NavGATE

ADMINISTRATOR GUIDE

NAVGATE OS · NAVIJIN GATEWAYS

NavGATE OS Administrator Guide

Set up and manage a Navijin gateway from its web interface: internet and multi-WAN, networks and VLANs, guest Wi-Fi, firewall and threat protection, VPN, connected Navijin devices, users, maintenance and NavCloud.

First sign-in · Internet & VLANs · Guest Wi-Fi · Security · VPN · Devices · Maintenance

Applies to
NG-GE504-P with NavGATE OS 1.0.19 or later

Document
NJ-AG-GW-001 · Rev. 1.0

Published
November 2026

ABOUT THIS GUIDE

About NavGATE OS

NavGATE OS is the operating system of Navijin gateways. It combines an internet router, firewall, DHCP and DNS server, VPN gateway, guest-Wi-Fi portal and controller for Navijin access points, switches and cameras in one web interface. This guide follows the menu of the web interface. Features can be switched on or off centrally under **Features**, so you may not see every page described here.

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 installing Navijin gateways in offices, hotels, shops and branches
- IT administrators running day-to-day operations
- Partners offering managed services with NavCloud

What you need

- A Navijin gateway running NavGATE OS
- A computer connected to a LAN port
- Your internet connection details (DHCP, static or PPPoE)

Factory defaults

Setting	Default
Web interface	`https://192.168.1.1` (from a LAN port)
Administrator password	None. You create it at first sign-in
Remote management	Web interface only; no SSH or Telnet services
NavCloud	Enabled; check-in every 300 seconds

Contents

01 First sign-in

02 Monitoring

03 Internet and routing

04 Networks, VLANs and DHCP

05 Wi-Fi, guests and Navijin devices

06 Security

07 VPN

08 System, maintenance and NavCloud

SECTION 01

First sign-in

1 Connect

Connect your computer to a LAN port of the gateway. It receives an address automatically.

2 Open the web interface

Browse to `https://192.168.1.1`. Your browser warns about the certificate on first use; continue to the page. You can install your own certificate later under **Certificates**.

3 Create the administrator password

Navijin gateways have **no default password**. Create a strong password; NavGATE OS rejects weak and easy-to-guess passwords. Then sign in again.

4 Connect to the internet

Open **Internet** and choose DHCP, static or PPPoE (see section 3).

5 Check the dashboard

The **Dashboard** shows internet links and quality, throughput, CPU and memory, sessions, ports, Wi-Fi clients, recent DHCP clients, devices by type and the latest security events.

> **TIP**
> Prefer the command line? Every basic setting is also available in NavCLI. See the NavCLI 2.0 Command Reference.

SECTION 02

Monitoring

Page	What you see
Dashboard	Internet links, internet quality and throughput, CPU, memory, sessions, ports, Wi-Fi clients, DHCP pool, top devices, devices by type, security over 24 h, system information, NavCloud, firmware and admin sessions
Clients	Connected devices and the top internet users
Web activity	Live web activity and top websites over 24 hours
Events / Alerts	Recent events and alerts; choose which events send an alert
Topology	Live view of how the gateway, switches, access points and other devices are connected

Logs	Log storage and forwarding to a remote syslog / SIEM server

SECTION 03

Internet and routing

1

Primary internet (WAN)

In **Internet**, select the connection type: **DHCP** (automatic), **Static** (address, gateway, DNS) or **PPPoE** (username and password from your provider).

2

Multi-WAN

Add a second internet line for **failover** or load balancing, for example fibre plus a 4G router. NavGATE OS monitors each link and moves traffic when one fails.

3

Routing

Under **Routing** configure policy routing (choose the internet line by source or destination), static routes, NAT, IP–MAC binding and connection limits.

4

Internet limits and QoS

Internet limits caps bandwidth per device or group. **Smart QoS** keeps calls and meetings smooth on busy lines with application priority, bandwidth rules and schedules.

> **NOTE**
>
> Some routing and QoS functions must be enabled first under **Features**.

SECTION 04

Networks, VLANs and DHCP

1 Networks and VLANs

Under **LAN → Networks & VLANs** create a network for each group of users (staff, voice, cameras, IoT), each with its own VLAN ID, subnet and DHCP server.

2 DHCP reservations

Give printers, cameras and servers a fixed address by reserving it for their MAC address.

3 Local DNS

Add local names, for example `nvr.office`, so users reach devices by name.

Example network	VLAN	Subnet	Purpose
Staff	10	10.10.0.0/24	Employees
Voice	20	10.20.0.0/24	IP phones
Cameras	30	10.30.0.0/24	CCTV
Guests	40	10.40.0.0/22	Visitors, Internet only

SECTION 05

Wi-Fi, guests and Navijin devices

1 Adopt devices

Devices lists new devices found on the network and the devices already managed. Adopt Navijin access points, switches, cameras and CPEs to manage them from the gateway. A device can be restarted or removed from here.

2 Wi-Fi networks

Under **Wi-Fi networks** create SSIDs once and push them to all access points; apply **AP profiles** for radio settings. Access point firmware is updated under **Device firmware**.

3 Guest Wi-Fi and captive portal

Guest creates an internet-only guest network with an optional captive portal: choose sign-in methods, customise the sign-in page, create **passes** (dedicated passwords) and see guests online.

4 Switches and cameras

Switches shows managed Navijin switches and their ports; **Cameras** lists cameras and recorders. Port settings such as VLAN profile, speed, PoE and power-cycling are available for adopted switches.

> **TIP**
> Hotels and venues: combine the captive portal with passes to give each guest or event its own Wi-Fi password.

SECTION 06

Security

Page	What you configure
Firewall	Port forwarding and traffic rules between networks and the internet
Threat protection	Intrusion prevention with IP reputation, DNS security (malware and phishing blocking), blocked websites and allow-list
Users	Administrator accounts and roles, password and login policy, who is signed in now, your own password
Remote access	Web management access, command-line access and Navijin remote support
Certificates	Gateway certificates, local certificate authority, trusted CAs and user certificates

> **IMPORTANT**
> Avoid port forwarding for cameras, recorders and admin pages. Use the gateway's VPN for remote access instead.

- Enable **admin two-step login** and **login lockout** under Features.
- Restrict web management to trusted networks.
- Keep NavGATE OS updated; firmware images are digitally signed and verified before installation.

SECTION 07

VPN

1 Site-to-site

Connect branches with **Site-to-site VPN** tunnels. With NavCloud, **Auto-VPN** can build tunnels between sites for you.

2 Remote access for staff

Give employees secure access from laptops and phones with the remote-access VPN or the SSL VPN for working from home.

3 Encryption policy

Choose the encryption settings used by tunnels under **Encryption policy**.

SECTION 08

System, maintenance and NavCloud

Page	Use it to
System	Set the device name and system time
Maintenance	Update firmware, back up and restore the configuration, view configuration history, schedule reboots, power options
Tools	Run network diagnostics (ping, trace, lookup)
NavCLI	Use the command line inside the web interface
Features	Switch functions on or off: security, network, traffic, Wi-Fi & guests, VPN & cloud, admin & monitoring, PoE
NavCloud	See the cloud connection status and the claim code

1 Update firmware

Download the `.nfw` file for your exact model from the Navijin documentation page and install it under **Maintenance → Firmware**. NavGATE OS verifies the digital signature before installing; unsigned or modified files are rejected.

2 Back up

Download a backup under **Maintenance → Backup & restore** after every important change and store it securely.

3 Connect to NavCloud

Open **NavCloud**, note the **claim code** and add the gateway to your site in NavCloud. From then on you can monitor and manage it remotely.

I forgot the administrator password.

Use the reset procedure (factory reset) and configure the gateway again from your backup. There is no master password.

Can I manage the gateway without the cloud?

Yes. Everything is available in the local web interface; NavCloud adds multi-site management.

Why is SSH not available?

NavGATE OS removes SSH and Telnet to reduce attack surface. Use the authenticated web interface and its NavCLI page.

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-AG-GW-001 · Rev. 1.0 · 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.