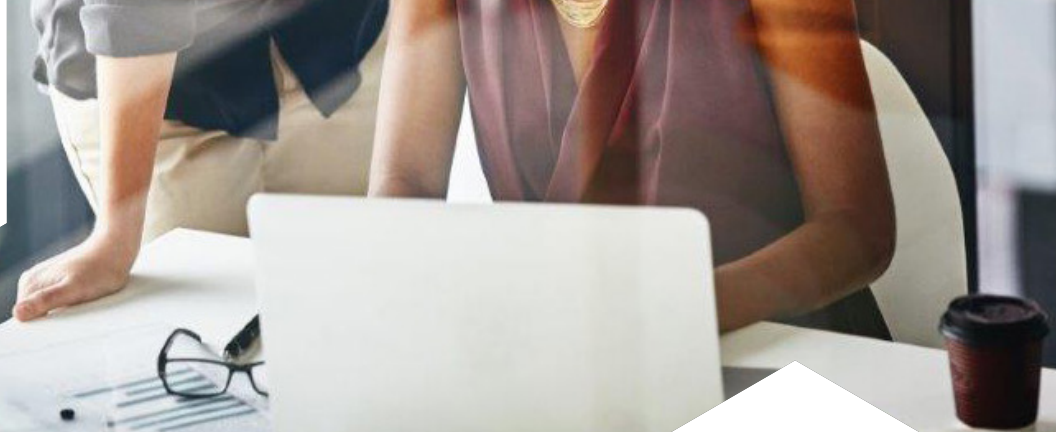




ENTRUST



nShield Monitor

Consolidated monitoring of distributed HSMs

HIGHLIGHTS

- Provides 24 x 7 visibility on all nShield hardware security modules (HSMs)
- Identifies performance bottlenecks to improve capacity planning
- Enables immediate response to potential issues through comprehensive alerts
- Eliminates the need to physically access HSMs to retrieve important data
- Integrates seamlessly with existing HSM hardware and software configurations

nShield Monitor is a comprehensive HSM monitoring platform that enables operations teams to gain 24x7 visibility into the status of all their nShield HSMs, including those residing across distributed data centers. With this solution, security teams can efficiently inspect HSMs and find out immediately if any potential security, configuration or utilization issue may compromise their mission-critical infrastructure.

Central monitoring capabilities

- Refreshes utilization statistics for all HSMs on a per minute basis
- Provides a series of warnings based on user-defined thresholds
- Delivers critical alerts based on independent user-defined thresholds
- Allows users to define the time period for in-depth analysis (last hour, 24 hours, 7 days, 30 days or custom)
- Delivers warnings and alarms via email, SNMP and remote syslog server

HSM compatibility

- nShield Edge, Solo+, Solo XC, Connect+ and Connect XC with Security World software v12.40 and higher



[LEARN MORE AT ENTRUST.COM/HSM](https://www.entrust.com/HSM)



nShield Monitor

Role-based access control

- Supports three distinct roles – administrator, group manager and auditor
- Distinct set of tasks applicable to each role supporting clear separation of duties
- Enhances security in terms of configuration and administration for overall nShield Monitor system
- Administrator manages deployment
- Group manager controls monitoring of HSMs
- Auditor views data and reports

Solution components

- nShield Monitor is provided in open virtual appliance (OVA) format and the Microsoft Hyper-V format
- Web based management interface and command line interface (CLI)
- Firefox, Internet Explorer and Chrome browser support
- Flexible endpoint licensing mechanism supporting up to 500 HSMs

Virtual appliance min specification

- 2 CPUs with 2 cores each
- 8 GB RAM
- Thin provisioned hard drives
- Hypervisor compatibility

- The OVA can be installed on the following virtual platforms:
 - vSphere ESXi 6.0, ESXi 6.5
 - VMware Workstation 12, 14
 - VMware Fusion 10
 - Oracle VirtualBox 6.0
- Hyper-V image can be installed on the following virtual platforms:
 - Microsoft Hyper-V, Azure

Security

- Web server certificate management providing client browser to nShield Monitor authentication as part of session establishment
- Secure segregation of roles and responsibilities for administrators and group managers
- Strong password policy - control of expiry and auto-logout duration
- Choice of algorithms for authentication and privacy
- Uses SNMP v3 for nShield Monitor-to-HSM connectivity

Learn more

To find out more about Entrust nShield HSMs visit [entrust.com/HSM](https://www.entrust.com/HSM). To learn more about Entrust's digital security solutions for identities, access, communications and data visit [entrust.com](https://www.entrust.com)



Learn more at

[entrust.com/HSM](https://www.entrust.com/HSM)



ENTRUST

Contact us:

HSMinfo@entrust.com