About this Document
The intended use of this guide is to harden devices and also provide collateral for deployment teams to deal with local network policy, configurations and specification.
All settings described in this document are made in the product’s webpages. To access the webpages, see the User Manual of the specific product.

Liability
Every care has been taken in the preparation of this document. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material. This product is only to be used for its intended purpose.

Intellectual Property Rights
Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at www.axis.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.
This product contains licensed third-party software. See the menu item “About” in the product’s user interface for more information.
This product contains source code copyright Apple Computer, Inc., under the terms of Apple Public Source License 2.0 (see www.opensource.apple.com/apsl). The source code is available from https://developer.apple.com/bonjour/

Trademark Acknowledgments
AXIS COMMUNICATIONS and AXIS are registered trademarks or trademark applications of Axis AB in various jurisdictions. All other company names and products are trademarks or registered trademarks of their respective companies.
Apple, Boa, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows, Windows Vista and WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates. UPnP™ is a certification mark of the UPnP™ Implementers Corporation.

Contact Information
Axis Communications AB
Emdalavägen 14
223 69 Lund
Sweden
Tel: +46 46 272 18 00
Fax: +46 46 13 61 30
www.axis.com

Support
Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response. If you are connected to the Internet, you can:
• download user documentation and software updates
• find answers to resolved problems in the FAQ database. Search by product, category, or phrase
• report problems to Axis support staff by logging in to your private support area
• chat with Axis support staff
• visit Axis Support at www.axis.com/techsup/
Should you require any technical assistance, please contact ADP Helpdesk to ensure a rapid response.

Learn More!
# Table of Contents

**Introduction** ................................................. 4  
Security cameras in a network environment ........................ 4  
Compensating controls ......................................... 4  

**About the protection levels** ................................ 5  

**Default protection** ........................................ 6  

**Standard protection** ....................................... 7  
Check the firmware ............................................ 7  
Upgrade the firmware ......................................... 7  
Reset to factory default settings .............................. 8  
Set the root password ......................................... 8  
Set user permissions .......................................... 8  
Configure basic network settings .............................. 9  
Set time and date .............................................. 9  
Disable audio .................................................. 10  

**Enterprise protection** ..................................... 12  
Enable encryption .............................................. 12  
Create a backup admin account ................................ 13  
Create video client account .................................. 13  
Disable AVHS ................................................... 14  
Disable discovery services .................................... 14  
Configure advanced network settings ......................... 16  
Disable SOCKS .................................................. 17  
Disable QoS ..................................................... 18  
Disable always multicast video ............................... 18  
Disable SSH ..................................................... 19  
Set IP address filter .......................................... 19  

**Managed enterprise protection** ........................... 21  
Access to IEEE 802.1x network ................................ 21  
Configure SNMP monitoring .................................... 22  
Remote system log .............................................. 23
Introduction

The responsibility to secure a network, its devices, and the services it supports falls across the entire vendor supply chain, as well as on the end-user organization. A secure environment depends on its users, processes, and technology.

This hardening guide provides technical advice for anyone involved in deploying Axis video solutions. It establishes a baseline configuration and a hardening strategy that deals with the evolving threat landscape. Like many other security organization do, the Axis baseline uses the SANS Top 20 Critical Security Controls – Version 5, see www.sans.org/critical-security-controls

Security cameras in a network environment

The most apparent threat to a network camera is physical sabotage, vandalism and tampering. To protect the product from these threats, it is important to select a vandal-resistant model or casing, to mount it in the recommended way, and to protect the cables.

From an IT/network perspective, the camera is a network endpoint similar to business laptops, desktops, and mobile devices. Unlike a business laptop, a network camera is not exposed to the common threat of users visiting potentially harmful websites, opening malicious email attachments, or installing untrusted applications. However, the camera is a network device with an interface that may expose risk. This guide focuses on reducing the exposure area of these risks.

Compensating controls

Compensating controls are solutions (add-ons, customizations, rules or tuning of the deployment) that address controls that a system cannot otherwise address.

For example, if a network camera does not support remote syslog or SNMP, it is possible to connect the camera through a switch that supports these control functions. Firewalls, encrypted access methods, and constrained configuration on switches, for example ACLs (Access Control Lists), are other examples of commonly used compensating controls.

These compensating controls are part of the industry’s control sets (the SANS list of compliances) that Axis uses for hardening cameras and video surveillance solutions.
This guide uses different protection levels depending on system size and needs. Each level assumes that the previous level’s recommendations are followed.

<table>
<thead>
<tr>
<th>Protection level</th>
<th>Recommended for</th>
<th>Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Default protection</td>
<td>Only recommended for demo purposes and test scenarios.</td>
</tr>
</tbody>
</table>
| 1                | Standard protection | Minimum recommended level of protection. This level is adequate for small businesses or office installations where, typically, the operator is also the administrator. | Check the firmware  
Upgrade the firmware  
Reset to factory default settings  
Set the root password  
Set user permissions  
Configure basic network settings  
Set time and date  
Disable audio |
| 2                | Enterprise protection | Recommended settings for corporations that have a dedicated system administrator. | Enable encryption  
Create a backup admin account  
Create video client account  
Disable AVHS  
Disable discovery services  
Configure advanced network settings  
Disable SOCKS  
Disable QoS  
Disable always multicast video  
Disable SSH  
Set IP address filter |
| 3                | Managed enterprise protection | Large network infrastructure with an IT/IS department. For environments where cameras may need to be integrated into an enterprise network infrastructure. | Access to IEEE 802.1x network  
Configure SNMP monitoring  
Remote system log |
Cameras are delivered with predefined default settings and a default password. Adjust the settings to meet the challenges from the network environment and the result of a risk analysis.
Standard protection

The standard protection level is the minimum recommended level of protection. This level is adequate for small businesses or office installations where, typically, the operator is also the administrator.

Check the firmware

Firmware is the software that enables and controls the functionality of network devices. Always use the latest firmware so that you get all possible security updates and bug fixes.

Check the current firmware version in page Setup > Basic Setup or in Setup > About.

Upgrade the firmware

SANS #1: Inventory of authorized and unauthorized devices.

SANS #2: Inventory of authorized and unauthorized software.

Before upgrading the firmware, read the instructions in the User Manual.

1. Download the latest firmware file to your computer, available free of charge at www.axis.com/techsup/firmware.php
2. Upgrade the firmware.

Note: Do not disconnect power to the unit during the upgrade. The unit restarts automatically after the upgrade has completed (1-30 minutes).
Reset to factory default settings

Make sure that the product is in a known state by resetting to factory default settings. For instructions, see the User Manual.

Set the root password

SANS #3: Secure configuration for hardware and software.
SANS #12: Controlled use of administrative privileges.

The password is the most important protection measure of a network camera. Make sure to use a strong password and keep it protected. On a multi-camera installation the cameras can have the same password or unique passwords. Using the same password simplifies management but increases the risk if one camera's security is compromised.

**Important**
- When setting the initial password, the password is sent in clear text over the network. If there is a risk of network sniffing, first set up a secure an encrypted HTTPS connection before resetting the passwords.
- Axis' cameras do not impose a password policy as products may be used in various types of installations. Use a password with at least 8 characters, preferably using a password generator.

To set the password via a standard HTTP connection, enter it directly in the dialog.

---

Set user permissions

SANS #3: Secure configuration for hardware and software.
SANS #11: Limitation and control of network ports, protocols, and services.

2. To prevent clients to login with plain text passwords, make sure that Allow password type is set to Encrypted only.
3. Make sure that both Enable anonymous viewer login and Enable anonymous PTZ control login are disabled.
4. Click Save.

Configure basic network settings

SANS #3: Secure configuration for hardware and software.

1. Go to System Options > Network to get the expanded list of basic network settings.
3. Select Use the following IP address and specify the IP address, subnet mask and default router.
4. If the network uses IPv6, select Enable IPv6. Otherwise leave it disabled to avoid unintended access.
5. Clear Enable ARP/Ping setting of IP address.
6. Save parameters and reconnect to management interface on the assigned IP address.

Set time and date

SANS #3: Secure configuration for hardware and software.
Hardening Guide

Standard protection

From a security perspective it is important that the date and time is correct so that, for example, the system logs are time-stamped with the right information.

It is recommended to synchronize the camera clock with an Network Time Protocol (NTP) server. If there are no NTP servers on the system, use a public NTP server (available online, for example, pool.ntp.org). Without NTP synchronization date and time must be set manually. Most cameras models has a battery backup RTC (Real-Time Clock) that will maintain the time without power.

1. Go to System Options > Date & Time.
2. Set Time mode to Synchronize with NTP server.
3. Click Save.
4. Click on the link NTP server.
5. Set the NTP server and click Save.
6. Set the Time zone.
7. Select Automatically adjust for daylight saving time changes.

Disable audio

SANS #11: Limitation and control of network ports, protocols, and services.

If the network camera has audio support that is not used in daily operation, you should prevent clients from requesting audio streams by disabling the audio support.

1. Go to System Options > Security > Audio Support.
2. Clear Enable audio support.
# Hardening Guide

## Standard protection

- Basic Setup
- Video & Audio
- Live View Config
- Detectors
- Applications
- Events
- Recordings
- Languages
- System Options
  - Security
    - Users
    - ONVIF
    - IP Address Filter
    - HTTPS
    - IEEE 802.1X
    - Certificates
  - Audio Support
  - Date & Time

### Audio Support

#### Settings

<table>
<thead>
<tr>
<th>Enable audio support.</th>
<th>Save</th>
<th>Reset</th>
</tr>
</thead>
</table>

11
Enterprise protection

The enterprise protection level is about minimizing risks by reducing the possible attack area of the network camera.

Note
Some of the settings described in this section are preset at the factory. Make sure that they are correct by following the instructions below.

Enable encryption

SANS #17: Data protection.
Access the camera using HTTPS, which encrypts the traffic between the client and the camera. All camera administrative tasks should go through HTTPS. Video streamed over RTP/RTSP is still unencrypted. If the video stream contains sensitive data, tunnel RTP/RTSP over HTTPS. This is controlled by (and depends on) the video client/VMS capabilities.

Create certificate

SANS #3: Secure configuration for hardware and software.

A self-signed certificate is adequate for providing encryption, but the web browser will warn that the certificate cannot be validated. A CA-signed certificate is needed for the client to authenticate that it is accessing the correct camera.

1. Go to System Options > Security > Certificates.

2. Create a self-signed certificate. For instructions, see the User Manual.

Enable HTTPS

SANS #3: Secure configuration for hardware and software.

Users with administration rights should encrypt traffic between the clients and the camera. This requires that the client supports HTTPS.

1. Go to System Options > Security > HTTPS.

2. To enable HTTPS, select the created certificate in the drop-down list.

3. Demand that administrators use HTTPS. If additional user accounts are added with viewer and operator level privileges, set the connection policy accordingly.
4. Click Save.

Create a backup admin account

SANS #3: Secure configuration for hardware and software.

SANS #12: Controlled use of administrative privileges.

Good practice is to create a backup administrator account with a different password than the primary administrator account.

1. Go to System Options > Users.

2. Add a backup administrator account. For password requirements, see Set the root password.

3. Click Save.

Create video client account

SANS #3: Secure configuration for hardware and software.

SANS #12: Controlled use of administrative privileges.

A client or a Video Management System (VMS) should normally use the operator group with restricted administrator privileges. Video systems and clients should not use the administrator account. In most cases the operator group is sufficient. However, the VMS may use services that require administrator rights.

1. Go to System Options > Users.
2. Add a new account with an appropriate user group and set a strong password that matches the video system and clients. For password requirements, see Set the root password.

Disable AVHS

SANS #11: Limitation and control of network ports, protocols, and services.

If the camera is not connected to a hosted video service, disable AVHS.

1. Go to System Options > Network.
2. Clear Enable AVHS.
3. Click Save.

Disable discovery services

SANS #3: Secure configuration for hardware and software.

Discovery protocols are support services that make it easier to find the cameras on the network. After deployment, you should stop the cameras from announcing their presence on the network by disabling the discovery protocol.
Hardening Guide

Enterprise protection

Disable UPnP™

1. Go to System Options > Network > UPnP.
2. Clear Enable UPnP. You can enable it temporarily when needed for maintenance.
3. Click Save.

Disable Bonjour

1. Go to System Options > Network > Bonjour.
2. Clear Enable Bonjour. You can enable it temporarily when needed for maintenance.
3. Click Save.

Disable link-local address

1. Go to System Options > Network > Advanced.
2. Clear Auto-Configure Link-Local Address.
Configure advanced network settings

SANS #1: Inventory of authorized and unauthorized devices.

SANS #3: Secure configuration for hardware and software.

SANS #11: Limitation and control of network ports, protocols, and services.

1. Go to System Options > Network > Advanced.
2. Configure Domain Name Service (DNS). If possible, use both a primary and a secondary DNS.
3. To set the fully qualified domain name (FQDN) manually, select Use the host name.
4. Select Use the following DNS server address and specify the following:
   - Enter the domain(s) to search for the host name used by the Axis product. Multiple domains can be separated by semicolons. The host name is always the first part of a fully qualified domain name, for example, myserver is the host name in the fully qualified domain name myserver.mycompany.com where mycompany.com is the domain name.
   - Enter the IP addresses of the primary and secondary DNS servers. The secondary DNS server is optional and is used if the primary is unavailable.
5. Keep the default values HTTP port: 80, and HTTPS port: 443.
7. To keep H.264 video streams available, select Enable RTSP. Keep the default port 554.
8. Click Save and reconnect to management interface on the assigned IP address.
Disable SOCKS

SANS #11: Limitation and control of network ports, protocols, and services.

If the network is not using SOCKS, disable it in the network camera as well.

1. Go to System Options > Network > SOCKS.
2. Clear Enable SOCKS.
3. Click Save.
Disable QoS

SANS #11: Limitation and control of network ports, protocols, and services.

If Quality of Services is not being used, QoS should be disabled.

1. Go to System Options > Network > QoS.
2. To disable QoS, enter the value zero in the QoS DSCP Settings fields.
3. Click Save.

Disable always multicast video

SANS #11: Limitation and control of network ports, protocols, and services.

To prevent the camera from multicasting video by default, disable multicast video streaming. The camera can still multicast video upon request.

1. Go to System Options > Network > RTP.
2. Clear Always Multicast Video.
3. Click Save.

---

### Disable SSH

SANS #11: Limitation and control of network ports, protocols, and services.

Axis' cameras support Secure Shell (SSH) and is disabled by default. Make sure that it is disabled by doing the following:

1. Go to System Options > Advanced > Plain Config

2. In the drop-down menu, select Network and click Select group.

3. Make sure that Network SSH is disabled by clearing SSH Enabled.

4. If needed, click Save.

---

### Set IP address filter

SANS #13: Boundary defense.
SANS #15: Controlled access based on the need to know.

We recommend that video clients access live and recorded video only through the VMS, they should not be allowed to access any video directly through the cameras.

Enabling IP filtering for authorized clients will prevent the camera from responding to network traffic from any other clients. Make sure to add all authorized clients (VMS server and administrative clients) to the white list.

1. Go to System Options > Security > IP Address Filter.
2. Select Enable IP address filtering and add the allowed IP addresses. For more instructions, see the User Manual.
Managed enterprise networks are systems that typically have additional management tools and services that the cameras need to be aligned with.

**Access to IEEE 802.1x network**

SANS #1: Inventory of authorized and unauthorized devices.

SANS #13: Boundary defense.

To be accepted in a network protected by IEEE 802.1x, the cameras need to have appropriate certificates and settings.

1. Go to System Options > Security > Certificates.
2. Install the CA certificate for the network.
3. Install the client certificate.
4. Go to System Options > Security > IEEE 802.1x.
5. Select the CA certificate and the Client Certificate.
6. Configure the settings.
7. Select Enable IEEE 802.1x.
8. Click Save.
Configure SNMP monitoring

SANS #14: Maintenance, monitoring, and analysis of audit logs.

Axis’ cameras support the following SNMP protocols:

- **SNMP v1**: Supported only for legacy reasons and should not be used.
- **SNMP v2c**: May be used on a protected network segment.
- **SNMP v3**: Recommended for monitoring purposes.

The cameras support monitoring MIB-II and Axis Video MIB. Axis Video MIB can be downloaded at www.axis.com/global/en/support/downloads/axis-video-mib

For more information about SNMP, see the User Manual.

1. Go to System Options > Network > SNMP.

2. If needed, install certificates and enable HTTPS for SNMP v3, see also Enable encryption on page 12.
Remote system log

SANS #4: Continuous vulnerability assessment and remediation.
SANS #14: Maintenance, monitoring, and analysis of audit Logs.
SANS #16: Account monitoring and control.
SANS #18: Incident response and management.

1. Go to System Options > Advanced > Scripting > Open Script Editor.
2. For cameras with firmware 5.80 and later, select /etc/rsyslog.d/40-remote_log.conf.
   For cameras with firmware 5.70 and older, select /etc/rsyslog.conf.

3. Add credentials for remote syslog server, e.g. (*. @10.2.0.2) and click Save file.
4. Reconnect to activate the changes.