NETGEAR ENTERPRISE

Hardening Guide

# Security Hardening Guide for M4350 Fully Managed Switches

Model: M4350

202-12917-01
April 2026

## Support and Community

Visit netgear.com/support to get your questions answered and access the latest downloads.

You can also check out our NETGEAR Community for helpful advice at community.netgear.com.

## 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/download/.

(If this product is sold in Canada, you can access this document in Canadian French at https://www.netgear.com/support/download/.)

For 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

# Contents

# Introduction

This Security Hardening Guide provides a practical hardening baseline for NETGEAR M4350 Fully Managed Switches. It focuses on minimizing exposure to threats, ensuring access privileges are correct, and improving auditing for daily operations.

The guide is specifically tailored for traditional Enterprise and IT deployments. Review each control for operational impact, especially in live production environments. Implementing these strict IT security measures globally directly conflicts with the plug-and-play requirements essential for Audio/Video over IP (ProAV) networks.

For AV deployments on the NETGEAR M4350, we recommended to configure the switch using NETGEAR Engage or the AV UI. These tools are purpose-built to automatically apply the correct, optimized profiles for AV protocols (such as Dante, NDI, AES67, and SDVoE), ensuring seamless plug-and-play functionality while maintaining network stability.

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.

## Before you begin

Before you can apply any hardening changes, you need to have console or out-of-band (OOB) access available. You must also maintain a tested method to recover access, for example, console access and a secured break-glass account.

For information about configuring the switch using the command-line interface (CLI), see the CLI manual, which you can download by visiting https://www.netgear.com/support/.

## Recommended baseline

You can achieve strong protection with a small set of controls, by choosing those controls with the greatest impact. Focus on the following measures for 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 for CLI management and disable Telnet.
- Use HTTPS to access the device UI and disable HTTP.
- Restrict management access to a dedicated management VLAN or OOB port and apply a management access control list (ACL).
- Use SNMPv3. If you use SNMPv1/v2c, lock the community strings down with client IP restrictions.
- Enable remote logging to a syslog collector and synchronize the time with NTP.

- Enable Layer 2 protections on edge ports: BPDU Guard, storm control, and port security, where supported.
- Enable DHCP Snooping and Dynamic ARP Inspection on user/edge VLANs where DHCP is in use.

# Management Plane

Use the management plane to configure, monitor, and control how the switch operates. You can begin by using management access lists (ACLs) and then incrementally applying inter-VLAN policies. Use ACLs for the following tasks:

- Protecting the management plane by limiting who can connect.
- Limiting Layer 3 traffic between VLANs according to least privilege.

For information about configuring the management plane using the command-line interface (CLI), see the CLI manual, which you can download by visiting netgear.com/support/download.

## Account and credential hygiene

Use individually assigned administrator accounts and avoid shared accounts to ensure a clear attribution of all actions. Integrate the accounts with centralized authentication systems (RADIUS or TACACS+) when available, and maintain a local break-glass account for emergency access.

**Recommended practices (where supported)**:

- Enforce strong local password policy and disable weak or default credentials:

```
(NETGEAR Switch)(Config)# username admin password <password>
(NETGEAR Switch)(Config)# no username guest
(NETGEAR Switch)(Config)# username localuser password <password>
```

- 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:

```
(NETGEAR Switch)(Config)# passwords lock-out 3
(NETGEAR Switch)(Config)# passwords aging 90
(NETGEAR Switch)(Config)# passwords strength-check
(NETGEAR Switch)(Config)# passwords strength keyboard-sequences
```

## 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. Enforcing encrypted management reduces the risk of credential interception, session compromise, and unauthorized configuration activity within the environment.

**Recommended practices**:

- Reduce password-guessing noise by limiting authentication retries.
- Disable HTTP and use HTTPS for the device UI:

```
(NETGEAR Switch)# no ip http server
(NETGEAR Switch)# no ip http port
(NETGEAR Switch)# ip http secure-port 49152
(NETGEAR Switch)# ip http secure-server
```

- Disable Telnet.
- Enable SSH for CLI access and restrict SSH to management subnets.
- Use modern SSH algorithms, where supported:

**Command example: Enable SSHv2 / Disable Telnet**:

```
(NETGEAR Switch)(Config)# crypto key generate rsa 2048
(NETGEAR Switch)(Config)# crypto key generate dsa
(NETGEAR Switch)(Config)# exit
(NETGEAR Switch)# ip ssh server enable
(NETGEAR Switch)# no ip telnet server enable
(NETGEAR Switch)# configure
(NETGEAR Switch)(Config)# line console
(NETGEAR Switch)(line console)# no transport input telnet
(NETGEAR Switch)(line console)# no transport output telnet
```

## Restrict who can manage the switch

The management plane acts as a privileged server. We recommend to restrict administrative access to known subnets and jump hosts, and create a dedicated management VLAN or an out-of-band interface. By limiting management access to known admin subnets and jump hosts, you can decrease the attack surface and block user VLANs from reaching the management plane.

**Recommended practices**:

Use an infrastructure or management ACL that permits only your jump hosts, NMS systems, and AAA, logging, and NTP sources. For example, use an IP ACL that allows SSH, HTTPS, and SNMP from the management subnet, but also blocks all other management plane traffic.

**Before you begin**:

Confirm that your current admin IP or subnet is allowed. Ensure you have console or OOB access so you can recover it if you lose connectivity.

Use a management ACL to control who can manage the switch. This control defines exactly which systems can use SSH, HTTPS, and SNMP, and ensures that even if credentials leak, only authorized jump hosts and NMS systems can reach the management plane.

**Command example**:

```
(NETGEAR Switch)(Config)# management access list MGMT-ACCESS
(NETGEAR Switch)(Config-macl)# permit ip-source <admin ip/subnet> mask
<subnet mask>
(NETGEAR Switch)(Config-macl)# exit
(NETGEAR Switch)(Config)# management access-class MGMT-ACCESS
```

## Centralized authentication (AAA)

Use AAA to centralize authentication and strengthen auditability. Use TACACS+ for administrative command authorization when it is available, or use RADIUS when TACACS+ is not an option. Configure redundant servers and a secure fallback policy to keep access reliable.

M4350 switches support AAA authentication lists. RADIUS server configuration is available in the CLI.

Centralized AAA improves accountability and revokes access quickly. It also reduces reliance on shared local credentials and enables consistent policy enforcement across devices.

> **NOTE:** When you enable AAA, verify the console access and fallback first to avoid lockout.

**TACACS+ command example**:

```
(NETGEAR Switch)(Config)# authentication enable
(NETGEAR Switch)(Config)# aaa authentication login "defaultList" tacacs
local
(NETGEAR Switch)(Config)# tacacs-server host "<tacacs server ip/name>"
(NETGEAR Switch)(Config)# tacacs-server key <shared-secret>
(NETGEAR Switch)(Config)# tacacs-server source-interface <source
interface>
```

**RADIUS command example**:

```
(NETGEAR Switch)(Config)# radius server host auth "<radius server ip/
name>" name "RADIUS"
(NETGEAR Switch)(Config)# radius server key auth "<radius server ip/
name>" <shared-secret>
(NETGEAR Switch)(Config)# radius source-interface <source interface>
```

## SNMP hardening

Use SNMPv3 with authentication and privacy, and avoid SNMPv1/v2c because they transmit community strings in cleartext. If you must use SNMPv1/v2c, use long random community strings and restrict access by client IP.

SNMPv3 adds authentication and encryption, and restricts SNMP by source IP limits that can query each device.

**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.

**Command example**:

```
(NETGEAR Switch)(Config)# snmp-server user "snmpuser" DefaultWrite
auth-sha512 <auth-password> priv-aes128 <priv-password>
(NETGEAR Switch)(Config)# snmp-server password-strength
(NETGEAR Switch)(Config)# snmp-server v3-host <nms server ip/name>
"snmpuser" traps priv
```

## Logging, time, and audit trail

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

**Recommended practices**:

- Enable syslog logging and configure a remote log host. Centralized logs provide the evidence trail needed for incident response and change accountability.

```
(NETGEAR Switch)(Config)# logging host "<syslog server ip/name>"
ipv4 514 notice
(NETGEAR Switch)(Config)# logging syslog
(NETGEAR Switch)(Config)# logging syslog source-interface <source
interface>
```

- Configure accurate time (NTP) for events to correlate correctly across switches, servers, and security tools.

```
(NETGEAR Switch)(Config)# ntp server <ntp server ip/name> prefer
(NETGEAR Switch)(Config)# no ntp server time-a.netgear.com
(NETGEAR Switch)(Config)# ntp source-interface <source interface>
```

## Session management

Idle sessions and extended web sessions create opportunities for misuse, particularly when privileged terminals remain unattended or browser sessions stay active longer than necessary. Short timeouts and strict session limits narrow the window available for exploitation, while still supporting routine administrative activity.

**Recommended practices**:

Use idle timeouts and limit concurrent management sessions. If you use the device UI, configure reasonable HTTPS session timeouts and limit maximum sessions.

**Command example**:

```
(NETGEAR Switch)(Config)# line console
(NETGEAR Switch)(line console)# session-timeout 5
(NETGEAR Switch)(line console)# exit
(NETGEAR Switch)(Config)# exit
(NETGEAR Switch)# sshcon timeout 5
(NETGEAR Switch)# ip http secure-session soft-timeout 5
```

# Control Plane

Control plane protections keep the switch stable and resilient under misconfiguration or attack. For M4350 deployments, the most impactful controls are at Layer 2, including spanning-tree protections, discovery-protocol controls, and targeted rate limiting.

For information about configuring the control plane using the command-line interface (CLI), see the CLI manual, which you can download by visiting https://www.netgear.com/support/.

## Spanning tree protections

Spanning tree protocol (STP) protects the network from Layer 2 loops, but it can also be abused to disrupt the topology. Use the following commands to apply edge protections on your access ports and to enforce stable root guard or loop guard on the appropriate uplinks.

- Enable BPDU Guard on access/edge ports.

```
(NETGEAR Switch)(Config)# spanning-tree bpduguard
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# spanning-tree edgeport
```

- Enable root guard or loop guard on appropriate uplinks.

```
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# spanning-tree guard loop
```

## Link discovey protocols (LLDP)

Disable discovery protocols on untrusted edge ports unless you need them for operations. If you require LLDP, consider limiting which TLVs are advertised and avoid advertising management addresses on untrusted segments.

Discovery protocols can leak topology and device details to adjacent hosts. Disabling or limiting LLDP/ISDP advertisements on user-facing ports reduces reconnaissance data available to an attacker while keeping it available where operationally needed. Remove LLDP optional TLVs or management address advertisement.

**Command example**:

```
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# no lldp transmit
(NETGEAR Switch)(Interface 1/0/X)# no lldp receive
(NETGEAR Switch)(Interface 1/0/X)# no lldp med
```

## Routed interface safety settings

Source routing is rare in modern networks, but creates opportunities for attackers to redirect traffic or bypass policy intent.

**Recommended practices**:

- Disable ICMP redirects on routed interfaces.
- Disable ICMP destination unreachables where appropriate (evaluate operational needs).
- Disable proxy ARP on routed interfaces unless explicitly required.

These settings reduce the ability of an attacker to manipulate host routing decisions, use the switch as a reflector, or leverage protocol side effects on routed interfaces.

If you use VLAN routing interfaces (SVIs) on the M4350, apply conservative defaults that reduce information leakage and prevent certain amplification and redirection behaviors.

```
NETGEAR Switch(Config)# interface vlan <ID>
NETGEAR Switch(Config-if-vlan<ID>)# no ip redirects
NETGEAR Switch(Config-if-vlan<ID>)# no ip unreachables
NETGEAR Switch(Config-if-vlan<ID>)# no ip proxy-arp
```

## Denial-of-Service (DoS) protection

Fully managed 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.

Floods and malformed packets can consume control-plane resources, disrupt topology protocols, or reduce management responsiveness. Enabling DoS protections helps to preserve availability and operational stability, often the primary security objective for a switch.

**Recommended actions**:

- 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.

> **NOTE:** Enable DoS progressively in staging, then production, while watching logs and counters, and validating latency-sensitive and AV-over-IP traffic profiles.

**Command example**:

```
(NETGEAR Switch)(Config)# dos-control firstfrag
(NETGEAR Switch)(Config)# dos-control sipdip
(NETGEAR Switch)(Config)# dos-control smacdmac
(NETGEAR Switch)(Config)# dos-control tcpfinurgpsh
(NETGEAR Switch)(Config)# dos-control tcpflagseq
(NETGEAR Switch)(Config)# dos-control tcpsyn
(NETGEAR Switch)(Config)# dos-control tcpsynfin
(NETGEAR Switch)(Config)# dos-control tcpfrag
(NETGEAR Switch)(Config)# dos-control tcpoffset
```

# Data Plane

The data plane moves packets at high speed, applying forwarding rules to keep traffic flowing efficiently. Data plane hardening focuses on segmentation, anti-spoofing, and limiting blast radius. For many deployments, the strongest baseline comes from VLAN separation along with edge port protections.

For information about configuring the data plane using the command-line interface (CLI), see the CLI manual, which you can download by visiting https://www.netgear.com/support/.

## Network segmentation

Separate management traffic from user and AV device traffic. Use VLANs to segment endpoints by trust level or function, for example: Management, AV endpoints, control systems, user/IT, and services.

Network segmentation limits blast radius. Separating management, AV, and user traffic reduces lateral movement, helps to contain misconfigurations, and makes it easier to apply targeted policies (ACLs, QoS, IGMP/PIM where used).

> **NOTE:** Always validate with representative AV endpoints; some media protocols rely on expected multicast group behavior and timing.

**Recommended practices**:

Enable IGMP plus on VLANs that carry multicast and validate behavior with your AV-over-IP workflows. Use IGMP plus for unregistered multicast handling.

Dropping unregistered multicast is a common hardening goal to prevent multicast flooding and reduce the blast radius of misbehaving endpoints. On the M4350, IGMP plus provides an integrated approach to manage multicast registration behavior. IGMP plus helps to control delivery without relying on Cisco-specific commands.

## Port security: MAC limiting and sticky learning

Where appropriate, typically in IT/access edge networks, enable port security to limit the number of MAC addresses learned on a port. Consider using sticky MAC learning for fixed endpoints.

**Command example**:

```
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# port-security
(NETGEAR Switch)(Interface 1/0/X)# port-security max-dynamic 1
(NETGEAR Switch)(Interface 1/0/X)# port-security violation shutdown
(NETGEAR Switch)(Interface 1/0/X)# port-security mac-address sticky
```

## Parking VLAN

After shutting down a port, operators might temporarily re-enable ports during troubleshooting. A parking VLAN pattern reduces the chance that an accidentally enabled port lands on a sensitive production VLAN.

If a port is accidentally enabled, a parking VLAN restricts access to a production network segment.

> **NOTE:** Document the parking VLAN in your standards so it is not accidentally reused for production.

**Recommended practices**:

- Create a dedicated unused/parking VLAN, for example: VLAN 666.
- Set the port PVID to the parking VLAN.
- Set unused ports to Access Mode and assign them to this VLAN.
- Administratively shut down the port.

**Command example**:

```
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# shutdown
(NETGEAR Switch)(Interface 1/0/X)# vlan pvid <parking vlan>
(NETGEAR Switch)(Interface 1/0/X)# vlan participation exclude <vlan>
(NETGEAR Switch)(Interface 1/0/X)# vlan participation include <parking
vlan>
```

## Storm control

Use storm control to prevent broadcast, multicast, or unknown-unicast storms from impacting the switch or the broader network.

> **NOTE:** For AV-over-IP: Avoid enabling multicast storm control (or set overly aggressive thresholds) on ports/VLANs carrying high-bandwidth multicast workflows (for example, Dante or NDI). These protocols can legitimately use substantial multicast bandwidth; tight storm limits can cause audio/video dropouts. Validate in staging and prefer applying storm control primarily on IT/user edge ports.

Broadcast, multicast, or unknown unicast storms can saturate links and overwhelm switching resources. Storm control enforces a ceiling, a percentage of link speed, to preserve availability during faults or attacks.

**Command example**:

```
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# storm-control broadcast action
shutdown
(NETGEAR Switch)(Interface 1/0/X)# storm-control multicast action
shutdown
(NETGEAR Switch)(Interface 1/0/X)# storm-control unicast action
shutdown
```

### DHCP snooping and dynamic ARP inspection (DAI)

If your VLAN uses DHCP, enable DHCP Snooping to build a trusted binding table and block rogue DHCP servers on untrusted ports. Then enable Dynamic ARP Inspection (ARP inspection) to block ARP spoofing using the DHCP Snooping bindings.

Rogue DHCP and ARP spoofing are common Layer 2 attacks that enable man-in-the-middle traffic interception. DHCP Snooping builds a trusted binding table, and DAI uses that table to block invalid ARP replies.

**Recommended practices**:

- Mark uplinks/DHCP server-facing ports as trusted.
- Keep edge/user ports untrusted (default).
- Enable ARP inspection on the VLANs, and only trust uplinks.

**Command example**:

```
(NETGEAR Switch)(Config)# ip dhcp snooping
(NETGEAR Switch)(Config)# ip dhcp snooping vlan 110,120,130
(NETGEAR Switch)(Config)# ip arp inspection vlan 110,120,130
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# ip dhcp snooping trust
(NETGEAR Switch)(Interface 1/0/X)# ip arp inspection trust
```

For an optional enhancement, enable IP Source Guard on untrusted access ports to block IP spoofing based on the DHCP snooping binding table.

```
(NETGEAR Switch)(Config)# interface 1/0/X
(NETGEAR Switch)(Interface 1/0/X)# ip verify source
```

# 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 switch configuration as code: document changes, use a standard template, back up configuration after every change window, and keep copies in a secure repository.

## Firmware and vulnerability management

Maintain an upgrade cadence. Track firmware versions in inventory and subscribe to vendor security bulletins. In AV environments, validate upgrades in a staging rack before production rollout.

## Physical security

Use physical controls such as locked racks, port blockers/covers, tamper seals, and controlled-access rooms. If the environment is high risk, consider additional compensating controls (cameras, access logs, escorted access).

For USB/Console port security, limit physical access to switches, especially console ports and OOB management ports. Use locked racks, controlled access rooms, and documented break-glass procedures.

Document all hardening changes, including:

- Date and time of any change.
- Features you enabled or modified.
- Validation results.
- Any deviations from the baseline guidance in this document.

For best practices, use the following guidelines:

- Maintain a known-good configuration backup prior to hardening.
- Use staged rollbacks whereby you disable one feature at a time to isolate issues.
- Use configuration rollbacks instead of firmware downgrades, unless explicitly required.
- Keep console access available until you can validate your changes.

Use the following table as a template to document the status of the following areas:

| Area | Control | Status / Notes |
|---|---|---|
| Firmware | Approved firmware installed; versions recorded | |
| Accounts | Break-glass account stored securely | |
| Mgmt protocols | SSH enabled; Telnet disabled | |
| Mgmt protocols | HTTPS enabled; HTTP disabled | |
| Mgmt access | Management VLAN/OOB used; management ACL restricts source IPs | |
| AAA | RADIUS/TACACS+ integrated; fallback verified | |
| SNMP | SNMPv3 used; communities restricted or disabled | |
| Logging | Syslog enabled to central collector; timestamps present | |
| Time | NTP configured; time verified | |
| STP | BPDU Guard on edge; root/ loop guard where appropriate | |
| Storm | Storm control on edge/ access ports | |

| Area | Control | Status / Notes |
|---|---|---|
| Anti-spoof | DHCP Snooping enabled on DHCP VLANs; trusted ports set | |
| Anti-spoof | Dynamic ARP Inspection enabled on DHCP VLANs | |
| Port security | MAC limiting/sticky enabled where appropriate | |
| Config mgmt | Configuration backed up after changes; restore tested | |
| Anti-spoof | IP Source Guard enabled (ip verify source) on access ports | |

# Change Management and Rollback Considerations

Security hardening changes can affect management reachability, traffic forwarding, and control-plane stability. Apply changes using a structured change-management process to reduce the risk of outages or administrative lockout. This section provides a safe implementation sequence and rollback approach for NETGEAR M4350 deployments.

## Pre-change planning

Before making changes, confirm the operational context and capture a recovery point.

- Identify the switch role (access, distribution, core, AV aggregation) and the VLAN/port trust boundaries.
- Export a complete configuration backup and record the current firmware version.
- Verify you have console and/or out-of-band access before applying management-plane restrictions.

If AV-over-IP is in use, document multicast requirements (IGMP Snooping/Querier, PTP, bandwidth patterns).

## Change sequencing recommendations

Apply controls in an order that preserves reachability and prevents dependent-feature breakage.

- Enable logging (syslog) and time sync (NTP) early, so changes are fully audit-tracked.
- Enable DHCP Snooping first, then Dynamic ARP Inspection (DAI), then IP Source Guard (dependency chain).
- Apply STP guard features on edge ports before connecting end devices where feasible.
- Introduce DoS protections incrementally; monitor counters/logs for false positives.
- Apply management access restrictions (Management Access List, disabling Telnet/HTTP) last, after validation.

## Validation and monitoring

After each change window, validate both reachability and functional traffic flows.

- Confirm SSH/HTTPS access from authorized subnets and that unauthorized sources are blocked.
- Verify syslog messages are received centrally with correct timestamps.
- Check STP stability (root bridge placement, no unexpected topology changes).
- Validate DHCP operation, ARP resolution, and IP connectivity for representative endpoints.

For AV deployments, validate stream stability and latency/jitter expectations after each step.

## Rollback strategy

Plan for rollback before implementation to reduce mean time to recovery.

- Keep a known-good configuration backup taken immediately before the change.
- Rollback in stages (disable one feature at a time) to isolate the control causing impact.
- Prefer configuration rollback over firmware downgrade unless a confirmed software defect requires it.

Maintain console access until validation is complete and monitoring confirms stability.

## Change documentation

Document changes for audits, troubleshooting, and consistent future rollouts.

- Change date/time, engineer, and approved change record ID (if applicable).
- Features enabled/modified and the exact CLI commands applied.
- Validation results and any deviations from the baseline guidance in this document.
- Rollback actions taken (if any) and final operational state.

# Appendices

The appendices provide supporting material that helps you apply this hardening baseline consistently across different M4350 deployments.

## Appendix A: Threat Model and Hardening Rationale

This appendix provides additional context on the threat model assumed by this guide and explains how each class of control contributes to reducing risk.

### Management plane threats

Use the management plane hardening recommendations to secure your environment from:

- Credential theft through cleartext protocols or compromised endpoints.
- Unauthorized lateral access from user or AV VLANs to the management plane.
- Brute-force or password-spraying attacks against exposed management services.
- Configuration tampering by insiders or compromised admin accounts.

### Control plane threats

Use the control plane hardening recommendations to secure your environment from:

- CPU exhaustion through malformed packets or protocol abuse.
- Topology manipulation through rogue STP devices or BPDU injection.
- Broadcast and multicast amplification attacks affecting availability.

### Data plane threats

Use the data plane hardening recommendations to secure your environment from:

- MAC flooding and CAM table exhaustion.
- ARP spoofing and man-in-the-middle attacks.
- Rogue DHCP servers disrupting address assignment.
- IP spoofing from compromised endpoints.

## Appendix B: Deployment Profiles

The following profiles illustrate how you can apply the hardening recommendations depending on the operational role of the fully managed switch.

### Enterprise IT access switch profile

- Use strict port-security limits, with 1 MAC per access port.
- Use aggressive storm control settings for broadcast and unknown unicast traffic.
- Use full DHCP Snooping, DAI, and IP Source Guard on all user VLANs.
- Restrict management ACL to jump hosts and NMS systems only.

### AV-over-IP / media network profile

- Use relaxed multicast storm control thresholds or disable on AV ports.
- Enable IGMP Snooping and validate for each AV VLAN.
- Adjust port-security limits to account for endpoints with auxiliary MAC addresses.
- Clearly separate AV VLANs and management interfaces.

## Appendix C: Minimum Secure Baseline Checklist

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

- Enable SSHv2 and disable Telnet.
- Enable HTTPS with restricted management access and disable HTTP.
- Apply the appropriate management ACL.
- Enable AAA with TACACS+ or RADIUS with a local fallback.
- Creatre a strong local admin password and configure password aging where appropriate.
- 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 and verify accurate time synchronization.
- Disable unused services and discovery protocols on edge ports.
- Enable BPDU Guard on access ports.
- Enable root Guard on downstream switch links.
- Enable DoS protection.
- Enable DHCP Snooping on user VLANs.
- Enable Dynamic ARP Inspection where DHCP Snooping is active.
- Enable IP Source Guard on untrusted access ports.
- Enable port security with appropriate MAC limits.
- Enable storm control on IT/user ports and validate for AV exceptions.
- Restrict physical access to the console and USB ports.

## Appendix D: Security Control Mapping (CIS / NIST Alignment)

This appendix maps the controls recommended in this guide to common industry security frameworks.

> **NOTE:** The appendix is reference only and does not imply formal certification or compliance.

- Secure management access (SSHv2, HTTPS, ACLs) > CIS 4, CIS 12, NIST PR.AC-3.
- AAA with central authentication > CIS 5, CIS 6, NIST PR.AC-1.
- Logging and time synchronization > CIS 8, NIST DE.AE-3.
- DoS and control plane protection > CIS 13, NIST PR.PT-5.

- STP protection and loop prevention > CIS 11, NIST PR.PT-4.
- DHCP Snooping / DAI / IP Source Guard > CIS 12, NIST PR.AC-5.
- Port security and storm control > CIS 9, NIST PR.DS-5.
- Physical security controls > CIS 1, NIST PR.AC-2.

## Appendix E: Common Pitfalls and Misconfigurations

This appendix highlights the configuration mistakes frequently observed in production deployments. Avoid the following pitfalls to preserve availability, prevent accidental lockouts, and ensure that security controls function as intended.

- **Locking out management access**:

  Applying a management ACL without first permitting the current administrator IP range or without maintaining console/OOB access can result in complete loss of management connectivity.
- **Using SNMPv2c in production**:

  SNMPv2c exposes community strings in clear text and provides no integrity or confidentiality. Disable SNMPv2c after you configure and validate SNMPv3.
- **Applying aggressive storm control on AV ports**:

  Applying multicast storm control to AV-over-IP ports (Dante, NDI, AES67) can cause intermittent audio and video loss. Validate storm control on each VLAN and port role.
- **Forgetting trust boundaries with DHCP Snooping**:

  Failing to mark uplinks as trusted can break legitimate DHCP services. Marking user ports as trusted can enable rogue DHCP attacks.
- **Enabling IP Source Guard without DHCP Snooping**:

  IP Source Guard relies on DHCP Snooping bindings. Enabling it without DHCP Snooping blocks valid traffic.
- **Disabling LLDP globally without considering operations**:

  You might LLDP require for inventory, monitoring, or AV device discovery. Disable LLDP selectively on untrusted edge ports rather than globally.
- **Ignoring STP guard features**:

  Leaving BPDU Guard and Root Guard disabled increases the risk of topology loops or unintended root bridge elections caused by user-connected switches.
- **Using weak or shared local admin credentials**:

  Use strong, unique credentials for local fallback accounts and review them periodically to reduce insider and credential-reuse risks.
- **No centralized logging**:

  Relying only on local logs makes forensic analysis impossible after a reboot or power failure.

Always forward logs to a central syslog server.

- **Unrestricted physical access**:

  Restrict physical access; you cannot disable the USB-C console and USB-A storage ports in software.