Ncore SAN

Quick Start Guide

Product Version 26.1 | Guide Revision 1.1 | August 2026

Table of Contents

Welcome to Ncore SAN

Ncore SAN transforms any Linux server into a high-performance storage platform, allowing available disks and block devices to be discovered, provisioned, and exposed through industry-standard block-storage protocols.

With Ncore SAN, you can:

- Expose available disks and block devices through iSCSI targets.
- Expose available disks and block devices through NVMe-oF using TCP or RDMA.
- Provide block-storage access to Windows, Linux, and enterprise applications.
- Manage disks, block devices, iSCSI targets, and NVMe-oF subsystems from one desktop interface.

Ncore SAN architecture overview

Operational model: The Windows management application connects securely to the Ncore SAN service. Ncore SAN provisions block devices and presents them to remote clients through iSCSI or NVMe-oF.	
Capability	**Purpose**
Unified management	Manage disks and storage exports from one interface.
Enterprise-ready operation	Use authenticated management, TLS, and protocol-level host controls.
High-performance data path	Use dedicated CPU processing groups and accelerated storage transports.
Observability	Review attachment state, export assignment, active connections, and gateway status.

1. Ncore SAN - CPU Core Isolation

Each exported block device is assigned a dedicated CPU core. When the configured exports exceed the available cores, Ncore distributes additional exports across the existing processing cores.

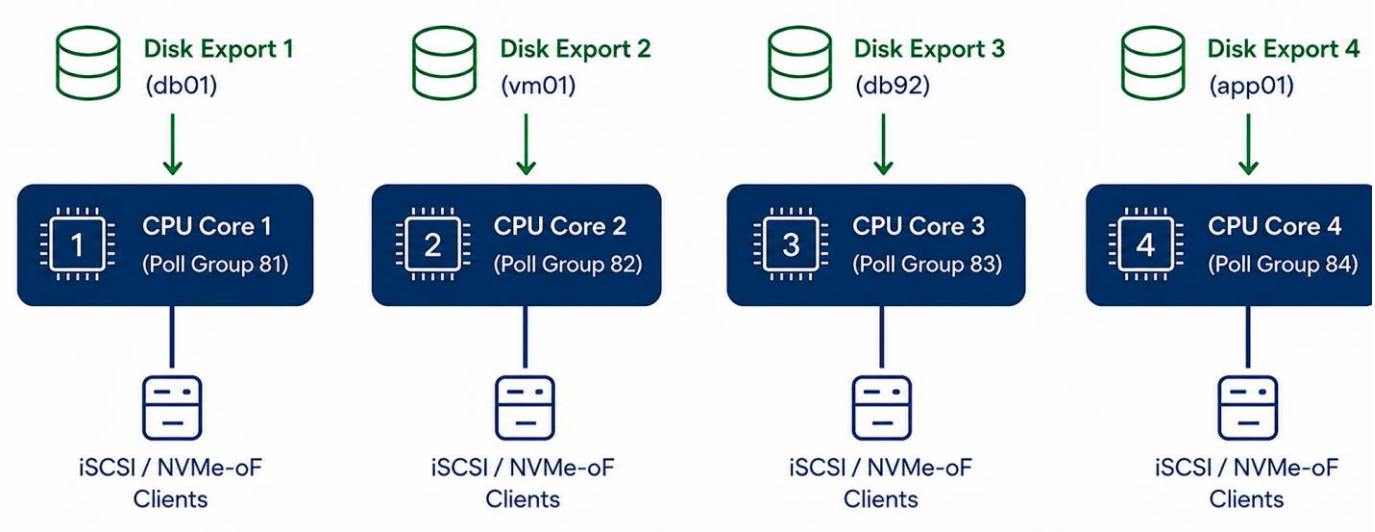

Figure 1 - CPU core and export mapping

Benefit	Description
Parallel processing	Each export is processed independently when a dedicated core is available.
Minimal contention	Dedicated processing groups provide predictable workload isolation.
Optimized mapping	The gateway pins protocol processing groups to configured CPU cores.

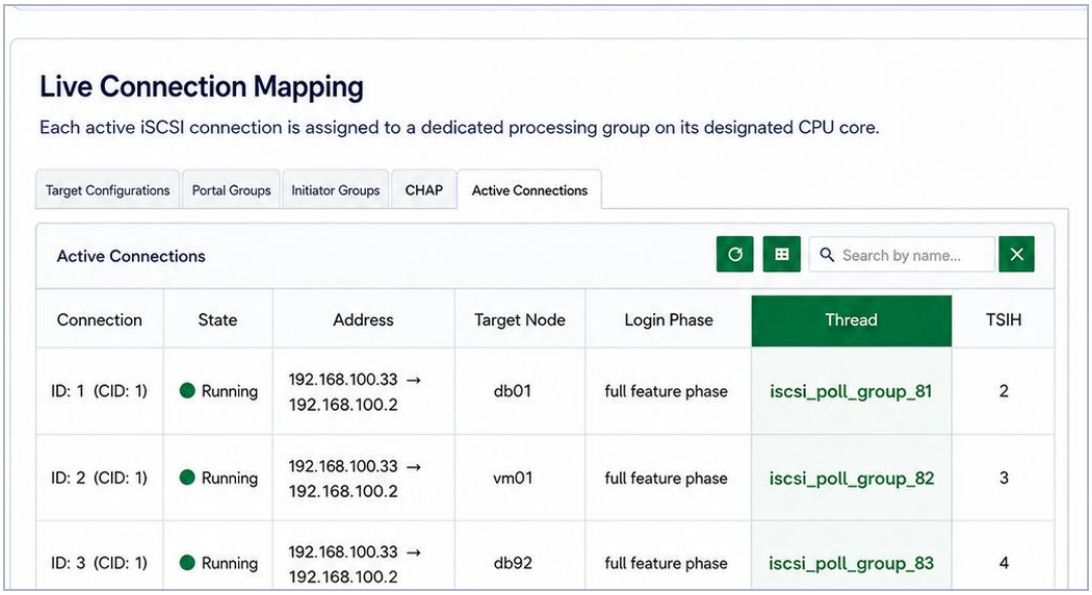

Figure 2 - Live connection mapping

2. Quick Start

Prepare the Linux host by configuring HugePages, optional RDMA modules, the container runtime, and the Ncore SAN service.

Component	Recommended
Operating system	64-bit Linux distribution, such as Ubuntu, Red Hat Enterprise Linux, or Rocky Linux
CPU	Multi-core x86_64 processor
Memory	16 GB RAM minimum
HugePages	8 GB reserved using either 8 x 1 GB pages or 4,096 x 2 MB pages
Network	10 GbE or faster
Container runtime	Docker Engine or Podman

Configure HugePages

Ncore SAN supports either 1 GB or 2 MB HugePages. Choose one configuration; both examples reserve 8 GB.

Important: Configure only one HugePage size. Reserved HugePage memory is unavailable for normal system use.

1 GB HugePages	**2 MB HugePages**
8 pages x 1 GB = 8 GB	4,096 pages x 2 MB = 8 GB
default_hugepagesz=1G hugepagesz=1G hugepages=8	default_hugepagesz=2M hugepagesz=2M hugepages=4096

Ubuntu or Debian

Add the selected options to GRUB_CMDLINE_LINUX_DEFAULT in /etc/default/grub, preserving existing options. Then run:

```
sudo update-grub
sudo reboot
```

Red Hat Enterprise Linux or Rocky Linux

Add the selected options to all installed kernel entries, then restart the host:

```
sudo grubby --update-kernel=ALL --args="<selected HugePage options>"
sudo reboot
```

Verify HugePages

```
grep -E '^HugePages_|^Hugepagesize|^Hugetlb' /proc/meminfo
```

Expected: 1 GB pages = HugePages_Total 8 and Hugepagesize 1048576 kB; 2 MB pages = HugePages_Total 4096 and Hugepagesize 2048 kB.

Configure optional RDMA modules

For NVMe-oF over RDMA, load the modules applicable to the installed adapter: **rdma_cm, rdma_ucm, ib_uverbs, ib_core, and iw_cm.** RDMA modules are not required for iSCSI or NVMe-oF over TCP.

Verify the container and gateway

- Confirm Docker Engine or Podman is installed and enabled.
- Confirm the Ncore SAN container is running.
- Confirm a valid Ncore SAN license is installed.
- Launch the Windows management application and connect to the configured gateway URL.

3. Connection Settings

Configure the management application to connect to the Ncore SAN, authenticate, install the TLS certificate, and verify connectivity.

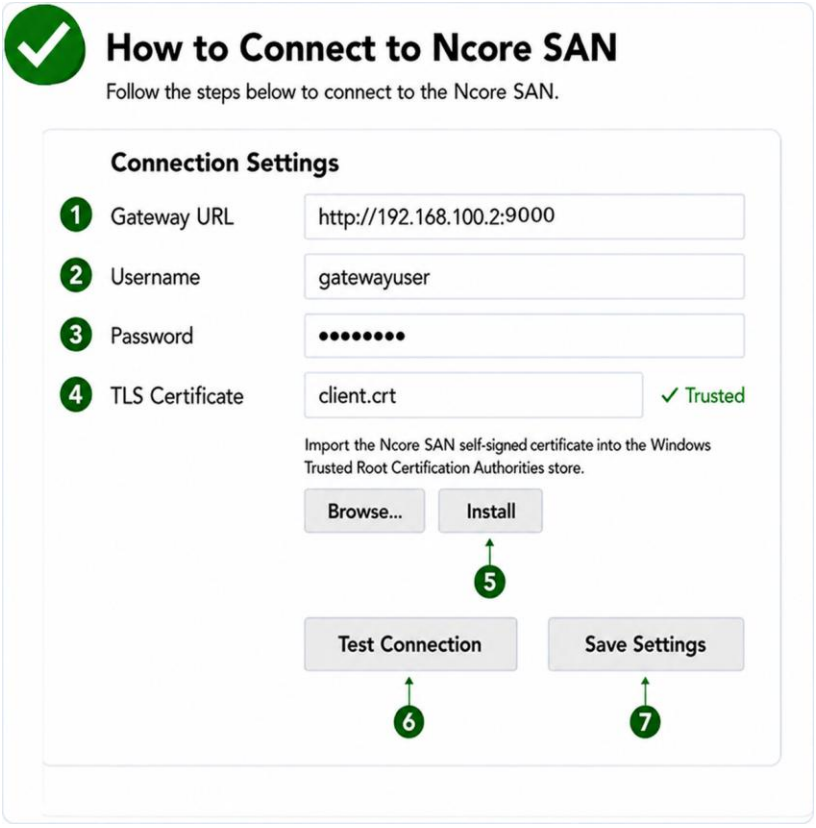

Figure 3 - Connect to Ncore SAN

Setting	Description
Gateway URL	Ncore SAN HTTPS management endpoint, for example https://192.168.100.2:9000.
Username	User account configured for gateway authentication.
Password	Password associated with the configured user account.
TLS certificate	Certificate used to establish trusted HTTPS communication.
Install certificate	Imports the certificate into the Windows Trusted Root Certification Authorities store.
Test Connection	Verifies HTTPS connectivity and authentication before saving.
Save Settings	Stores the connection configuration for future sessions.
Result: After a successful test, the application status bar displays Connected and the management functions become available.	

4. Dashboard Overview

The main dashboard lists all attached disks and provides direct access to metrics, protocol exports, settings, search, refresh, and connection status.

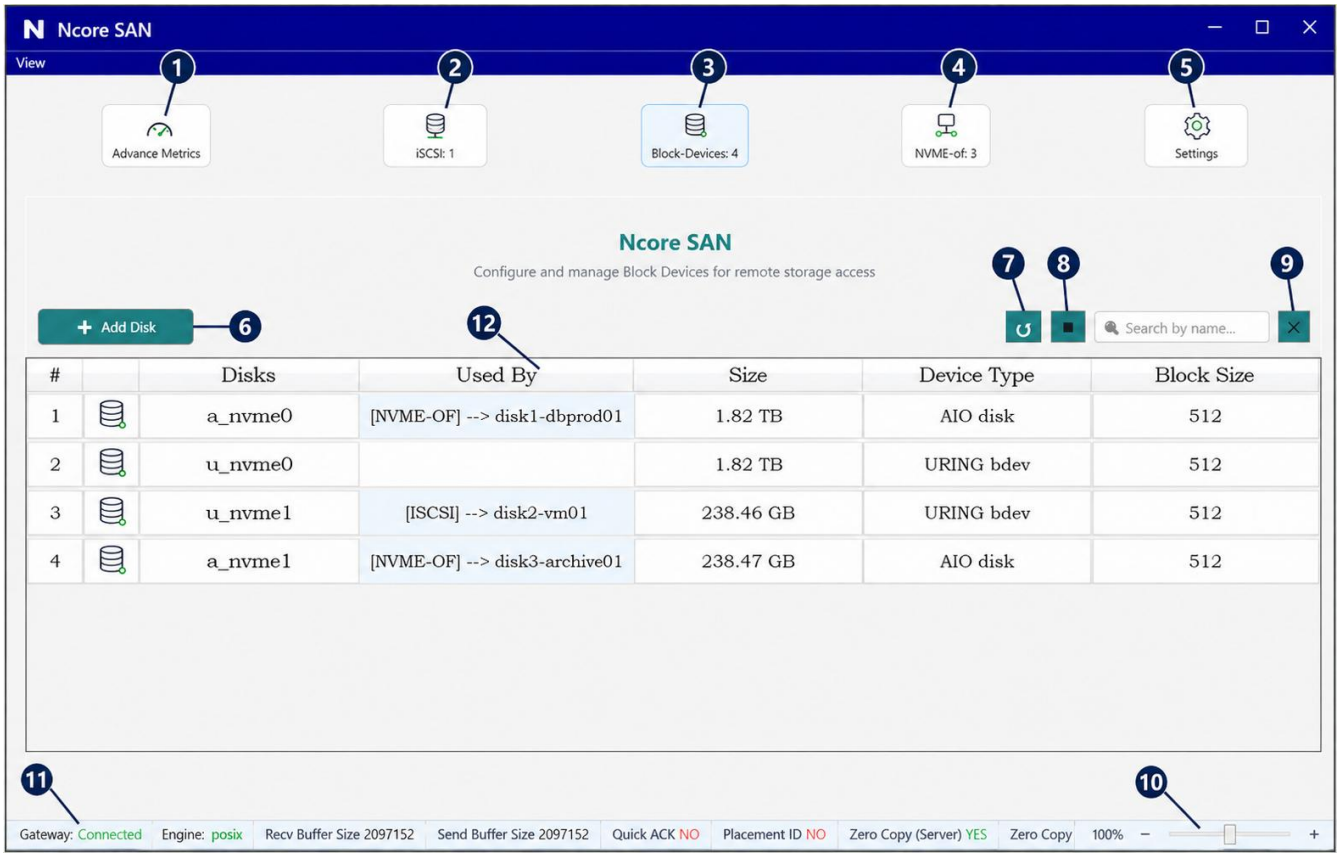

Figure 4 - Ncore SAN dashboard

#	Control	Description
1	Advanced Metrics	Open the metrics and performance dashboard.
2	iSCSI	Navigation Icon, Open iSCSI management window and display device count.
3	Block Devices	Navigation Icon, Open block device management window and list all attached block devices.
4	NVMe-oF	Navigation Icon, Opens NVMe-oF management window and display device count
5	Settings	Open application settings.
6	Add Disk	Open the dialog window to attach disk to Ncore SAN
7-9	Refresh and search	Reload the list, search by name, or clear the search.
10-12	Status and assignment	Adjust zoom, review gateway status, and see where each block device is used or exported.

5. Attach disks to Ncore SAN

Select any available disk and attach it to Ncore SAN.

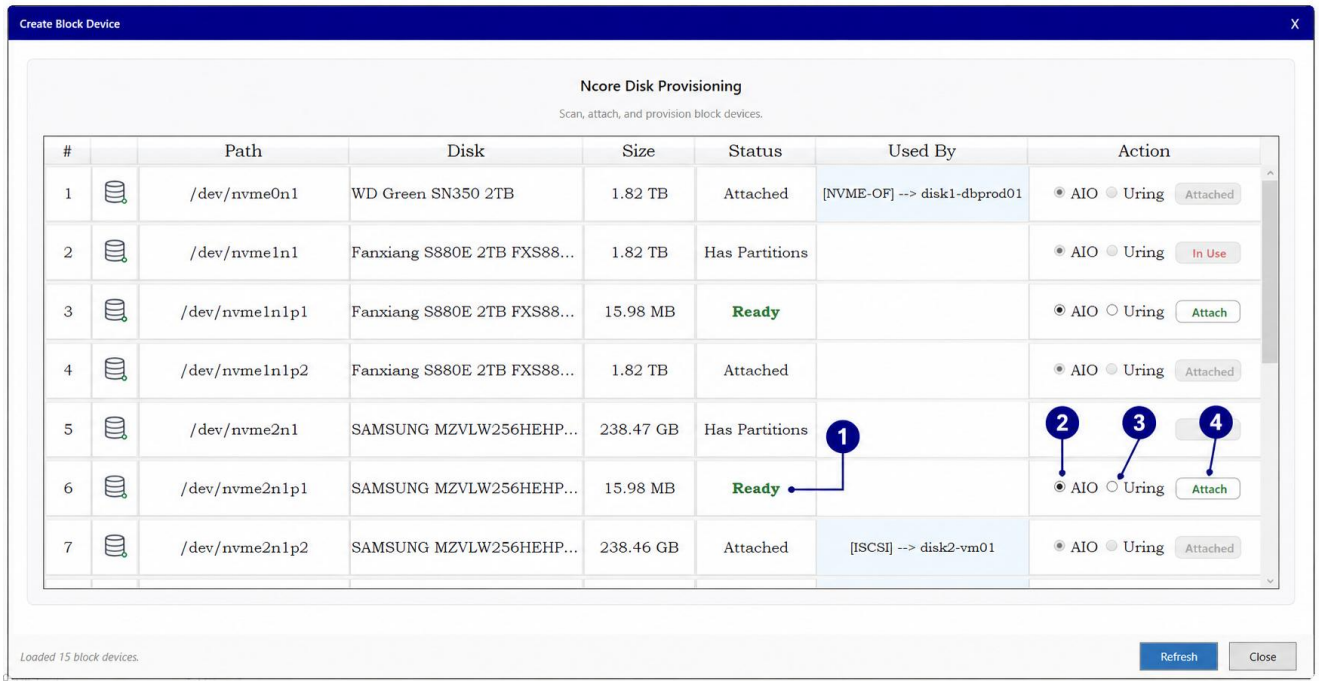

Figure 5 - Attach an available block device using AIO or URING

AIO (Asynchronous I/O) and URING (io_uring) are Linux I/O technologies that Ncore SAN uses to read from and write to storage devices. AIO provides broad compatibility, while URING is a newer technology designed to reduce processing overhead and improve performance. Neither option formats the device or changes its data.

Attach the device

1. **Confirm availability:** Select a block device with a Ready status.
2. **Choose the I/O method:** In the Action column, select AIO or URING.
3. **Attach the device:** Click Attach.
4. **Finish:** Click Close when finished.

Device status reference

Status	Meaning
Ready	The block device is available and can be attached using AIO or URING.
Has Partitions	The disk contains partitions and cannot be attached as a whole. An available partition may be attached separately.
Attached	The block device is already attached to Ncore SAN.
In Use	The block device is currently in use and cannot be attached.

6. iSCSI Targets

Create and manage iSCSI targets that expose attached disks over standard IP networks.

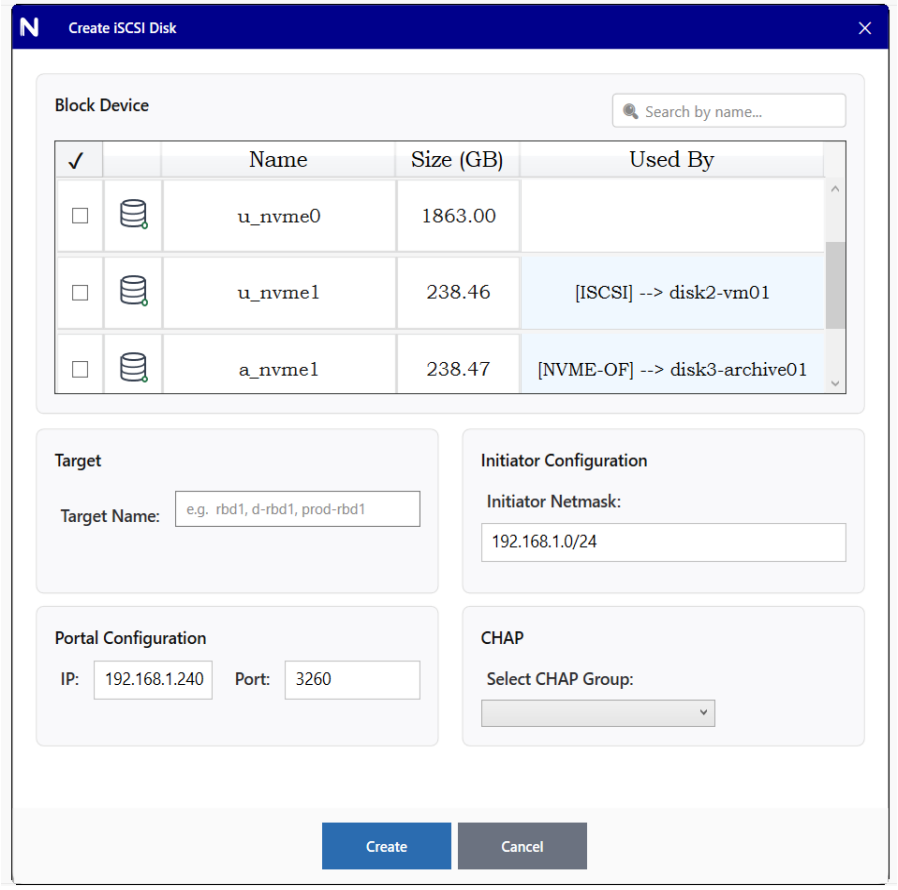

Figure 6a - Create an iSCSI target

1. Select iSCSI from the navigation panel and click Create iSCSI Disk.
2. Select one or more unassigned disk.
3. Enter a unique target name, initiator network, and portal IP address. The default iSCSI port is 3260.
4. Optionally select a CHAP authentication group.
5. Review the configuration and click Create.

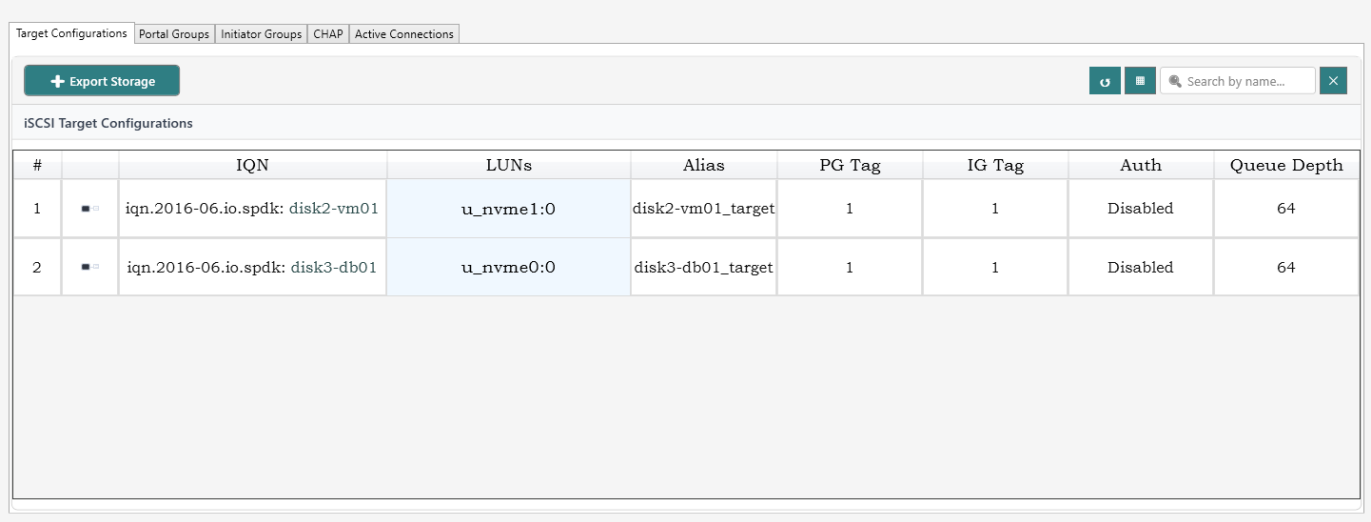

Figure 6b - iSCSI target configurations

7. CHAP Management - Create CHAP User and Auth Group

Create CHAP authentication groups and user credentials for authenticated iSCSI access.

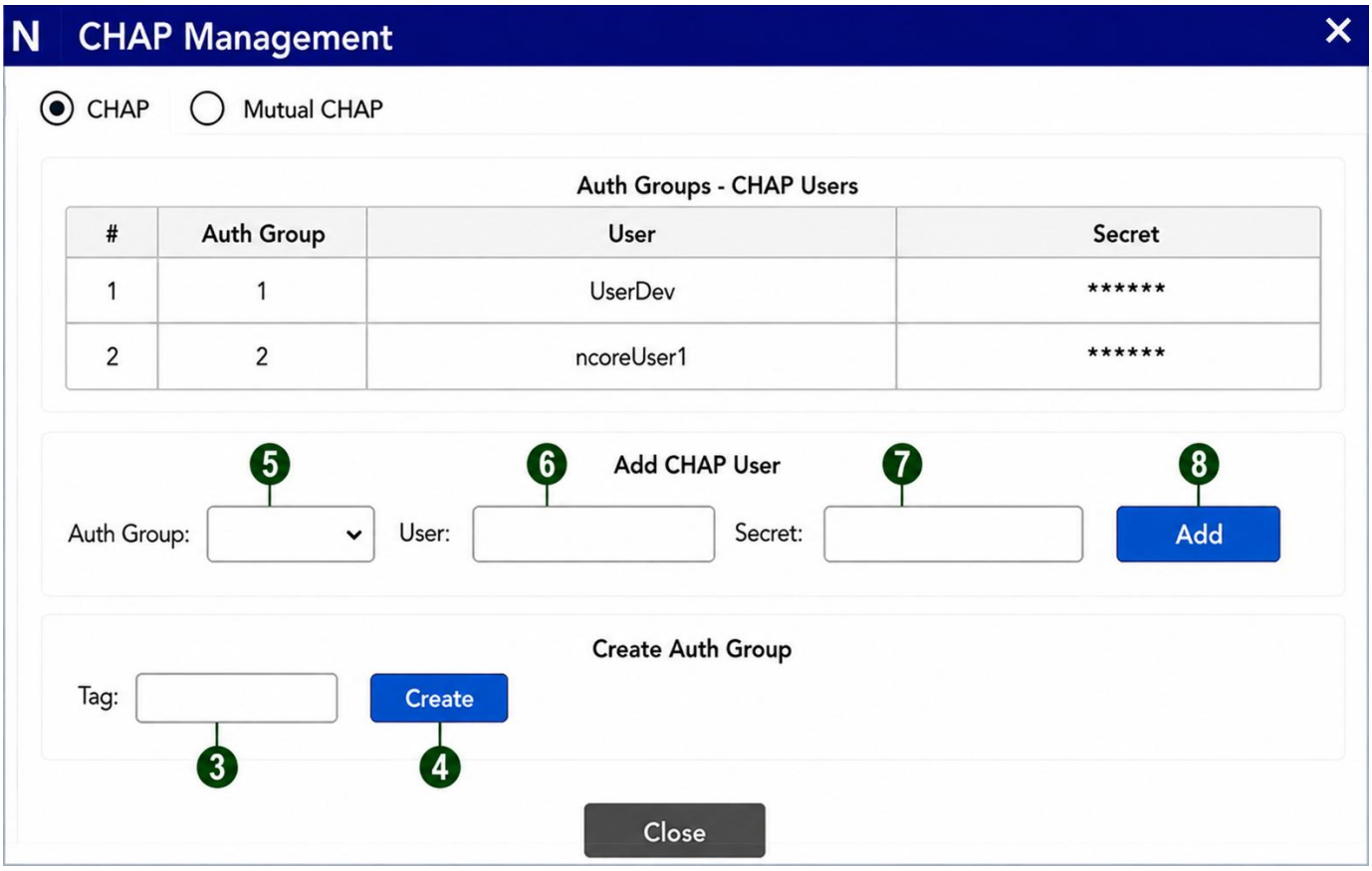

Figure 7 - CHAP management

1. Open iSCSI management and select CHAP Management.
2. Select the CHAP tab.
3. Enter a numeric Tag value (e.g. 2) if the ID does not exist, else go to Step 5.
4. click Create to create an authentication group.
5. Select the new or existing authentication group (select a Tag ID from the drop-down list).
6. Enter the CHAP username
7. Enter user secret.
8. Click Create.

Security: Use unique CHAP credentials for each intended access scope and store secrets securely.

7a. CHAP Management - Create Mutual CHAP User

Add mutual CHAP credentials when both the initiator and target must authenticate each other.

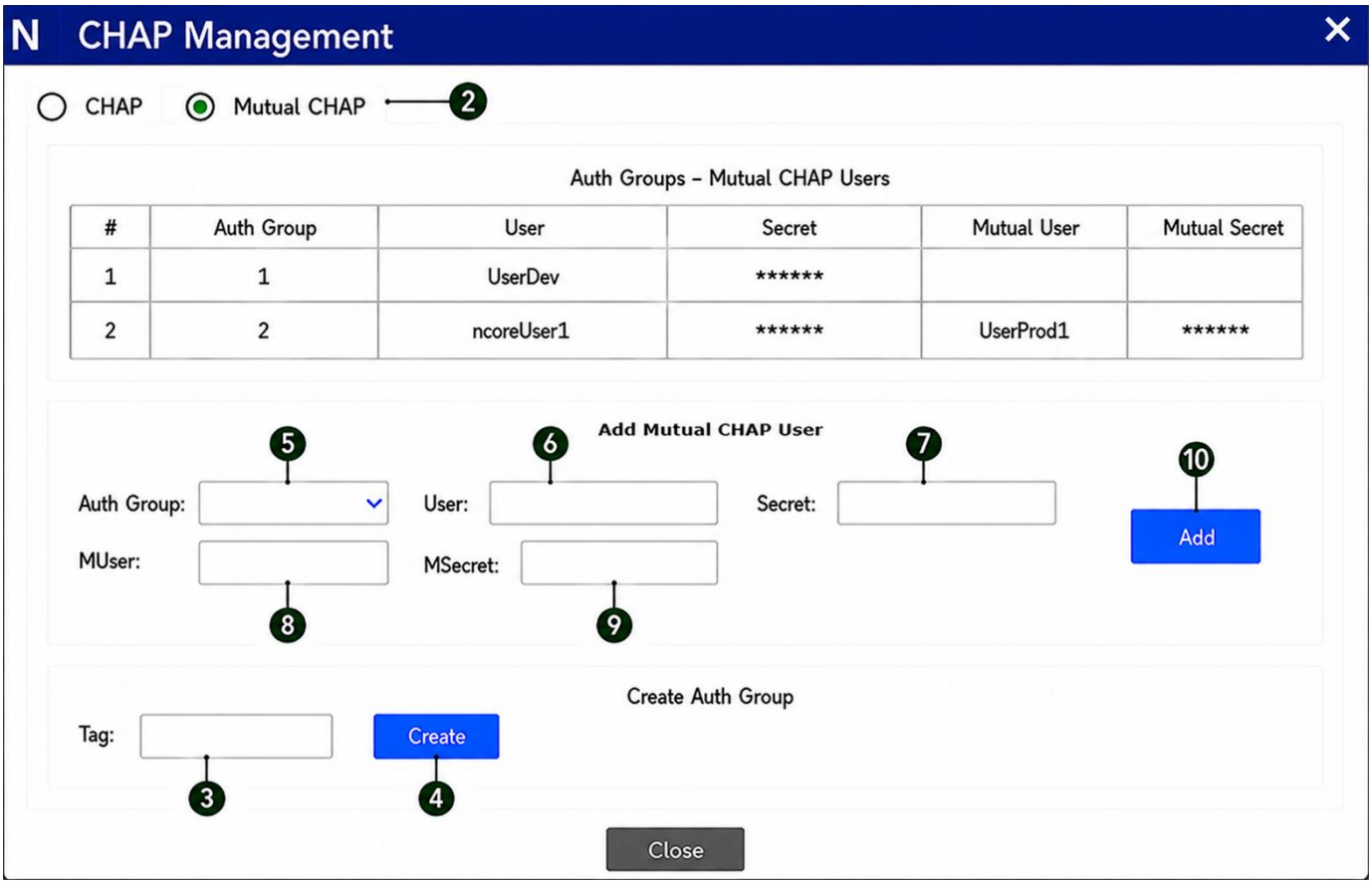

Figure 8 - Mutual CHAP management

1. Open iSCSI management and select CHAP Management.
2. Select the Mutual CHAP tab.
3. Enter new Tag ID if not already created
4. Click Create to add new Tag ID (e.g. 2) if the ID don't exist, else go to Step 5.
5. Select an authentication group (select a Tag ID from the drop-down list)
6. Enter the CHAP username
7. Enter the User secret.
8. Enter the Mutual Chap username.
9. Enter the Mutual Chap secret.
10. Click Add.

8. NVMe-oF Subsystems

Create NVMe-oF subsystems that expose attached disks to remote hosts using TCP or RDMA.

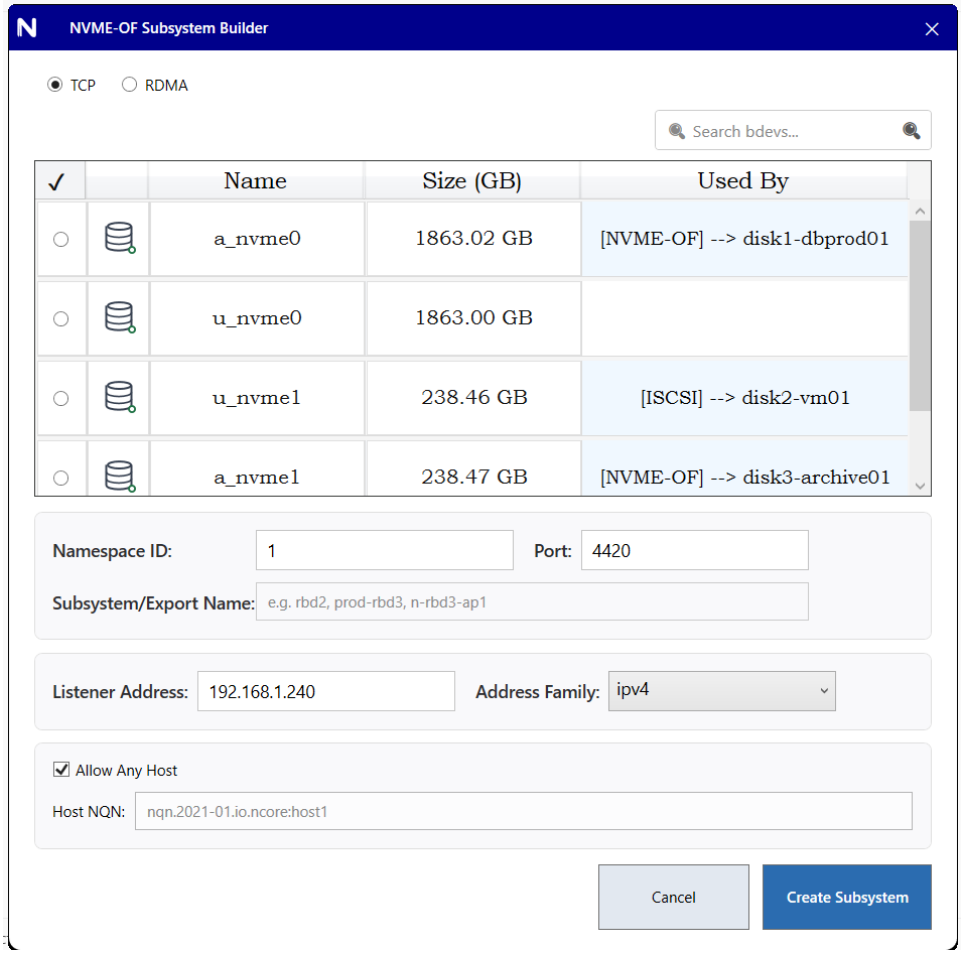

Figure 9a - NVMe-oF subsystem builder

1. Select NVMe-oF from the navigation panel and click Create Subsystem.
2. Choose TCP or RDMA.
3. Select an unassigned disk.
4. Enter the namespace ID, subsystem NQN, listener address, port, and address family.
5. deselect “Allow Any Host” to authorized specific host NQN.
6. Review the configuration and click Create Subsystem.

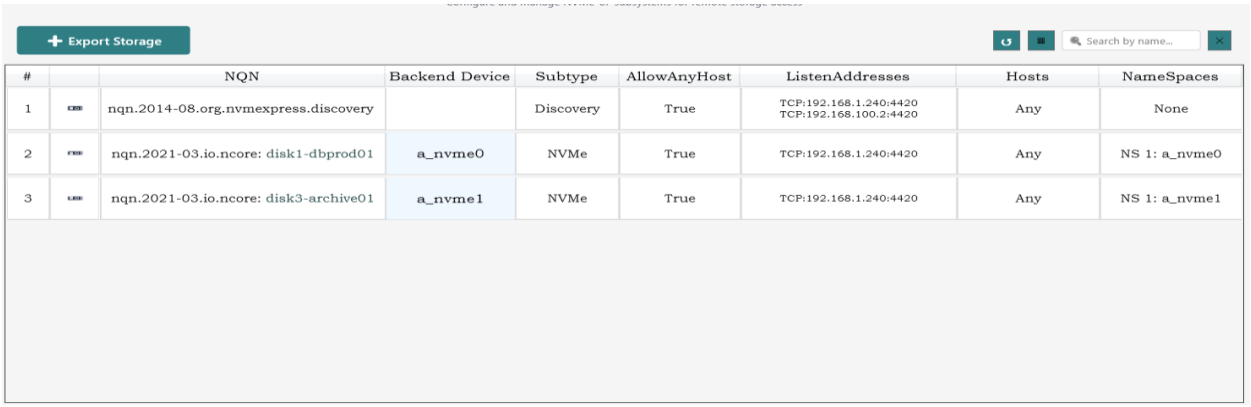

Figure 9b - NVMe-oF subsystems

9. Basic Troubleshooting

Use these checks to resolve common issues in the Ncore management interface. Record the displayed error and affected object name if assistance is required.

Issue	Initial check
Cannot connect to the gateway	Verify the HTTPS gateway URL, username, password, TLS certificate, and license status. Click Test Connection.
AIO or URING disk is not listed	Click Refresh, clear the search text, and confirm that the device path exists, is not mounted or otherwise in use, and is accessible to Ncore SAN.
Disk cannot be attached	Confirm the disk status is Ready and enter a unique block-device name.
Disk cannot be selected for export	Check Used By. Select an unassigned disk or remove the existing export first.
Cannot create an iSCSI target	Verify the target name, initiator network, portal address, port 3260, selected block device, and optional CHAP group.
iSCSI client cannot connect	Verify the portal, initiator network, firewall, and CHAP credentials.
NVMe-oF connection fails	Verify transport, listener address, port 4420, host NQN, and block device assignment.
CHAP authentication fails	Verify the authentication group, username, secret, and mutual credentials when enabled.
Changes are not displayed	Click Refresh, clear search filters, or reopen the applicable Ncore page.
Operation remains unavailable	Check the gateway connection and license status; record the exact error before contacting support.

Still need assistance?

Provide the error message, Ncore SAN status, and affected disk, target, or subsystem name to support@ncorestorage.com.