VIVOTEK Security Hardening Guide

Security Configuration Guidelines

Version 2.1

Disclaimer

The security recommendations and best practices provided in this guide are based on information and technical standards known at the time of publication. Given the continuous evolution of cybersecurity threats, VIVOTEK strongly advises all users to keep their product firmware updated to the latest version and to stay informed of the latest security advisories released by the company. VIVOTEK shall not be held liable for any security incidents, data breaches, system failures, or related losses resulting from the failure to update firmware in a timely manner, non-compliance with the recommendations in this guide, or improper configuration. Users assume full responsibility for ensuring the security of their system deployment and maintenance.

Table of Contents

1. Executive Summary

This hardening guide is designed to provide a comprehensive set of security configurations and best practices for the deployment of VIVOTEK IP surveillance systems. By integrating industry-leading security standards (such as CIS Controls) and practical experience, this document aims to assist system integrators, IT administrators, and end-users in building a surveillance infrastructure that has defense-in-depth and meets regulatory requirements.

Critical Security Requirements:

- **Network Segmentation:** Isolate camera networks from critical business systems
- **ARP Protection:** Deploy DAI-capable switches to prevent ARP spoofing
- **Email Security:** Use SMTP over TLS 1.2+ with authentication
- **SNMP Security:** Change default community strings, migrate to SNMPv3
- **Access Control:** Implement strong authentication and encryption

Key Principles:

- **Defense in Depth:** Multiple layers of security controls
- **Least Privilege:** Minimal access rights for users and services
- **Secure by Default:** Strong security configurations out of the box
- **Continuous Monitoring:** Regular updates and security assessments

2. Introduction and Scope

Target Audience: This guide is primarily intended for professionals responsible for planning, deploying, managing, and maintaining VIVOTEK surveillance systems, including but not limited to:

- Network Administrators

- IT Security Professionals
- System Integrators
- Managers responsible for physical security

Shared Responsibility Model: The security of a surveillance system is a shared responsibility that spans the supply chain, system integrators, and end-user organizations. A truly secure environment depends on the synergy of people, processes, and technology. VIVOTEK is committed to providing secure products and maintaining a dedicated information security team responsible for reviewing product designs, collaborating with leading security firms, and managing the vulnerability reporting process.

However, product-level security is only one part of the overall security strategy. Proper camera and network infrastructure configuration is critical for defending against real-world threats. This guide aims to provide the knowledge and tools necessary to achieve this goal.

Scope: The recommendations in this guide follow the CIS Critical Security Controls for Effective Cyber Defense and integrate best practices from industry leaders to provide comprehensive security guidance, from basic setups to enterprise-level deployments.

3. Security Levels Overview

- **Level 1: Basic Security (Mandatory)** This is the minimum-security baseline for all VIVOTEK device deployments. All recommendations in this section should be considered mandatory requirements, designed to defend against common automated attacks. It is applicable to any network environment, especially closed networks with limited external access.

- **Level 2: Advanced Security** This level is applicable to scenarios where devices may be exposed to the internet or deployed in higher-risk network environments. This section provides enhanced security, including stricter encryption, access control, and log monitoring to counter more targeted threats.

- **Level 3: Enterprise Security** This level is designed for large organizations with complex network infrastructures, requirements for integration with existing IT management systems (like RADIUS, SIEM), and strict compliance needs. This section covers the highest level of security measures, such as 802.1X, PKI, and advanced network segmentation.

4. Basic Security (Mandatory)

4.1 Firmware Management

Critical Requirements:

- Always use the latest firmware version available from VIVOTEK
- Subscribe to VIVOTEK security notifications for vulnerability updates
- Establish a Standard Operating Procedure (SOP) to schedule regular maintenance windows for firmware updates.
- Verify firmware signatures before installation
- Maintain a firmware update log for compliance

4.2 Password and Authentication

Password Requirements:

- Minimum 12 characters (8 absolute minimum)
- Include: uppercase [A-Z], lowercase [a-z], numbers [0-9], special characters [!$%-.@^_~]
- Unique passwords per device (no password reuse)
- Change default credentials immediately upon installation
- Implement password rotation policy (90 days recommended)

Authentication Configuration:

- Disable anonymous viewing unless explicitly required
- Enable HTTP Digest authentication. HTTP Basic authentication transmits credentials in Base64 encoding (not encryption), making them easy to steal, and should always be disabled.
- Enable RTSP streaming authentication
- Enable brute-force attack protection. This feature detects and blocks IP addresses that attempt multiple password guesses in a short period, serving as a key barrier against automated attacks.
- Configure account lockout after 5 failed attempts

4.3 User Access Management

User Privilege Levels:

- **Administrator:** Full system configuration and management
- **Operator:** Camera controls and settings adjustment
- **Viewer:** View-only access to video streams

Best Practices:

- Create dedicated accounts for VMS integration (never use root)
- Assign minimum necessary privileges to each user
- Maintain user access audit log
- Regular review of user accounts (quarterly)
- Disable or remove unused accounts immediately

4.4 Network Services

Disable Unused Services:

- Audio (if not required)
- UPnP (Universal Plug and Play). This service may automatically open ports on the router without authorization, posing a serious security risk, and should always be disabled.
- IPv6 (if not used)
- Always Multicast (unless specifically required)
- SNMP v1/v2 (migrate to SNMPv3 for security)
- ⚠️ **SECURITY ALERT:** Default SNMP community strings ‘public’ and ‘private’ are well-known and MUST be changed immediately. These are equivalent to using ‘admin/admin’ as credentials.
- SSH/Telnet/FTP access
  - **Special Note:** Telnet (defaulting to 23/TCP, with some devices possibly using 2323/TCP) is an unencrypted protocol. All transmitted content, including usernames and passwords, is sent in clear text, posing an extremely high security risk and should always be disabled.
- Discovery protocols (Bonjour, WS-Discovery) after setup

4.5 Time Synchronization

Requirements:

- Configure NTP synchronization with trusted servers
- Use multiple NTP servers for redundancy
- **NTP Security:** As the device does not currently support Network Time Security (NTS), it is recommended to set the NTP server to a trusted internal source and use firewall rules to restrict traffic to only UDP port 123 from the NTP server to mitigate risk.
- Verify correct time zone configuration
- Monitor time synchronization status regularly

---

5. Advanced Security

5.1 Encryption and HTTPS

HTTPS Configuration:

- Enable HTTPS with TLS 1.2 minimum (TLS 1.3 preferred)
- Disable TLS 1.0 and TLS 1.1
- Use CA-signed certificates (avoid self-signed in production)
- Configure strong cipher suites only
- Enable HSTS (HTTP Strict Transport Security)
- Force HTTPS-only connections

Recommended Cipher Suites:

- `ECDHE-ECDSA-AES256-GCM-SHA384`
- `ECDHE-RSA-AES256-GCM-SHA384`
- `ECDHE-ECDSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES128-GCM-SHA256`

5.2 Access Control Lists

Implementation:

- Enable IP address filtering
- Configure allow-list for known VMS/client IPs only
- Limit concurrent streaming connections
- Configure host-based firewall rules
- Implement port-based access restrictions
- Regular review and update of access lists

5.3 Remote Logging

Configuration:

- Configure remote syslog server
- Use encrypted syslog (TLS) when possible
- Enable comprehensive access logging
- Log authentication attempts (successful and failed)
- Log configuration changes
- Implement log retention policy (minimum 90 days)

5.4 Port Management

Non-Default Port Configuration:

- Change the default HTTP port from 80. While this does not stop targeted attacks, it effectively avoids large-scale automated scans targeting the default port.
- Change default HTTPS port from 443
- Change default RTSP port from 554
- Document all port changes
- Update firewall rules accordingly

5.5 Email Notification Security

SMTP Configuration Requirements:

- Enable SMTP over TLS/SSL for all email notifications
- Restrict to TLS 1.2 or higher (disable TLS 1.0/1.1)
- Use Primary SMTP Authentication mechanism
- Configure trusted mail server for authentication
- Use dedicated service account for SMTP authentication
- Enable STARTTLS for opportunistic encryption
- Verify server certificate validity

Security Benefits:

- Prevents eavesdropping of email content during transmission
- Protects authentication credentials from interception
- Ensures email integrity through encryption
- Prevents email spoofing and tampering
- Compliance with data protection regulations

5.6 SNMP Security Configuration

Critical SNMP Security Requirements:

- **MANDATORY:** Change default community strings immediately
    - Never use default ‘public’ for read-only access
    - Never use default ‘private’ for read-write access
    - Use complex, unique community strings (minimum 12 characters)
    - Treat community strings as passwords

SNMPv3 Migration (Strongly Recommended):

- Migrate to SNMPv3 for all production environments
- Configure user-based security model (USM)
- Enable authentication (SHA-256 or stronger)
- Enable encryption (AES-256 recommended)
- Configure view-based access control (VACM)
- Use unique credentials per device or device group

SNMPv1/v2c Security (If Migration Not Possible):

- Restrict SNMP access by IP address (ACLs)
- Use read-only community strings whenever possible
- Implement separate community strings for read and write
- Monitor SNMP access logs for unauthorized attempts
- Consider SNMP over VPN for remote monitoring
- Disable SNMP write access if not required

WARNING: SNMPv1 and SNMPv2c transmit community strings in clear text and provide no encryption. These protocols should only be used in isolated, trusted networks and should be replaced with SNMPv3 as soon as possible.

5.7 Edge Storage Security

SD Card Security:

- **Future Feature - SD Card Encryption:** Future product models or new firmware versions will support SD card encryption with the AES-256 standard. When using a device that supports this feature, it is strongly recommended to enable it to protect the confidentiality of stored data.
- **Security Recommendations for Current Devices:** For devices that do not currently support SD card encryption, physical security is paramount. Please ensure that:
    - The camera is installed in a location that is not easily accessible or vulnerable to tampering.
    - A vandal-resistant housing is used to protect the camera where appropriate.
    - Physical access to the device is strictly controlled to prevent unauthorized removal of the SD card.
- **When Not in Use:** If the edge storage function is not used, it is recommended to disable the SD card slot or not insert an SD card.

Network Attached Storage (NAS):

- **Protocol Version:** Due to licensing restrictions, the product supports up to SMBv2.1. Please ensure your NAS device is configured to use this version for connections.
- **Security Hardening Measures:** Since SMBv2.1 does not support the end-to-end encryption offered by SMB 3.0, it is **strongly recommended** to deploy the camera and NAS in a dedicated, isolated network environment to protect data in transit.
- **Access Control:**
  - Configure a dedicated service account for the NAS connection with the minimum necessary permissions.
  - Strictly limit access to the NAS share to only the camera's IP address.
- **Log Monitoring:** Monitor the storage device's access logs to detect unusual activity in a timely manner.

---

6. Enterprise Security

6.1 IEEE 802.1X Authentication

Implementation:

- Deploy 802.1X port-based network access control
- Use EAP-TLS for strongest security
- Configure RADIUS authentication servers
- Deploy certificate-based authentication
- Implement dynamic VLAN assignment
- **Traffic Protection:** As the device does not support MACsec (IEEE 802.1AE) for link-layer encryption, ensure that the device is deployed in a trusted and physically secure network segment. All remote management should be conducted over HTTPS or other encrypted protocols to protect data in transit.

6.2 Network Segmentation

VLAN Configuration:

- Create dedicated surveillance VLAN
- **CRITICAL:** Isolate camera network from critical business systems
- Separate camera, storage, and viewing networks
- Implement strict inter-VLAN routing controls
- Configure VLAN access control lists (ACLs)
- Enable private VLANs for camera isolation

- Prohibit direct routing between surveillance and critical infrastructure VLANs
- Document network topology and VLAN assignments

6.3 Public Key Infrastructure

Certificate Management:

- Deploy enterprise Certificate Authority (CA)
- Issue unique certificates per device
- Implement certificate lifecycle management
- Configure certificate revocation lists (CRL)
- Enable OCSP for real-time validation
- Regular certificate audits and renewal

6.4 Advanced Monitoring

Security Information and Event Management (SIEM):

- Integrate camera logs with SIEM platform
- Configure real-time security alerts
- Monitor authentication anomalies
- Track configuration changes
- Analyze network traffic patterns
- Generate security metrics and reports

---

7. Network Architecture Guidelines

7.1 Physical Security

Camera Protection:

- Install cameras in tamper-resistant locations
- Use vandal-resistant housing where appropriate
- Protect cables in conduits or walls
- Deploy tamper detection switches
- Secure physical access to network equipment
- Lock server rooms and network closets

7.2 Network Design Best Practices

Architecture Principles:

- **Prohibit Direct Internet Exposure:** This is the most important architectural principle. Exposing cameras directly to the public internet makes them a target for global attackers' scanning and attacks. All remote access should be conducted through a VPN or other secure proxy methods.
- Implement defense-in-depth strategy
- Use jump servers for remote access
- Deploy intrusion detection systems (IDS)
- Configure redundant network paths
- Implement Quality of Service (QoS) for video traffic

7.3 Switch Security Configuration

Dynamic ARP Inspection (DAI):

- Deploy switches with DAI (Dynamic ARP Inspection) capability
- Enable DAI to mitigate ARP spoofing attacks
- Configure DHCP snooping as prerequisite for DAI
- Define trusted ports for uplinks and servers
- Monitor ARP inspection logs for anomalies
- Enable IP Source Guard for additional protection

Additional Switch Security:

- Enable port security to limit MAC addresses per port
- Configure storm control for broadcast/multicast traffic
- Disable unused switch ports
- Enable BPDU Guard on access ports
- Configure Root Guard on designated ports

7.4 Remote Access Security

VPN Configuration:

- Use enterprise VPN for all remote access
- Implement multi-factor authentication (MFA)
- Configure split-tunneling restrictions
- Use certificate-based VPN authentication
- Monitor VPN access logs
- Regular review of VPN user access

8. Compliance and Standards

8.1 Industry Standards

Applicable Standards:

- CIS Critical Security Controls v8
- NIST Cybersecurity Framework
- ISO/IEC 27001:2022
- UL 2900-2-3 (Cybersecurity for Network Cameras)
- GDPR (for privacy compliance)
- NDAA Section 889 (US Government compliance)

8.2 Audit and Assessment

Regular Security Assessments:

- Quarterly vulnerability scanning
- Annual penetration testing
- Configuration compliance audits
- User access reviews
- Security incident response drills
- Third-party security assessments

---

9. Security Maintenance

9.1 Patch Management

Process:

- Subscribe to vendor security advisories
- Test firmware updates in lab environment
- Schedule maintenance windows
- Document all changes
- Verify functionality post-update
- Maintain rollback procedures

9.2 Incident Response

Response Plan:

- Define incident response team
- Establish escalation procedures

- Document incident response playbooks
- Configure automated alerts
- Conduct post-incident reviews
- Update security controls based on lessons learned

9.3 Device Decommissioning

IoT products (like network cameras), if not properly handled during decommissioning, disposal, or resale, can pose serious information security risks. Residual sensitive information on the device, such as configuration settings, user credentials, and video recordings, could be accessed by unauthorized third parties, leading to privacy breaches or becoming a steppingstone for network intrusion. Therefore, a strict end-of-life procedure must be followed to ensure all data is thoroughly erased.

Secure Disposal Process:

- **Perform a Factory Reset:** This is the primary step to clear most user configurations and settings.
- **Verify Data Erasure:** After a factory reset, the device should be rebooted and checked to ensure all accounts, network settings, and other custom configurations have been removed.
- **Securely Erase Storage Media:**
  - **Internal Storage/SD Card:** If the device supports it, perform a format or secure erase of the encrypted storage media. For physical SD cards, physical destruction (e.g., shredding or drilling) is recommended.
  - **Video Recordings:** Confirm that all video stored locally or on a NAS has been deleted or destroyed.
- **Remove Device Credentials and Connections:**
  - Remove the device from the VMS or other management platforms.
  - If using 802.1X or PKI, the device's certificate should be revoked.
- **Update Asset Inventory:** Mark the device as 'decommissioned' in the asset management system.
- **Follow Standard Guidelines:** It is recommended to follow international standards like NIST SP 800-88 (Guidelines for Media Sanitization) to perform data sanitization procedures, ensuring data cannot be recovered.

10. Appendices

Appendix A: Security Checklist

Initial Deployment:

- ☐ Latest firmware installed
- ☐ Default password changed
- ☐ Strong password configured
- ☐ Anonymous access disabled
- ☐ HTTPS enabled
- ☐ Unused services disabled
- ☐ NTP configured
- ☐ Access list configured
- ☐ Logging enabled
- ☐ Camera network isolated from critical systems
- ☐ DAI enabled on switch
- ☐ SMTP over TLS configured
- ☐ SNMP default community string changed
- ☐ SNMPv3 configured (if SNMP is required)
- ☐ Documentation completed
- ☐ Verified location of Vulnerability Disclosure Policy (see Appendix D)

Appendix B: Common Ports Reference

Service	Default Port	Protocol	Security Note
HTTP	80	TCP	Disable in production
HTTPS	443	TCP	Required for secure access
RTSP	554	TCP	Enable authentication
RTP	Dynamic	UDP	Use SRTP when possible
SNMP	161	UDP	Use SNMPv3 only, change defaults

Appendix C: Resources

- **VIVOTEK Support:** https://www.vivotek.com/resource/support/cybersecurity
- **CIS Controls:** https://www.cisecurity.org/controls
- **NIST Cybersecurity Framework:** https://www.nist.gov/cyberframework
- **CVE Database:** https://cve.mitre.org
- **VIVOTEK Security Advisories:** Subscribe via VIVOTEK newsletter

Appendix D: Vulnerability Disclosure Policy Summary

VIVOTEK is committed to protecting our customers and products. We encourage security researchers and users to report potential vulnerabilities to us in good faith. The following is a summary of our vulnerability handling process:

1. How to Report a Vulnerability

We have established clear channels for receiving vulnerability reports:

- **Email:** Please send your findings to `security@vivotek.com`.
- **Web Form:** You can also submit a report through our official website: `https://www.vivotek.com/resource/support/cybersecurity`

2. How We Will Contact and Respond to You

- **Initial Response:** Upon receiving your report, our Global Technical Service Department will acknowledge receipts within **five business days**.
- **Internal Handling:** Our PSIRT (Product Security Incident Response Team) will immediately conduct an initial triage and evaluation, completing the assessment, prioritization, and remediation plan within **72 working hours**.
- **Staying in Touch:** Throughout the process, we will assign a dedicated contact person to keep you informed of the progress.

3. Vulnerability Investigation and Announcement

- **Investigation and Remediation:** Before a fix is available, our team will conduct technical validation and impact analysis, providing temporary mitigation measures or recommendations as appropriate.
- **Status Management and Announcement:** Once a fix (such as a firmware update) is ready, we will issue a public disclosure through the “Security Advisories” section of our official website. The content will include the affected products, the severity of the vulnerability (CVSS score), the CVE number, and remediation advice.

4. Safe Harbor

We pledge not to take legal action against any reporter who acts in good faith and adheres to the following principles:

- Your research activities do not cause harm to our products, services, or customers.
- You do not store, share, or disclose any data that does not belong to you.
- You provide us with a reasonable amount of time to respond and remediate before publicly disclosing any vulnerability information.

We thank all security researchers for their contributions to protecting cybersecurity together.