



NSP

Network Services Platform

Release 24.8

Security Hardening Guide

3HE-20027-AAAB-TQZZA
Issue 1
August 2024

© 2024 Nokia.

Use subject to Terms available at: www.nokia.com/terms

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2024 Nokia.

Contents

- About this document.....5**
- 1 NSP OS security.....7**
 - 1.1 Host OS hardening.....7
- 2 Database security9**
 - 2.1 Database hardening for classic management.....9
- 3 Kubernetes security.....11**
 - 3.1 Kubernetes hardening11
- 4 Communications and network security13**
 - 4.1 Network and mediation13
 - 4.2 Transport Layer Security (TLS).....15
 - 4.3 Artifact signatures19
- 5 NSP user security21**
 - 5.1 NSP user authentication21
 - 5.2 NSP User Access Control (UAC)22
 - 5.3 Login banner customization23
- 6 NE security25**
 - 6.1 Encryption25
- 7 RHEL OS security hardening27**
 - 7.1 NSP support for RHEL 8 CIS benchmark recommendations27
 - 7.2 RHEL sudoer configuration56
- 8 Data privacy summary59**
 - 8.1 NSP network and user data privacy59
- 9 NSP interface cryptography65**
 - 9.1 Algorithms per NSP component.....65

About this document

Purpose

The *NSP Security Hardening Guide* is a reference document for increasing NSP security at the physical, OS, transport, user, and application levels.

Scope

The scope of this document is limited to describing the security hardening requirements and recommendations for an NSP deployment. In order to provide context for hardening practices, the guide also describes rigidly enforced security measures that are built into the product.

Document support

Customer documentation and product support URLs:

- [Documentation Center](#)
- [Technical support](#)

How to comment

Please send your feedback to [Documentation Feedback](#).

1 NSP OS security

1.1 Host OS hardening

1.1.1 General OS hardening measures

The following general OS hardening measures are recommended:

- Install a clean operating system environment with the minimum required packages as described in the *NSP Installation and Upgrade Guide*.
- Install the latest Recommended Patch Cluster from Red Hat (apply the patches supplied by Nokia for the NSP RHEL OS qcow2 image).
- Nokia supports customers applying RHEL, or Windows patches provided by Red Hat, which include security fixes as well as functional fixes. If a patch is found to be incompatible with NSP/NFM-P, the patch may need to be removed until a solution to the incompatibility is provided by Red Hat or Nokia. Consult the *Host Environment Compatibility Reference for NSP and CLM* for up-to-date information about the recommended RHEL maintenance update and patch levels. Operating system patches of NSP-provided RHEL OS qcow2 images must be obtained from the NSP product group. Nokia supports only Nokia-provided RHEL OS disk images and OS patch bundles for qcow2 / OVA.
- Harden the RHEL operating system installation based on the CIS best practices described in [Chapter 7, “RHEL OS security hardening”](#). The NSP RHEL OS qcow2 image is hardened in accordance with these supported CIS requirements only.
- The system clocks of the NSP components must always be closely synchronized. The RHEL chronyd service is the mandatory time-synchronization mechanism to engage on each NSP component during deployment. For availability reasons, redundant external servers must be accessible to the NSP.
- Disable mDNS.
- NSP components have no ingress or egress requirements to access the public Internet; hosts must be isolated with correctly configured firewalls. See “NSP Port Communications” in the *NSP Planning Guide* for information.
- Enable restricted root access to the NSP deployment, as described in [7.2.2 “Restricted root-user access”](#) (p. 56).

 **Note:** An NSP station cannot serve as a time-synchronization source.

1.1.2 RHEL CIS OS benchmarks

Operating System security hardening is a broad topic with a great many possible customization options. The NSP supports hardening recommendations from the Center for Internet Security (CIS). Only hardening recommendations that are described as being supported may be applied to a RHEL OS instance that hosts any NSP software.

Nokia does not recommend applying additional OS security hardening measures, as these can affect NSP operation, support, and product upgrades. Basic customer testing is required to verify

that any additional platform hardening does not affect NSP operation. The NSP Product Group makes no commitment to making the NSP compatible with specific customer hardening requirements.

See [Chapter 7, “RHEL OS security hardening”](#) for information about the NSP support levels for specific RHEL CIS benchmarks.

1.1.3 NSP RHEL OS disk images

The Nokia-provided RHEL OS disk images are based upon RHEL 8 and are available for KVM and Openstack hypervisors. An NSP RHEL OS image can be used only for the deployment of NSP software, and not for the deployment of any other Nokia or third-party product.

An application that Nokia does not sanction must not be deployed on any OS instance that hosts an NSP component. Nokia reserves the right to remove any applications that are suspected of affecting NSP operation.

1.1.4 SELinux

The NSP supports RHEL SELinux for enhanced system security and logging functions. See the *NSP System Administrator Guide* for information about SELinux implementation and management in the NSP, and the RHEL documentation for comprehensive SELinux configuration and implementation information.

All NSP system elements support SELinux in enforcing mode, except for an auxiliary database, which supports only permissive mode.

1.1.5 Sudoer file configuration

Some NSP components create rules in RHEL sudoers.d directories during installation. These rules allow NSP functions to run certain programs required for NSP operations. Rule files can be found in the `/etc/sudoers.d/` directory and rule entries apply to NSP users. See [7.2 “RHEL sudoer configuration” \(p. 56\)](#) for more information.

Also

2 Database security

2.1 Database hardening for classic management

2.1.1 Security recommendations

If an NSP deployment includes classic management, Nokia recommends the following:

- Enable IP validation on each main database. IP validation restricts the components that have database access to only those required. See the *NSP Installation and Upgrade Guide* for more information.
- Enable Oracle database error monitoring. Oracle database errors provide monitoring information that may help with troubleshooting or the detection of security violations, such as SQL injection attacks. When database error monitoring is enabled, the NFM-P raises an alarm when the Oracle software reports an error, such as an invalid SQL statement.

3 Kubernetes security

3.1 Kubernetes hardening


3.1.1 Pod Security Admission (PSA) for Kubernetes cluster

Kubernetes PSA standards define different isolation levels for pods. The PSA controller is a built-in feature of Kubernetes that enforces pod security standards. Pod security restrictions are applied at the namespace level when pods are created. Pod security standards define three different policies (described below) to broadly cover the security spectrum.

Namespaces can be labelled to enforce the following pod security standards:

- **Privileged**—unrestricted policy that provides the widest possible level of permissions. This policy allows for known privilege escalations.
- **Baseline**—minimally restrictive policy that prevents known privilege escalations. Allows the default (minimally specified) pod configuration.
- **Restricted**—heavily restricted policy that follows current pod hardening best practices.

NSP deploys pods in three namespaces that map to the pod security standards listed above. The namespace labels are configurable from the NSP deployer using attributes defined under the *kubernetes* section of *nsp-config.yml*.

 **Note:** Most pods in the NSP cluster are deployed using the restricted pod security standard, however, certain pods require additional privileges and must be deployed with a less restrictive pod security standard.

4 Communications and network security

4.1 Network and mediation

4.1.1 Network separation

Nokia recommends configuring multiple NSP network interfaces to segregate different types of NSP traffic. You can segregate NSP client, mediation, and internal traffic by configuring the NSP to use interfaces in separate networks for each traffic type.

The multi-interface implementation isolates different traffic types to one or more of the following networks:

- client—for GUI, OSS, REST, and browser clients, and clients such as Kafka subscribers
- mediation—for direct communication with managed NEs
- internal—for communication such as the following:
 - traffic within an NSP cluster
 - communication with NSP components and other systems for example, the VSR-NRC, NFM-P, and NSP auxiliary databases
 - traffic related to NSP DR functions such as data replication and keep-alive messaging between data centers


Using separate networks allows for additional security policies. For example, the NSP PostgreSQL service is an internal service with NSP components as the only legitimate clients; northbound browser or API clients are not applicable to this service. To help secure the PostgreSQL service from unintended access, you could apply a firewall rule to block the PostgreSQL port on the northbound client interface.

To accommodate a deployment environment that hosts only one network, the use of multiple NSP network interfaces is optional. When the NSP uses only one network for all communication, the NSP client traffic shares the same network as the NE management traffic and the communication between NSP components. This type of configuration can pose a considerable security risk.

4.1.2 Firewall configuration

An NSP deployment has no ingress or egress requirement for access to the public Internet; each NSP host must be isolated using a properly configured firewall.

The NSP supports firewall deployment on all NSP host interfaces, however, firewall support among system components may vary. Components such as the NFM-P or WS-NOC that have multiple system elements may have additional firewall requirements. See the *NSP Planning Guide* and any specific component planning documentation, as required, for firewall port requirements and restrictions.

 **Note:** Firewall deployment between the members of an NSP cluster is not supported.

4.1.3 Mediation

The following is a summary of recommendations for mediation security:

- Enable secure transport protocols with CLI, NETCONF, and gRPC mediation. Similarly, use SCP or SFTP instead of clear file transfer equivalents such as TFTP and FTP.
- SNMPv3 supports authentication and encryption and is recommended for security reasons over SNMPv1/v2. SNMPv1/v2 provides no confidentiality and must be avoided.
- The mandatory RHEL chronyd service ensures that timestamps of logged activity are synchronized with other network elements. This is especially useful for precisely identifying timelines when troubleshooting an event or issue.
- Segregate the traffic between the NSP and managed NEs in a separate network.

SSH

The NSP supports strong SSH cryptographic algorithms by default. The default algorithms are updated as required to account for changes in the security level of specific algorithms.

SNMP

When SNMP mediation is required, SNMPv3, which supports authentication and encryption, is strongly recommended over SNMPv1/v2.

The SNMP recommendations are:

- Configure SNMPv3 to use both authentication and privacy protocols. This enables authentication and encryption features, and enhances overall network security.
- Ensure that administrative credentials are properly configured with different passwords for authentication and encryption.

Lawful Intercept and data privacy

An NSP system that includes classic management can act as an optional remote controller for Lawful Intercept (LI) functions on SNMP devices that have native LI support. LI is a highly secure function that is built into the device hardware; the NSP LI capabilities are limited to LI target specification, and enabling or disabling LI on a target.

As a remote controller, the NSP has no visibility of intercepted traffic; see “Lawful Intercept concepts” in the *NSP NFM-P Classic Management User Guide* for more information.

gRPC

When gRPC mediation is required, the NSP gRPC client can be configured to use two-way TLS to protect communication between NSP and the NEs; see the *NSP System Administrator Guide* for configuration information.

The gRPC recommendations are:

- Ensure that the "Secure" attribute slider is enabled when the gRPC mediation policy is created.
- Enable TLS communication between MDM and managed NEs by importing the NEs self-signed TLS certificate into each MDM truststore. The NE certificate files must be transferred to the NSP over a secure connection.

NETCONF or CLI

When NETCONF or CLI mediation is required, Telnet or SSH may be used as the transport protocol.

The NETCONF and CLI recommendations are:

- Telnet is unsecure and must be avoided. Enable SSH2 transport protocol when the NETCONF or CLI mediation policy is created.

VSR-NRC communication to the network

See the following documentation references for information about VSR-NRC communication to the network.

IP Routing Protocols

See “Unicast routing and MPLS” in the *VSR-NRC Security Best Practices and Hardening Guide*.

PCEP

See “PCEP over TLS” in the *Segment Routing and PCE User Guide*.

4.2 Transport Layer Security (TLS)

4.2.1 TLS support

Transport Layer Security, or TLS, is a cryptographic protocol for establishing encrypted communication between a client and server. NSP supports TLSv1.2 protocol by default. While not recommended, administrators can still enable TLSv.1.1 and/or TLSv1.0 in NFM-P on certain external interfaces, such as OSS clients. Upgrading legacy clients to support TLSv1.2 is preferable to enabling TLSv.1.1 and/or TLSv1.0 in NFM-P.

i **Note:** The ability to enable unsecure protocols in NSP will be removed with little notice in a future release.

i **Note:** Outdated TLS versions present a security risk and are disabled by default in NSP. Customers that enable older unsecure TLS protocols do so at their own risk. TLSv1.2 is the recommended version.

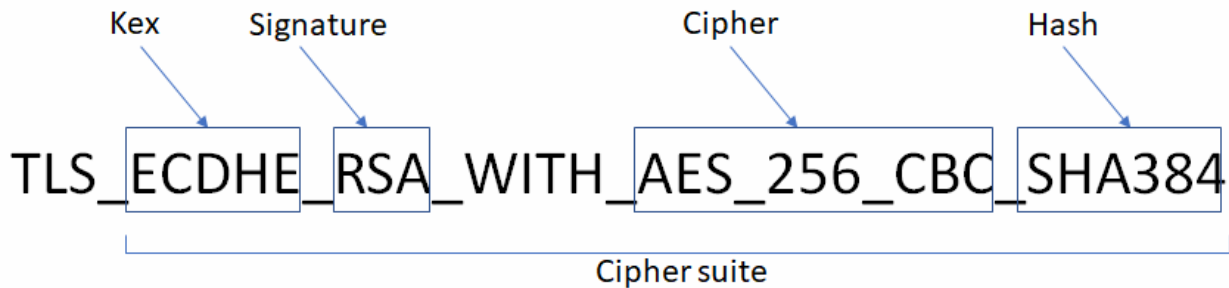
4.2.2 Cipher suites

Cipher suites define a set of cryptographic algorithms for each TLS connection. During cipher suite negotiation, both server and client must agree on the same cipher suite in order to establish a connection. A cipher suite defines the combination of key exchange, authentication, encryption, and integrity algorithms for the TLS connection.

- Key exchange (asymmetric cipher): Ex. ECDHE, DHE, RSA
- Authentication (signature/certificate type): Ex. RSA, DSA, ECDSA
- Confidentiality (symmetric cipher): Ex. AES_256_CBC, AES_256_GCM
- Integrity (hash): Ex. SHA384, SHA256, SHA

The following example displays the format of a TLS cipher suite.

Figure 4-1 TLS cipher suite example



NSP supports strong TLSv1.2 cipher suites by default. The default list of supported cipher suites may be updated in future releases to account for changes in the security level of cryptographic algorithms.

4.2.3 Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy (PFS) is a feature of certain key agreement protocols in which there is no link between the server's private key and each session key. Therefore, if an attacker gains access to a server private key, the attacker cannot use the private key to decrypt any archived TLS sessions. Cipher suites prefixed with "TLS_DHE" and "TLS_ECDHE" support PFS.

i **Note:** Exercise caution when removing TLS cipher suites; incompatible cipher suites prevent NSP system access from browser and OSS clients.

4.2.4 Authenticated Encryption with Additional Data (AEAD)

In general, TLSv1.2 ciphers compute a mac over the plaintext then the authenticated payload is encrypted. Although highly unlikely in an NSP environment, this "mac-then-encrypt" approach could open the possibility for some sophisticated padding attacks. Authenticated Encryption with Additional Data (AEAD) is a special class of ciphers that combines encryption and integrity into one operation (ie. mac-and-encrypt). These ciphers compute mac and encrypt simultaneously which can mitigate padding attacks. In NSP, AEAD cipher suites are supported with TLSv1.2. These cipher suites are identified with Galois Counter Mode algorithms (ie. AES-GCM) and CHACHA20_POLY1305.

4.2.5 ECC curves

For cipher suites using EC based DHE key exchange, NSP supports standard TLS curves.

4.2.6 Diffie-Hellman Parameters

For cipher suites using non-EC based DHE key exchange, NSP supports 2048-bit DH parameters. Clients that do not support 2048-bit DH modulus cannot connect to NSP with a DHE cipher.

NSP clusters do not offer any cipher suites supporting DHE key exchange.

4.2.7 Cipher Preference

Certain attacks on TLS server's can be mitigated by enforcing the server's cipher order instead of allowing the client to choose the cipher. NSP server interfaces accessible by external TLS clients are configured to enforce server-side cipher order.

4.2.8 Cipher Customization

NFM-P supports the ability for administrators to customize the list of supported TLS cipher suites. The default list of cipher suites provides a balance of algorithm strength and compatibility. That said, NFM-P administrators may still chose to customize the list of supported cipher suites. See the *NSP System Administrator Guide* for more information about updating TLS versions and ciphers.

i **Note:** Exercise caution when customizing TLS protocols/cipher suites. Incompatible cipher suites will prevent NSP/NFM-P system access from browser and OSS clients.

4.2.9 TLS certificates

NSP currently supports RSA certificates. ECC certificates may be supported in the future. DSA certificates are not supported.

i **Note:** Certificates with RSA key size of 2048-bits are recommended.

NSP PKI server

The NSP PKI server is a standalone utility that signs TLS certificate signing requests (CSRs) from requesting entities in an NSP system. The NSP PKI server utility is mandatory and is used sign TLS certificates for internal services used by NSP components. It can also be optionally used to sign TLS certificates presented by NSP to external clients (ie. Automated TLS deployment) when a custom NSP certificate is not provided. The PKI server must continue to run until the installation of all products and NSP components that use the PKI server is complete. Root user privileges are required on the station where the PKI server utility is run.

i **Note:** The PKI server utility only needs to run during installation of NSP components. After installation is complete, the NSP PKI server utility must be stopped.

Certificates signed by the NSP PKI server have the following characteristics:

- Signature Algorithm: sha256WithRSAEncryption
- RSA key length: 2048-bit
- Validity period: configurable at NSP PKI initialization
- Organization Name: configurable at NSP PKI initialization
- Country Name: configurable at NSP PKI initialization
- State or Province Name: configurable at NSP PKI initialization

During NSP deployment, a CSR is sent to a local PKI server, which returns a signed certificate. The NSP uses a server certificate and key to 'seed' a local copy of the PKI utility, which is active long enough to sign the pod certificates.

i **Note:** The PKI server is intended for use by NSP components only.

Certificate Expiry

NSP TLS certificate replacement may be required when:

- a component is added to the NSP system
- a system IP/hostname changes
- a TLS certificate nears or reaches expiry

An NSP/NFM-P checks the expiry date of each local TLS certificate during installation, and every 24 hours thereafter. If a certificate is expired or approaching expiry, the NSP raises one of the following *SSLKeystore* or *SSLClientKeystore* alarms:

- Warning, if the certificate is to expire within 30 days of the current time
- Critical, if the certificate is to expire within 7 days of the current time
- Critical, if the certificate is expired

NFM-P expiry alarms are shown in the NSP and the Alarm Window of the NFM-P GUI.

Configuring advance warning for certificate expiry

Administrators must carefully monitor and refresh NSP TLS certificates before expiry. If certificates expire, some NSP functions that depend on secure communication may be inoperable. For example, NSP clients may be completely unable to connect to the NSP.

Using the NSP and NFM-P GUI, administrators can configure alarm policies (referred to in the NSP as “e-mail policies” and the NFM-P as “alarm e-mail policies”) to ensure that advance warning emails are sent for certificate expiry events. For example, an NSP policy containing an advanced filter for “*Alarm Name equals SSLKeystoreCertificateExpiring*” sends an email to the recipient list when the NSP raises the initial warning alarm for TLS certificate expiry.

See the *NSP Network and Service Assurance Guide* or *NSP System Administrator Guide* for more information about configuring alarm e-mail policies, depending on platform installation type.

Certificate revocation

Certificate revocation is a mechanism, normally for clients, to identify and reject connections to a server with a revoked certificate. The primary use-case for revoking a server's certificate is if the private key of server or CA has been compromised. Clients have two options to determine when a server's certificate has been revoked:

- Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP)

The client-side mechanisms listed above have some drawbacks related to performance and privacy. OCSP 'stapling' is an attempt to avoid these drawbacks by moving the revocation check to the server. The NSP does not support OCSP 'stapling'.

4.3 Artifact signatures

4.3.1 Self-signing artifact bundles

NSP supports self-signing for customer-created artifact bundles to verify that installed artifacts come from trusted sources. Once you have created a key pair and loaded the secret file into Kubernetes, you can use the artifact-bundle-builder tool to create signed artifact bundles. See the *NSP System Administrator Guide* for more information about artifact administration.

5 NSP user security

5.1 NSP user authentication

5.1.1 Basic elements

The NSP user-authentication mechanism, OAUTH2, provides the following single sign-on (SSO) functions:

- local and remote user authentication
- configurable login protection

“Configuring single sign-on” in the *NSP Installation and Upgrade Guide* describes the NSP SSO functions and parameters.

5.1.2 OAUTH2

OAUTH2 is an implementation of the Keycloak open-source identity and access-management solution that employs the standard OAuth 2.0 protocol. OAUTH2 maintains a local user database, supports remote users, and can temporarily or permanently lock out users to prevent brute-force or random-guess attacks.

5.1.3 Local user authentication

NSP local user authentication uses robust password encryption, and has rules that govern the password change and complexity requirements.

Password encryption

A one-way cryptographic hash is applied to all NSP user passwords stored in the local database. The encryption protects against an accidental or intentional database disclosure, as the password cannot be decrypted. To further mitigate against password attacks, a randomized salt is added to each user password before the one-way cryptographic hash is applied.

Password complexity

User password complexity rules are configurable; the following are the defaults, which state that a password must:

- be at least ten characters
- not be the same as the previous three passwords
- include at least one of the following special characters
() ? ~ ! @ # \$ % & * _ +
- include at least one lowercase character
- include at least one uppercase character
- include at least one digit
- not be the username

- not equal the email address

Password changes

One administrator account is created by default during NSP system installation. During the initial administrator login using the default password, the user is prompted to change the password. The creation of additional local users includes an option to force the user to change the password during the initial login.

i **Note:** Nokia recommends that you enable the initial password-change option.

5.1.4 Remote user authentication

The NSP supports LDAP/S, RADIUS, and TACACS+ remote user access. The NSP cannot authenticate NFM-P remote users, but can import NFM-P users to the NSP local user database.

See the *NSP Installation and Upgrade Guide* for remote-user configuration information.

i **Note:** If LDAP is used for remote access, it is strongly recommended that you use LDAPS to secure the LDAP communication.

5.1.5 Login protection

You cannot enable both temporary and permanent user lockout; if user lockout is to be enforced, only one mechanism can be active at any time.

i **Note:** Temporary user lockout is enabled by default.

i **Note:** Nokia recommends deploying the NSP with brute-force protection enabled and the parameters configured in accordance with your security policy.

5.1.6 Session controls

To enhance security, an idle session timeout and token lifespan can be applied. The timeout and lifespan apply to NSP SSO and REST sessions:

i **Note:** Functions that require near-real-time event updates communicate continuously with the NSP, so do not time out from inactivity.

You are encouraged to assess the number of concurrent sessions that your deployment requires, and to set the maximum allowed number to the lowest value that meets the requirement.

5.2 NSP User Access Control (UAC)

5.2.1 User groups and roles

NSP UAC is an optional mechanism that enables an NSP administrator to define user access rights to NSP functions and data. When UAC is disabled, the NSP user access is unrestricted.

The NSP enables you to define resource groups that contain NSP data-model objects; for example, equipment and service components. The NSP also enables the creation of user groups and roles. A role, which is assigned to a user group, can be given read, write, or execute permission to specific

functions and resource groups. Consequently, an NSP user has the access defined in a role to only the resources in the associated resource groups.

A UAC resource group can include objects such as the following:

- service—IP links, services, service sites, service endpoints, service bindings
- equipment—chassis, LAGs, devices
- KPI—NE and service performance indicators
- Analytics—Analytics resources

5.3 Login banner customization

5.3.1 Customizing the NSP login banner

A login banner warns or advises a user during a login attempt of the acceptable system use policies. In general, such a banner must warn unauthorized users not to proceed, and display a clear statement about system logging and monitoring to detect unauthorized use or access. It is recommended that you configure an NSP login banner in accordance with your security policy.

An NSP administrator can create a customized security statement that is presented to the NSP operator at each NSP login attempt. An administrator can optionally force operator acknowledgement of the security statement.

The *NSP System Administrator Guide* describes how to enable and configure the NSP login banner, which is disabled by default.

6 NE security

6.1 Encryption

6.1.1 MACsec Pre-Shared Keys (PSK)

The NFM-P may optionally be used to configure MACsec PSKs for encrypted switch-to-switch connectivity between supported NEs. Each Security Association in the NE contains a Single Secret Key (SAK) where the cryptographic operations used to encrypt the datapath PDUs. SAK is the secret key used by an SA to encrypt the channel.

A pre-shared key may be created by NSP. Each PSK is configured with two fields:


- Connectivity Association Key Name
- Connectivity Association Key (CAK) value

The NFM-P can be configured with scheduled hitless re-keying of PSK.

The NFM-P supports two sources for keying material:

1. Local: PSK is generated locally
2. Hardware Security Module (HSM): PSK is generated by a supported HSM; see the *NSP NFM-P Network Element Compatibility Guide* for a list of supported HSMs


Before an HSM can be used for key management, the HSM must be added to the NFM-P configuration. See the *NSP System Administrator Guide* for more information.


 **Note:** The NFM-P does not store CAKs generated by an HSM

 **Note:** For increased security, Nokia recommends scheduling periodic re-keying of PSK.

6.1.2 Network Group Encryption

The NFM-P may optionally be used to deploy Network Group Encryption (NGE) attributes to NEs. The NFM-P uses SNMP to deploy general NGE attributes to NEs, and SSH2 sessions to configure the key values. You can use an existing SSH2 user account on each NE, or, to facilitate the tracking of key value configuration activity, you can use the User NGE account. The NFM-P creates the account on each participating NGE NE and uses the account only for creating and updating key values. The NFM-P user activity log records all NGE configuration activity.

 **Note:** To facilitate the tracking of key value configuration activity, use the "User NGE" account on each NE.

 **Note:** For increased security, Nokia recommends using a scheduled task for the regular and automatic replacement of the keys in the key group.

6.1.3 FIPS

The NFM-P supports Federal Information Processing Standards (FIPS) for NE management and client communication. See the *NSP Installation and Upgrade Guide* for information about enabling FIPS.

7 RHEL OS security hardening

7.1 NSP support for RHEL 8 CIS benchmark recommendations

7.1.1 Overview

The NSP can be installed and operate on a RHEL 8 OS that is hardened in accordance with the supported recommendations in this chapter.

The following are within the support scope:

- NSP
- NFM-P

[Table 7-1, “NSP support levels, CIS RHEL 8 recommendations” \(p. 28\)](#) describes the NSP support for the Center for Information Security (CIS) Red Hat Enterprise Linux 8 Benchmark, version 1.0.1.

CIS profiles

The following CIS compliance profiles are referenced:

- Level 1—Server, or L1:

Intent of recommendations is to:

- be practical and prudent
- provide clear security benefit
- not inhibit utility of technology beyond acceptable degree

- Level 2—Server, or L2:

Extension of L1 profile; recommendations have one or more of the following characteristics:

- intended for environments or use cases in which security is crucial
- considered intensive defense measure
- may inhibit technology utility or performance

i **Note:** It is strongly recommended that you maintain a log of the configuration changes that affect the CIS benchmark support. Such a log may be of great value during system troubleshooting. Each log entry must be dated and include the configuration details.

RHEL OS deployment types

The following columns in the support provided by the following NSP-supported RHEL OS deployments:

- **Manual OS installation**—OS deployed manually as described in NSP product documentation
- **Container host image**—OS for NSP deployer host or cluster VM deployed using NSP qcow or OVA disk image
- **Component host image**—OS for NSP component outside NSP cluster deployed using NSP qcow or OVA disk image

Support levels

The following indicate the level of support for a recommended configuration:

- **S**—supported; also implemented by default in NSP qcow2 and OVA images
- **S/ND**—supported; not implemented by default in NSP qcow2 or OVA image
- **NI**—no expected impact; explicit recommendation not tested, but no effect on system functions foreseen

Note: It is strongly recommended that you test such a configuration to ensure that system operation is unaffected; no commitment is offered to ensure product compatibility with a specific requirement.

- **P**—partially supported; conditional support provided as described in Notes column; conditional support implemented by default in NSP qcow2 and OVA images.
- **P/ND**—partially supported; conditional support provided as described in Notes column; conditional support not implemented by default in NSP qcow2 or OVA image
- **NS**—not supported; recommendation incompatible with product requirements
- **n/a**—not applicable

Table 7-1 NSP support levels, CIS RHEL 8 recommendations

Recommendation	CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1	Initial Setup				
1.1	Filesystem Configuration				
1.1.1	Disable unused filesystems				
1.1.1.1	L1	S			—
1.1.1.2	L2	S	n/a		—
1.1.1.3	L1	S			—
1.1.1.4	L1	S			—
1.1.2	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.1.3	Ensure nodev option set on /tmp partition (Automated)	L1	S			—
1.1.4	Ensure nosuid option set on /tmp partition (Automated)	L1	S			—
1.1.5	Ensure noexec option set on /tmp partition (Automated)	L1	S			—
1.1.6	Ensure separate partition exists for /var (Automated)	L2	S			Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP deployment documentation
1.1.7	Ensure separate partition exists for /var/tmp (Automated)	L2	S			Customer determines appropriate partition size; disk space cannot be taken from partitions defined in NSP deployment documentation
1.1.8	Ensure nodev option set on /var/tmp partition (Automated)	L1	S			—
1.1.9	Ensure nosuid option set on /var/tmp partition (Automated)	L1	S			—
1.1.10	Ensure noexec option set on /var/tmp partition (Automated)	L1	S			—
1.1.11	Ensure separate partition exists for /var/log (Automated)	L2	S			—
1.1.12	Ensure separate partition exists for /var/log/audit (Automated)	L2	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.1.13	Ensure separate partition exists for /home (Automated)	L2	S			—
1.1.14	Ensure nodev option set on /home partition (Automated)	L1	S			—
1.1.15	Ensure nodev option set on /dev/shm partition (Automated)	L1	S			—
1.1.16	Ensure nosuid option set on /dev/shm partition (Automated)	L1	P	S	NS	Not supported in NSP RHEL qcow2/OVA or for NFM-P database stations
1.1.17	Ensure noexec option set on /dev/shm partition (Automated)	L1	P	S	NS	Not supported in NSP RHEL qcow2/OVA or for NFM-P database stations
1.1.18	Ensure nodev option set on removable media partitions (Manual)	L1	S	n/a		Not applicable to NSP qcow2/OVA, which lacks removable partitions
1.1.19	Ensure nosuid option set on removable media partitions (Manual)	L1	S	n/a		Not applicable to NSP qcow2/OVA, which lacks removable partitions
1.1.20	Ensure noexec option set on removable media partitions (Manual)	L1	S	n/a		Not applicable to NSP qcow2/OVA, which lacks removable partitions
1.1.21	Ensure sticky bit is set on all world-writable directories (Automated)	L1	P	NS	S	Not supported on NSP Kubernetes deployer, cluster nodes.
1.1.22	Disable Automounting (Automated)	L1	S			—
1.1.23	Disable USB Storage (Automated)	L1	S			—
1.2	Configure Software Updates					

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.2.1	Ensure Red Hat Subscription Manager connection is configured (Manual)	L1	S	n/a		Not applicable to NSP qcow2/OVA; patch updates provided only via NSP RHEL update patch bundle
1.2.2	Disable the rhnsd Daemon (Manual)	L1	S			—
1.2.3	Ensure GPG keys are configured (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA Nokia digitally signs each NSP software RPM file using GNU Privacy Guard, or GPG, which enables you to ensure the integrity of a file before use. See the <i>NSP Installation and Upgrade Guide</i> for information about importing NSP GPG keys.
1.2.4	Ensure gpgcheck is globally activated (Automated)	L1	S			—
1.2.5	Ensure package manager repositories are configured (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA; NSP RHEL qcow2/OVA OS updates provided only via NSP RHEL update patch bundle.
1.3	Configure sudo					
1.3.1	Ensure sudo is installed (Automated)	L1	S			See 7.2 “RHEL sudoer configuration” (p. 56) .
1.3.2	Ensure sudo commands use pty (Automated)	L1	S			—
1.3.3	Ensure sudo log file exists (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation	CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.4	Filesystem Integrity Checking				
1.4.1	Ensure AIDE is installed (Automated)	L1	S		—
1.4.2	Ensure filesystem integrity is regularly checked (Automated)	L1	NS		AIDE initialization and execution cause increased disk I/O and CPU usage that reduce performance; the risk of causing NSP service disruption prevents NSP support for AIDE.
1.5	Secure Boot Settings				
1.5.1	Ensure permissions on bootloader config are configured (Automated)	L1	S		—
1.5.2	Ensure bootloader password is set (Automated)	L1	S		—
1.5.3	Ensure authentication required for single user mode (Automated)	L1	S		—
1.6	Additional Process Hardening				

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.6.1	Ensure core dumps are restricted (Automated)	L1	S	S/ND		<p>Disabling core dumps may adversely affect ability to provide NSP customer support</p> <p>The risk associated with compromising customer support capabilities must be accepted unless core dumps are enabled for the following RHEL users, as recommended by Nokia:</p> <ul style="list-style-type: none"> • root • nsp • samadmin • oracle • td-agent • samauxdb • kube • etcd
1.6.2	Ensure address space layout randomization (ASLR) is enabled (Automated)	L1	S			—
1.7	Mandatory Access Control					
1.7.1	Configure SELinux					
1.7.1.1	Ensure SELinux is installed (Automated)	L2	S			—
1.7.1.2	Ensure SELinux is not disabled in bootloader configuration (Automated)	L2	S			—
1.7.1.3	Ensure SELinux policy is configured (Automated)	L2	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.7.1.4	Ensure the SELinux state is enforcing (Automated)	L2	P	P/ND		SELinux is enabled in permissive mode by default on NSP RHEL qcow2/OVA. SELinux is supported only in permissive mode on auxiliary database cluster stations. See “SELinux administration” in the <i>NSP System Administrator Guide</i> for configuration information.
1.7.1.5	Ensure no unconfined services exist (Automated)	L2	S			—
1.7.1.6	Ensure SETroubleshoot is not installed (Automated)	L2	S			—
1.7.1.7	Ensure the MCS Translation Service (mcstrans) is not installed (Automated)	L2	S			—
1.8	Warning Banners					
1.8.1	Command Line Warning Banners					
1.8.1.1	Ensure message of the day is configured properly (Automated)	L1	S			—
1.8.1.2	Ensure local login warning banner is configured properly (Automated)	L1	S			—
1.8.1.3	Ensure remote login warning banner is configured properly (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.8.1.4	Ensure permissions on /etc/motd are configured (Automated)	L1	S			—
1.8.1.5	Ensure permissions on /etc/issue are configured (Automated)	L1	S			—
1.8.1.6	Ensure permissions on /etc/issue.net are configured (Automated)	L1	S			—
1.8.2	Ensure GDM login banner is configured (Automated)	L1	S			—
1.9	Ensure updates, patches, and additional security software are installed (Manual)	L1	P	P/ND		Applying RHEL patches is supported, but compatibility issues require backing out RHEL updates until a fix is available. Nokia does not recommend installing any additional software on the OS that hosts the NSP because it may affect NSP operation. Any non-sanctioned software must be removed if the software is suspected of causing NSP issues. NSP RHEL qcow2/OVA OS-package updates provided only via NSP RHEL update patch bundle
1.10	Ensure system-wide crypto policy is not legacy (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
1.11	Ensure system-wide crypto policy is FUTURE or FIPS (Automated)	L2	P			System-wide crypto policy level of FUTURE supported; NSP and NFM-P require custom sub-policy to support 2048-bit RSA length Note: Wavence UBT-SA devices require a crypto policy setting of DEFAULT.
2	Services					
2.1	inetd Services					
2.1.1	Ensure xinetd is not installed (Automated)	L1	S			—
2.2	Special Purpose Services					
2.2.1	Time Synchronization					
2.2.1.1	Ensure time synchronization is in use (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
2.2.1.2	Ensure chrony is configured (Automated)	L1	S			Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
2.2.2	Ensure X Window System is not installed (Automated)	L1	S			—
2.2.3	Ensure rsync service is not enabled (Automated)	L1	S			—
2.2.4	Ensure Avahi Server is not enabled (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
2.2.5	Ensure SNMP Server is not enabled (Automated)	L1	S			—
2.2.6	Ensure HTTP Proxy Server is not enabled (Automated)	L1	S			—
2.2.7	Ensure Samba is not enabled (Automated)	L1	S			—
2.2.8	Ensure IMAP and POP3 server is not enabled (Automated)	L1	S			—
2.2.9	Ensure HTTP server is not enabled (Automated)	L1	S			—
2.2.10	Ensure FTP Server is not enabled (Automated)	L1	S			—
2.2.11	Ensure DNS Server is not enabled (Automated)	L1	S			—
2.2.12	Ensure NFS is not enabled (Automated)	L1	S			—
2.2.13	Ensure RPC is not enabled (Automated)	L1	S			—
2.2.14	Ensure LDAP server is not enabled (Automated)	L1	S			—
2.2.15	Ensure DHCP Server is not enabled (Automated)	L1	S			—
2.2.16	Ensure CUPS is not enabled (Automated)	L1	S			—
2.2.17	Ensure NIS Server is not enabled (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
2.2.18	Ensure mail transfer agent is configured for local-only mode (Automated)	L1	S			—
2.3	Service Clients					
2.3.1	Ensure NIS Client is not installed (Automated)	L1	S			—
2.3.2	Ensure telnet client is not installed (Automated)	L1	S			—
2.3.3	Ensure LDAP client is not installed (Automated)	L1	S			—
3	Network Configuration					
3.1	Network Parameters (Host Only)					
3.1.1	Ensure IP forwarding is disabled (Automated)	L1	P	NS	S	IP forwarding required by NSP Kubernetes deployer, cluster nodes
3.1.2	Ensure packet redirect sending is disabled (Automated)	L1	S			—
3.2	Network Parameters (Host and Router)					
3.2.1	Ensure source routed packets are not accepted (Automated)	L1	S			—
3.2.2	Ensure ICMP redirects are not accepted (Automated)	L1	S			—
3.2.3	Ensure secure ICMP redirects are not accepted (Automated)	L1	S			—
3.2.4	Ensure suspicious packets are logged (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
3.2.5	Ensure broadcast ICMP requests are ignored (Automated)	L1	S			—
3.2.6	Ensure bogus ICMP responses are ignored (Automated)	L1	S			—
3.2.7	Ensure Reverse Path Filtering is enabled (Automated)	L1	S			—
3.2.8	Ensure TCP SYN Cookies is enabled (Automated)	L1	S			—
3.2.9	Ensure IPv6 router advertisements are not accepted (Automated)	L1	S			—
3.3	Uncommon Network Protocols					
3.3.1	Ensure DCCP is disabled (Automated)	L2	S			—
3.3.2	Ensure SCTP is disabled (Automated)	L2	S			—
3.3.3	Ensure RDS is disabled (Automated)	L2	S			—
3.3.4	Ensure TIPC is disabled (Automated)	L2	S			—
3.4	Firewall Configuration					
3.4.1	Ensure Firewall software is installed					
3.4.1.1	Ensure a Firewall package is installed (Automated)	L1	S			—
3.4.2	Configure firewalld					

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
3.4.2.1	Ensure firewalld service is enabled and running (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.2.2	Ensure iptables service is not enabled with firewalld (Automated)	L1	S			Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.2.3	Ensure nftables is not enabled with firewalld (Automated)	L1	S			Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.2.4	Ensure firewalld default zone is set (Automated)	L1	S			Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.2.5	Ensure network interfaces are assigned to appropriate zone (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.2.6	Ensure firewalld drops unnecessary services and ports (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.3	Configure nftables					
3.4.3.1	Ensure iptables are flushed with nftables (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
3.4.3.2	Ensure an nftables table exists (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information Calico network policies required for NSP deployer / cluster host deployment; nftable rules must not be changed.
3.4.3.3	Ensure nftables base chains exist (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information Calico network policies are required for NSP deployer / cluster host deployment, and nftable rules must not be changed.
3.4.3.4	Ensure nftables loopback traffic is configured (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.3.5	Ensure nftables outbound and established connections are configured (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.3.6	Ensure nftables default deny firewall policy (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.3.7	Ensure nftables service is enabled (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
3.4.3.8	Ensure nftables rules are permanent (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4	Configure iptables					
3.4.4.1	Configure IPv4 iptables					
3.4.4.1.1	Ensure iptables default deny firewall policy (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4.1.2	Ensure iptables loopback traffic is configured (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4.1.3	Ensure iptables outbound and established connections are configured (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4.1.4	Ensure iptables firewall rules exist for all open ports (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4.1.5	Ensure iptables is enabled and active (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4.2	Configure IPv6 ip6tables					
3.4.4.2.1	Ensure ip6tables default deny firewall policy (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
3.4.4.2.2	Ensure ip6tables loopback traffic is configured (Automated)	L1	S			—
3.4.4.2.3	Ensure ip6tables outbound and established connections are configured (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4.2.4	Ensure ip6tables firewall rules exist for all open ports (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.4.4.2.5	Ensure ip6tables is enabled and active (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
3.5	Ensure wireless interfaces are disabled (Automated)	L1	S			—
3.6	Disable IPv6 (Manual)	L2	S	S/ND		Supported, but not configured by default in NSP qcow2/OVA
4	Logging and Auditing					
4.1	Configure System Accounting (auditd)					
4.1.1	Ensure auditing is enabled					
4.1.1.1	Ensure auditd is installed (Automated)	L2	S			—
4.1.1.2	Ensure auditd service is enabled (Automated)	L2	S			—
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	L2	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
4.1.1.4	Ensure audit_backlog_limit is sufficient (Automated)	L2	S			—
4.1.2	Configure Data Retention					
4.1.2.1	Ensure audit log storage size is configured (Automated)	L2	S			—
4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	L2	S	S/ND		Supported, but not configured by default in NSP qcow2/OVA
4.1.2.3	Ensure system is disabled when audit logs are full (Automated)	L2	S	S/ND		To avoid causing NSP service disruption, disabling system when audit logs full not recommended
4.1.3	Ensure changes to system administration scope (sudoers) is collected (Automated)	L2	S			—
4.1.4	Ensure login and logout events are collected (Automated)	L2	S			—
4.1.5	Ensure session initiation information is collected (Automated)	L2	S			—
4.1.6	Ensure events that modify date and time information are collected (Automated)	L2	S			—
4.1.7	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	L2	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
4.1.8	Ensure events that modify the system's network environment are collected (Automated)	L2	S			—
4.1.9	Ensure discretionary access control permission modification events are collected (Automated)	L2	S			—
4.1.10	Ensure unsuccessful unauthorized file access attempts are collected (Automated)	L2	S			—
4.1.11	Ensure events that modify user/group information are collected (Automated)	L2	S			—
4.1.12	Ensure successful file system mounts are collected (Automated)	L2	S			—
4.1.13	Ensure use of privileged commands is collected (Automated)	L2	S			—
4.1.14	Ensure file deletion events by users are collected (Automated)	L2	S			Supported, but may affect system performance
4.1.15	Ensure kernel module loading and unloading is collected (Automated)	L2	S			—
4.1.16	Ensure system administrator actions (sudolog) are collected (Automated)	L2	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
4.1.17	Ensure the audit configuration is immutable (Automated)	L2	S			—
4.2	Configure Logging					
4.2.1	Configure rsyslog					
4.2.1.1	Ensure rsyslog is installed (Automated)	L1	S			—
4.2.1.2	Ensure rsyslog Service is enabled (Automated)	L1	S			—
4.2.1.3	Ensure rsyslog default file permissions configured (Automated)	L1	S			—
4.2.1.4	Ensure logging is configured (Manual)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
4.2.1.5	Ensure rsyslog is configured to send logs to a remote log host (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
4.2.1.6	Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	L1	S			—
4.2.2	Configure journald					
4.2.2.1	Ensure journald is configured to send logs to rsyslog (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
4.2.2.2	Ensure journald is configured to compress large log files (Automated)	L1	S			—
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk (Automated)	L1	S			—
4.2.3	Ensure permissions on all logfiles are configured (Automated)	L1	NI	NS		—
4.3	Ensure logrotate is configured (Manual)	L1	S	S/ND		Supported, but not configured by default in NSP qcow2/OVA
5	Access, Authentication and Authorization					
5.1	Configure cron					
5.1.1	Ensure cron daemon is enabled (Automated)	L1	S			—
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	L1	S			—
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	L1	S			—
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	L1	S			—
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	L1	S			—
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	L1	S			—
5.1.8	Ensure at/cron is restricted to authorized users (Automated)	L1	S			—
5.2	SSH Server Configuration					
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	L1	S			—
5.2.2	Ensure SSH access is limited (Automated)	L1	S	S/ND		Supported; not configured by default in NSP qcow2/OVA, as configuration requires site-specific information
5.2.3	Ensure permissions on SSH private host key files are configured (Automated)	L1	S			—
5.2.4	Ensure permissions on SSH public host key files are configured (Automated)	L1	S			—
5.2.5	Ensure SSH LogLevel is appropriate (Automated)	L1	S			—
5.2.6	Ensure SSH X11 forwarding is disabled (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
5.2.7	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	L1	S			—
5.2.8	Ensure SSH IgnoreRhosts is enabled (Automated)	L1	S			—
5.2.9	Ensure SSH HostbasedAuthentication is disabled (Automated)	L1	S			—
5.2.10	Ensure SSH root login is disabled (Automated)	L1	S			—
5.2.11	Ensure SSH PermitEmptyPasswords is disabled (Automated)	L1	S			—
5.2.12	Ensure SSH PermitUserEnvironment is disabled (Automated)	L1	S			—
5.2.13	Ensure SSH Idle Timeout Interval is configured (Automated)	L1	S			—
5.2.14	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	L1	S			—
5.2.15	Ensure SSH warning banner is configured (Automated)	L1	S			—
5.2.16	Ensure SSH PAM is enabled (Automated)	L1	S			—
5.2.17	Ensure SSH AllowTcpForwarding is disabled (Automated)	L2	P	S	P	AllowTcpForwarding is required for auxiliary database stations.

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
5.2.18	Ensure SSH MaxStartups is configured (Automated)	L1	S			—
5.2.19	Ensure SSH MaxSessions is set to 4 or less (Automated)	L1	S			—
5.2.20	Ensure system-wide crypto policy is not over-ridden (Automated)	L1	S			—
5.3	Configure authselect					
5.3.1	Create custom authselect profile (Automated)	L1	NS			Custom authselect profile not supported
5.3.2	Select authselect profile (Automated)	L1	NS			Custom authselect profile not supported
5.3.3	Ensure authselect includes with-faillock (Automated)	L1	NS			Custom authselect profile not supported
5.4	Configure PAM					
5.4.1	Ensure password creation requirements are configured (Automated)	L1	S			—
5.4.2	Ensure lockout for failed password attempts is configured (Automated)	L1	S	S/ND		—
5.4.3	Ensure password reuse is limited (Automated)	L1	S			—
5.4.4	Ensure password hashing algorithm is SHA-512 (Automated)	L1	S			—
5.5	User Accounts and Environment					

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation	CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
5.5.1	Set Shadow Password Suite Parameters				
5.5.1.1	Ensure password expiration is 365 days or less (Automated)	L1	P	P/ND	Note: The password expiration period of the following RHEL users must not be altered: <ul style="list-style-type: none"> • root • nsp • samadmin • oracle • td-agent • samauxdb • kube • etcd
5.5.1.2	Ensure minimum days between password changes is 7 or more (Automated)	L1	S	S/ND	Supported, but not configured by default in NSP qcow2/OVA
5.5.1.3	Ensure password expiration warning days is 7 or more (Automated)	L1	S		—
5.5.1.4	Ensure inactive password lock is 30 days or less (Automated)	L1	S		—
5.5.1.5	Ensure all users last password change date is in the past (Automated)	L1	S		—
5.5.2	Ensure system accounts are secured (Automated)	L1	S		—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
5.5.3	Ensure default user shell timeout is 900 seconds or less (Automated)	L1	S	S/ND		Supported, but not configured by default in NSP qcow2/OVA; setting of 1800 seconds (30 minutes) recommended to avoid missing console output of long operations
5.5.4	Ensure default group for the root account is GID 0 (Automated)	L1	S			—
5.5.5	Ensure default user umask is 027 or more restrictive (Automated)	S				Must exclude following RHEL users: <ul style="list-style-type: none"> • root • nsp • samadmin • oracle • td-agent • samauxdb • kube • etcd
5.6	Ensure root login is restricted to system console (Manual)	L1	S	S/ND		Supported, but not configured by default in NSP qcow2/OVA
5.7	Ensure access to the su command is restricted (Automated)	L1	S			—
6	System Maintenance					
6.1	System File Permissions					
6.1.1	Audit system file permissions (Manual)	L2	n/a			Manual audit recommendation only; transferred to customer for review
6.1.2	Ensure permissions on /etc/passwd are configured (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
6.1.3	Ensure permissions on /etc/passwd- are configured (Automated)	L1	S			—
6.1.4	Ensure permissions on /etc/shadow are configured (Automated)	L1	S			—
6.1.5	Ensure permissions on /etc/shadow- are configured (Automated)	L1	S			—
6.1.6	Ensure permissions on /etc/gshadow are configured (Automated)	L1	S			—
6.1.7	Ensure permissions on /etc/gshadow- are configured (Automated)	L1	S			—
6.1.8	Ensure permissions on /etc/group are configured (Automated)	L1	S			—
6.1.9	Ensure permissions on /etc/group- are configured (Automated)	L1	S			—
6.1.10	Ensure no world writable files exist (Automated)	L1	P	NS	S	Not supported by NSP Kubernetes deployer, cluster nodes; not fully supported until resolved by Kubernetes
6.1.11	Ensure no unowned files or directories exist (Automated)	L1	P	NS	S	Not supported by NSP Kubernetes deployer, cluster nodes

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
6.1.12	Ensure no ungrouped files or directories exist (Automated)	L1	P	NS	S	Not supported by NSP Kubernetes deployer, cluster nodes
6.1.13	Audit SUID executables (Manual)	L1	n/a			Manual audit recommendation only; transferred to customer for review
6.1.14	Audit SGID executables (Manual)	L1	n/a			Manual audit recommendation only; transferred to customer for review
6.2	User and Group Settings					
6.2.1	Ensure password fields are not empty (Automated)	L1	S			—
6.2.2	Ensure no legacy + entries exist in /etc/passwd (Automated)	L1	S			—
6.2.3	Ensure root PATH Integrity (Automated)	L1	S			—
6.2.4	Ensure no legacy + entries exist in /etc/shadow (Automated)	L1	S			—
6.2.5	Ensure no legacy + entries exist in /etc/group (Automated)	L1	S			—
6.2.6	Ensure root is the only UID 0 account (Automated)	L1	S			—
6.2.7	Ensure users' home directories permissions are 750 or more restrictive (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
6.2.8	Ensure users own their home directories (Automated)	L1	S			—
6.2.9	Ensure users' dot files are not group or world writable (Automated)	L1	S			—
6.2.10	Ensure no users have .forward files (Automated)	L1	S			—
6.2.11	Ensure no users have .netrc files (Automated)	L1	S			—
6.2.12	Ensure users' .netrc Files are not group or world accessible (Automated)	L1	S			—
6.2.13	Ensure no users have .rhosts files (Automated)	L1	S			—
6.2.14	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	L1	S			—
6.2.15	Ensure no duplicate UIDs exist (Automated)	L1	S			—
6.2.16	Ensure no duplicate GIDs exist (Automated)	L1	S			—
6.2.17	Ensure no duplicate user names exist (Automated)	L1	S			—
6.2.18	Ensure no duplicate group names exist (Automated)	L1	S			—
6.2.19	Ensure shadow group is empty (Automated)	L1	S			—

Table 7-1 NSP support levels, CIS RHEL 8 recommendations (continued)

Recommendation		CIS profile	Manual install	k8s host OS image	NSP host OS image	Notes
6.2.20	Ensure all users' home directories exist (Automated)	L1	S			—

7.2 RHEL sudoer configuration

7.2.1 Default configuration mapping

The following table provides the default mapping between NSP components, sudoer files, and users.

NSP component	Sudoer file(s)	User
NFM-P main or auxiliary server	nfmp-main, nspos-sudo	nsp
NFM-P main database	nfmp-main-db	oracle
NSP auxiliary database	nspos-auxdb, nspos-auxdbproxy	samauxdb
CLM	clm-sudo, nspos-sudo	nsp

7.2.2 Restricted root-user access

If you employ a special sudoers configuration, privileged users that you create can execute only specific NSP management and deployment commands. If a user other than the privileged non-root user attempts to execute a restricted command, the command fails.

You can also prevent remote root-user access to the stations in an NSP deployment by designating a specific privileged user for remote access.

You can restrict root-user access on the NSP deployer host and cluster VMs; NSP auxiliary database; and on NFM-P main server, auxiliary server, and main database stations.

i **Note:** Client delegate servers do not support restricted root access.

The root user performs the initial OS and VM setup for an NSP deployment and creates the alternative users with restricted access. The root user is not required for NSP deployment operations afterward.

Restricted root-user access:

- assigns sudo privileges for only the required commands per user
- ensures that any configuration or control actions are traceable to a specific user
- meets an important CIS security benchmark

See “Restricting root-user system access” in the *NSP Installation and Upgrade Guide* for more information.

8 Data privacy summary

8.1 NSP network and user data privacy

8.1.1 Purpose

This appendix summarizes how the NSP treats private data that is collected, processed, or retained, such as:

- user authentication data
- NE data
- subscriber data
- e-mail notification policy data

See [8.1.2 “NSP data privacy” \(p. 59\)](#) or [8.1.3 “NFM-P data privacy” \(p. 60\)](#) for specific summary information.

8.1.2 NSP data privacy

The following table lists and describes, by category, how the NSP treats network and user data.

Table 8-1 NSP treatment of private data

Data category	Description and treatment
NE data	
Type of data	<ul style="list-style-type: none"> • Username and password • IP address
Purpose	<ul style="list-style-type: none"> • NE authentication • NE IP address for NE discovery/access
Storage	<ul style="list-style-type: none"> • Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups.
Processing	NE data is processed for the stated purpose.
Access	Authorized users
Safeguards	<ul style="list-style-type: none"> • NEs are configured by authorized users. • Database access is restricted to authorized users. • Secure transit option is available. • Passwords for NE users are encrypted before being stored. • Log file access is restricted to authorized users.

Table 8-1 NSP treatment of private data (continued)

Data category	Description and treatment
Subscriber data	
Type of data	<ul style="list-style-type: none"> • MAC address • IP address
Purpose	<ul style="list-style-type: none"> • Statistics • SLA support • Troubleshooting
Storage	<ul style="list-style-type: none"> • Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups. Retention period for statistics can be configured.
Processing	Subscriber data is processed for the stated purpose.
Access	Authorized users
Safeguards	<ul style="list-style-type: none"> • NEs are configured by authorized users. • Database access is restricted to authorized users. • Log file access is restricted to authorized users.
E-mail notification policy data	
Type of data	<ul style="list-style-type: none"> • Username and password • E-mail address (sender) • E-mail address (recipient)
Purpose	<ul style="list-style-type: none"> • Username, password and sender's e-mail address are used for SMTP configuration • Recipient e-mail addresses are required to create e-mail notification policies in supported functions
Storage	<ul style="list-style-type: none"> • Local database
Retention	Data is retained in the database until an authorized user deletes it. By default, SMTP server and e-mail notification policies are not configured.
Processing	SMTP server configuration and e-mail notification policies are processed for the stated purpose.
Access	Authorized users
Safeguards	<ul style="list-style-type: none"> • SMTP configuration and e-mail policies are configured by authorized users. • Database access is restricted to authorized users. • Password for SMTP configuration is encrypted before being stored.

8.1.3 NFM-P data privacy

The following table lists and describes, by category, how the NFM-P treats network and user data.

Table 8-2 NFM-P treatment of private data

Category	Description
Local user data (local authentication)	
Type of data	<ul style="list-style-type: none"> • Username and password • E-mail • IP address
Purpose	<ul style="list-style-type: none"> • Authentication of local NSP users • User e-mail addresses (optional) to send notifications for certain events; for example, alarms or account status • IP address provides accountability of individual product access.
Storage	<ul style="list-style-type: none"> • Local database • Logs
Retention	Data is retained in the database until an authorized user deletes it. Log retention time can vary based on log file size and the number of log backups.
Processing	Local user data is processed for the stated purpose.
Access	Authorized users
Safeguards	<ul style="list-style-type: none"> • Additional local users must be created by an authorized user. • Database access is restricted to authorized users. • TLS secures data in transit. • Passwords for local users are hashed before they are stored. • Log file access is restricted to authorized users.
Comments	Local authentication is performed using a local database of users and a local security scheme.
Customer profile data	
Type of data	<ul style="list-style-type: none"> • Name • E-mail • Address • Phone
Purpose	Data may be used by an authorized user for associating customers to configured services.
Storage	Local database
Retention	Data is retained in the database until an authorized user deletes it.
Processing	Customer profile data is processed for the stated purpose.
Access	Authorized users

Table 8-2 NFM-P treatment of private data (continued)

Category	Description
Safeguards	<ul style="list-style-type: none"> • Customer profile must be created by an authorized user. • Database access is restricted to authorized users.
NE data	
Type of data	<ul style="list-style-type: none"> • Username and password • IP address
Purpose	<ul style="list-style-type: none"> • NE authentication • NE IP address for NE discovery/access
Storage	<ul style="list-style-type: none"> • Local database • Logs <p>Note that NE backups that are stored on the NFM-P server may contain data that is not stored in the NFM-P database. Data contained in the NE backup files will be dependent upon the NE type and version; therefore the privacy statements for the individual NEs must be consulted.</p>
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups.
Processing	NE data is processed for the stated purpose.
Access	Authorized users
Safeguards	<ul style="list-style-type: none"> • NEs are configured by authorized users. • Database access is restricted to authorized users. • Secure transit option is available. • Passwords for NE users are encrypted before being stored. • Log file access is restricted to authorized users.
Subscriber data	
Type of data	<ul style="list-style-type: none"> • MAC address • IP address • International Mobile Subscriber Identity (IMSI) • International Mobile Station Equipment Identity (IMEI) • Mobile Station International Subscriber Directory Number (MSISDN) • Access Point Name (APN)
Purpose	<ul style="list-style-type: none"> • Statistics • SLA support • Troubleshooting • Analytics • UE or network node performance information

Table 8-2 NFM-P treatment of private data (continued)

Category	Description
Storage	<ul style="list-style-type: none"> • Main database • NSP auxiliary database • Logs • Auxiliary servers (optional): statistics
Retention	Data is retained in the database until an authorized user deletes it. Log retention can vary based on the log file size and number of log backups. Retention period for auxiliary servers can be configured.
Processing	Subscriber data is processed for the stated purpose.
Access	Authorized users
Safeguards	<ul style="list-style-type: none"> • NEs are configured by authorized users. • Database access is restricted to authorized users. • Secure transit option is available. • File access is restricted to authorized users. • Log file access is restricted to authorized users.
E mail notification policies	
Type of data	<ul style="list-style-type: none"> • Username and password • E-mail address (sender) • E-mail address (recipient)
Purpose	<ul style="list-style-type: none"> • Username, password and sender's e-mail address are used for SMTP configuration • Recipient e-mail addresses are required to create e-mail notification policies in supported functions
Storage	<ul style="list-style-type: none"> • Local database
Retention	Data is retained in the database until an authorized user deletes it. By default, SMTP server and e-mail notification policies are not configured.
Processing	SMTP server configuration and e-mail notification policies are processed for the stated purpose.
Access	Authorized users
Safeguards	<ul style="list-style-type: none"> • SMTP configuration and e-mail policies are configured by authorized users. • Database access is restricted to authorized users. • Password for SMTP configuration is encrypted before being stored.

9 NSP interface cryptography

9.1 Algorithms per NSP component

9.1.1 TLS server algorithms for client networks

Component	Protocol	Ciphersuites	Signatures	Groups
NSP Web Server	TLSv1.3	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_128_GCM_SHA256	rsa_pss_rsae_sha256 rsa_pss_rsae_sha384 rsa_pss_rsae_sha512	secp256r1 secp384r1 secp521r1
	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA	rsa_pss_rsae_sha256 rsa_pss_rsae_sha384 rsa_pss_rsae_sha512 rsa_pkcs1_sha256 rsa_pkcs1_sha384 rsa_pkcs1_sha512 rsa_pkcs1_sha224	x25519 x448

Component	Protocol	Ciphersuites	Signatures	Groups
NFM-P Web Server for Java Client connection (tcp/8444)	TLSv1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	rsa_pkcs1_sha1 rsa_pkcs1_sha224 rsa_pkcs1_sha256	secp256r1 secp384r1 secp521r1

9.1.2 TLS client algorithms for mediation networks

Supported TLS client algorithms for gRPC mediation policies.

Protocol	Ciphersuites	Signatures	Groups
TLSv1.3	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256	ecdsa_secp256r1_sha256 rsa_pss_rsae_sha256 rsa_pkcs1_sha256	x25519 secp256r1 secp384r1 secp521r1
TLSv1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA	ecdsa_secp384r1_sha384 rsa_pss_rsae_sha384 rsa_pkcs1_sha384 rsa_pss_rsae_sha512 rsa_pkcs1_sha512 rsa_pkcs1_sha1	N/A

9.1.3 SSH client algorithms for mediation networks

Supported SSH client algorithms for CLI and NETCONF mediation policies.

Mediation type	Crypto function	Default algorithms (non-FIPS)	Default algorithms (FIPS)	Configurable	Configuration procedure
Classic	Key exchange	curve25519-sha256 curve25519-sha256@libssh.org curve448-sha512 ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group-exchange-sha256 diffie-hellman-group18-sha512 diffie-hellman-group17-sha512 diffie-hellman-group16-sha512 diffie-hellman-group15-sha512 diffie-hellman-group14-sha256	ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group-exchange-sha256 diffie-hellman-group18-sha512 diffie-hellman-group17-sha512 diffie-hellman-group16-sha512 diffie-hellman-group15-sha512 diffie-hellman-group14-sha256	Yes	<i>NSP System Administrator Guide</i>
	Host key	ecdsa-sha2-nistp256-cert-v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com ssh-ed25519-cert-v01@openssh.com rsa-sha2-512-cert-v01@openssh.com rsa-sha2-256-cert-v01@openssh.com ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 ssh-rsa	ecdsa-sha2-nistp256-cert-v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com ssh-ed25519-cert-v01@openssh.com rsa-sha2-512-cert-v01@openssh.com rsa-sha2-256-cert-v01@openssh.com ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 ssh-rsa	Yes	<i>NSP System Administrator Guide</i>
	Cipher	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc	Yes	<i>NSP System Administrator Guide</i>
	MAC	hmac-sha2-256-etm@openssh.com hmac-sha2-256 hmac-sha2-512-etm@openssh.com hmac-sha2-512 hmac-sha1-etm@openssh.com hmac-sha2-256	hmac-sha2-256-etm@openssh.com hmac-sha2-256 hmac-sha2-512-etm@openssh.com hmac-sha2-512 hmac-sha1-etm@openssh.com hmac-sha2-256 hmac-sha2-512	Yes	<i>NSP System Administrator Guide</i>
Release 24.8 August 2024 Issue 1		© 2024 Nokia User Subject to Terms available at www.nokia.com/terms 3HE-20027-AAAB-022A			

Mediation type	Crypto function	Default algorithms (non-FIPS)	Default algorithms (FIPS)	Configurable	Configuration procedure
Model-driven	Key exchange	ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group15-sha512 diffie-hellman-group16-sha512 diffie-hellman-group17-sha512 diffie-hellman-group18-sha512 diffie-hellman-group1-sha1	N/A	No	N/A
	Host key	ecdsa-sha2-nistp256-cert-v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com ssh-ed25519-cert-v01@openssh.com rsa-sha2-512-cert-v01@openssh.com rsa-sha2-256-cert-v01@openssh.com ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 ssh-ed25519 rsa-sha2-512 rsa-sha2-256 ssh-rsa	N/A	No	N/A
	Cipher	chacha20-poly1305@openssh.com aes256-ctr aes192-ctr aes128-ctr aes256-gcm@openssh.com aes128-gcm@openssh.com aes256-cbc aes192-cbc aes128-cbc	N/A	No	N/A

Mediation type	Crypto function	Default algorithms (non-FIPS)	Default algorithms (FIPS)	Configurable	Configuration procedure
MAC	hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1	N/A	No	N/A	

