Security Analytics and Logging (SAL)

Cisco Partner
https://cs.co/1page

Security Analytics and Logging (SAL) aggregates logs from various Cisco devices and providing an intuitive view of network activity. Security Analytics and Logging can be expanded at the user's discretion, allowing for longer retention and analysis, and even alerts on potential threats found in your firewall and other networking devices.

Benefits:

Simplify security management. Greatly reduce false positives with high-fidelity alerts and simplified policy orchestration.

Provide better intelligence to harmonize policy management. Monitor your networks and deploy behavioral-based analytics on firewall logs and network telemetry.

Enhance threat detection across the organization. Detect internal and external threats or suspicious activity by proactively monitoring network behavior. Using advanced analytics powered by Secure Network Analytics SaaS, detect threats such as C&C attacks, ransomware, DDoS attacks, illicit cryptomining, known malware, and insider threats.

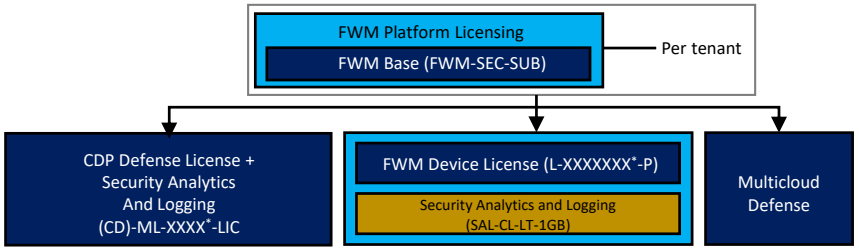
Meet compliance mandates. Enable logging and analytics capabilities to easily monitor your organization for compliance with industry regulations such as PCI, HIPAA, FISMA, and more.

FAQs:

Q: Do I have to buy Security Cloud Control (SCC) to buy SAL (SaaS)?
A: No. SAL's event viewer in SCC is included as part of the SAL license/ trial.

Q: What log types does SAL support?
A: SAL (SaaS) supports Cisco Firewalls (FTD & ASA) managed by FMC, SCC, FDM, CSM, ASDM or ASA-CLI. Also, logs from network endpoints. SAL (On Prem) only supports FTD-NGFW logging.

Q: How long can logs sent to SAL (SaaS) be retained?
A: Device log data sent to SAL is retained by default for 90 days at no extra charge. One, two, and three-year data retention plans are available for a nominal license fee.



Combined CDO device license and unlimited logging and 90 days retention with one part number

CDO device license and logging (1GB/day) Offered as separate part number's

** Secure Firewall model*

Licensing:

Essentials (formerly Logging and Troubleshooting or LT): Scalable central logging service with long-term retention options, with drill—down enabled through advanced viewer controls such as search, filer, download, etc.

Advantage (formerly Log Analytics or LA): An optional capability to analyze logs for advanced threats using behavioral modelling techniques. These threat detection algorithms leverage existing Cisco Secure Cloud Analytics ("SCA") or Secure Network Analytics ("SNA") analytics, as well as trigger new alerts customized for Product logs.

Premier (formerly Total Network Analytics or TA): Aggregates log analysis with native Cisco SCA or SNA logs, for end-to-end analysis.

SAL On-Premise Features:

- **FTD** (including data plane logs) and **ASA** logging in a scalable data store hosted on-premises.
- **Logging wizard** in FMC 7.0+ simplifies on-premises and cloud logging configuration.
- **FMC 7.0+ logging and analytics** scale drastically extended by a significant 300X magnitude via remote query of SAL/ SNA 7.3.2+.
- **Context pivot** to SAL's event viewer in Secure Network Analytics for context.
- **Multiple Flow Collector** support with Firewall to Flow Collect mapping.
- **Easy button for setup:**
  - Setup FMC analytics cross launch links to Secure Analytics console
  - Setup remote query credentials from Secure Analytics datastore
- **Longer Event Retention and increased scale:**
  - External Storage through Cisco Security Analytics and Logging On-Prem
  - Auto select event source or manually specify
  - Multiple Flow Collectors as event destination

Resources:

At-a-Glance	Install/Upgrade Guide	Select EOS
Ordering Guide	Config Guides	SAL Offer Description	Free Trial
Documents	Log Estimator	Security Cloud Control	Public page

Example SKUs: ***SAL-SUB***