NOZOMI NETWORKS

Federal Information Processing Standards
Reference Guide

2025-03-18

Legal notices

Information about the Nozomi Networks copyright and use of third-party software in the Nozomi Networks product suite.

Copyright

Third Party Software

Nozomi Networks uses third-party software, the usage of which is governed by the applicable license agreements from each of the software vendors. Additional details about used third-party software can be found at https://security.nozominetworks.com/licenses.

Contents

Chapter 1. Introduction

Federal Information Processing Standards

A description of the use of Federal Information Processing Standards in the Nozomi Networks software.

You can configure the *Nozomi Networks Operating System (N2OS)* software to use the FIPS-140-2 approved cryptography module. The develops *Federal Information Processing Standards (FIPS)* for non-military American government agencies, and government contractors, to use in computer systems.

The FIPS-140 series specifies requirements for cryptography modules within a security system to protect sensitive, but unclassified, data.

To enable *FIPS* mode, you must install a *FIPS*-enabled license. To obtain a license, refer to your Nozomi Networks representative.

Important:

To enable *FIPS* mode, you must be running version N2OS 22.2.1 or later.

Important:

You can only connect *FIPS* products to other *FIPS* products. The use of mixed environments is not allowed.

Important:

Enabling *FIPS* mode:

- If you are running a version of *N2OS* that is between 22.2.1 and 23.1.0, you will need a valid *FIPS* license for both Guardians and *Central Management Console (CMC)*s
- Beginning with version 23.1.0 or later, *FIPS* mode can be enabled on Guardians without a license, but packet sniffing will be disabled until a valid license is activated
- The order of enabling *FIPS* on either device does not affect functionality
- You need a *FIPS* license for *CMC*s and Remote Collectors. Upstream sensors will manage these licenses

Compliant FIPS cryptography features

A description of the features that are compliant with Federal Information Processing Standards (FIPS), and those that are non-compliant.

To achieve full compliance with *FIPS*, make sure that the system is configured in *FIPS*-mode and only uses *FIPS*-compliant features.

FIPS-compliant features

After enabling *FIPS* mode, these features will use compliant cryptography:

- *hypertext transfer protocol secure (HTTPS)* Web interface
- *secure shell (SSH)* remote access
- Remote Collector and *CMC* data flows
- Local users password encryption
- Configuration secrets stored in the local configuration file

Non-compliant features

The Nozomi Networks software does not prevent you from using features that are not compliant with *FIPS*. If you want to achieve full compliance with *FIPS*, make sure that the system:

- Is configured in *FIPS* mode
- Only uses *FIPS*-compliant features

The list below shows some, but not all, non-compliant features:

- *server message block (SMB)* remote backup transfer
- Unencrypted Syslog forwarding
- *simple network management protocol (SNMP)* with users configured with MD5 or DES protocols
- Any cryptography usage outside the security boundary of the *FIPS* library

FIPS operations auditing

The Federal Information Processing Standards (FIPS) audit trail tracks specific FIPS events.

These events log *FIPS* status changes into the audit trail:

- *FIPS* mode enabled
- *FIPS* mode disabled

When booting, the sensors report *FIPS* mode operations using the message

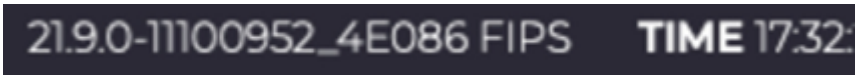
```
System running in FIPS mode
```

Figure 1. FIPS mode operations - messages

FIPS mode status

When running in Federal Information Processing Standards (FIPS) mode, the sensor adds a FIPS indicator after the version string.

In the Web *user interface (UI)*, look to see if `FIPS` is shown after the version string.



If you want to add FIPS to the version string, you can enter the command:

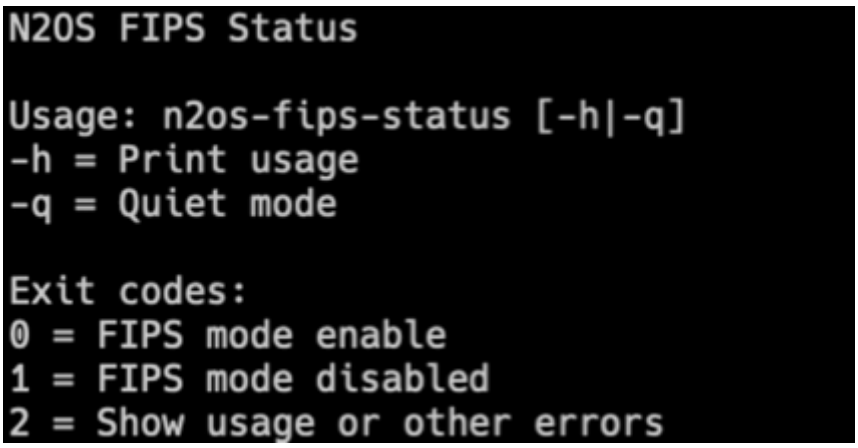
```
n2os-version
```

If you want to check the *FIPS* status, you can enter the command:

```
n2os-fips-status
```

To support additional parameters for extended usage, you can enter the command:

```
n2os-fips-status [-h | -q]
```



Supported SSH protocols in FIPS mode

A list of all the secure shell (SSH) protocols that are supported in Federal Information Processing Standards (FIPS) mode.

Table 1. Supported SSH protocols in FIPS mode

Function	Algorithms
Key exchange	ecdh-sha2-nistp256
	ecdh-sha2-nistp384
	ecdh-sha2-nistp521
	diffie-hellman-group-exchange-sha256
	diffie-hellman-group14-sha256
	diffie-hellman-group16-sha512
	diffie-hellman-group18-sha512
Ciphers	aes256-gcm@openssh.com
	aes256-ctr
	aes128-gcm@openssh.com
	aes128-ctr
MACs	hmac-sha2-256-etm@openssh.com
	hmac-sha2-512-etm@openssh.com
	hmac-sha2-256
	hmac-sha2-512
Host key algorithms	ecdsa-sha2-nistp256
	ecdsa-sha2-nistp384
	ecdsa-sha2-nistp521
	rsa-sha2-256
	rsa-sha2-512

Supported HTTPS protocols in FIPS mode

A list of all the Hypertext Transfer Protocol Secure (HTTPS) protocols that are supported in Federal Information Processing Standards (FIPS) mode.

Table 2. Supported HTTPS protocols in FIPS mode

TLS version	Cipher Suite Name (IANA/RFC)
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS 1.3	TLS_AES_256_GCM_SHA384
	TLS_AES_128_GCM_SHA256

Important notes

Important notes that you should be aware of.

Product version compatibility

To enable *FIPS* mode, you must be running version *N2OS* version 22.2.1 or later.

Product inter-operability

FIPS products can only be connected to other *FIPS* products. The use of mixed environments is not allowed.

FIPS license

To use the *FIPS* add-on, you will need an additional license. Contact your sales representative for additional information.

Enabling FIPS mode

If you're running an *N2OS* version between 22.2.1 and 23.1.0, both Guardians and *CMC* require a valid *FIPS* license.

Beginning with *N2OS* version 23.1.0 or later, *FIPS* mode can be enabled on Guardians without a license, but packet sniffing will be disabled until a valid license is activated.

The order of enabling *FIPS* on either device does not affect functionality.

FIPS licenses are required for *CMC*s and Remote Collectors (RCs) and managed by upstream sensors.

Chapter 2. Configuration

Enable FIPS mode

It is important that you follow this procedure to make sure that you enable Federal Information Processing Standards (FIPS) mode correctly.

About this task

When you switch to *FIPS* mode, local user Web *UI* passwords become invalid. To take advantage of *FIPS* encryption, you can use the `n2os-passwd` command to reset the passwords.

The `n2os-passwd <USER>` command takes several seconds to several minutes to prompt the user for a new password. On the R50 platform, the prompt may take up to three minutes.

Important:

When you enable *FIPS*, it is critical that you change the password for **EVERY** Web *UI* local user.

Procedure

1. Log into the console.
2. To go to privileged mode, enter this command:

   ```
   enable-me
   ```

   Result: You can now perform system changes.

3. **Note:**

   For *CMC*s, version 23.1.0 or later, it is not necessary to do the next step.

   Note:

   For Guardians, version 23.1.0 or later, you can also do the next two steps after you have enabled *FIPS*.

   To configure the *FIPS* license, enter the command:

   ```
   echo 'conf.user configure license fips xxxxxxxx' | cli
   ```

4. **Note:**
   For *CMC*s, version 23.1.0 or later, it is not necessary to do the next step.

   To restart the *intrusion detection system (IDS)*, enter the command:

   ```
   service n2osids stop
   ```

   Result: The *IDS* stops. After a few seconds, it will automatically start again.

5. To enable *FIPS* mode, enter the command:

   ```
   n2os-fips-enable
   ```

   Result: The system automatically reboots.

6. In the container edition, stop the current container and start a new one with the same settings.
7. To change the password for every user, enter the command:

   ```
   n2os-passwd <USER>
   ```

8. Log in to the sensor.
9. In the top navigation bar, select 

   Result: The administration page opens.

10. In the **System** section, select **Updates and licenses**.

    Result: The **Updates and licenses** page opens.

11. In the **Current license** section for **FIPS**, make sure that the **License status** shows `ok`.
12. Do this procedure again for all *CMC*s and Guardians.

Disable FIPS mode

Do this procedure to disable Federal Information Processing Standards (FIPS) mode.

About this task

When you switch to *FIPS* mode, local user Web *UI* passwords become invalid. You can use the `n2os-passwd` command to reset the passwords.

Procedure

1. Log into the console, either directly or through *SSH*.
2. To go to privileged mode, enter this command:

   ```
   enable-me
   ```

   Result: You can now perform system changes.
3. To disable *FIPS* mode, enter the command:

   ```
   n2os-fips-disable
   ```
4. Reboot the system, or restart the container, to apply the changes.

Glossary

Central Management Console

The Central Management Console (CMC) is a Nozomi Networks product that has been designed to support complex deployments that cannot be addressed with a single sensor. A central design principle behind the CMC is the unified experience, that lets you access information in the similar method to the sensor.

Federal Information Processing Standards

FIPS are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

Hypertext Transfer Protocol Secure

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

Intrusion Detection System

An intrusion detection system (IDS), which can also be known as an intrusion prevention system (IPS) is a software application, or a device, that monitors a computer network, or system, for malicious activity or policy violations. Such intrusion activities, or violations, are typically reported either to a system administrator, or collected centrally by a security information and event management (SIEM) system.

Nozomi Networks Operating System

N2OS is the operating system that the core suite of Nozomi Networks products runs on.

Secure Shell

A cryptographic network protocol that let you operate network services securely over an unsecured network. It is commonly used for command-line execution and remote login applications.

Server Message Block

Is a communication protocol which provides shared access to files and printers across nodes on a network of systems. It also provides an authenticated interprocess communication (IPC) mechanism.

Simple Network Management Protocol

SNMP is an Internet Standard protocol for the collection and organization of information about managed devices on IP networks. It also lets you modify that information to change device behavior. Typical devices that support SNMP are: printers, workstations, cable modems, switches, routers, and servers.

User Interface

An interface that lets humans interact with machines.