Nexus OCSP Responder requirements and interoperability

This article provides installation requirements and interoperability data for Nexus OCSP Responder.

Expand/Collapse All

This article is valid from Nexus OCSP Responder 6.1.

Requirements

	Minimum
CPU	Quad Core 2.4 GHz
Disk size	20 GB
Memory	4 GB RAM
HSM	64-bit PKCS#11-driver

Nexus OCSP Responder scales well with a server of multiple cores. More memory can be required when many logical responders are hosted in a single server instance and large CRLs are loaded by the responder. For load tests, also consider the HSM performance to not introduce a bottle-neck. Performance is affected by the Nexus OCSP Responder signing key length.

The following operating systems are supported:

- CentOS 7, 8
- Red Hat Enterprise Linux 7, 8
- SUSE Linux Enterprise Server 15
- OpenSUSE Leap 15
- Microsoft Windows 2012 Server
- Microsoft Windows 2016 Server
- Microsoft Windows 2019 Server

The following software is supported:

- 64-bit Java Runtime Environment (JRE) version 11.
- Nexus OCSP Responder is compatible with both OpenJDK and Oracle Java.

It is important that all participants in a PKI use the same time standard. Specifically Nexus OCSP Responder has to agree on the time with the CAs issuing CRLs/CILs and with the OCSP clients.

Make sure these clocks are synchronized, that is, the participants are using a synchronization protocol such as Network Time Protocol, NTP.

Interoperability

A PKCS#11 compliant device can be used for handling of CA key pairs, system keys, protection of archived keys, and for key generation.

For functional specifications, known issues and limitations related to current PKCS#11 drivers, see each HSM vendor's web site.

The following devices are explicitly verified:

- AEP Systems Sureware Keyper, FIPS 140-1 level 4
- Atos Bull Trustway Proteccio NetHSM

Related information

- Nexus OCSP Responder
- Install and upgrade Nexus OCSP Responder

    - Note: Only verified with CIS, not with CCM and KAR.
- DocuSign ARX PrivateServer
- Gemalto SafeNet ProtectServer Internal - Express 2
- Gemalto SafeNet ProtectServer External 2
- Gemalto SafeNet Luna CA3, FIPS 140-1 lvl 3
- Gemalto SafeNet Luna CA4, FIPS 140-2 lvl 3
- Gemalto SafeNet Luna SA 4.4, FIPS 140-2 lvl 3
    - Note: Since SafeNet Luna disallow key export when in FIPS mode, enable non-FIPS mode for use with CM KAR, Key Archiving and Recovery.
- Gemalto SafeNet Luna SA 5.0, FIPS 140-2 lvl 3
    - Note: Since SafeNet Luna disallow key export when in FIPS mode, enable non-FIPS mode for use with CM KAR, Key Archiving and Recovery.
- Gemalto SafeNet Luna G5
- Gemalto SafeNet Luna HSM 6
- Gemalto SafeNet Luna Network HSM 7
- Gemalto SafeNet Luna PCIe HSM 7
- IBM 4758, FIPS 140-1 level 3 and 4
- Nitrokey HSM 2
- Thales nShield Connect+, FIPS 140-2 level 3
- Thales nShield Solo+, FIPS 140-2 level 3
- Thales nShield Edge
- Thales WebSentry PCI, FIPS 140-1 level 4
- Thales WebSentry Ethernet, FIPS 140-1 level 4
- Utimaco CryptoServer Security Server CS 10/50 LAN/PCI, FIPS 140-2 level 3 (level 4 for physical)
- Utimaco CryptoServer Security Server Se 12/52/420/1200 LAN/PCI, FIPS 140-2 level 3
- Yubico YubiHSM 2

⚠ PIN decryption is not allowed using a FIPS mode HSM.

The following key types and corresponding signature algorithms in certificate, CA, CRL, CIL, and responder certificate are supported:

Key types

- RSA
- RSASSA-PSS
- EC
- Edward

Algorithms

- SHA-1
- SHA-2
- ECDSA
- EDDSA