NAS Series
Web GUI Manual

Switch configuration through the web interface

Contents

01	First login	**3**
02	Navigate and save changes	**4**
03	System and management	**5**
04	Ethernet ports	**6**
05	Link aggregation and VLANs	**7**
06	Layer 3 addressing and routing	**8**
07	Security and access lists	**9**
08	Authentication and management access	**10**
09	DHCP services	**11**
10	Multicast switching and routing	**12**
11	PIM sparse mode	**13**
12	Spanning tree and ring protection	**14**
13	Quality of service	**15**
14	Save, back up, and maintain	**16**

01 / NAS SERIES

First login

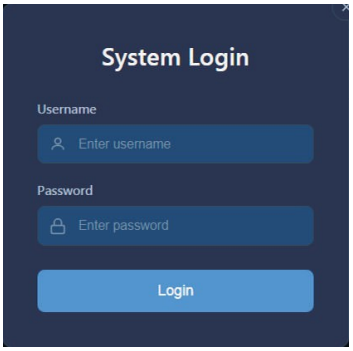
Connect a laptop and open the switch management address in a browser. Have the switch model, its current management IP address, and an authorized account available.

1. Connect the laptop

Use the Ethernet management port if your model has one. Otherwise, use a network port assigned to the management VLAN. For a direct connection to a factory-configured NAS24T4XP, set the laptop to an unused address such as 192.168.0.2 with subnet mask 255.255.255.0.

2. Sign in

For the NAS24T4XP at factory settings, open http://192.168.0.1 and enter admin for both username and password in lowercase. Click Login. For an installed switch, use its assigned management address and account. Check the model's quick installation guide for its factory settings.



NAS24T4XP / Login screen

3. Identify the switch

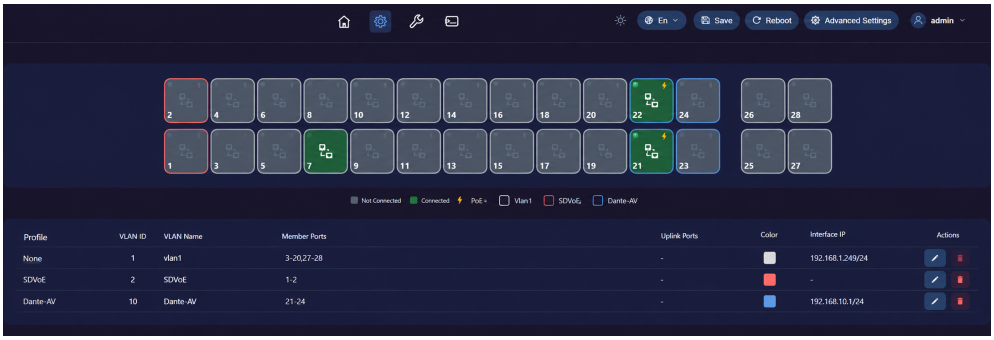
Open System Information. Record the firmware version, serial number, and base MAC address before changing settings. The pages and options available depend on the NAS model, firmware, and account privileges.

> **If the page fails to load, check the port link, laptop address, subnet mask, and management VLAN. If the login page opens but rejects the password, check the account and capitalization.**

02 / NAS SERIES

Navigate and save changes

Choose a menu group, then a page in its navigation tree. The main pane displays the settings or status for that selection. Some firmware versions display a dashboard after login.



NAS24T4XP / Dashboard detail

Work with controls and tables

Control	Action
Refresh	Read the current values from the switch.
Apply	Validate the entries and update the running configuration. If the switch reports an error, correct the indicated field and apply again.
New	Select New in the entry selector, complete the active row, and click Apply.
Existing entry	Select the row number to load it into the edit fields. Change the values and click Apply, or select Delete to remove that record.
Status and Help	Status reports the entry state. Help opens instructions for the current page.

Keep changes after a restart

Check the result in the corresponding status page. Open Tools, select the save configuration page, and click Save. Allow the write to finish. Backup downloads the saved configuration to your computer.

System and management

Use the System menu to identify the switch, set its management address, manage accounts, and configure time and monitoring.

Management access

Page	What to do
System Information	Read the hardware and firmware versions, serial number, base MAC address, system object ID, and uptime. Set the system clock if manual time is required.
IP Address	Select the management VLAN and enter its IP address, subnet mask, and gateway. Apply. If your session closes, move the laptop to the new subnet if necessary and reconnect at the new address.
User Management	Enter the account name, select common or privileged access, enter and confirm the password, then apply. Names and passwords are case-sensitive.
Serial Information	Read the baud rate, character size, parity, stop bits, and flow control before opening a console session.

Time, monitoring, and logs

Page	What to do
SNTP	Enter up to three time server IP addresses. Set the synchronization interval in seconds and the site time zone. Enable SNTP, apply, then check Last Update Time and System Date Time.
SNMP Community	Enter a community name and choose its access level. Use read-only access for polling. To change a configured entry, delete it and create its replacement. The documented public entry is read-only and cannot be deleted.
SNMP Trap	Enter a target name, receiver IP address, and supported SNMP version. Apply and verify receipt at the monitoring system. To change a target, delete it and create its replacement.
Log Information	Filter by Critical, Warning, Informational, or Debugging and click Refresh to retrieve the latest entries.

Ethernet ports

Select one port for an individual change. When you select several ports, the switch applies the same values to every selected port. Check the selection before clicking Apply.

Port configuration and counters

Page	Procedure
Port Basic Configuration	Select the ports. Set administrative state, speed/duplex, flow control, and maximum jumbo-frame size as required. Use a speed supported by the physical port and its link partner.
Port Statistics	Read packet and octet counters, errors, and discards for each port. Refresh twice to determine which counters are increasing while traffic is present.
Storm Control	Select the ports and enable suppression for broadcast, multicast, or destination lookup failure (DLF) traffic. Enter the limit in kbit/s. The selected traffic classes on a port share the configured rate setting.
Port Speed Limit	Set the receive and transmit rate controls separately. Enable the direction to be limited, enter the rate in kbit/s, and apply. Clear the corresponding control to remove the limit.
Protected Port	Select ports and click Protected Port to isolate them from other protected ports. They can still communicate with unprotected ports. Select Unprotected Port to reverse the setting.
DDM Information	View digital diagnostic monitoring information for installed optical modules where available.

Mirror traffic for inspection

On Port Mirroring, select one Listen Port for the analyzer. Select one or more source ports and choose Receive, Transmit, or both directions as needed. Keep the listen port separate from the source ports. Apply and verify that the analyzer receives traffic. To end mirroring, select the unset listen-port option and apply.

Link aggregation and VLANs

The Port menu uses Trunk Group for link aggregation. The VLAN menu uses Trunk for a port carrying multiple VLANs. Choose the menu for the task you intend to perform.

Combine physical links

1. Open Create Trunk Group. Choose a group ID and either static aggregation or dynamic LACP. Configure a matching aggregation mode on the peer.

2. Select a load-balancing method based on source, destination, or combined source/destination MAC or IP addresses. Create the group.

3. Open Trunking Configuration. Select the group and member ports, then apply. Review Trunk Information to verify membership.

Create VLANs and assign ports

Open VLAN Configuration. Enter a VLAN ID from 2 to 4094 and apply. VLAN 1 already exists. The membership table shows T for tagged and U for untagged. Delete All removes all deletable VLANs.

Port mode	Configuration
Access	Select the port and one VLAN. Apply, then verify that the port appears as an untagged member of the intended VLAN.
Trunk	Select the port and the VLANs it should carry. Shift-select a consecutive range where supported. Apply and verify membership against the other end of the link.
Hybrid	Select one default VLAN. Select the tagged and untagged VLANs required for the port. In this GUI, assign each VLAN to only one of the three selections.

Changing the mode or VLAN of the port carrying your management session can disconnect your laptop. Check the management path first.

Layer 3 addressing and routing

Use Layer 3 to assign addresses to VLAN interfaces, inspect address resolution, and select routes between IP networks.

Configure interfaces and static routes

Page	Procedure
VLAN Interface	Select the VLAN interface and assign or remove its IP address. Verify the address in the interface list.
ARP	Review the IP-to-MAC mapping. To add a static entry, enter the IP address and its unicast MAC address and apply. The page also supports deleting an entry or converting a learned mapping to a static one.
Static Routing	Add the destination network, prefix, and next hop for the required route. Use 0.0.0.0/0 for a default route. Select the corresponding entry to remove a route.
Routing Table Information	Filter by Active or All. Filter by Connected, Static, RIP, OSPF, or All to check which route is available for the destination.

Dynamic routing

Protocol	Configure and verify
RIP	Enable RIP and add each participating network. The switch activates RIP on the corresponding VLAN interface. Inspect RIP Interface and RIP Route to verify participation and learned routes.
OSPF	Select the OSPF process ID, enable the process, and associate each participating network with the intended area ID. Review OSPF Interface, Neighbor, LSA, and Route to check interface participation, adjacencies, advertisements, and learned routes.

Virtual gateway with VRRP

Select a Layer 3 VLAN interface and a virtual router ID (1–255). Set the virtual IP address, priority, advertisement interval, preemption, and matching authentication settings. When the virtual IP is the interface's own IP address, select Owner and use priority 255. Enable the virtual router and review its role on VRRP Information.

Security and access lists

Use the Security menu to bind or filter MAC addresses and to apply access control lists (ACLs) to incoming traffic.

MAC address controls

For manual binding, select the port and enter the device MAC address and VLAN ID. To retain a learned binding, select the learned MAC/VLAN entry on the automatic conversion page and convert it to static. Use MAC Filtering to enter the MAC address and VLAN for a filter on the selected port.

Create an ACL group

ACL type and group IDs	Fields available for matching
Standard IP: 1–99 or 1300–1999	Source IP address and wildcard mask.
Extended IP: 100–199 or 2000–2699	Source and destination IP addresses with wildcard masks, protocol, TCP/UDP ports, and TCP flags where applicable.
MAC IP: 700–799	Source MAC address, source IP address, and destination IP address, with their match masks.
MAC ARP: 1100–1199	ARP operation, sender MAC address, and sender IP address, with their match masks.

For each rule, select allow or deny and enter the matching criteria. For example, source 192.168.0.0 with wildcard mask 0.0.0.255 matches 192.168.0.0 through 192.168.0.255. The switch assigns rule numbers.

Apply and verify the list

Open the port ACL application page. Select the port, choose an existing group, and click Add. Open ACL Configuration Information to review the rules and their port references. To detach a group, select it in the referenced group list and click Delete.

Authentication and management access

Configure authentication in the AAA pages. Keep a working management connection available while changing access controls.

Configure 802.1X and RADIUS

1. Open AAA Global Configuration and enable 802.1X. Enter the primary RADIUS server address and the shared key configured on the server. Enter a standby server address if used.

2. Enable accounting when required. If periodic reauthentication is required, enable it and set the interval in seconds.

3. Open AAA Port Configuration. Select the intended ports, choose the authentication mode, set the maximum host count, and apply.

Port mode	Effect
Auto	Uses 802.1X authentication to control access.
Force-authorized	Forces the port into the authorized state.
Force-unauthorized	Forces the port into the unauthorized state.
N/A	Allows access without 802.1X authentication on the port.

Open AAA User Information and select a port to review the state of connected users.

Restrict management services

Open Safe Management Configuration. Select the Telnet, Web, or SNMP service to enable or disable. To restrict a service by source IP address, enable it and select an existing standard IP ACL group in the range 1–99.

> **Before restricting Web access, confirm that the ACL permits your management laptop. Disabling Web or excluding the laptop can require console access to restore browser management.**

DHCP services

Choose the role needed on each Layer 3 VLAN interface. A client obtains an address for the switch interface. A relay forwards requests to a server. A server assigns addresses to clients.

Client and relay

On DHCP Client, select the interface, enable the client, and inspect DHCP Client Information. On DHCP Relay, select the interface, enter the primary and optional backup server IP addresses, enable relay, and check DHCP Relay Information.

Configure an address pool

1. On the DHCP Server global and interface page, enable the global server. Select the Layer 3 VLAN interface and enable DHCP Listen for that interface.

2. Open Address Pool Configuration, enter a pool name, and click Create. Select the newly created pool for editing.

3. Set the address range, subnet mask, default router, and DNS servers. Set the lease duration in days, hours, and minutes, or select an infinite lease. Add excluded address ranges. Set an Option 82 Circuit ID if the design uses it.

4. Apply. Connect a client and inspect DHCP Server Address Information to verify the assigned address.

DHCP snooping

Open DHCP Snooping Global Configuration and identify the trusted port or ports through which authorized server replies arrive. The documented page provides up to four trusted server-port selections. Enable global snooping and apply the required settings on the interface page. Review the DHCP Snooping Binding Table after a client obtains a lease.

Multicast switching and routing

For multicast within one VLAN, start with IGMP Snooping. For forwarding between Layer 3 interfaces, start with Multicast Routing.

Configure IGMP snooping on a VLAN

1. On IGMP Snooping Configuration, enable global snooping. Select the VLAN ID and enable VLAN IGMP Snooping for that VLAN.

2. If this switch should send membership queries on the VLAN, enable Querier and set the query interval. Review the query membership and group membership timeouts.

3. Enable Fast Leave only where a leave from one receiver can safely remove forwarding on that port. Check the fast-leave timeout before applying.

4. Start a receiver and open Multicast Group Information. Verify the expected group and member ports in the selected VLAN.

Enable multicast routing and interface IGMP

Enable Multicast Routing before configuring routed IGMP or PIM-SM. Use the multicast routing table to inspect forwarding entries. On IGMP Configuration, select the Layer 3 interface, enable IGMP, and check IGMP Status.

IGMP setting	What it controls
Query Interval and Max Response Time	How frequently the interface sends queries and how long hosts have to reply.
Robustness Variable	Retransmission behavior and associated timers.
Last Member Query Interval and Count	Spacing and number of group-specific queries after a leave.
IGMP Version	Version of IGMP packets the interface sends.

Review IGMP Interface and IGMP Group to verify the running interface and group membership. Enabling PIM-SM on an interface also keeps IGMP running there.

PIM sparse mode

Use PIM-SM when the network design calls for routed multicast. Enable global multicast routing first.

Global configuration

Field	Action
RP Address	Enter the static rendezvous point address if the design uses a static RP.
Candidate RP and Candidate BSR	Select the Layer 3 interface for each dynamic role used in the design. Selecting none disables that local candidate role.
JP Interval	Set the interval between join/prune messages.
SPT Switch	Select whether to switch from the shared tree to the shortest-path tree.

Interface configuration

Select a participating Layer 3 interface and enable PIM-SM. Use passive mode only where the interface should receive PIM-SM packets without sending them. Set Hello Interval, Hello Holdtime, and DR Priority as required for the design.

Verify the multicast path

Information page	Check
Interface Information	Expected participating interfaces.
Neighbor Information	Expected PIM neighbors on routed links.
RP Information	Rendezvous point mappings for the multicast groups.
BSR Information	Bootstrap router information when dynamic RP discovery is used.
Mroute Information	Multicast routing entries for the active traffic.

Spanning tree and ring protection

Use the Ring menu for spanning tree, Ethernet Ring Protection Switching (ERPS), or Ethernet Automatic Protection Switching (EAPS). Select the protocol specified in the network design.

Spanning tree

Open the global spanning tree page to configure the switch parameters. Open the port page to inspect MSTP state on each participating port.

ERPS

1. On Predefined Configuration, choose the predefined mode only if its node role, ring ports, protocol VLAN, protected VLANs, and timers match the installation. Review the displayed values.

2. For manual setup, open Instance Configuration. Select an unused instance, specify the role, and click Apply. A role can be changed while the instance has no associated ring.

3. Open Ring Configuration. Select a ring, associate it with one instance, enter the ring settings, and apply. Open ERPS Information and select the ring number to verify its state. Use Manual Restore only when the ring is ready to be restored.

EAPS

Select the ring number and node mode. Set primary and secondary ports, control VLAN, and protected VLANs. Set the health-message interval shorter than the fail timer. Set the compatibility option if required by the ring design. Enable the domain and review EAPS Information.

Quality of service

The Advanced menu separates traffic classification from queue scheduling. Configure both for the selected ports according to the traffic policy.

Classify incoming traffic

Open QoS Apply Configuration. Select the ports and choose a QoS Type. Apply and confirm the selected ports show the intended settings.

QoS type or field	Use
CoS-based	Classify using the Layer 2 class of service.
DSCP-based	Classify using the IP packet's DSCP value.
Apply-policy	Select an existing Policy ID. Create the required policy before assigning it here.
User Priority	Set the port priority used for incoming untagged frames.

Schedule outgoing queues

Open QoS Schedule Configuration. Select the ports, choose the scheduling mode, and enter queue weights for a weighted mode. Click Apply.

Mode	Scheduling method
SP	Strict priority.
RR	Round robin.
WRR	Weighted round robin.
WDRR	Weighted deficit round robin.

The documented scheduler exposes queues 0–7 and weights from 1 to 127. The displayed default weights in queue order are 1, 2, 4, 8, 16, 32, 64, and 127. Check the actual queue settings on the switch before changing them.

Save, back up, and maintain

Use Tools for configuration files, firmware, factory reset, and restart. Perform disruptive operations during an appropriate maintenance window.

Save and back up

1. Open Save Configuration and review the running configuration. Click Save and wait for the write to finish. The saved file is used at startup.

2. Open Backup Configuration and click Backup. Choose a folder on the laptop. The documented default filename is switch.cfg. Keep a copy identified by switch and date.

Restore a configuration

Open Restore Configuration and select Browse. Choose the intended .cfg file and click Upload. Keep the session on this page and leave the switch powered on until the transfer result appears. Check the management address and configuration after the operation.

Update the firmware

On Software Upgrade, browse to the Niveo Professional .img firmware file for the exact model and click Upload. Keep the switch powered on and remain on the page until the result appears. Follow the displayed completion instructions. Check the firmware version under System Information afterward.

Restart or restore factory settings

Operation	What happens
System Reboot	Restarts the switch and interrupts management and network traffic. Save changes first. Confirm the restart and reconnect when the switch is ready.
Restore Factory Configuration	Deletes the saved configuration and restarts with factory settings. Back up the configuration first. After restart, reconnect using the model's factory management address and credentials.