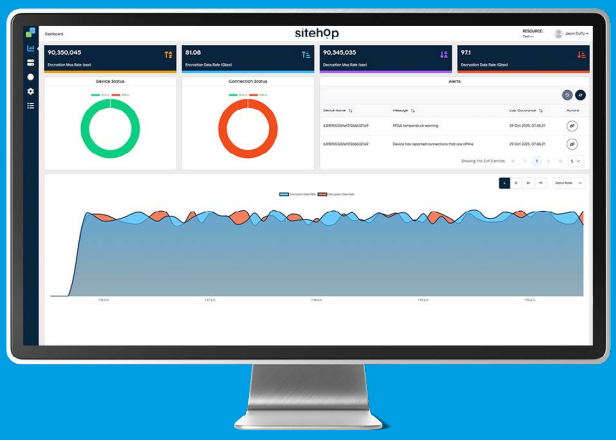
Sitehop SAFEnms

Engineered for management. Built for the future.

Sitehop SAFEnms: The next generation of powerful network management systems

Sitehop SAFEnms is a powerful cloud-based Enterprise NMS and easy to use platform that simplifies the deployment and management of global encryption devices. Its intuitive platform enables high speed configuration of certificates and permissions and enables easy management of your fleet of multi-tenanted encryptors.

Sitehop SAFEnms lets you configure user's certificates and permissions in minutes. Alternatively, Sitehop can pre-load SAFE Series devices, so they arrive on site ready for installation. Either way, you can then manage your fleet of multi-tenant SAFE Series encryptors from a centralised system.



Single Pane of Glass with real-time insights into network performance.

Get ready for a seamless transition to PQC

Future-proof your network with high-throughput security that's ready for tomorrow's challenges. Remote firmware updates, managed through Sitehop SAFEnms, ensure a smooth transition to Post Quantum Cryptography (PQC) while maintaining robust protection today.

Organize users into tenants and resource groups, for tailored monitoring, resource allocation, and customized settings

sitehop.com

sitehop

info@sitehop.com

Sitehop SAFEnms

Sitehop SAFEnms Benefits

Crypto agile secure remote updates

SAFEnms enables cloud-to-device firmware updates over authenticated, encrypted channels, ensuring only trusted images are installed. Seamless crypto upgrades, including PQC–deliver true crypto agility without downtime or site visits.

Role-based access control for all sites

Sitehop SAFEnms offers a flexible, secure permissions system with SSO and role-based access, supporting multi-tenanted configurations for complex networks. This enables precise access control, letting users manage individual sites and separate customers with ease, ensuring only authorized access.

Centralised dashboard

The dashboard delivers Single Pane of Glass, real-time insights into network performance, displaying total throughput and IPsec connectivity. Through a single view, administrators can organize users into tenants and resource groups, enabling tailored monitoring, resource allocation, and customized security settings for efficient management and optimal performance.

REST API integration

Easily integrate Sitehop SAFEnms with your existing OSS/BSS or other management systems using its REST API. This ensures seamless interoperability with your operational workflows and readiness for Infrastructureas-Code applications.

Cloud or on-premise deployment

Designed for rapid setup even in high-pressure environments, SAFEnms minimizes complexity with intuitive workflows, zero-touch provisioning, and centralized control driving down operational overhead and total cost of ownership.

Certificate management, logging and auditing

Maximize your network's performance with advanced certificate management, data tracking, auditing, and logging features. Harness the power of enterprise-grade audits, alerts, and webhook integrations. These tools provide real-time insight into network activity, ensuring peak performance and that your infrastructure operates at its full potential.

Multi-tenanted separation

SAFEnms supports full customer isolation with dedicated tenants per organization, enabling strict separation of data, policies, and visibility. Each tenant can manage multiple resource groups, mapping to individual SAFEcore or SAFEmini deployments, ensuring secure, scalable control across complex environments.

Built-In PKI

Sitehop SAFEnms includes a built-in PKI system, enabling users to create and manage certificates, with support for third-party certificates and AWS KMS integration for easier deployment and compliance.

SAFEnms Specifications

System Performance and Capacity	
Centralised dashboard	Per resource showing aggregated statistics / alerts
Easy to use	Each resource starts at the dashboard and allows for granular view into each level from viewing a device statistics to an individual Ipsec tunnel.
Policy and route based connections (each connection can be configured individually)	Ability to configure both policy and route-based connections on a per device basis. With the ability to mix and match on a per tunnel requirement.
Scalable multi-tenant and multi-device management	Designed to scale horizontally as demand increases.
Assign devices to virtually separated resource groups	Example: PreProduction, Production or even customer A, customer B etc

Flexible Deployment Options	
SaaS cloud platform (High availability, multi region active/ active cluster)	Fully managed by Sitehop, no setup or maintenance required by clients. Same platform shared by multiple clients.
Private Sitehop managed cloud deployment (Dedicated)	As SaaS deployment but completely isolated to a single client.
On premise	Fully managed by the client, full control over data and system.
Scalability - how many connections supported and overall network topography	Delivered as a docker image allowing for ease of deployment and scale within an existing or cloud-based containerisation cluster.

Certificate Management	
Certificates support RSA and ECDSA algorithms	"Key Lengths Supported: RSA: 4096, 6144, 7680, 8192 ECDSA: prime256v1, secp384r1, secp521r1 ML-DSA-87: Coming Soon"
X509 Certificate root of trust generation and management.	In built PKI for generation, management and deployment of certificates used by the devices during tunnel authentication.
Bring your own certificates	Ability to upload third party certificates
Revoke certificates generated by the SAFEnms	Certificates generated and managed by the SAFEnms can be revoked in instances where keys are being retired or misplaced allowing devices to de-trust any connection attempts.

SAFEnms Specifications

Integrations	
REST API access allowing the SAFEnms to be fully integrated into other systems	Fully documented REST API to ease deployment into existing environments.
AWS KMS integration to generate and secure certificate keys	Allows for complete offloading of the certificate authority private keys and customer managed encryption at rest
Webhook integration for SAFEnms alerts	Receive device alerts generated within the SAFEnms in real-time on third party systems.

Logging and Monitoring	
Real time SAFE device statistics logging	Devices report current statistics every 5 seconds to the SAFEnms.
View real time device alerts and alert history	Continuous device monitoring and alerting, email and webhook notifications. Auto closure following incident resolution.
Audit log (can be exported to CSV)	All changes to a device configuration within the SAFEnms is recorded.
KPIs Reported	Throughput data and message rates (packets per second) are collected on a per device / tunnel basis. Real time for the last 5 minutes with the ability to view averaged data for the past 6 months.

Device Management	
Use SAFE and third party devices	Third party devices can be listed within the system as remote devices, allowing for quick selection of third party devices whilst setting up IPSec connections from multiple devices.
Manage remote firmware upgrades for latest cryptographical updates	Hosting and central deployment of device firmware release, allowing ease of upgradability from one release to the next from a central location.
Multi tenant resource management	Devices can be organised into customisable groupings
Custom tagging	Additional device grouping and filtering within a resource. Tagging allows for quick labelling of connection's, certificates and associated devices.

Security	
Role based permissions	Users can be granted access at the tenant level or only to a specific resource
SSO (Single Sign On)	SAML 2.0 based authentication for authentication against existing identity providers
Firmware validation / signing checks.	Firmware images upon upload to the SAFEnms are checked and validated to ensure the signature of each file has been signed by Sitehop and have not been tampered with. Devices only show firmware releases that are available for the device in question.
Device enrolment	Device handshake upon enrolment ties the device to the SAFEnms and enables a per device encryption key for management data transferred
HTTPS utilising TLS1.2 and above	All management connectivity to the SAFEnms is secured using industry recommended protocols.
Data encrypted in transit and at rest	Management data transferred between the SAFEnms, users and devices is encrypted in motion and stored on encrypted media*.

* Subject to deployment option chosen and environment architecture options.