Navijin

CONFIGURATION GUIDE

NAVIJIN L2 MANAGED SWITCHES

L2 Managed Switch: Secure Management and SSH

Move switch management into a dedicated VLAN, assign a management IP address and enable SSH, so only administrators can reach the switch, over an encrypted connection.

Management VLAN | Static IP | SSH v2 | Web interface | CLI | Hardening

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

Document
NJ-CG-L2-003 · Rev. 2.0

Published
November 2026

ABOUT THIS GUIDE

Before you begin

Out of the box, the switch is managed in VLAN 1 on `192.168.1.1`, reachable from every port. In production, management should live in its own VLAN that users cannot reach, and administrators should connect with **SSH** instead of Telnet. In this guide we create **VLAN 100 (MGMT)**, give the switch the address `192.168.100.100/24`, use port **23** as the management port and enable SSH v2.

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 handing over secure installations
- IT and security teams hardening network devices

What you need

- Console access (recommended while changing management settings)
- Your management subnet, switch IP and gateway
- An SSH client (PuTTY, MobaXterm or the OpenSSH client)

Factory defaults

Setting	Default
Management IP	`192.168.1.1/24` in VLAN 1
Credentials	`admin` / `admin`
Example in this guide	VLAN 100 MGMT, `192.168.100.100/24`, gateway `192.168.100.1`, port 23

Contents

01 Why a management VLAN and SSH

02 Configure management and SSH in the CLI

03 Configure management and SSH in the web interface

04 Test, harden and troubleshoot

SECTION 01

Why a management VLAN and SSH

- **Isolation:** users, guests and IoT devices cannot reach the switch's login pages.
- **Encryption:** SSH and HTTPS protect passwords and configuration in transit; Telnet and HTTP send them in clear text.
- **Control:** you can allow management only from administrator workstations or a jump host.
- **Compliance:** segmented, encrypted management is expected by most security standards and audits.

> **IMPORTANT**
> Changing the management VLAN or IP disconnects your current session. Work from the console, or follow the steps in order, so you do not lock yourself out.

SECTION 02

Configure management and SSH in the CLI

Connect through the console (see Initial Setup) and enter configuration mode.

1 Create VLAN 100 for management

```
Switch# configure
Switch(config)# vlan 100
Switch(config-vlan)# name MGMT
Switch(config-vlan)# exit
```

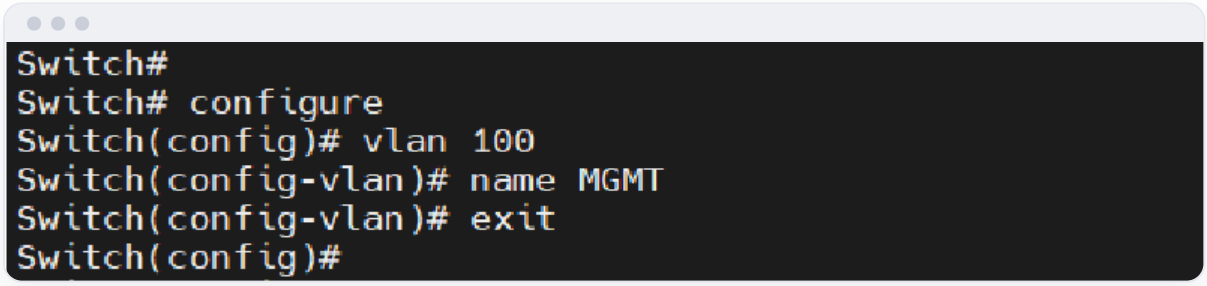


Figure 1. Creating the MGMT VLAN.

2 Assign the management port

Make port 23 an access port in VLAN 100. Administrators will connect here or through a trunk carrying VLAN 100.

```
Switch(config)# int gi23
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# exit
```

3 Set the management IP, gateway and VLAN

After this step the switch is no longer reachable on 192.168.1.1; it answers on `192.168.100.100` in VLAN 100.

```
Switch(config)# ip address 192.168.100.100 mask 255.255.255.0
Switch(config)# ip default-gateway 192.168.100.1
Switch(config)# management-vlan vlan 100
```

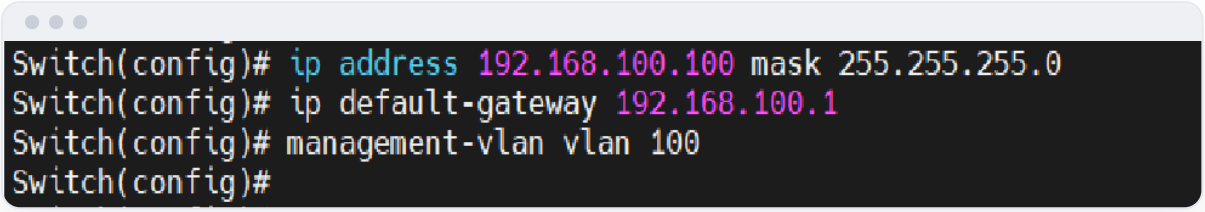


Figure 2. Management IP, gateway and VLAN in the CLI.

4 Enable SSH version 2

The switch generates RSA and DSA host keys. This can take a few minutes.

```
Switch(config)# ip ssh v2
```

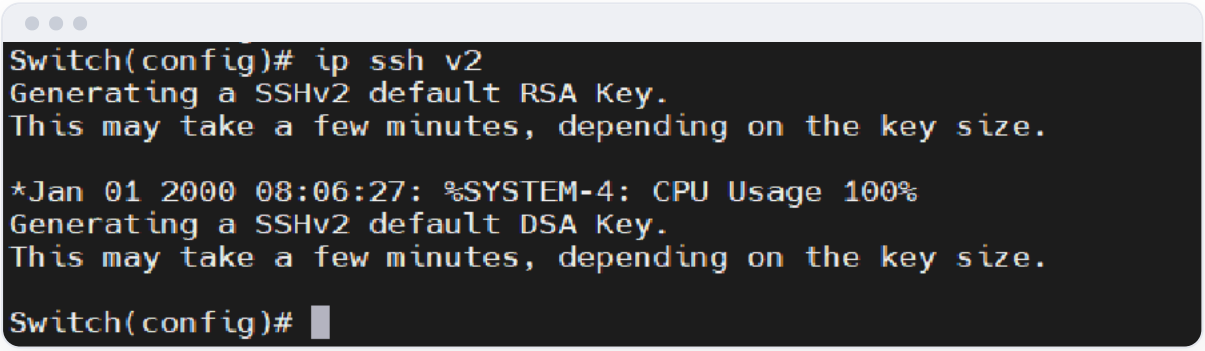


Figure 3. Generating SSH host keys.

5 Start the SSH service

```
Switch(config)# ip ssh
SSH daemon enabled.
```

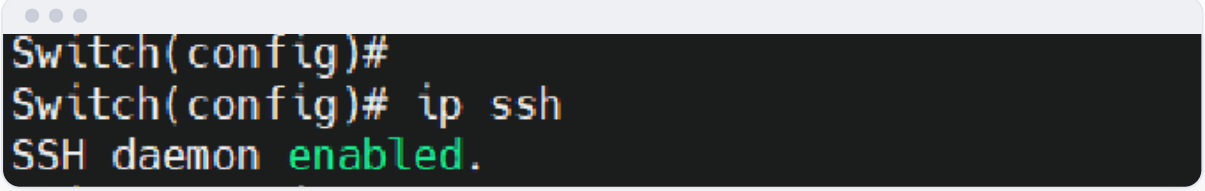


Figure 4. SSH daemon enabled.

6 Save the configuration

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

SECTION 03

Configure management and SSH in the web interface

1 Create VLAN 100

Go to **VLAN** → **Create VLAN**, move VLAN 100 to Created VLAN and click **Apply**.

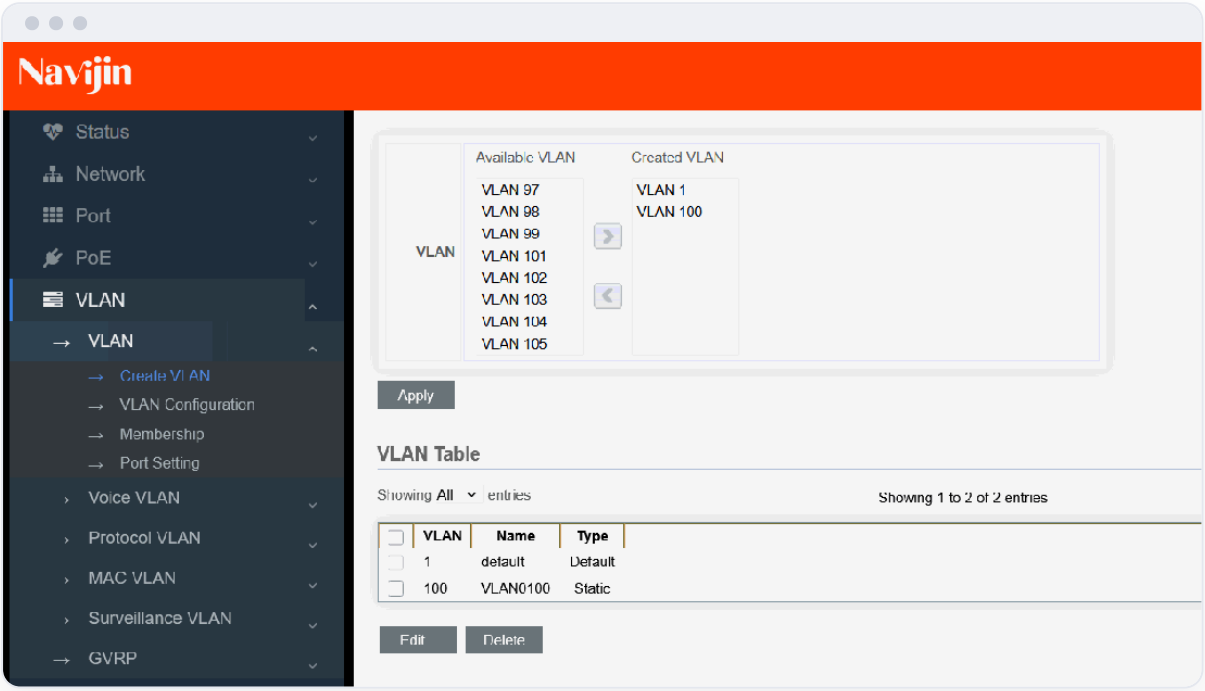


Figure 5. Creating VLAN 100 in the web interface.

2 Name it MGMT

Select VLAN 100 in the VLAN Table, click **Edit**, enter `MGMT` and click **Apply**.

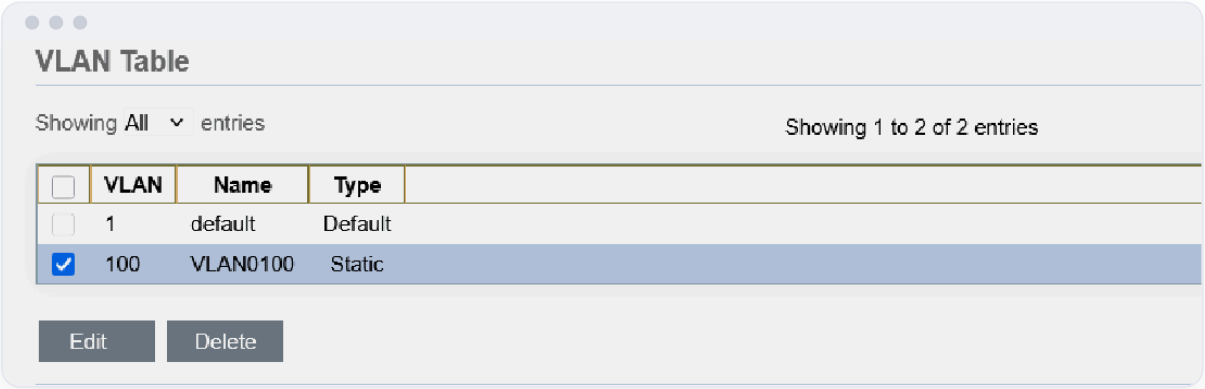


Figure 6. VLAN 100 listed in the VLAN Table.

3 Assign port 23 to VLAN 100

Go to **VLAN → Port Setting**, select port 23, click **Edit**, set **Mode: Access** and **PVID: 100**, then **Apply**.



Figure 7. Port 23 in access mode with PVID 100.

4 Set the switch IP address

Go to **Network → IP Address**, choose **Static**, enter `192.168.100.100`, mask `255.255.255.0`, gateway `192.168.100.1` and click **Apply**.

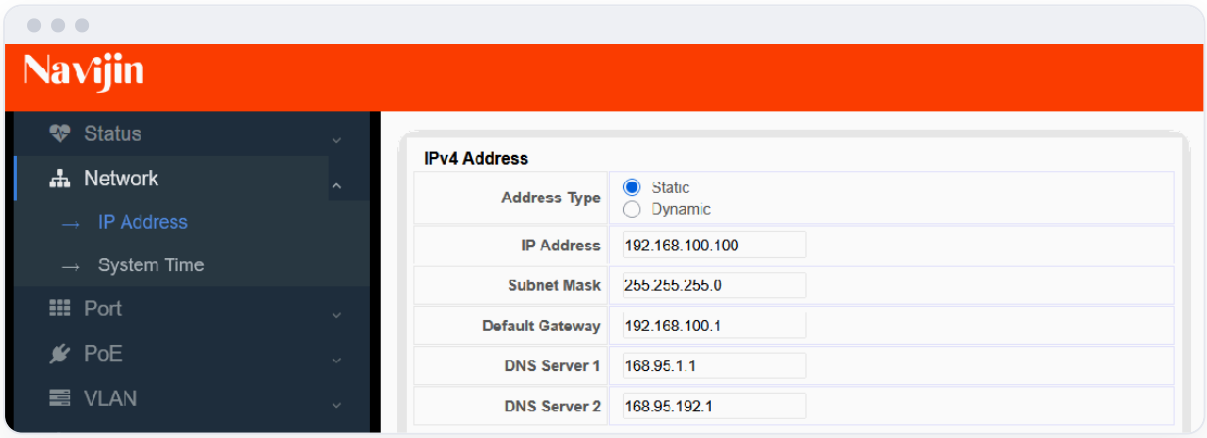


Figure 8. Static IPv4 management address.

5 Set the management VLAN

Go to **Security → Management Access → Management VLAN**, select **100 (MGMT)** and click **Apply**. Your browser session will disconnect; this is expected.

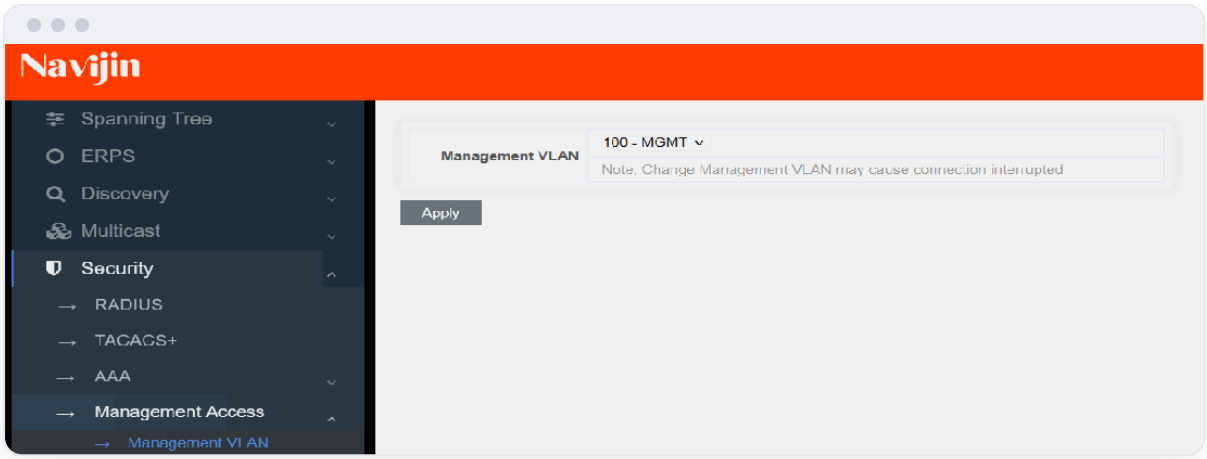


Figure 9. Selecting VLAN 100 as the management VLAN.

6 Reconnect

Connect your computer to port 23, set its IP to `192.168.100.2/24` and browse to `http://192.168.100.100`.

7 Enable SSH

Go to **Security → Management Access → Management Service**, tick **SSH** (and HTTPS), untick Telnet and HTTP if your policy allows, and click **Apply**.

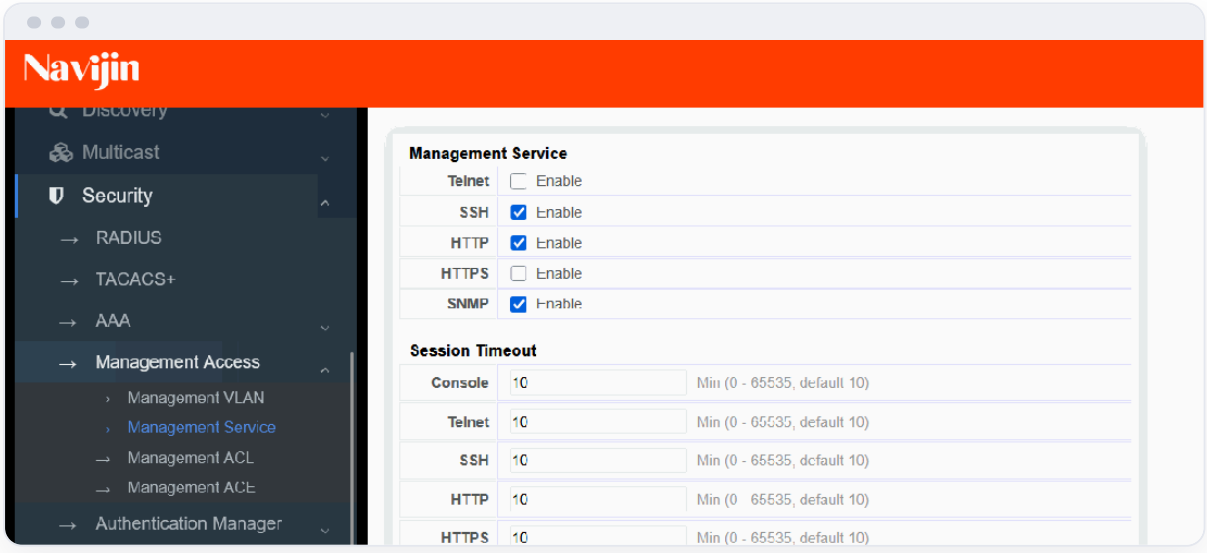


Figure 10. Management services: SSH enabled.

SECTION 04

Test, harden and troubleshoot

1 Test SSH

From an administrator PC in VLAN 100:

```
ssh admin@192.168.100.100
```

2 Harden further

- Change the admin password and create named admin accounts.
- Disable Telnet and HTTP once SSH and HTTPS work.
- Allow management only from your admin subnet.
- Send logs to a syslog server and keep time with NTP.
- Back up the configuration.

Symptom	Likely cause	Fix
Cannot reach 192.168.100.100	PC not in VLAN 100 or wrong IP	Connect to port 23 (or a trunk with VLAN 100) and set 192.168.100.x/24
SSH connection refused	SSH service not started	Run `ip ssh` or enable SSH in Management Service
SSH key warning on the client	Host keys regenerated	Verify you are connecting to the right switch, then update the known-hosts entry
Locked out completely	Management VLAN or IP mis-set	Use the console to correct the configuration

Can I still use the web interface after enabling SSH?

Yes. SSH is for the CLI; use HTTPS for the web interface.

Do I need a separate physical port for management?

No. Any access port in VLAN 100, or any trunk carrying VLAN 100, can be used.

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-L2-003 · 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.