Navijin

CONFIGURATION GUIDE

NAVIJIN L2 MANAGED SWITCHES

L2 Managed Switch: Working with VLANs

Segment your network into secure, manageable groups. Create VLANs, name them, assign access ports and carry VLANs over trunks, in the web interface and in the CLI.

VLAN design | Access ports | Trunk ports | Web interface | CLI | Verification

Applies to
Navijin L2 managed switches (e.g. GE6010 series)

Document
NJ-CG-L2-002 · Rev. 2.0

Published
November 2026

ABOUT THIS GUIDE

Before you begin

A VLAN (Virtual Local Area Network) divides one physical switch into several logical networks. Devices in different VLANs cannot talk to each other unless a router or Layer 3 switch allows it. This improves **security** (guests cannot see staff PCs), **performance** (smaller broadcast domains) and **management** (policies per group). This guide shows a complete example: VLAN 10 named **IT**, with port GE5 as an access port and port GE24 as a trunk uplink.

Conventions: menu paths are shown in **bold** (for example **Network** → **VLAN**); commands and values in `monospace`. Screenshots may differ slightly by firmware version.

Who this guide is for

- Integrators deploying Navijin switches in offices, hotels and campuses
- IT administrators separating staff, guest, voice and CCTV traffic

What you need

- Admin access to the switch (see **Initial Setup**)
- Your VLAN plan: IDs, names and which ports belong where
- A backup of the current configuration

Factory defaults

Setting	Default
Default VLAN	VLAN 1 on all ports
Default port mode	Trunk
Management VLAN	VLAN 1 (change it, see Management and SSH)

Contents

01 Plan your VLANs

02 Create and name a VLAN (web interface)

03 Assign an access port (web interface)

04 Allow the VLAN on a trunk (web interface)

05 The same configuration in the CLI

06 Verify and troubleshoot

SECTION 01

Plan your VLANs

Five minutes of planning saves hours of troubleshooting. Decide the VLANs, their subnets and the role of every port before you configure anything.

VLAN ID	Name	Typical use	Example subnet
10	IT / STAFF	Office PCs and laptops	10.10.0.0/24
20	VOICE	IP phones	10.20.0.0/24
30	CCTV	IP cameras and NVR	10.30.0.0/24
40	GUEST	Visitor Wi-Fi	10.40.0.0/22
100	MGMT	Switch and AP management	192.168.100.0/24

Port type	Carries	Connects to
Access	One untagged VLAN	PCs, printers, cameras, phones
Trunk	Several VLANs, 802.1Q tagged	Other switches, routers, firewalls, Wi-Fi access points

TIP

Do not use VLAN 1 for user traffic. Keep it unused and move management to a dedicated VLAN.

SECTION 02

Create and name a VLAN (web interface)

1 Open VLAN creation

Log in to the web interface and go to **VLAN → Create VLAN**. The page shows two columns: **Available VLAN** (not yet created) and **Created VLAN**. By default only VLAN 1 exists.

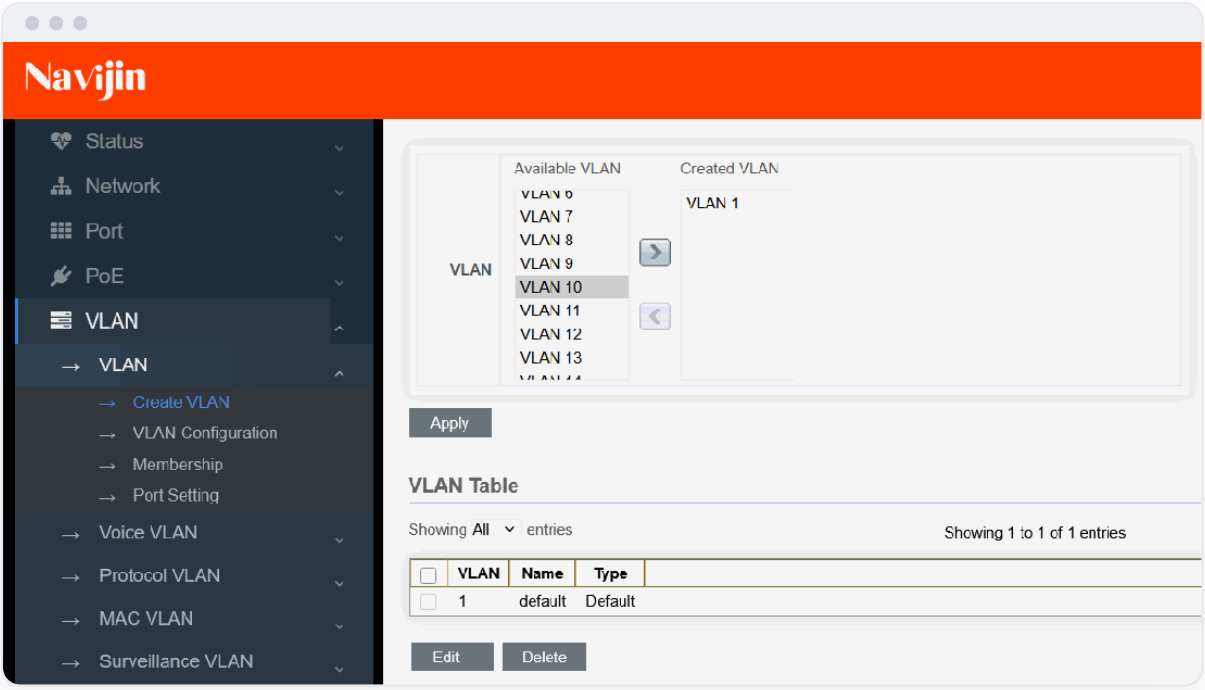


Figure 1. Create VLAN page with available and created VLAN lists.

2 Create VLAN 10

Select **VLAN 10** in the Available VLAN column, move it to the Created VLAN column with the arrow button and click **Apply**. VLAN 10 now appears in the VLAN Table.

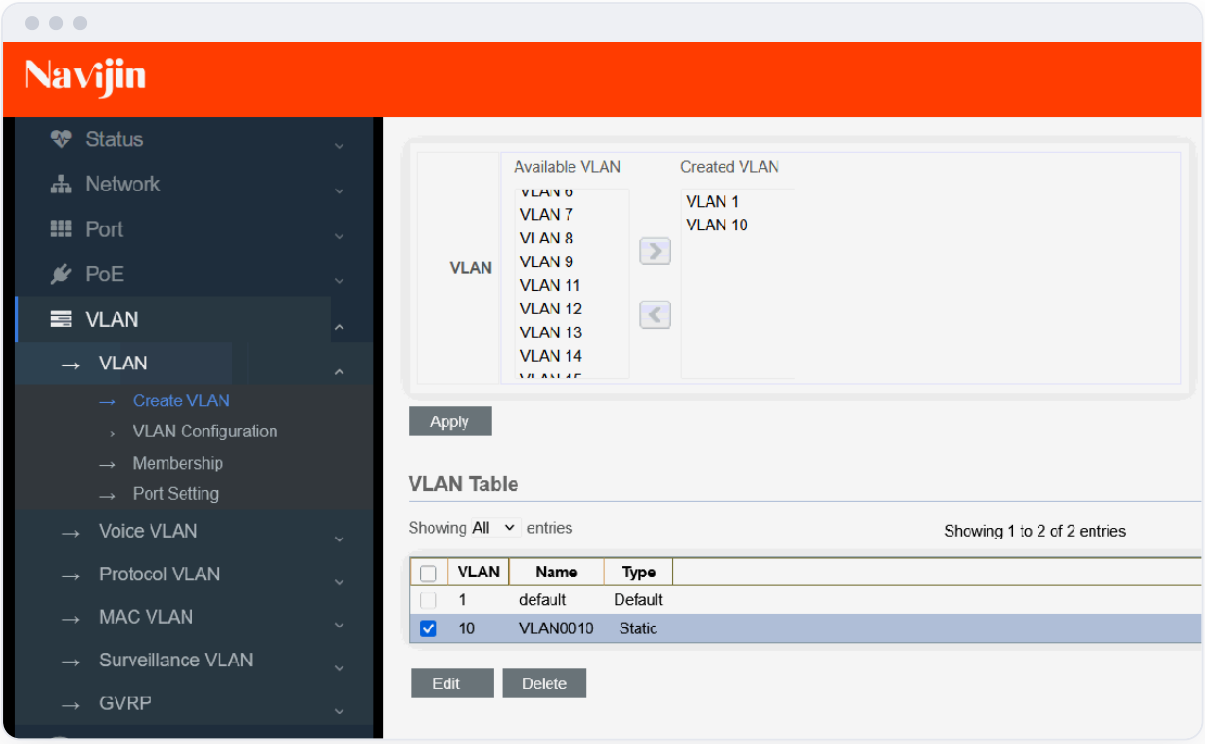


Figure 2. VLAN 10 created and listed in the VLAN Table.

3 Name the VLAN

Select VLAN 10 in the table, click **Edit**, enter the name `IT` and click **Apply**. Clear names make troubleshooting much easier.

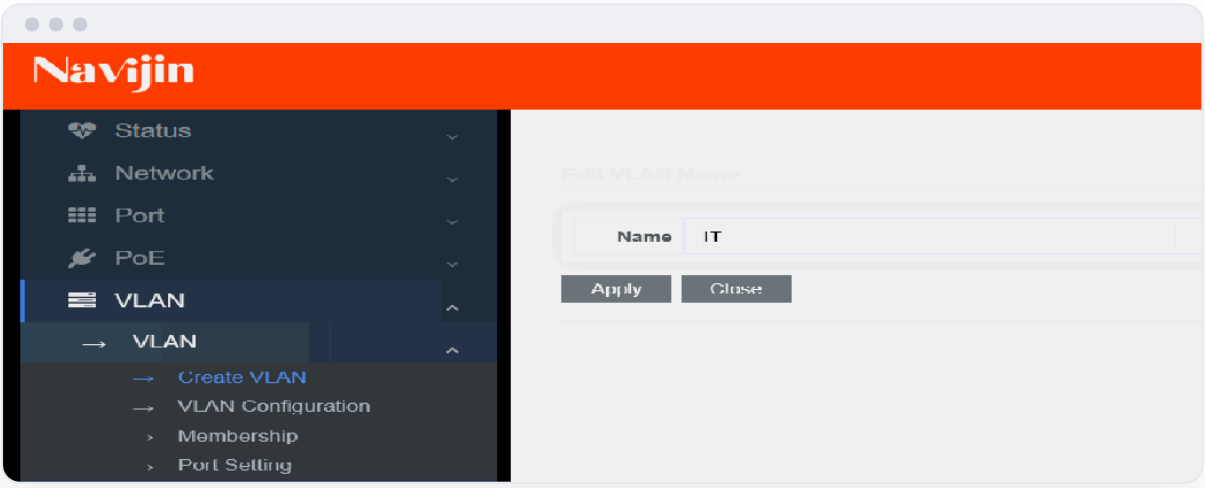


Figure 3. Editing the VLAN name.

SECTION 03

Assign an access port (web interface)

Access ports connect end devices. Each access port belongs to exactly one VLAN, set by its PVID.

1 Open port settings

Go to **VLAN → Port Setting**. Select the port, for example **GE5**, and click **Edit**.

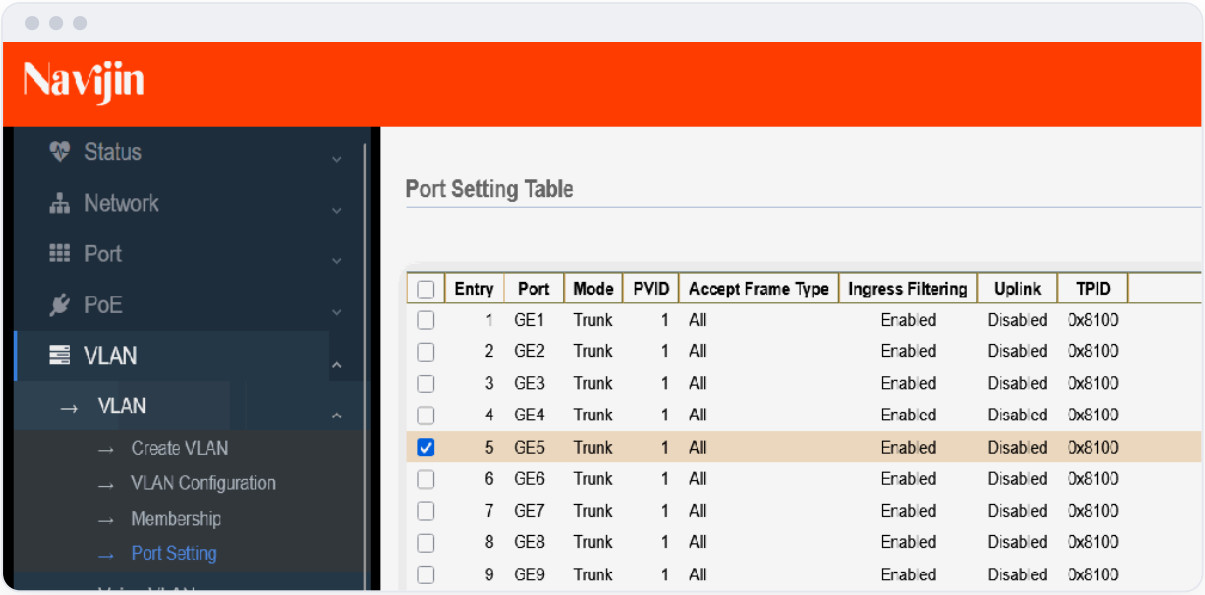


Figure 4. Port Setting table: GE5 selected.

2 Set access mode and PVID

Set **Mode** to **Access** and change **PVID** from `1` to `10`. Click **Apply**. Port GE5 is now an untagged member of VLAN 10.

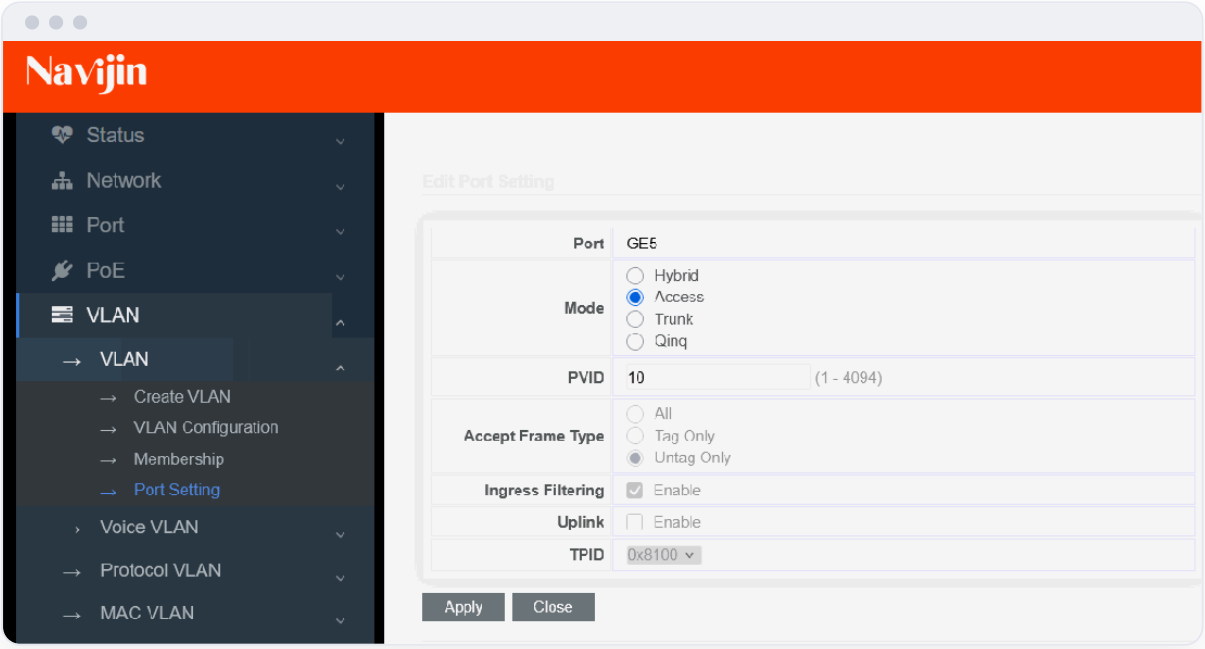


Figure 5. Access mode with PVID 10.

> **NOTE**
>
> Repeat for every port that connects a device of this group. For many ports, use the CLI interface-range commands to save time.

SECTION 04

Allow the VLAN on a trunk (web interface)

Trunks carry several VLANs between switches and to routers, firewalls and access points. On Navijin L2 switches all ports are trunks by default; you choose which VLANs each trunk carries.

1 Open membership

Go to **VLAN → Membership**, select uplink port **GE24** and click **Edit**.

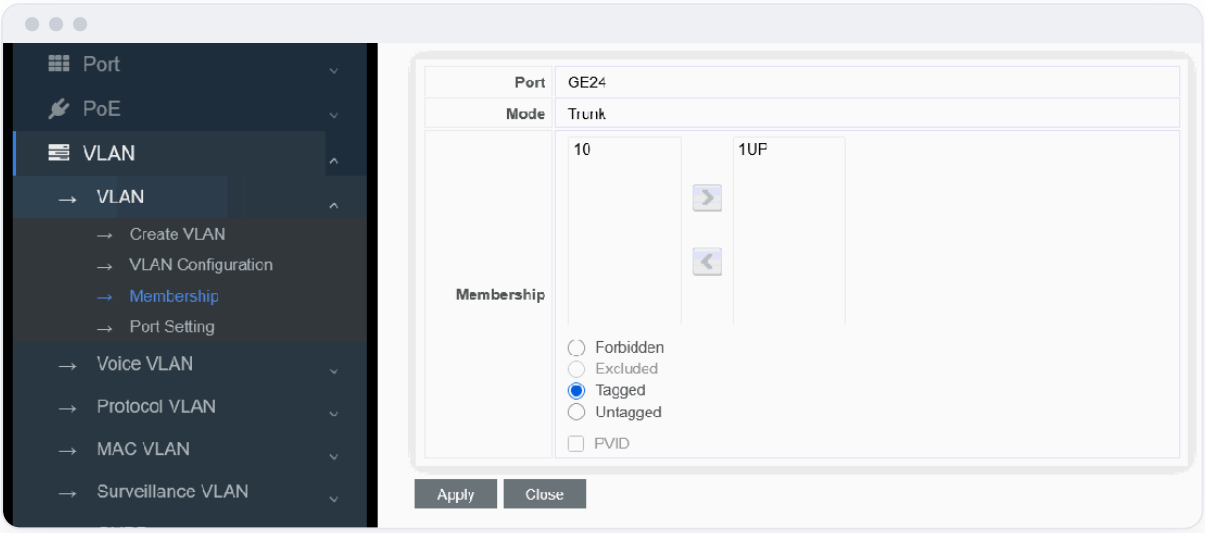


Figure 6. Membership settings for trunk port GE24.

2 Add VLAN 10 as tagged

Move **VLAN 10** from the left column to the allowed (right) column, keep it **Tagged**, and click **Apply**.

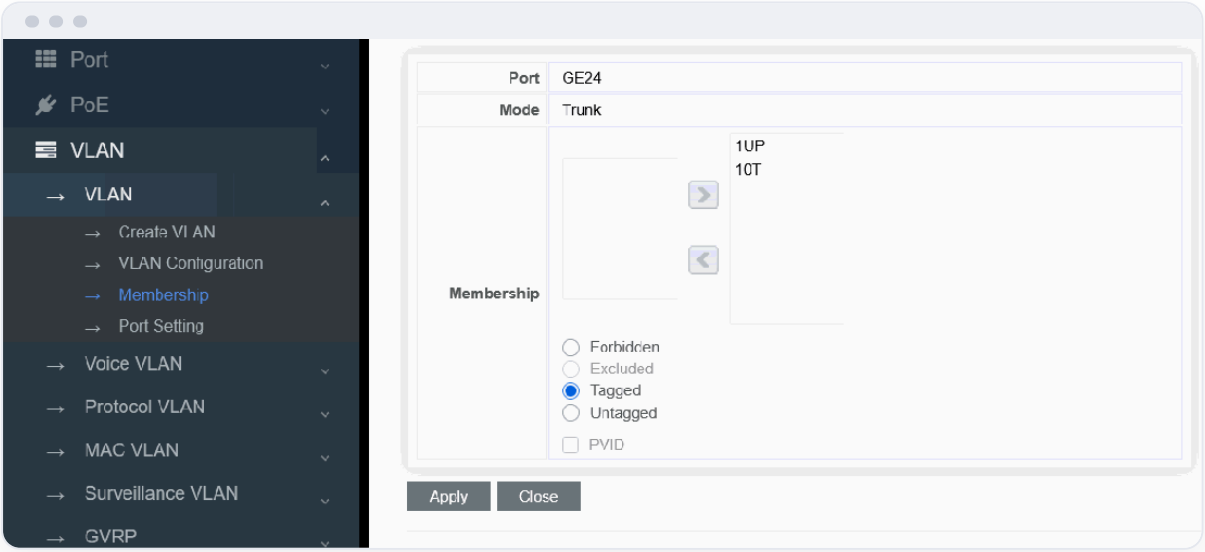


Figure 7. VLAN 10 allowed and tagged on GE24.

IMPORTANT

Configure the same VLANs on both ends of a trunk. If the neighbouring switch or access point does not allow VLAN 10, traffic for that VLAN will not pass.

SECTION 05

The same configuration in the CLI

The command line is faster for repeat work and scripting. Enter global configuration mode with `configure` (or `conf`).

1 Create and name VLAN 10

```
Switch# conf
Switch(config)# vlan 10
Switch(config-vlan)# name IT
Switch(config-vlan)# exit
```

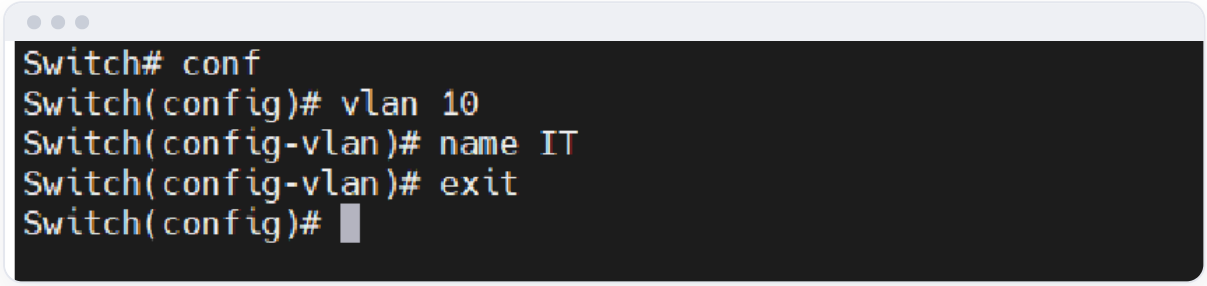


Figure 8. Creating VLAN 10 in the CLI.

2 Make GE5 an access port in VLAN 10

```
Switch(config)# int gi5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

3 Allow VLAN 10 on trunk GE24

```
Switch(config)# int gi24
Switch(config-if)# switchport trunk allowed vlan add 10
Switch(config-if)# exit
```

4 Save

```
Switch# copy running-config startup-config
```

SECTION 06

Verify and troubleshoot

- Check the VLAN Table lists VLAN 10 with the correct name.

- Connect a PC to GE5: it should receive an address from the VLAN 10 DHCP scope.
- From the PC, confirm you cannot reach devices in other VLANs unless routing allows it.
- Check the trunk: devices in VLAN 10 on the next switch should be reachable.

Symptom	Likely cause	Fix
PC gets no IP address	No DHCP for VLAN 10, or the trunk does not carry VLAN 10	Add the VLAN to every trunk on the path; configure DHCP/relay for VLAN 10
Device works on one switch but not across the trunk	VLAN missing on the far end	Allow the VLAN on both ends of the trunk
Lost access to the switch	Management VLAN removed from your port	Reconnect via console and restore the management VLAN
All VLANs can talk to each other	A router or L3 switch routes between VLANs without ACLs	Add firewall or ACL rules between VLANs

Do I need a router for VLANs?

Devices in the same VLAN communicate directly. Communication between VLANs needs a router, firewall or Layer 3 switch.

How many VLANs can I create?

Up to 4094 VLAN IDs are available in 802.1Q. Check your model's datasheet for the number of active VLANs supported.

Should access points be on access or trunk ports?

Trunk ports, so each SSID can map to its own VLAN.

Navijin

Need help?
We are here for you.

TECHNICAL SUPPORT
navijin.com/en/contact/technical

DOCUMENTATION & FIRMWARE
navijin.com/en/documentation

COMMUNITY TUTORIALS
navijin.com/en/tutorials

VERIFY YOUR PRODUCT
navijin.com/en/verification

NJ-CG-L2-002 · Rev. 2.0 · November 2026. Information in this document is subject to change without notice. Screenshots are for illustration and may differ by firmware version. Navijin® is a registered trademark in the United Arab Emirates. © 2026 Navijin. All rights reserved.