NETGEAR ENTERPRISE

Hardening Guide for Smart Switches

202-12979-02
September 2026

Support

For product support and to access the latest product firmware, visit netgear.com/support.
For the duration of software and cyber security updates, visit netgear.com/about/eos/.

Regulatory and Legal

Si ce produit est vendu au Canada, vous pouvez accéder à ce document en français canadien à https://www.netgear.com/support/enterprise.
(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/enterprise.)
For safety and regulatory compliance information including the EU Declaration of Conformity, visit https://www.netgear.com/about/regulatory/.
See the regulatory compliance document before connecting the power supply.
For NETGEAR's Privacy Policy, visit https://www.netgear.com/about/privacy-policy.
Where permitted by law, by using this device, you are agreeing to NETGEAR's Terms and Conditions at https://www.netgear.com/about/terms-and-conditions and if you do not agree, return the device to your place of purchase within your return period.
This product is designed and warranted for indoor use only. Do not use this device outdoors. The PoE source is intended for intra-building connection only.

Trademarks

© 2026 NETGEAR, Inc., NETGEAR, and the NETGEAR Logo are trademarks of NETGEAR, Inc.
Any non-NETGEAR trademarks are used for reference purposes only.

Contents

Introduction 1

Management Plane 2

Control Plane 4

Data Plane 5

Operational Security 6

Change Management 7

Appendix: Minimum secure baseline checklist 8

Copyright © 2026 NETGEAR

Introduction

This guide provides a practical hardening baseline for NETGEAR smart switches. It focuses on minimizing exposure to threats, making sure that access privileges are correct, and improving auditing for daily operations.

This guide reflects common NETGEAR Enterprise deployments, though features can vary by model and firmware. The recommendations are generally safe for all smart switches, but every network is different, so review each control for operational impact, especially in production.

While based on the GS728TXv3/GS728TXPv3/GS728TXUPv3 and GS752TXv3/GS752TXPv3/GS752TXUPv3 models, the guidance applies broadly to NETGEAR smart switches.

Controls are grouped into the following three planes:

- **Management plane**: Use this plane for device access and administration.
- **Control plane**: Use this plane for network stability protocols.
- **Data plane**: Use this plane for traffic forwarding and segmentation.

⚠ **CAUTION:** NETGEAR smart switches do not have a console or management port. You must be careful when you apply a management ACL to avoid lockouts. Add the IP address of your personal device to the ACL before you apply it to the management VLAN.

Recommended baseline

You can still achieve strong protection even if you apply only a small set of controls, as long as you choose the ones with the greatest impact. Focus on the following measures, which deliver solid security benefits while keeping operational complexity low.

- Upgrade to an approved firmware release and document the version in your change log.
- Change the default admin password to a strong passphrase.
- Use encrypted management access: enable SSH (where supported) and disable Telnet.
- Use HTTPS to access the device UI and disable HTTP.
- Restrict management access to a dedicated management VLAN and apply a management ACL.
- Use SNMPv3. If you use SNMPv1/v2c, make sure that you lock community strings down with client IP restrictions.
- Enable remote logging to a syslog collector and synchronize time with NTP/SNTP.
- Enable Layer-2 protections on edge ports: Storm control and port security (where supported).
- Enable DHCP Snooping and Dynamic ARP Inspection on user/edge VLANs where DHCP is in use, where supported.

Management Plane

The management plane of a switch allows administrators to configure, monitor, and control how the switch operates.

Account and credential hygiene

Use individually assigned administrator accounts and avoid shared accounts to make sure that you can attribute all actions clearly. Integrate with centralized authentication systems (RADIUS or TACACS+) when available, and maintain a local break-glass account for emergency access.

Recommended settings (where supported):

- Enforce strong local password policy and disable weak or default credentials.
- Enable account lockout after repeated failed logins (do not apply to console recovery).
- Enable password aging only if it aligns with your security policy and operational model.

Use secure management protocols only

Disable insecure management services and use encrypted protocols for all device administration. Legacy management protocols expose credentials and session data, making them vulnerable to interception and replay attacks.

Recommended practices:

- Disable Telnet and use SSH (CLI-capable models).
- Disable HTTP and use HTTPS for the device UI.
- Restrict management services to management networks only.

Restrict who can manage the switch

The management plane acts as a privileged server. We recommended restricting administrative access to known subnets and jump hosts, and create a dedicated management VLAN or an out-of-band interface.

Recommended controls:

- Place management IP addresses in a dedicated management VLAN/subnet.
- Apply a management ACL permitting HTTPS/SSH/SNMP only from management sources.
- Deny management-plane access from user VLANs by default.

Centralized authentication (AAA)

Where supported, use RADIUS or TACACS+ for administrator authentication and authorization. Keep local administrator access as a controlled fallback for outages.

Recommended practices:

- Use centralized AAA for routine admin access.
- Restrict which management sources may reach AAA services.
- Keep a break-glass local account and protect it with strong controls.

SNMP hardening

Use SNMPv3 with authentication and privacy, and avoid SNMPv1/v2c because they transmit community strings in cleartext.

Recommended practices:

- Use SNMPv3 and disable SNMPv1/v2c if your environment allows.
- Restrict SNMP to NMS IP addresses using ACLs and SNMP access controls.
- Use "read-only" access by default. Enable "write-only" access solely when there is a clearly documented justification and well-defined operational constraints.

Logging, Time Synchronization, and Audit Trails

Enable centralized logging and maintain reliable time synchronization to correlate configuration changes with security events during troubleshooting and incident response.

Recommended practices:

- Enable remote syslog and forward logs to a central collector.
- Synchronize time with NTP/SNTP and use consistent time sources across the network.
- Review log levels to balance signal vs. noise in production.

Session management

Reduce exposure from unattended management sessions. Use conservative session timeouts and restrict management access to trusted networks.

Control Plane

The control plane maintains stability by running protocols and uses them to detect topology changes, exchange status information with neighboring switches, and update forwarding decisions whenever the network shifts.

Link discovery protocols

Link discovery protocols (LLDP) can leak topology information. Disable them on untrusted edge ports where they are not in use.

Denial-of-Service protections

Smart switches include DoS protection features that rate-limit or drop suspicious traffic patterns. Use these controls to prevent attacks from disrupting legitimate high-rate traffic.

We recommend the following steps:

- Start with conservative, global protections, then add targeted signatures based on observed risk.
- Monitor logs and counters after each change to identify false positives.
- Record exceptions for known high-throughput workflows, such as multicast AV distributions.

Data Plane

The data plane moves packets at high speed, applying forwarding rules to keep traffic flowing efficiently.

Network segmentation

Use VLANs and ACLs to limit lateral movement and to isolate management, user/IT, AV endpoints, and services. Avoid placing management interfaces in the same VLAN as user endpoints.

Port security

Port security, when available, restricts which MAC addresses a port learns and helps prevent casual rogue device attachment. Apply stricter limits on user ports, and confirm the necessary settings on AV or trunk ports.

We recommend the following guidelines:

- Enable port security on access ports and configure an appropriate maximum MAC address count.
- Choose shutdown or restrict actions for violations, based on operational requirements.
- Avoid using port security on trunk or uplink ports unless a validated design explicitly requires it.

Unused ports (parking VLAN)

Place unused ports into a dedicated parking VLAN and administratively disable them. This reduces the risk of unauthorized access through open wall ports.

Storm control

Storm control helps prevent broadcast, multicast, and unknown-unicast floods from overwhelming a VLAN. Enable it on edge ports and tune thresholds to your environment.

We recommend the following guidelines:

- Enable storm control on user-facing ports with conservative thresholds.
- Monitor counters for sustained storms and investigate root causes.

DHCP Snooping and Dynamic ARP Inspection

DHCP Snooping creates a trusted table of IP-to-MAC-to-port bindings. Dynamic ARP Inspection (DAI) uses that table to block ARP spoofing attempts. Enable DHCP Snooping on VLANs that use DHCP, and enable DAI on user-facing VLANs where the platform supports it.

We recommend the following guidelines:

- Enable DHCP Snooping on all VLANs that use DHCP.
- Mark uplinks and DHCP-server-facing ports as trusted, and keep edge ports untrusted.
- Enable DAI on the same VLANs and monitor for packet drops during rollout.

Operational Security

We recommend you use the following measures to secure your switches, cut exposure, and keep threats from exploiting a critical network point.

Configuration management

Treat device configurations as controlled artifacts. Back up each configuration after every change, store the backups in a secure location, and document all modifications in a change log or ticketing system.

Firmware and vulnerability management

Maintain an upgrade schedule that aligns with your security program. Track deployed firmware versions and address known vulnerabilities as soon as your operations allow.

Physical security

Physical access often leads directly to unauthorized administrative access. To avoid this happening, secure racks and closets, protect console ports, and restrict entry to network rooms.

Change Management

Apply hardening controls in a deliberate, safe sequence and verify each step as you go. Create a rollback plan, maintain a tested recovery method, and confirm both are ready before tightening management access.

Recommended sequence:

1. Enable remote syslog and time synchronization to improve visibility.
2. Implement DHCP Snooping before you enable DAI, that depends on a trustworthy binding table.
3. Apply edge protections (storm control and port security) and validate access ports.
4. Apply the management plane access restrictions after you confirm out-of-band recovery.

Appendix: Minimum secure baseline checklist

Use this checklist to ensure the minimum secure baselines are in place in your environment.

- Deploy the approved firmware version and record it in your documentation.
- Create unique administrator accounts and remove or secure all default credentials.
- Enable HTTPS and disable HTTP.
- Enable SSH where the platform supports it, and disable Telnet.
- Restrict management access to dedicated management networks and apply the appropriate management ACL.
- Configure SNMPv3, and limit SNMPv1/v2c to tightly controlled use cases when required.
- Enable remote syslog and forward logs to a central collector.
- Configure NTP/SNTP and verify accurate time synchronization.
- Enable and tune storm control on edge ports where supported.
- Enable and tune port security on edge ports where supported.
- Enable DHCP Snooping and Dynamic ARP Inspection on user VLANs that rely on DHCP where supported.
- Enable IGMP Snooping on multicast or AV VLANs where supported.