarding configuration or a new feature/fix could change the hostname value and break event source mapping if you are using an exact match on the hostname.

If hostname exact matching is required by the SIEM, consider using a middle syslog host to rewrite the log forward to a static hostname so that changes to hostname values don't affect log source mappings.

Forward Logs to an HTTPS Server

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

To meet your long-term storage, reporting and monitoring, or legal and compliance needs, you can configure Strata Logging Service to forward logs to an HTTPS server or to the following SIEMs:

- Exabeam
- Google Chronicle
- Microsoft Sentinel
- Splunk HTTP Event Collector (HEC)

For successful log transmission, ensure that your HTTPS receiver:

- Accepts and parses the correct log format. The format in which Strata Logging Service forwards logs depends on the HTTPS receiver:

Google Chronicle

(JSON Array)

```
{
  "customer_id": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "log_type": "ARCSIGHT_CEF",
  "entries": [
    {
      "log_text": "CEF:0|palo alto networks|LF|2.0|DN
S|realtime_dns_query|3|ProfileToken=hello-cef dtz=UTC
 deviceExternalID=xxxxx rt=Jun 09 2022 18:08:31 start
Time=Dec 09 1654  PanOSRecordType=null PanOSCloudDNSC
lientIP= PanOSDNSResolverIP=9.9.9.9 PanOSThreatID=109
010001 PanOSDNSCategory=phishing cat=Phishing:blockch
ain.ppckite.com src= cs4= act= cs5= duser= Destinatio
nDNSDomain="
    },
    {
      "log_text": "CEF:0|palo alto networks|LF|2.0|DN
S|realtime_dns_query|3|ProfileToken=hello-cef dtz=UTC
 deviceExternalID=xxxxx rt=Jun 09 2022 18:08:31 start
Time=Dec 09 1654  PanOSRecordType=null PanOSCloudDNSC
lientIP= PanOSDNSResolverIP=9.9.9.9 PanOSThreatID=109
010001 PanOSDNSCategory=phishing cat=Phishing:blockch
ain.ppckite.com src= cs4= act= cs5= duser= Destinatio
nDNSDomain="
    },
    {
      "log_text": "CEF:0|palo alto networks|LF|2.0|DN
S|realtime_dns_query|3|ProfileToken=hello-cef dtz=UTC
```



```
 deviceExternalID=xxxxx rt=Jun 09 2022 18:08:31 start
Time=Dec 09 1654  PanOSRecordType=null PanOSCloudDNSC
lientIP= PanOSDNSResolverIP=9.9.9.9 PanOSThreatID=109
010001 PanOSDNSCategory=phishing cat=Phishing:blockch
ain.ppckite.com src= cs4= act= cs5= duser= Destinatio
nDNSDomain="
    }
  ]
}
```

Microsoft Sentinel

(JSON Array)

```
[
  {
    "time": 1437522387,
    "host": "stream-logfwd20",
    "source": "Palo Alto Networks FLS LF",
    "event": {
      "message": "Something happened",
      "severity": "INFO"
    }
  },
  {
    "time": 1437522387,
    "host": "stream-logfwd20",
    "source": "testapp",
    "event": {
      "message": "Something happened",
      "severity": "INFO"
    }
  }
]
```

Splunk HEC

(Stacked JSON)

```
{
  "time": 1437522387,
  "host": "stream-logfwd20",
  "source": "Palo Alto Networks FLS LF",
  "event": {
    "LogType": "THREAT",
    "Severity": "Critical",
    ...
  }
}
{
  "time": 1437522387,
  "host": "stream-logfwd20",
  "source": "Palo Alto Networks FLS LF",
  "event": {
    "LogType": "THREAT",
    "Severity": "Info",
    ...
  }
}
```

Exabeam
(JSON Array)
	{
	"DestinationDeviceCategory": "N-Phone",
	"DestinationDeviceOSFamily": "H1511",
	"DestinationDeviceOSVersion": "Android v7",
	"SourceDeviceOS": null,
	"NATDestination": "xxx.xx.x.xxx",
	"ApplicationSubcategory": "database",
	"VendorName": "Palo Alto Networks",
	"Protocol": "tcp",
	"IsServertoClient": false,
	"PacketID": 0,
	"NSSAINetworkSliceType": "fc",
	"DirectionOfAttack": "client to server",
	"EndpointSerialNumber": "SG0000001",
	"ApplicationTechnology": "network-protocol",
	"VendorSeverity": "Critical",
	"SubType": "data",
	"DeviceSN": "xxxxxxxxxx",
	"ConfigVersion": "10.2",
	"IsMptcpOn": false,
	"SourceDeviceModel": "Nexus",
	"InboundInterface": "ethernet1/1",
	"LogExported": false,
	"ParentSessionID": 0,
	"CloudHostname": "PA-VM-E2E-PCL-TEST",
	"SourcePort": 25195,
	"CaptivePortal": false,
	"LogSource": "firewall",
	"LogType": "THREAT",
	"InboundInterfaceDetailsType": "ethernet",
	"Severity": "Critical",
	"TimeReceived": "2023-07-22T08:49:30.000000Z",
	"SourceUserDomain": "paloaltonetwork",
	"IsDuplicateLog": false,
	}

For more information about HTTPS log format, see the Log Forwarding Schema Reference.

- Accepts and decompresses GZIP HTTPS payloads. Strata Logging Service compresses the JSON data using GZIP when forwarding through HTTPS.
- (For Microsoft Sentinel Only) - Microsoft Sentinel does not accept GZIP, so you must deploy a web app to decompress the data.
- Accepts a batch size of 500 logs, or 2.25 MB (500 logs x 4500 B = 2.25 MB). This does not apply to Google Chronicle, which accepts only 1 MB of data at a time, or a batch size of 250 logs. For each instance of Strata Logging Service, you can forward logs to up to 200 destinations.

- Can connect to Strata Logging Service -
  - Allow an inbound TLS feed to your HTTPS receiver from the IP address range for your Strata Logging Service region.
  - Obtain a certificate from a well-known, public CA.

    Because Strata Logging Service validates the server certificate to establish a connection, you must verify that you have configured the receiver to properly send the TLS certificate chain to Strata Logging Service. If the app can't verify that the certificate of the receiver and all CAs in the chain are trustworthy, it can't establish a connection. See the list of trusted certificates.

  If the connection with the HTTPS server fails, Strata Logging Service will wait 60 seconds and retry. If the connection times out, Strata Logging Service waits 20 seconds and drops the connection with the server before establishing a new one.

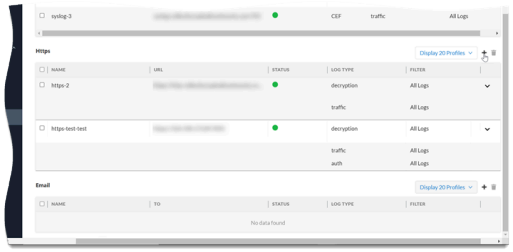
STEP 1 | **Sign In** to the hub.

STEP 2 | Select the Strata Logging Service instance that you want to configure for HTTPS forwarding.

If you have multiple Strata Logging Service instances, click the Strata Logging Service tile and select an instance from the list of those available.

*If you are using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Log Forwarding** to manage devices onboarded to your Strata Logging Service instance.*

STEP 3 | Select **Log Forwarding** > **Add** to add a new HTTPS forwarding profile.



STEP 4 | Enter a descriptive `Name` for the profile.

STEP 5 | Enter the URL that you copied in step 13 for the HTTPS receiver.

The URL entered must begin with **`https`**. At the end of the top-level domain, you can specify a port number. The default port is 443.

For Splunk HEC, ensure that the URL ends with **`/event`**.

If you're forwarding logs to Google Chronicle, you must enter the URL that corresponds to your Strata Logging Service region:

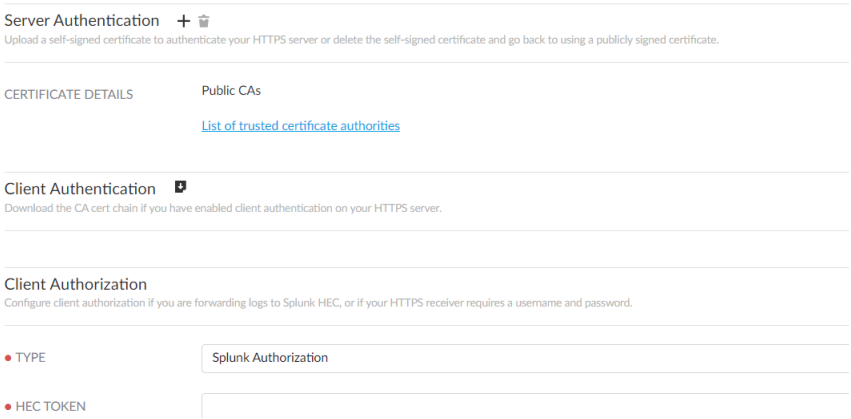
US	https://malachiteingestion-pa.googleapis.com/v2/unstructuredlogentries:batchCreate

EU	https://europe-malachiteingestion-pa.googleapis.com/v2/unstructuredlogentries:batchCreate
Asia	https://asia-southeast1-malachiteingestion-pa.googleapis.com/v2/unstructuredlogentries:batchCreate

STEP 6 | (Optional) Authenticate your https server. Click **+** to upload a certificate. You can upload:

- a self-signed certificate if you do not want to use a publicly signed certificate.
- the private Root CA and intermediate CAs (If an intermediate CA exists). Do not upload the certificate issued for the syslog server—only CA certificates are needed to verify the chain from the syslog server.

Only do this if you installed a private CA-signed, self-signed certificate on your receiver, or the public CA is not in the list of trusted CAs. The file containing the certificates must be in PEM format.



STEP 7 | (Optional) Enable client authentication.

Do this if company or regulatory policy requires client authentication when forwarding logs to your server.

1. **Download** the certificate chain.
2. Upload the certificate chain to your server.

   Refer to the documentation for your server management software to find out how to do this.

STEP 8 | Configure Client Authorization.

Do this if you're forwarding logs to a cloud HTTPS receiver, or if your HTTPS server requires a username and password.

1. Select the **Type** of client authorization and enter the necessary credentials.

HTTPS Receiver	Type	Credentials
Splunk HEC	**Splunk Authorization**	HEC Token
HTTPS Server (Password-protected)	**Basic Authorization**	• **Username** • **Password**
Exabeam	**Exabeam Authorization**	• Access Token
Microsoft Sentinel	**Sentinel Authorization**	• **Workspace ID** • **Primary Key** Find your workspace ID and key
Google Chronicle	**Chronicle Authorization**	• Customer ID • Service Account *This should be a properly formatted JSON document. If you don't know your Service Account credentials, contact Google Chronicle support.*
HTTPS Server	None	None

STEP 9 | **Acknowledge** to reach out to your Palo Alto Networks team to enable log forwarding from Strata Logging Service in China to an external log server. Be aware that configuring log forwarding profiles to send logs to servers outside China can result in personally identifiable information leaving China.

STEP 10 | **Test Connection** to ensure that Strata Logging Service can communicate with the receiver.

This sends an empty log to the configured destination to verify that transmission is possible.

If the test fails, you won't be able to proceed.

STEP 11 | Click **Next**.

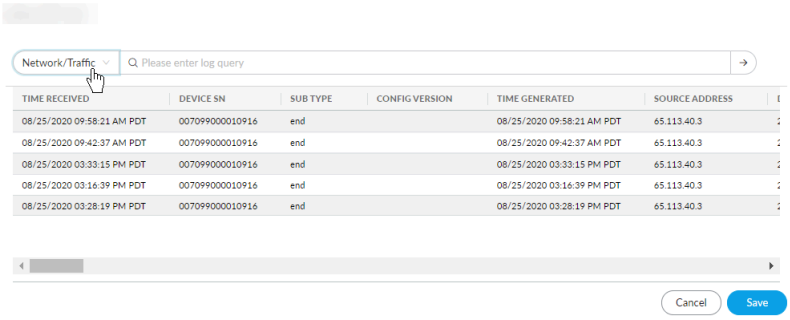
STEP 12 | (Optional) To receive a `STATUS NOTIFICATION` when Strata Logging Service is unable to connect to the HTTPS receiver, enter the email address at which you'd like to receive the notification.

You will continue to receive these notifications at least once every 60 minutes until the service restores connectivity. If the connectivity issue resolves within 72 hours, the service won't lose logs. However, the service could lose any log older than 72 hours following the service disconnection.

STEP 13 | Enter a unique PROFILE TOKEN if your receiver needs to distinguish logs coming from different tenants.

STEP 14 | Select the logs you want to forward.

1. **Add** a new log filter.
2. Select the log type.



The Threat log type does not include URL logs or Data logs. If you wish to forward these log types, you must add them individually.

3. (Optional) Create a log filter to forward only the logs that are most critical to you.

   You can either write your own queries from scratch or use the query builder. You can also select the query field to choose from among a set of common predefined queries.

   - No double quotes ("").
   - No subnet masks. To return IP addresses with subnets, use the `LIKE` operator. Example: src_ip.value LIKE "192.1.1.%".

   If you want to forward all logs of the type you selected, don't enter a query. Instead, proceed to the next step.
4. **Save** your changes.

STEP 15 | **Save** your changes.

STEP 16 | Verify that the `Status` of your HTTPS forwarding profile is `Running` ( ).

Immediately after creating or editing your profile, the `Status` might be `Provisioning` for up to 10 minutes.

STEP 17 | Verify that you can view logs on the HTTPS receiver.

> *For Splunk Common Information Model (CIM) fields and Enterprise Security, follow the guide at https://splunk.paloaltonetworks.com to install the Palo Alto Networks Splunk add-on and create a Splunk HEC input.*

STEP 18 | (Optional) You can use the running HTTPS forwarding profile to forward past logs spanning up to 3 days.

Create and Deploy a Agent Web Application

Microsoft Sentinel does not accept GZIP to compress the data when forwarding through HTTPS receiver. To enable this, you must deploy a web application.

STEP 1 | Log in to your Microsoft Azure account, and create a log analytics workspace in your Sentinel.

STEP 2 | Install Visual Studio Code version 1.64.1 or a later version.

STEP 3 | Install the Azure Tools and Azure App Service extensions in Visual Studio Code.

STEP 4 | Obtain the agent web application's code from GitHub - git clone https://github.com/PaloAltoNetworks/cdl-decompress-proxy-sentinel-ingest.git

> *This is a sample application code and is not maintained by Palo Alto Networks. Don't use the code as-is but we recommend you to develop your own agent or customize this base version to align with your specific needs and requirements.*

> *Download and extract the ZIP folder if you did not install Git. https://github.com/PaloAltoNetworks/cdl-decompress-proxy-sentinel-ingest/archive/refs/heads/master.zip*

STEP 5 | Open the **cdl-decompress-proxy-sentinel-ingest** folder in Visual Studio Code.

STEP 6 | Sign in to Azure and click **Resources** > **your subscription** > **App Services**.

STEP 7 | Right click and select **Create New Web App**. Select the advanced option if you want to make use of previously created Azure resources.

STEP 8 | Enter a name, choose the **Python 3.9** runtime stack, and select an appropriate pricing tier.

STEP 9 | Right click the new agent web app and select **Deploy to Web App**.

STEP 10 | Connect the web app to the Log Analytics workspace - In Azure, navigate to the desired Log Analytics workspace, and select **Agents management** > **Linux servers**. Copy the Workspace ID and Primary Key values. These details are used while adding a new setting in your agent web application.

STEP 11 | (Optional) In Azure, navigate to agent web app and select **Settings** > **Identity** > **System assigned**, change **Status** to **On**.

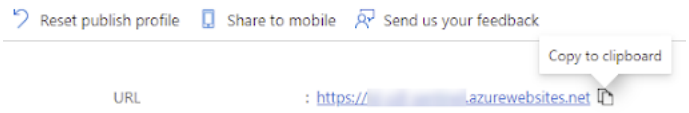
STEP 12 | (Optional) Access or create an Azure Key Vault to store the workspace ID and primary key values as secrets in the key vault. If you don't have an Azure key vault, you can add the values as settings directly in the agent web app.

- To create or import a key vault:
  1. Click **Settings > Secrets > and click Generate or Import**.
  2. Enter the name for the secret where you will store the Workspace ID value you collected earlier, enter the value, and click Create.
  3. Copy the secret URI you just created. For example, `https://<key vault name>.vault.azure.net/secrets/<secret name>`
  4. Click **Settings > Access policies** and click **Add Access Policy**.
  5. Select **Get** from the **Secret permissions** drop-down.
  6. Click **None selected**, select your agent web application and click **Add**.
  7. Save the access policy.
- Add Value in agent web application:
  1. In Visual Studio, open the agent web application, right-click **Application Settings** and select **Add New Settings**.
  2. Enter WORKSPACE_ID and press enter.

     If you have stored the values as secrets in a Key Vault, enter the Secret URI, that represents the Workspace ID you collected earlier, in this format - `@Microsoft.KeyVault(SecretUri=https://<key vault name>.vault.azure.net/secrets/<secret name>)`

     If you did not store the value as a secret in a Key Vault, enter in the WORKSPACE_ID value you copied down earlier ((step 10) while connecting to Log Analytics workspace).
  3. Follow the same process to add another new setting named SHARED_KEY with the Primary Key value collected earlier, or enter the SecretURI if you have this value stored in a Key Vault.
  4. Right click the web app and select **Restart**.

STEP 13 | In Azure, copy the URL from your web app (App Services). This URL is used in the URL field while adding a HTTPS forwarding profile.



Forward Logs to an Email Server

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

To get email notifications whenever critical issues occur on your network, you can configure Strata Logging Service to send notifications to an email destination. Strata Logging Service uses the Palo Alto Networks SMTP server to forward log information in an email format, and all emails are sent from noreply@cs.paloaltonetworks.com. The communication between Strata Logging Service and the email destination uses SMTP over TLS, and SMTP server certificate is signed by a trusted root CA.

STEP 1 | **Sign In** to the hub.

STEP 2 | Select the Strata Logging Service instance that you want to configure for email forwarding.

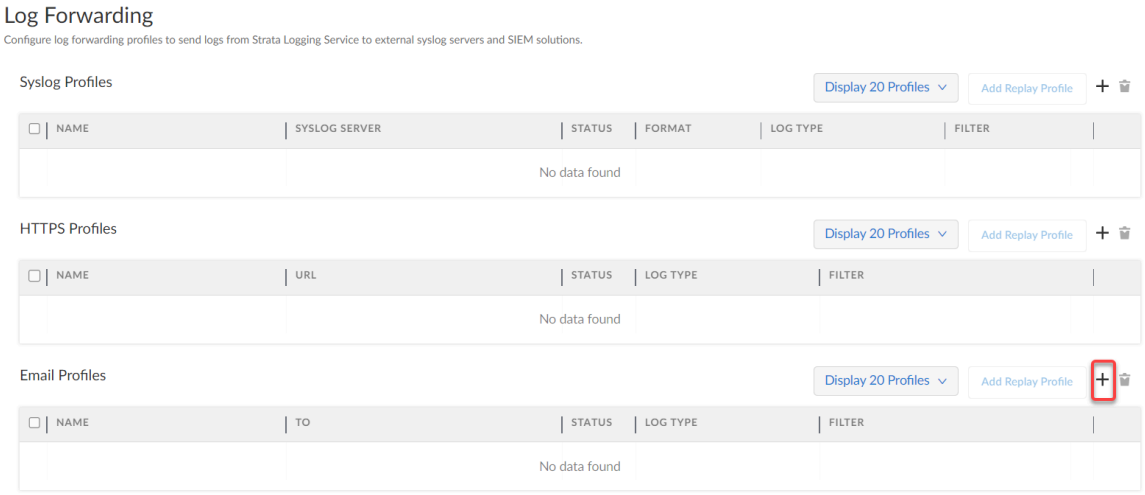
If you have multiple Strata Logging Service instances, hover over the Strata Logging Service tile and then select an instance from the list of available instances.

*If you are using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Log Forwarding** to manage log forwarding from Strata Logging Service instance to an external server.*

STEP 3 | Configure email forwarding.

You cannot add your SMTP server to Strata Logging Service currently.

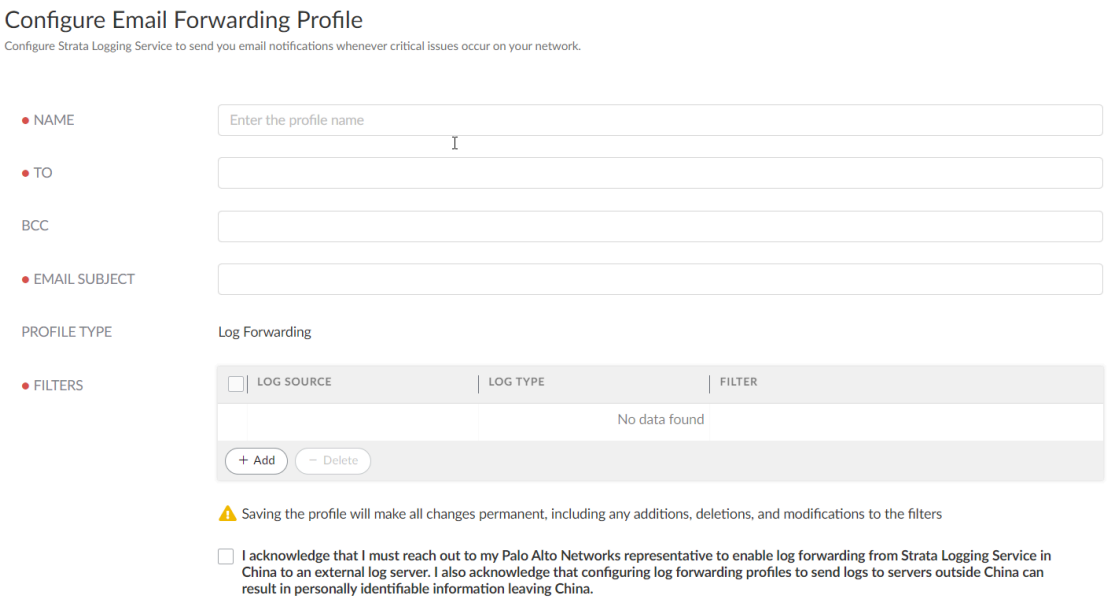
1. Select **Log Forwarding** > **Add** to add a new email forwarding profile.



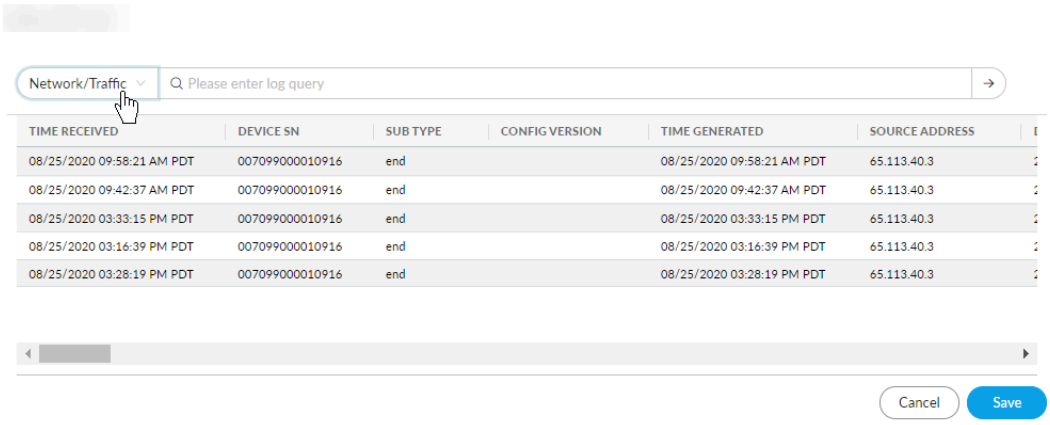
2. Enter a descriptive **Name** for the profile.
3. Enter the email address of the administrator **To** whom you want to send email.

   You can enter up to ten additional email addresses, separated by commas, to add as **BCC**.
4. Enter the **Email Subject** to clearly identify the purpose of the notification.
5. Select the logs you want to forward.

1. **Add** a new log filter.



2. Select the **Log Type**.



3. (Optional) Create a log filter to forward only the logs that are most critical to you.

   You can either write your own queries from scratch or use the query builder. You can also select the query field to choose from among a set of common predefined queries.

   - No double quotes (“”).
   - No subnet masks. To return IP addresses with subnets, use the `LIKE` operator. Example: src_ip.value LIKE “192.1.1.%”.

   If you want to forward all logs of the type you selected, do not enter a query. Instead, proceed to the next step.
4. **Save** your changes.
5. Add other log types for which you’d like to receive email notifications.

6. **Save** your changes.

Email forwarding is rate limited to allow 10 emails per second.

STEP 4 | **Acknowledge** to reach out to your Palo Alto Networks team to enable log forwarding from Strata Logging Service in China to an external log server. Be aware that configuring log forwarding profiles to send logs to servers outside China can result in personally identifiable information leaving China.

STEP 5 | Verify that the `Status` of your email forwarding profile is `Running` ( ).

STEP 6 | (Optional) You can use the running Email forwarding profile to forward past logs spanning up to 3 days.

Forward Logs to Amazon Security Lake

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

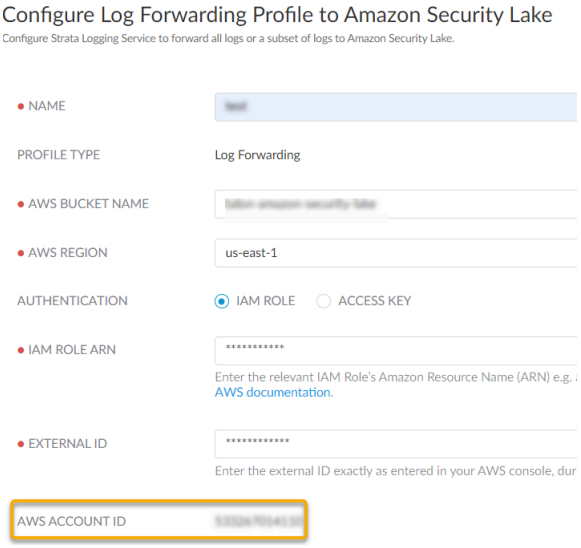
You can integrate the Strata Logging Service with Amazon Security Lake to enable forwarding of browser events and logs. These logs provide visibility into the website access activities, along with their browser-based data handling activities. To enable log forwarding from Strata Logging Service to Amazon Security Lake, create a log forwarding profile in Strata Logging Service and set filters to forward all or a subset of event logs to Amazon Security Lake. The events data sent by the Strata Logging Service is converted to the OCSF schema, and is saved in Parquet format in Amazon Security Lake.

You can forward only event endpoint logs from Strata Logging Service to Amazon Security Lake.

STEP 1 | Create an Identity and Access Management (IAM) role to permit write access to the Amazon Security Lake bucket location.

1. In the AWS Management Console navigation pane of the console, click **Roles** > **Create role**.
2. In the Select trusted entity page, select **AWS account** > **Another AWS account** and enter the Account ID displayed in the Strata Logging Service Configure Log Forwarding Profile

to Amazon Security Lake page. This allows your AWS account to assume this role, and share the logs to the desired destination.



3. Select **Require external ID** and enter a password to establish connection between Amazon Security Lake and Strata Logging Service.
4. **Create policy** or use an existing policy in the Add permissions page.
   1. When you create a new policy, select JSON as the **Policy Editor**
   2. Edit the following code to replace DOC-EXAMPLE-BUCKET1 and DOC-EXAMPLE-BUCKET1/* with your Amazon S3 bucket name.

```
# {
    "Version":"2012-10-17",
    "Statement":[
       {
         "Effect":"Allow",
          "Action":"s3:PutObject",
         "Resource": [
               "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
               "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/*"
         ]
        }
     ]
}
```

   3. Enter a policy name and create policy.
5. Provide a role name and save the changes.
6. In the Roles page, select the role you created and make a note of the IAM Role ARN. You need to use the same ARN when configuring a log forwarding profile.

STEP 2 | **Sign In** to the hub.

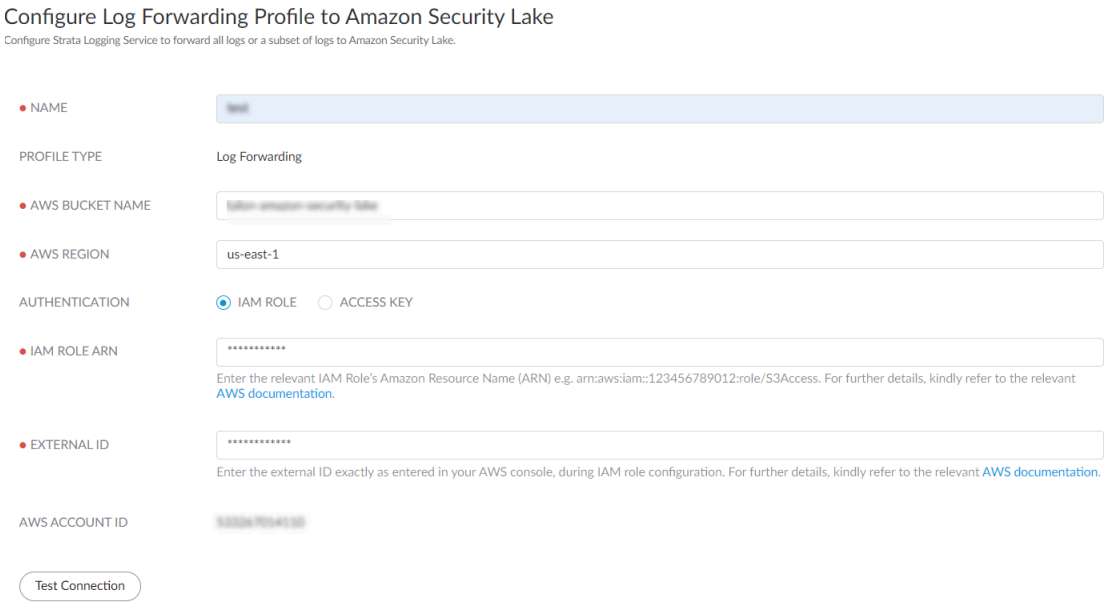
STEP 3 | Select the Strata Logging Service instance that you want to configure for log forwarding.

If you have multiple Strata Logging Service instances, click the Strata Logging Service tile and select an instance from the list of those available.

*If you are using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Log Forwarding** forward logs to external server.*

STEP 4 | Select **Log Forwarding** > **Amazon Security Lake** > **+** to add a new Amazon Security Lake profile.

STEP 5 | Configure a log forwarding profile to forward logs to Amazon Security Lake.



1. Enter a descriptive **Name** for the profile.
2. Enter the name of the Amazon Security Lake S3 configured bucket that is used as the storage container for your forwarded log data. You can get the name from the Amazon Console.
3. Enter the geographic region (regional code) where the Amazon Security Lake is hosted.
4. Select the external identification method to authenticate Amazon Security Lake.
   - **IAM Role**
     - **IAM Role ARN** - The Amazon Resource Names (ARN) of the role that has access to the Amazon S3 bucket. Enter the ARN you saved in step 1.f. The IAM Role ARN need to be in the following format: **`arn:partition:service:region:account-id:resource-`**

type:resource-id. For example, **arn:aws:iam::account:role/role-name-with-path**

- **External ID** - The external identifier that you defined while linking the IAM role to your AWS account.

- **Access Key**- If you have created a long-term access key to authenticate your AWS account, enter the key and secret password here.
  - To create an access key for the Amazon S3 bucket:
    1. Log in to AWS Management Console with your AWS account ID.
    2. On the **Console Home** page, select the IAM service.
    3. Select **Users** and then select **Create user** from the navigation pane.
    4. On the **Specify user details** page, enter the name for the new user.
    5. Do not select **Provide user access to the – AWS Management Console** and click **Next**.
    6. Set **Permissions** for the user. Here is a sample of the JSON code to set the permission boundaries in the policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/*"
            ]
        }
    ]
}
```

    7. Review the selection and create the user.
    8. In the **Summary** page, select **Security credentials > Create Access Key**.
    9. Select the **Third-party service** option as the reason for enabling the access key and confirm the recommendation to create the access key.
    10. Retrieve the access key and use it while configuring the log forwarding.

STEP 6 | Use this AWS Account ID to connect to the Amazon Security Lake bucket.

STEP 7 | **Test Connection** to ensure that the Strata Logging Service can communicate with the receiver.

This sends an empty log to the sls_test_events folder in the configured destination to verify that transmission is possible.

If the test fails, you won't be able to proceed.

STEP 8 | Click **Next**.

STEP 9 | Specify the `Payload Format` as PARQUET - the log format in which the Strata Logging Service forwards logs.

STEP 10 | (Optional) To receive a `STATUS NOTIFICATION` when Strata Logging Service is unable to connect to the Amazon Security Lake, enter the email address at which you'd like to receive the notification.

You will continue to receive these notifications at least once every 60 minutes until connectivity is restored. If the connectivity issue is addressed within 72 hours, no logs will be lost. However, any log older than 72 hours following the service disconnection could be lost.

STEP 11 | **Add** the log type as Endpoint > Events and optionally write a query to create filter to forward only the logs that are most critical to you. **Save** your changes

If you want to forward all logs of the type you selected, do not enter a query.

You can forward only the following events endpoint log fields to Amazon Security Lake. Refer to Log Reference guide for information on the log fields

- *Event Log Fields*
  - *policy.action*
  - *user.id*
  - *user.name*
  - *user.email*
  - *user.tenant_id*
  - *device.device_uuid*
  - *device.hostname*
  - *device.ip_address*
  - *device.os.type*
  - *network.http.method*
  - *network.http.url*
  - *network.http.classifications*
  - *network.http.url*
  - *network.http.status*
  - *id*
  - *batch_id*
  - *device.browser_type*
  - *device.browser_version*

STEP 12 | **Save** your changes.

STEP 13 | Verify that the `Status` of your forwarding profile is `Running` ( ).

STEP 14 | Verify if the logs are forwarded to the destination location. This is a sample path: `/Amazon S3 bucket location > folder name > logsource.logtype > year > month > date`

STEP 15 | (Optional) You can use the running Amazon Security Lake forwarding profile to forward past logs spanning up to 3 days.

Forward Logs to AWS S3 Bucket

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

To meet your long-term storage, reporting and monitoring, or legal and compliance needs, you can configure Strata Logging Service to forward all logs or a subset of logs to the AWS S3 Bucket. This integration enables you to make use of the beneficial features that both Strata Logging Service and Amazon S3 offer for log management.

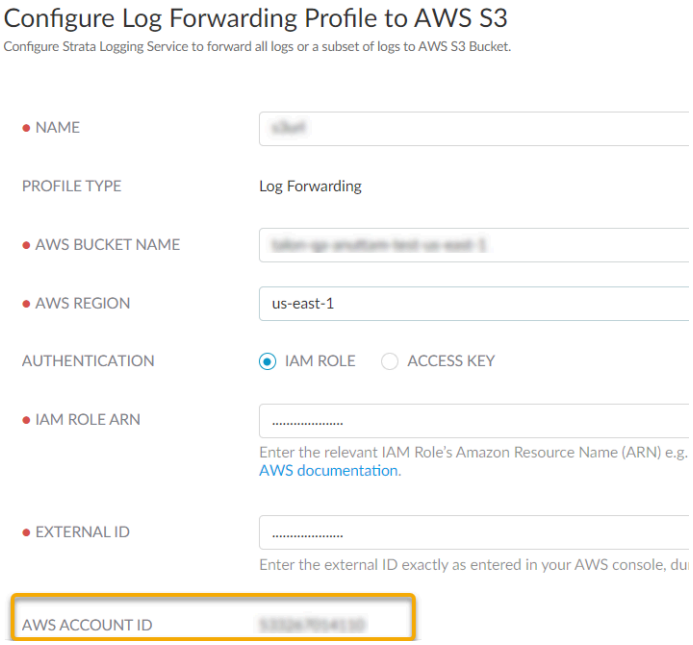
Strata Logging Service batch logs based on either a size limit of 1000 lines or a time limit of 10 seconds, whichever is reached first. Strata Logging Service compresses the log file using Snappy and forwards it to S3 bucket in JSON format. It is important to note that Palo Alto Networks is only responsible for delivering logs to the S3 bucket. Any other actions on logs, such as decompression or processing, should be taken care of by your organization based on its needs.

STEP 1 | Create and configure the Amazon S3 bucket in the AWS Management Console.

STEP 2 | Create an Identity and Access Management (IAM) role to permit write access to the Amazon Security Lake bucket location.

1. In the AWS Management Console navigation pane of the console, click **Roles** > **Create role**.
2. In the Select trusted entity page, select **AWS account** > **Another AWS account** and enter the Account ID displayed in the Strata Logging Service Configure Log Forwarding Profile

to AWS S3 page. This allows your AWS account to assume this role, and share the logs to the desired destination.



3. Select **Require external ID** and enter a password to establish connection between Amazon Security Lake and Strata Logging Service.
4. **Create policy** or use an existing policy in the Add permissions page.
   1. When you create a new policy, select JSON as the **Policy Editor**
   2. Edit the following code to replace DOC-EXAMPLE-BUCKET1 and DOC-EXAMPLE-BUCKET1/* with your Amazon S3 bucket name.

```
# {
    "Version":"2012-10-17",
    "Statement":[
       {
         "Effect":"Allow",
          "Action":"s3:PutObject",
         "Resource": [
               "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
               "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/*"
         ]
        }
     ]
}
```

   3. Enter a policy name and create policy.
5. Provide a role name and save the changes.
6. In the Roles page, select the role you created and copy and save the IAM Role ARN. You need to use the same ARN when configuring the log forwarding profile.

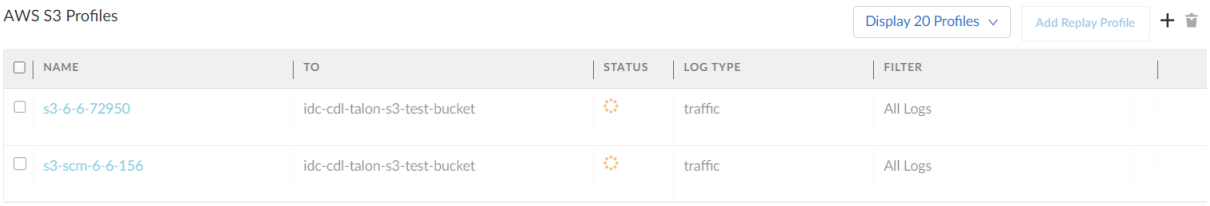
STEP 3 | **Sign In** to the hub.

STEP 4 | Select the Strata Logging Service instance that you want to configure for log forwarding.

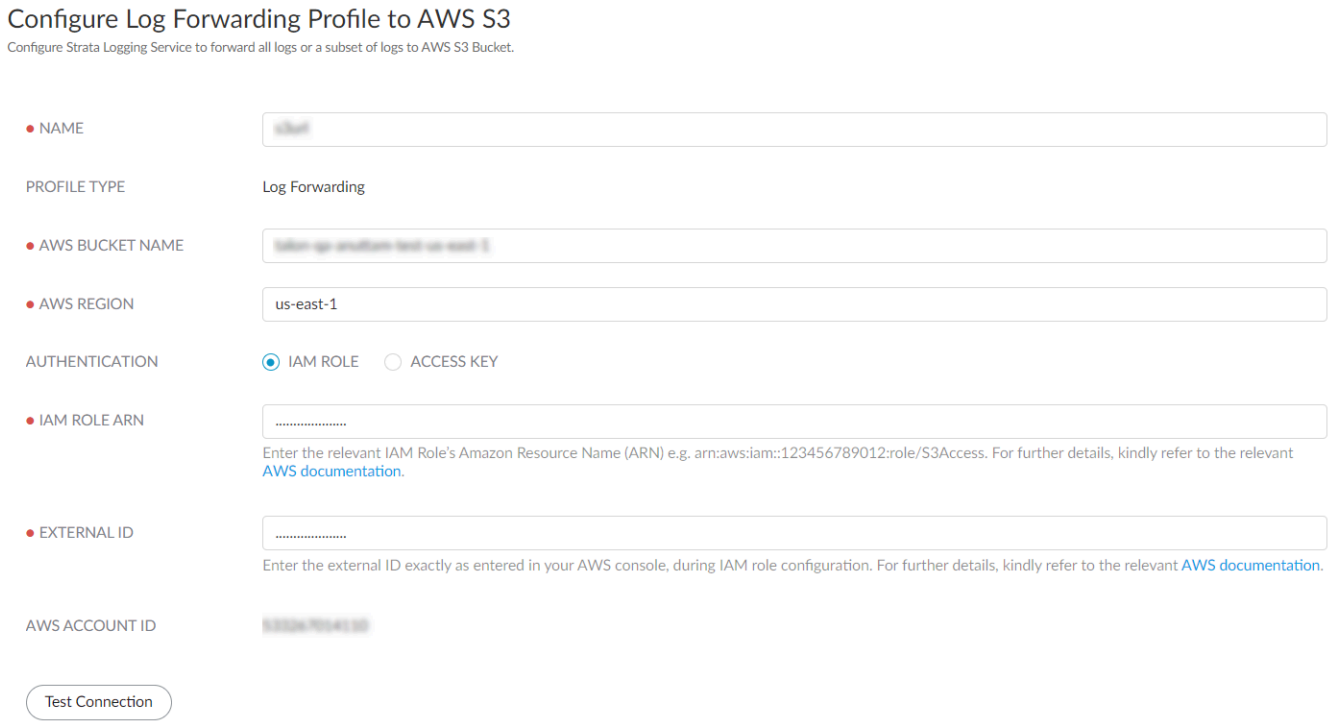
If you have multiple Strata Logging Service instances, click the Strata Logging Service tile and select an instance from the list of those available.

*If you're using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Log Forwarding** forward logs to an external server.*

STEP 5 | Select **Log Forwarding** > **AWS S3** > **+** to add a new Amazon S3 profile in Strata Logging Service.



STEP 6 | Configure the log forwarding profile to forward logs to the AWS S3 bucket.



1. Enter a descriptive **Name** for the profile.
2. Enter the name of the Amazon S3 configured bucket that is used as the storage container for your forwarded log data. You can get the name from the Amazon Console.
3. Enter the geographic region (regional code) where the Amazon S3 bucket is located.
4. Select the external identification method to authenticate the Amazon S3 bucket.
   - **IAM Role**
     - **IAM Role ARN** - The Amazon Resource Names (ARN) of the role that has access to the Amazon S3 bucket. Enter the ARN you saved in step 1.f. The IAM Role ARN needs to be in the following format:

arn:partition:service:region:account-id:resource-type:resource-id

- **External ID** - The external identifier that you defined while linking the IAM role to your Amazon account.

- **Access Key**- If you have created a long-term access key to authenticate your AWS account, enter the key and secret password here.
  - To create an access key for the Amazon S3 bucket:
    1. Log in to AWS Management Console with your AWS account ID.
    2. On the **Console Home** page, select the IAM service.
    3. Select **Users** and then select **Create user** from the navigation pane.
    4. On the **Specify user details** page, enter the name for the new user.
    5. Do not select **Provide user access to the – AWS Management Console** and click **Next**.
    6. Set **Permissions** for the user. Here is a sample of the JSON code to set the permission boundaries in the policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET1",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/*"
            ]
        }
    ]
}
```

    7. Review the selection and create the user.
    8. In the **Summary** page, select **Security credentials > Create Access Key**.
    9. Select the **Third-party service** option as the reason for enabling the access key and confirm the recommendation to create the access key.
    10. Retrieve the access key and use it while configuring the log forwarding.

STEP 7 | Use this AWS Account ID to connect to the AWS S3 bucket.

STEP 8 | **Test Connection** to ensure that the Strata Logging Service can communicate with the receiver.

This sends an empty log to the sls_test_events folder in the configured destination to verify that transmission is possible.

If the test fails, you won't be able to proceed.

STEP 9 | Click **Next**.

STEP 10 | Specify the **Payload Format** as JSON - the log format in which the Strata Logging Service forwards logs.

STEP 11 | (Optional) To receive a **STATUS NOTIFICATION** when the Strata Logging Service is unable to connect to the Amazon S3 bucket, enter the email address at which you'd like to receive the notification.

You will continue to receive these notifications at least once every 60 minutes until connectivity is restored. If the connectivity issue is addressed within 72 hours, no logs will be lost. However, service disconnection could lead to the loss of any logs older than 72 hour.

STEP 12 | **Add** the type of log you want to forward and optionally write a query to create filter to forward only the logs that are most critical to you. **Save** your changes

If you want to forward all logs of the type you selected, do not enter a query.

STEP 13 | **Save** your changes.

STEP 14 | Verify that the `Status` of your forwarding profile is `Running` ( ).

STEP 15 | Verify if the logs are forwarded to the destination location. This is a sample path: `/Amazon S3 bucket location > folder name > logsource.logtype > year > month > date`.

STEP 16 | (Optional) You can use the running Amazon S3 forwarding profile to forward past logs spanning up to 3 days.

Forward Logs to Snowflake

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

Configure log forwarding in Strata Logging Service to forward browser events and logs, device attributes, and audit logs in Strata Logging Service to a Snowflake warehouse. Strata Logging Service aggregates the data together for your organization before forwarding it to Snowflake for analytics and data processing. Strata Logging Service forwards logs to Snowflake warehouse in JSON format.

STEP 1 | Enable communication between the Strata Logging Service and your Snowflake account.

1. Log in to the Snowflake account with the ACCOUNTADMIN role.
2. Run the following script in the Snowsight worksheet:

```
CREATE WAREHOUSE IF NOT EXISTS SLS_WH;

CREATE DATABASE IF NOT EXISTS SLS_DB;

USE SCHEMA SLS_DB.PUBLIC;

CREATE OR REPLACE ROLE SLS_ROLE;

CREATE OR REPLACE USER SLS_USER
    LOGIN_NAME='<username'
    PASSWORD='<password>'
    DISPLAY_NAME='SLS Event Forwarding'
    DEFAULT_WAREHOUSE = SLS_WH
    DEFAULT_ROLE = SLS_ROLE;

GRANT USAGE ON WAREHOUSE SLS_WH TO ROLE SLS_ROLE;
GRANT USAGE ON DATABASE SLS_DB TO ROLE SLS_ROLE;
GRANT USAGE ON SCHEMA SLS_DB.PUBLIC TO ROLE SLS_ROLE;
GRANT CREATE PIPE ON SCHEMA SLS_DB.PUBLIC TO ROLE SLS_ROLE;
GRANT CREATE STAGE ON SCHEMA SLS_DB.PUBLIC TO ROLE SLS_ROLE;
GRANT CREATE TABLE ON SCHEMA SLS_DB.PUBLIC TO ROLE SLS_ROLE;
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA SLS_DB.PUBLIC TO
 ROLE SLS_ROLE;
GRANT ROLE SLS_ROLE TO USER SLS_USER;
GRANT OWNERSHIP ON USER SLS_USER TO ROLE SLS_ROLE;
```

Make a note of the username and password you provide here. You need to use the same credentials when configuring the Snowflake log forwarding profile.

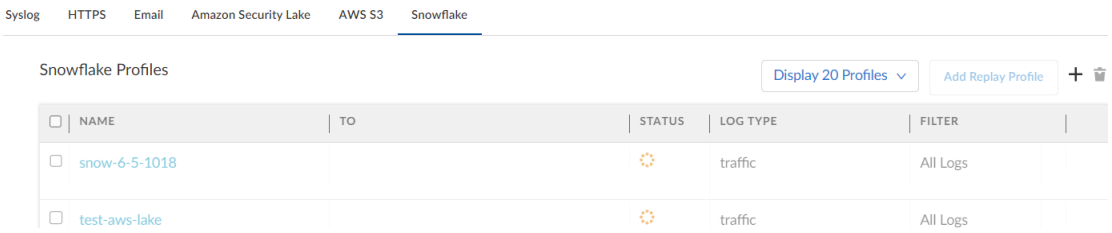
STEP 2 | **Sign In** to the hub.

STEP 3 | Select the Strata Logging Service instance that you want to configure for log forwarding.

If you have multiple Strata Logging Service instances, click the Strata Logging Service tile and select an instance from the list of those available.

*If you are using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Log Forwarding** to forward logs to an external server.*

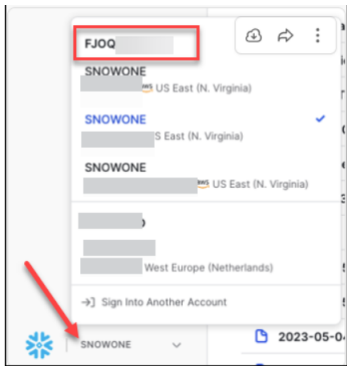
STEP 4 | Select **Log Forwarding** > **Snowflake** > **+** to add a new Snowflake log forwarding profile.



STEP 5 | Configure the log forwarding profile to forward logs to Snowflake.

1. Enter a descriptive **Name** for the profile.
2. Enter the Account Identifier of your Snowflake account. Ensure to replace the period with a hyphen in the Account Identifier.

   You can get the name from the Snowflake Console. Click the account name next to the Snowflake icon on the lower left of the screen. The Account Identifier is displayed at the top on the pop-up window.

3. Enter the credentials to authenticate your Snowflake account. Use the same username and password entered in step 1.
4. Enter a name for the table where you want to view the Strata Logging Service logs. To keep all log types organized in a single table, provide a table name. If you leave the field empty, logs are organized in separate tables based on the log type. You cannot edit or add a table name after the profile is configured.

STEP 6 | **Test Connection** to ensure that the Strata Logging Service can communicate with the receiver.

This sends an empty log to the configured destination to verify that transmission is possible.

If the test fails, you won't be able to proceed.

STEP 7 | Click **Next**.

STEP 8 | Specify the `Payload Format` as JSON - the log format in which the Strata Logging Service forwards logs.

STEP 9 | (Optional) To receive a `STATUS NOTIFICATION` when the Strata Logging Service is unable to connect to the Snowflake, enter the email address at which you'd like to receive the notification.

You will continue to receive these notifications at least once every 60 minutes until connectivity is restored. If the connectivity issue is addressed within 72 hours, no logs will be lost. However, any log older than 72 hours following the service disconnection could be lost.

STEP 10 | Select the log type and optionally write a query to create filter to forward only the logs that are most critical to you. **Save** your changes

If you want to forward all logs of the type you selected, do not enter a query.

STEP 11 | **Save** your changes.

STEP 12 | Verify that the `Status` of your forwarding profile is `Running` ( ).

STEP 13 | (Optional) You can use the running Snowflake forwarding profile to forward past logs spanning up to 3 days.

Create Log Filters

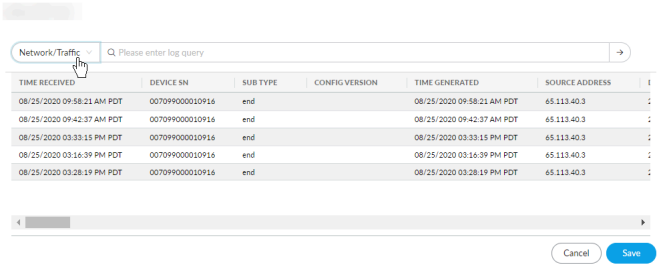
Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

When you're first setting up log forwarding to an external destination server, you must specify which logs to forward by using log filters. Log filters use the same query language as Explore to enable you to finely select which logs Strata Logging Service will forward to the destination of your choice. Set the log columns you want to send through those log types in log filters. You can also edit the log filters for an existing running log forwarding profile to add or remove the log columns you want to forward for the log type.

STEP 1 | Start creating a forwarding profile.

STEP 2 | Under `Filters`, select **Add**.

STEP 3 | Select a log type.



STEP 4 | Enter a query that describes the log fields you want to forward, or select one of the predefined filters.

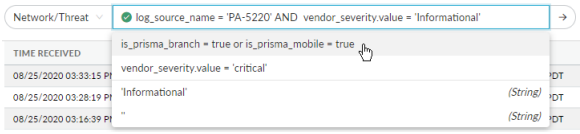
1. You can either write your own queries from scratch or use the Query Builder. You can also select the query field to choose from among a set of common predefined queries.

   Log filters function like queries in Explore, with the following differences:

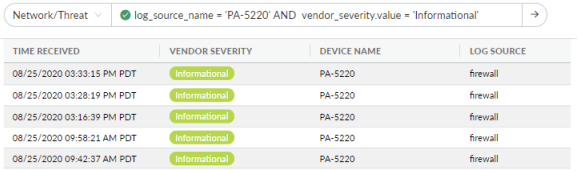
   - No double quotes (“”).
   - No subnet masks. To return IP addresses with subnets, use the LIKE operator. Example: src_ip.value LIKE “192.1.1.%”.

   If you want to forward all logs of the type you selected, do not enter a query.

Learn more about queries and using the query builder to help you write them.

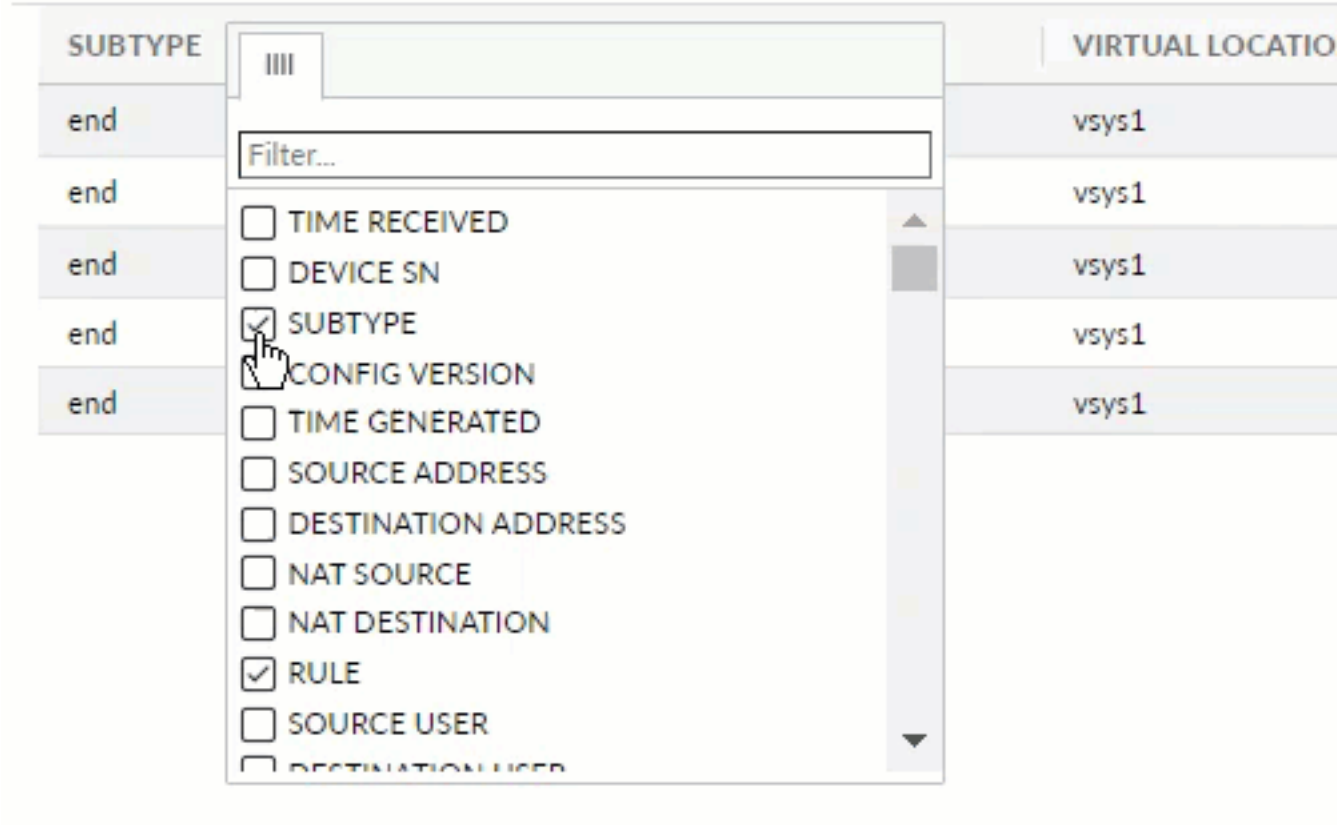


A green check mark indicates that the query is valid, and pressing enter or clicking the arrow should generate results that match the query. A red X means that the query is invalid and you will be unable to submit it.



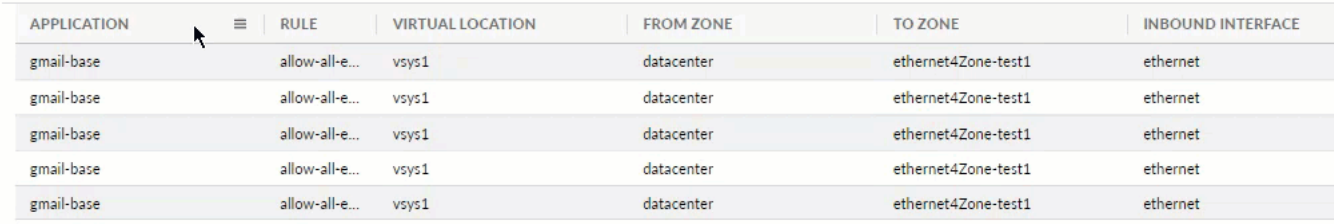
STEP 5 | (Optional) Customize how the field columns appear.

- Hover over any column header and select the hamburger icon to choose the columns that you want to forward through the selected log type to the external destination.



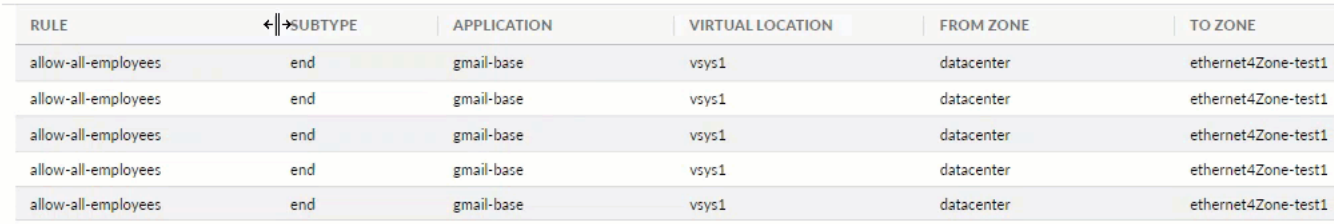
The data for the selected columns is forwarded to the destination server. You can also edit the filter for an existing running log forwarding profile to add or remove columns you want to forward. After making edits, save the filter and the log forwarding profile for the changes to reflect in the log forwarding message.

- Change column order by clicking anywhere on a column header and dragging to the left or right.



Rearranging columns changes the order of the fields in the Syslog message of the logs forwarded through the filter. For example, if you move RULE to the left of APPLICATION, the `Rule` field will appear before the `Application` field in the Syslog message.

- Change column width by clicking in between column headers and dragging to the left or right.



RULE	SUBTYPE	APPLICATION	VIRTUAL LOCATION	FROM ZONE	TO ZONE
allow-all-employees	end	gmail-base	vsys1	datacenter	ethernet4Zone-test1
allow-all-employees	end	gmail-base	vsys1	datacenter	ethernet4Zone-test1
allow-all-employees	end	gmail-base	vsys1	datacenter	ethernet4Zone-test1
allow-all-employees	end	gmail-base	vsys1	datacenter	ethernet4Zone-test1
allow-all-employees	end	gmail-base	vsys1	datacenter	ethernet4Zone-test1

STEP 6 | **Save** your filter.

Server Certificate Validation

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ❑ Strata Cloud Manager Pro ❑ Strata Logging Service

Strata Logging Service secures your log data by ensuring that the server you specify to receive your logs is trusted and legitimate.

When you configure syslog or HTTPS forwarding, Strata Logging Service ensures that your log data arrives safely to its intended destination by verifying the certificate on the receiving server. For maximum security, Strata Logging Service performs multiple validity checks:

Strata Logging Service checks...	to verify that...
Third-Party CA-Signed Certificates	The server has the full certificate chain. If the root CA is in the list of trusted CAs, you do not need to upload any CAs from the certificate chain. If the root CA is not in the list of trusted CAs, you need to upload the root CA to Strata Logging Service. OR The server has the server certificate and one or more intermediate CAs. If the root CA is in the list of trusted CAs, you do not need to upload any CAs from the certificate chain. If the root CA is not in the list of trusted CAs, you need to upload the root CA to Strata Logging Service. OR The server has only the server certificate. If the root CA is in the list of trusted CAs, then you need to upload only the intermediate CAs (one or multiple) to Strata Logging Service. If the root CA is not in the list of trusted CAs, you need to upload the root CA and one or more intermediate CAs to Strata Logging Service.
Private CA-Signed Certificates	The server has the full certificate chain, and only the root CA is uploaded to Strata Logging Service. OR

Strata Logging Service checks...	to verify that...
	The server has the server certificate and one or more intermediate CAs, and the root CA is uploaded to Strata Logging Service. OR The server has the server certificate only; the root CA and one or more intermediate CAs are uploaded to Strata Logging Service.
Self-Signed Certificates	The certificate is installed on the server and uploaded to Strata Logging Service.
Expiration	None of the certificates in the chain have expired.
Host Name Match	The value entered for the Syslog Server name matches the Subject Alternative Name (SAN) of the server certificate.
Revocation Status	None of the certificates in the chain have been revoked by its issuing CA.

List of Trusted Certificates for Syslog and HTTPS Forwarding

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

See below for a list of SSL certificates trusted by Strata Logging Service. You can also use wildcard certificates.

If you want to forward logs from the Strata Logging Service in China, CA must sign the endpoint's TLS certificate with a root certificate (C=CN) that is valid within China.

- Issuer: CN=GLOBALTRUST 2020, O=e-commerce monitoring GmbH, C=AT
- Issuer: CN=GlobalSign Root E46, O=GlobalSign nv-sa, C=BE
- Issuer: CN=GlobalSign Root R46, O=GlobalSign nv-sa, C=BE
- Issuer: CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
- Issuer: CN=QuoVadis Root CA 1 G3, O=QuoVadis Limited, C=BM
- Issuer: CN=QuoVadis Root CA 2, O=QuoVadis Limited, C=BM
- Issuer: CN=QuoVadis Root CA 2 G3, O=QuoVadis Limited, C=BM
- Issuer: CN=QuoVadis Root CA 3 G3, O=QuoVadis Limited, C=BM
- Issuer: CN=SwissSign Gold CA - G2, O=SwissSign AG, C=CH
- Issuer: CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH
- Issuer: CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH
- Issuer: CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH
- Issuer: CN=CFCA EV ROOT, O=China Financial Certification Authority, C=CN
- Issuer: CN=GDCA TrustAUTH R5 ROOT, O="GUANG DONG CERTIFICATE AUTHORITY CO.,LTD.", C=CN
- Issuer: CN=vTrus ECC Root CA, O="iTrusChina Co.,Ltd.", C=CN
- Issuer: CN=vTrus Root CA, O="iTrusChina Co.,Ltd.", C=CN
- Issuer: CN=UCA Extended Validation Root, O=UniTrust, C=CN
- Issuer: CN=UCA Global G2 Root, O=UniTrust, C=CN
- Issuer: CN=D-TRUST Root Class 3 CA 2 2009, O=D-Trust GmbH, C=DE
- Issuer: CN=D-TRUST Root Class 3 CA 2 EV 2009, O=D-Trust GmbH, C=DE

- Issuer: CN=T-TeleSec GlobalRoot Class 2, OU=T-Systems Trust Center, O=T-Systems Enterprise Services GmbH, C=DE
- Issuer: CN=T-TeleSec GlobalRoot Class 3, OU=T-Systems Trust Center, O=T-Systems Enterprise Services GmbH, C=DE
- Issuer: CN=Autoridad de Certificacion Firmaprofesional CIF A62634068, C=ES
- Issuer: CN=EC-ACC, OU=Jerarquia Entitats de Certificacio Catalanes, OU=Vegeu https://www.catcert.net/verarrel (c)03, OU=Serveis Publics de Certificacio, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), C=ES
- Issuer: OU=AC RAIZ FNMT-RCM, O=FNMT-RCM, C=ES
- Issuer: CN=AC RAIZ FNMT-RCM SERVIDORES SEGUROS, OID.2.5.4.97=VATES-Q2826004J, OU=Ceres, O=FNMT-RCM, C=ES
- Issuer: CN=Izenpe.com, O=IZENPE S.A., C=ES
- Issuer: CN=Certigna, O=Dhimyotis, C=FR
- Issuer: CN=Certigna Root CA, OU=0002 48146308100036, O=Dhimyotis, C=FR
- Issuer: CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB
- Issuer: CN=COMODO Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
- Issuer: CN=COMODO ECC Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
- Issuer: CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
- Issuer: CN=Hellenic Academic and Research Institutions ECC RootCA 2015, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR
- Issuer: CN=Hellenic Academic and Research Institutions RootCA 2015, O=Hellenic Academic and Research Institutions Cert. Authority, L=Athens, C=GR
- Issuer: CN=HARICA TLS ECC Root CA 2021, O=Hellenic Academic and Research Institutions CA, C=GR
- Issuer: CN=HARICA TLS RSA Root CA 2021, O=Hellenic Academic and Research Institutions CA, C=GR
- Issuer: CN=Hellenic Academic and Research Institutions RootCA 2011, O=Hellenic Academic and Research Institutions Cert. Authority, C=GR
- Issuer: CN=Hongkong Post Root CA 1, O=Hongkong Post, C=HK
- Issuer: CN=Hongkong Post Root CA 3, O=Hongkong Post, L=Hong Kong, ST=Hong Kong, C=HK
- Issuer: CN=e-Szigno Root CA 2017, OID.2.5.4.97=VATHU-23584497, O=Microsec Ltd., L=Budapest, C=HU
- Issuer: EMAILADDRESS=info@e-szigno.hu, CN=Microsec e-Szigno Root CA 2009, O=Microsec Ltd., L=Budapest, C=HU
- Issuer: CN=NetLock Arany (Class Gold) Főtanúsítvány, OU=Tanúsítványkiadók (Certification Services), O=NetLock Kft., L=Budapest, C=HU

- Issuer: CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
- Issuer: CN=emSign ECC Root CA - G3, O=eMudhra Technologies Limited, OU=emSign PKI, C=IN
- Issuer: CN=emSign Root CA - G1, O=eMudhra Technologies Limited, OU=emSign PKI, C=IN
- Issuer: CN=Actalis Authentication Root CA, O=Actalis S.p.A./03358520967, L=Milan, C=IT
- Issuer: CN=SecureSign RootCA11, O="Japan Certification Services, Inc.", C=JP
- Issuer: OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP
- Issuer: OU=Security Communication RootCA1, O=SECOM Trust.net, C=JP
- Issuer: CN=NAVER Global Root Certification Authority, O=NAVER BUSINESS PLATFORM Corp., C=KR
- Issuer: CN=Staat der Nederlanden EV Root CA, O=Staat der Nederlanden, C=NL
- Issuer: CN=Buypass Class 2 Root CA, O=Buypass AS-983163327, C=NO
- Issuer: CN=Buypass Class 3 Root CA, O=Buypass AS-983163327, C=NO
- Issuer: CN=TrustCor ECA-1, OU=TrustCor Certificate Authority, O=TrustCor Systems S. de R.L., L=Panama City, ST=Panama, C=PA
- Issuer: CN=TrustCor RootCert CA-1, OU=TrustCor Certificate Authority, O=TrustCor Systems S. de R.L., L=Panama City, ST=Panama, C=PA
- Issuer: CN=TrustCor RootCert CA-2, OU=TrustCor Certificate Authority, O=TrustCor Systems S. de R.L., L=Panama City, ST=Panama, C=PA
- Issuer: CN=Certum EC-384 CA, OU=Certum Certification Authority, O=Asseco Data Systems S.A., C=PL
- Issuer: CN=Certum Trusted Root CA, OU=Certum Certification Authority, O=Asseco Data Systems S.A., C=PL
- Issuer: CN=SZAFIR ROOT CA2, O=Krajowa Izba Rozliczeniowa S.A., C=PL
- Issuer: CN=Certum Trusted Network CA, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL
- Issuer: CN=Certum Trusted Network CA 2, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL
- Issuer: OU=certSIGN ROOT CA G2, O=CERTSIGN SA, C=RO
- Issuer: OU=certSIGN ROOT CA, O=certSIGN, C=RO
- Issuer: CN=CA Disig Root R2, O=Disig a.s., L=Bratislava, C=SK
- Issuer: CN=TunTrust Root CA, O=Agence Nationale de Certification Electronique, C=TN
- Issuer: CN=E-Tugra Certification Authority, OU=E-Tugra Sertifikasyon Merkezi, O=E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş., L=Ankara, C=TR
- Issuer: CN=TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1, OU=Kamu Sertifikasyon Merkezi - Kamu SM, O=Turkiye Bilimsel ve Teknolojik Arastirma Kurumu - TUBITAK, L=Gebze - Kocaeli, C=TR
- Issuer: CN=HiPKI Root CA - G1, O="Chunghwa Telecom Co., Ltd.", C=TW
- Issuer: OU=ePKI Root Certification Authority, O="Chunghwa Telecom Co., Ltd.", C=TW
- Issuer: CN=TWCA Global Root CA, OU=Root CA, O=TAIWAN-CA, C=TW

- Issuer: CN=TWCA Root Certification Authority, OU=Root CA, O=TAIWAN-CA, C=TW
- Issuer: CN=AffirmTrust Commercial, O=AffirmTrust, C=US
- Issuer: CN=AffirmTrust Networking, O=AffirmTrust, C=US
- Issuer: CN=AffirmTrust Premium, O=AffirmTrust, C=US
- Issuer: CN=AffirmTrust Premium ECC, O=AffirmTrust, C=US
- Issuer: CN=Amazon Root CA 1, O=Amazon, C=US
- Issuer: CN=Amazon Root CA 2, O=Amazon, C=US
- Issuer: CN=Amazon Root CA 3, O=Amazon, C=US
- Issuer: CN=Amazon Root CA 4, O=Amazon, C=US
- Issuer: CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert Assured ID Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert Assured ID Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert Global Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=DigiCert Trusted Root G4, OU=www.digicert.com, O=DigiCert Inc, C=US
- Issuer: CN=Entrust Root Certification Authority - G2, OU="(c) 2009 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
- Issuer: CN=Entrust Root Certification Authority - EC1, OU="(c) 2012 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
- Issuer: CN=Entrust Root Certification Authority - G4, OU="(c) 2015 Entrust, Inc. - for authorized use only", OU=See www.entrust.net/legal-terms, O="Entrust, Inc.", C=US
- Issuer: CN=Entrust Root Certification Authority, OU="(c) 2006 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated by reference, O="Entrust, Inc.", C=US
- Issuer: CN=GTS Root R1, O=Google Trust Services LLC, C=US
- Issuer: CN=GTS Root R2, O=Google Trust Services LLC, C=US
- Issuer: CN=GTS Root R3, O=Google Trust Services LLC, C=US
- Issuer: CN=GTS Root R4, O=Google Trust Services LLC, C=US
- Issuer: CN=IdenTrust Commercial Root CA 1, O=IdenTrust, C=US
- Issuer: CN=IdenTrust Public Sector Root CA 1, O=IdenTrust, C=US
- Issuer: CN=ISRG Root X1, O=Internet Security Research Group, C=US
- Issuer: CN=ISRG Root X2, O=Internet Security Research Group, C=US
- Issuer: CN=Microsoft ECC Root Certificate Authority 2017, O=Microsoft Corporation, C=US
- Issuer: CN=Microsoft RSA Root Certificate Authority 2017, O=Microsoft Corporation, C=US
- Issuer: CN=Network Solutions Certificate Authority, O=Network Solutions L.L.C., C=US
- Issuer: CN=Secure Global CA, O=SecureTrust Corporation, C=US

- Issuer: CN=SecureTrust CA, O=SecureTrust Corporation, C=US
- Issuer: OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US
- Issuer: OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US
- Issuer: CN=emSign ECC Root CA - C3, O=eMudhra Inc, OU=emSign PKI, C=US
- Issuer: CN=emSign Root CA - C1, O=eMudhra Inc, OU=emSign PKI, C=US
- Issuer: CN=XRamp Global Certification Authority, O=XRamp Security Services Inc, OU=www.xrampsecurity.com, C=US
- Issuer: CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US
- Issuer: CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US
- Issuer: CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US
- Issuer: CN=Trustwave Global Certification Authority, O="Trustwave Holdings, Inc.", L=Chicago, ST=Illinois, C=US
- Issuer: CN=Trustwave Global ECC P256 Certification Authority, O="Trustwave Holdings, Inc.", L=Chicago, ST=Illinois, C=US
- Issuer: CN=Trustwave Global ECC P384 Certification Authority, O="Trustwave Holdings, Inc.", L=Chicago, ST=Illinois, C=US
- Issuer: CN=USERTrust ECC Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
- Issuer: CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
- Issuer: CN=SSL.com EV Root Certification Authority ECC, O=SSL Corporation, L=Houston, ST=Texas, C=US
- Issuer: CN=SSL.com EV Root Certification Authority RSA R2, O=SSL Corporation, L=Houston, ST=Texas, C=US
- Issuer: CN=SSL.com Root Certification Authority ECC, O=SSL Corporation, L=Houston, ST=Texas, C=US
- Issuer: CN=SSL.com Root Certification Authority RSA, O=SSL Corporation, L=Houston, ST=Texas, C=US
- Issuer: C=ES, O=ACCV, OU=PKIACCV, CN=ACCVRAIZ1
- Issuer: C=DE, O=Atos, CN=Atos TrustedRoot 2011
- Issuer: CN=Entrust.net Certification Authority (2048), OU=(c) 1999 Entrust.net Limited, OU=www.entrust.net/CPS_2048 incorp. by ref. (limits liab.), O=Entrust.net
- Issuer: CN=TeliaSonera Root CA v1, O=TeliaSonera
- Issuer: CN=GlobalSign, O=GlobalSign, OU=GlobalSign ECC Root CA - R4
- Issuer: CN=GlobalSign, O=GlobalSign, OU=GlobalSign ECC Root CA - R5
- Issuer: CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
- Issuer: CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R6

- Issuer: CN=Palo Alto Networks Inc Root CA, O=Palo Alto Networks Inc, C=US
- Issuer: CN=ANF Secure Server Root CA, OU=ANF CA Raiz, O=ANF Autoridad de Certificacion, C=ES, SERIALNUMBER=G63287510

Log Forwarding Errors

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

When a problem occurs that disrupts the flow of your log data to its destination, you may see an error in the app UI. See the table below to find out what these errors mean and, if applicable, how you can resolve them.

Error Message	Description
connection to server failed due to incomplete CA chain	The CA chain provided by the server is incomplete. Check that the certificate chain is complete. You can check this by running **`openssl s_client`** on the server.
resolving host name failed	The IP address of the host could not be determined. Make sure that you have a DNS entry for the host.
TLS handshake with server failed	Verify that you are using an allowed TLS version and cipher suite. You can find this information in your server configuration.
subject alternative names do not match	The syslog server and the subject alternative name (SAN) in the server certificate do not match.
connection to server failed due to revoked cert in chain	The server certificate has been revoked. Contact your CA to get a new one.
protocol error	An HTTP protocol error occurred. Verify that the URI path exists.
TCP connection to server failed	The connection to the syslog or HTTP server timed out. Verify that the server FQDN and port are correct and that a server is listening at this FQDN and port.
Unable to save the profile because it is too large. Please reduce the number of filters for different log types or the number of columns in the filters and try again.	The profile that you are trying to save exceeds the size limit. Many factors determine the size limit: the number of log types, filters, and columns, as

Error Message	Description
	well as the type of log message (CEF, LEEF, HTTPS, EMAIL, or CSV). To resolve this error, try distributing the number of log filters among different log forwarding profiles. For example, if you have a profile with ten filters and you see this error, try creating two profiles with five filters each instead.

Forward Logs With Log Replay

Where Can I Use This?	What Do I Need?
• NGFW, including those funded by Software NGFW Credits • Prisma Access	One of these: ☐ Strata Cloud Manager Pro ☐ Strata Logging Service

You can forward old logs spanning up to the past 3 days from Strata Logging Service to the preferred external destination with a log replay profile. This option is useful to retrieve old logs in case of connection failures or outages at the destination server.

To get started, create a log replay profile based on an existing log forwarding profile for the syslog server, HTTPS server, or email server. Once you create the profile, the system forwards the logs in the configured date range to the destination server.

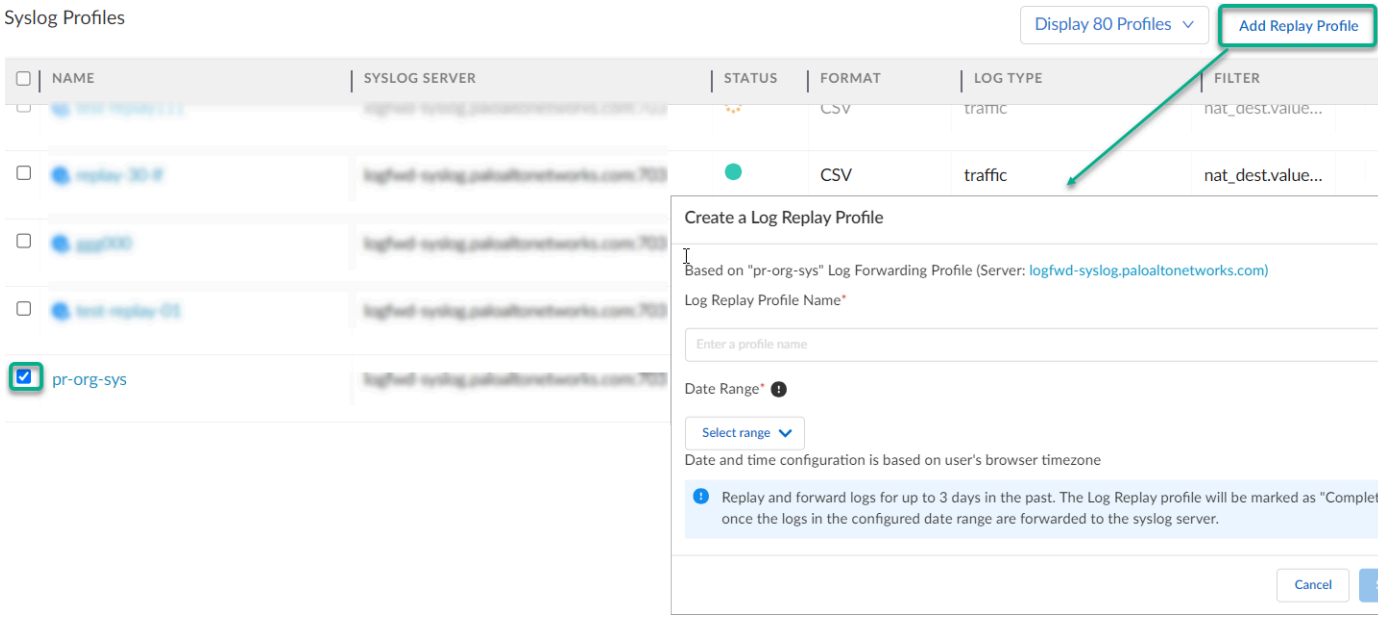
Once you create the log replay profile, you can't modify it. Also, any changes made to the existing log forwarding profile used to create the replay profile don't impact the replay profile.

STEP 1 | Log in to the hub and open the Strata Logging Service app to the instance.

STEP 2 | Select **Log Forwarding** from the left navigation menu.

*If you are using Strata Cloud Manager to manage Strata Logging Service, click **Settings** > **Strata Logging Service** > **Log Forwarding** to manage devices onboarded to your Strata Logging Service instance.*

STEP 3 | Select a log forwarding profile that is **Running** and click **Add Replay Profile**. This replicates the parameters defined in the log forwarding profile to the replay profile.



STEP 4 | Enter a name for the replay profile and select the date range for which you want to forward the logs.

You can select a date range up to 3 days before the current date.

STEP 5 | Save the changes.

STEP 6 | Verify the status of your replay profile is **Running**. The log replay profile status indicates “completed” 3 days from the creation date of the replay profile.

