

USER MANUAL

AXIS SNMP MIB



About this Document

This document describes how to use the AXIS Video SNMP MIB.

Legal Considerations

Video and audio surveillance can be regulated by laws that vary from country to country. Check the laws in your local region before using this product for surveillance purposes.

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 documentation 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 <http://www.axis.com/patent.htm> and one or more additional patents or pending patent applications in the US and other countries.

Trademark Acknowledgments

AXIS COMMUNICATIONS, AXIS, ETRAX and ARTPEC 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. UPnPTM is a certification mark of the UPnPTM Implementers Corporation.

SD, SDHC and SDXC are trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both. Also, miniSD, microSD, miniSDHC, microSDHC, microSDXC are all trademarks or registered trademarks of SD-3C, LLC in the United States, other countries or both.

WPA, WPA2 and Wi-Fi Protected Setup are marks of the Wi-Fi Alliance.

Microsoft, Windows, Windows Vista, WWW, Internet Explorer, DirectX, Intel, Intel Core, Pentium and Xeon are registered trademarks of the respective holders.

Acrobat, Adobe, Apache, Debian, Ethernet, Internet Explorer, Iomega, LaCie, Linux, Macintosh, Microsoft, Mozilla, MySQL, Red Hat, UNIX, Windows, WWW, Wi-Fi 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. UPnPTM is a certification mark of the UPnPTM Implementers Corporation. WPA is a mark of the Wi-Fi Alliance.

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 (selected countries only)
- visit Axis Support at www.axis.com/techsup/

Learn More!

Visit Axis learning center www.axis.com/academy/ for useful trainings, webinars, tutorials and guides.

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

1	Introduction	5
2	Technical Overview	5
2.1	Requirements	5
3	Configuration	6
3.1	Enable SNMP	6
3.2	Enable Traps	6
3.3	Configure General Trap	6
3.4	Verify SNMP Functionality	7
4	Trap Types	8
4.1	alarmNew	8
4.2	alarmCleared	8
4.3	alarmSingle	8
5	Traps	9
	Multiple Power Supply Operation	9
	Fan Operation	9
	Temperature Limit	9
	Analog Camera Connection	9
	Audio Input Connection	9
	Product Casing	9
	Mechanical PTZ Operation	9
	Edge Storage Operation	9
	Camera Tampering	9
	General Trap	10
6	SNMP Tree	11
7	Status	12
	Get Power Supply Status	12
	Get Fan Status	12
	Get Temperature Value	12
	Get Temperature Status	12
	Get Video Status	12
	Get Audio Signal Status	12
	Get Casing Status	12
	Get Storage Disruption Status	12
8	Special Conditions	13
8.1	Camera Restore (Soft Reset)	13
8.2	Factory Default (Hard Reset)	13
8.3	Reboot	13
8.4	Upgrade	13
8.5	Downgrade	13

9 Examples	14
9.1 Trap	14
9.2 Net-SNMP walk.....	15
9.3 Net-SNMP get	15

1 Introduction

This document describes how to use AXIS Video SNMP MIB. It is assumed that the reader is familiar with the SNMP protocol.

SNMP/MIBs allows network management operators to use standard Simple Network Management Protocol (SNMP) tools to monitor the status of Axis products. The Axis Management Information Base (MIB) for video hardware enables monitoring of hardware-related issues that may need administrative attention.

This document applies to firmware 5.55 and later. New functionality may be added in later releases, for detailed information, please read the MIB file. The latest versions of the MIBs are available on www.axis.com/techsup

2 Technical Overview

Some products will not have all the hardware as specified below and there will only be one MIB defined for all hardware. If the agent requests the status of such hardware that is not included in the product, then the device will return `noSuchObject`.

Which hardware is supported is handled at run time. This means that there is no need for product specific configuration.

2.1 Requirements

The Axis video MIB, which is the same for all Axis video product, can be downloaded from www.axis.com/techsup. This MIB is then imported into an agent software such as Tivoli.

These MIBs are required to use AXIS Video MIB:

- SNMPv2-TC
- SNMPv2-SMI
- SNMPv2-CONF
- AXIS-ROOT-MIB

3 Configuration

3.1 Enable SNMP

To use this functionality, SNMP must be enabled in the cameras and encoders on the network. To use SNMPv3, HTTPS has to be enabled. For information about how to enable HTTPS, see the User Manual for the product.

Use AXIS Camera Management or AXIS Camera Station to enable SNMP on multiple devices. AXIS Camera Management is available for download from www.axis.com

3.2 Enable Traps

The configuration of traps, which to send and where to send them, is done differently for the different SNMP versions.

For SNMPv1 and SNMPv2c, all Axis Video MIB will be sent when traps are enabled. It will not be possible to turn on or off any specific traps.

For SNMPv3 it is possible to configure which traps are sent to which management station. This is done using the SNMP-TARGET-MIB and SNMP-NOTIFICATION-MIB modules, defined in RFC3413. In short, this means using SNMP to add entries to `snmpNotifyTable`, `snmpTargetAddrTable`, `snmpTargetParamsTable`, `snmpNotifyFilterProfileTable`, and `snmpNotifyFilterTable`. These tables contain information about the recipients of traps, and which stations are to receive which traps.

3.3 Configure General Trap

It is possible to configure a general trap by creating an action rule in the product. Choose the event that shall trigger the general trap and use **SNMP trap** as action type. It can be configured with a string as trap text. For an example, see [9.1 Trap](#), on page 13.

3.4 Verify SNMP Functionality

After setting up the system, it is a good idea to verify that the SNMP MIB works as expected. This can be done by manually triggering an SNMP trap from a product's web pages. For an example, see [9.1 Trap](#), on page 13.

4 Trap Types

There are only three kinds of traps that can be generated by a video product. These three kinds are defined in the Axis Video MIB and they should cover all the future needs of traps and thus they are defined in general terms. They are described below.

4.1 alarmNew

This trap is sent to warn about a status change. Additional parameters include a unique trap ID (**alarmID**), a text string identifying the event (**alarmName**) and an additional string (**alarmText**) that specifies more detailed information about the event, for instance the unique identifier of the hardware or its status. This new state is valid until it is cleared by an **alarmCleared** trap. In general the state can be obtained through an SNMP get command as well.

4.2 alarmCleared

This trap is sent to indicate that some hardware has gone back to its normal state. The **alarmID** specifies the ID of a previous **alarmNew** trap that is cleared by this trap. Additional parameters include the same **alarmName** and **alarmText** that was sent by the **alarmNew** trap.

4.3 alarmSingle

This trap is sent to warn about a certain event. Additional parameters include a unique trap ID (**alarmID**), a text string identifying the event (**alarmName**) and an additional string (**alarmText**) that specifies more detailed information about the event, for instance the unique identifier of the hardware or its status.

The difference from the **alarmNew** trap is that this trap refers to a stateless event. For this reason there is no **alarmCleared** and hence several traps indicating the same event might follow each other. Since this is a stateless event it is impossible to get any related information through SNMP get.

5 Traps

These traps are available in the products.

Note: New functionality may be added in later releases, for detailed information, please read the MIB file. The latest versions of the MIBs are available on www.axis.com/techsup

Multiple Power Supply Operation

The product sends an **alarmNew** trap when a power supply fails. It uses **powerSupplyAlert** as alarm name and the alarm text states that a power supply is failing and it specifies the ID of that power supply. When the power supply is working again an **alarmCleared** is sent. This trap can only be sent by a rack with dual power supplies.

Fan Operation

The product sends an **alarmNew** trap when a fan fails. It uses **fanAlert** as alarm name and the alarm text states that a fan is failing and it specifies the ID of that fan. When the fan is working again an **alarmCleared** is sent.

Temperature Limit

The product sends an **alarmNew** trap when the value of a temperature sensor comes out of a specified domain. It uses **temperatureAlert** as alarm name and the alarm text specifies the ID of the sensor and whether the temperature is above or below limits. When the temperature is within limits again an **alarmCleared** is sent.

Analog Camera Connection

The product sends an **alarmNew** trap when the video signal disappears. It uses **videoSignalAlert** as alarm name and the alarm text specifies the ID of the channel and that the signal is lost. When the signal is back again an **alarmCleared** is sent. This trap can only be sent by a video encoder connected to analog cameras. The trap is triggered by disconnecting the BNC connector, cutting the coax cable, or if the power supply is disconnected from the camera.

Audio Input Connection

The product sends an **alarmNew** trap when the audio signal disappears from an external audio input, such as a line in or microphone connector. It uses **audioSignalAlert** as alarm name and the alarm text specifies the ID of the channel and that the signal is lost. When the signal is back again an **alarmCleared** is sent.

Product Casing

The product sends an **alarmNew** trap when the casing is opened. It uses **openCasingAlert** as alarm name and the alarm text states that the casing is opened, including the name of the casing. When the casing is closed again an **alarmCleared** is sent.

Mechanical PTZ Operation

The product sends an **alarmSingle** trap if an error occurs in any part of the PTZ. It uses **PTZAlert** as alarm name and the alarm text states that the PTZ is failing. This trap can only be sent by network PTZ cameras, not analog PTZ cameras connected to a video encoder.

Edge Storage Operation

The product sends an **alarmNew** trap when the storage enters a disruption state. It uses **storageMediaAlert** as alarm name and the alarm text states that a media is disrupted and it specifies which media. When the disruption is neutralised an **alarmCleared** is sent.

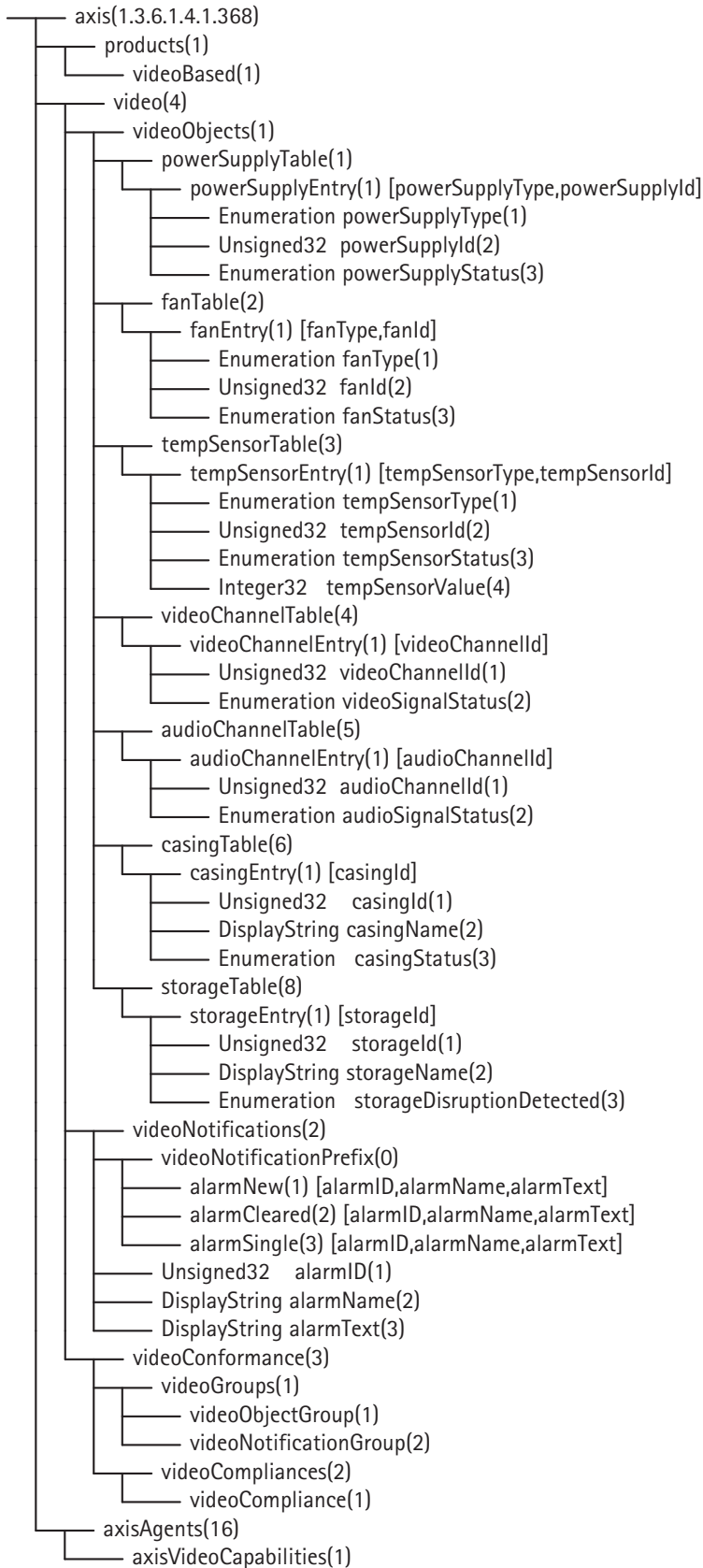
Camera Tampering

The product sends an **alarmSingle** trap when the lens is redirected, covered or defocused. It uses **tamperingAlert** as alarm name and the alarm text states the product is being tampered.

General Trap

Generic SNMP trap. The trap is only sent if it is configured through an action rule in the product. This includes configuring the reason for sending the trap, which is copied into the alarm text, while the alarm name states **General Trap**. Depending on whether the event is stateless or stateful the trap is of type **alarmNew** or **alarmSingle**. For an example, see **9.1 Trap**, on page 13.

6 SNMP Tree



7 Status

These are the status operations that are available in the AXIS SNMP MIB.

Note: All statuses are read-only objects. If a set operation is requested on the OID it will return 17, `notWritable` (or 2, `noSuchName`, for protocol version 1).

Get Power Supply Status

Returns the status of a power supply. The status is either `ok` or `failure`.

Get Fan Status

Returns the status of a fan. The status is either `ok` or `failure`.

Get Temperature Value

Returns the current temperature in degrees Celsius.

Get Temperature Status

Returns the current temperature status, i.e. whether it is working well and whether the temperature is within boundaries. Return values are `ok`, `failure`, or `outOfBoundary`.

Get Video Status

Returns whether the video signal for a certain channel is available or not. Return values are either `signalOk` or `noSignal`.

Get Audio Signal Status

Returns whether the audio signal for a certain channel is available or not. Return values are either `signalOk` or `noSignal`.

Get Casing Status

Returns the status of a casing, i.e. whether it is open or closed. Return values can be `closed` or `open`.

Get Storage Disruption Status

Returns the status of the storage. Return values can be `no` or `yes`, where `no` means that no problems are found for the storage.

8 Special Conditions

8.1 Camera Restore (Soft Reset)

All SNMP settings that are related to the Axis MIB will have to be reconfigured after a restore. This means that if a general trap had been configured, this needs to be recreated. Also if it was enabled through the SNMP settings, it needs to be enabled again.

8.2 Factory Default (Hard Reset)

All SNMP settings that are related to the Axis MIB will have to be reconfigured after a factory default. This means that if a general trap had been configured, this needs to be recreated. Also if it was enabled through the SNMP settings, it needs to be enabled again.

8.3 Reboot

No special actions need to be taken after reboot.

8.4 Upgrade

New traps may be introduced in new firmware upgrades.

8.5 Downgrade



Traps introduced in newer firmware may become unavailable after a downgrade.

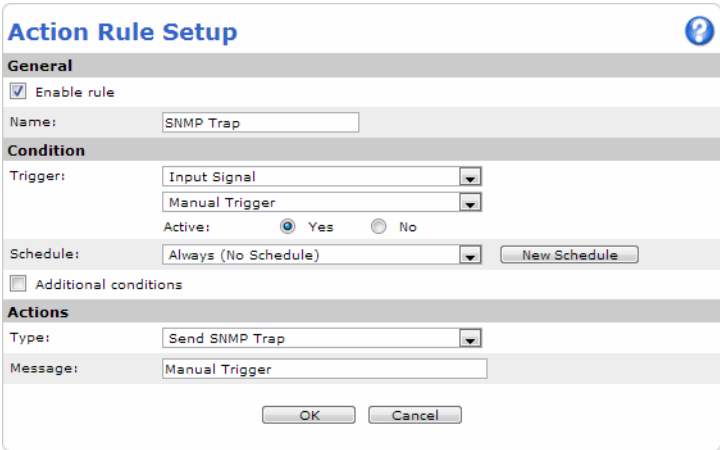
9 Examples

9.1 Trap

To test the SNMP functionality it is possible to set up an action rule with a manual trigger from the product's web pages. That way it is possible to trigger an SNMP trap from the product and verify that this is received by the agent.

Go to the product's web pages to set up the action rule.

1. Select **Setup > Live View Config > Layout** and enable a manual trigger button on the live view page.
2. Select **Events > Action Rules** and select **Add**.
3. Enter a name for the rule, for example **SNMP Trap**.
4. Under **Trigger** select **Input Signal** and **Manual Trigger**.
5. Under **Type**, select **Send SNMP Trap**.
6. Under **Message**, type a message that the trap should send, for example **Manual trigger**.
7. Click **OK**.
8. Go to the Live View page and click  under **Trigger** to activate the manual trigger. The product sends an **alarmNew** trap. It uses **General Trap** as alarm name and the alarm text is the message from the action rule.
9. Click  under **Trigger** to deactivate the manual trigger. The product sends an **alarmCleared** trap. It uses **General Trap** as alarm name and the alarm text is the message from the action rule.



Action Rule Setup

General

Enable rule

Name:

Condition

Trigger:

Active: Yes No

Schedule:

Additional conditions

Actions

Type:

Message:

9.2 Net-SNMP walk

```
$ snmpwalk -v 2c -c public 192.168.0.90 video
AXIS-VIDEO-MIB::videoSignalStatus.1 = INTEGER: signalOk(1)
AXIS-VIDEO-MIB::videoSignalStatus.2 = INTEGER: noSignal(2)
AXIS-VIDEO-MIB::videoSignalStatus.3 = INTEGER: noSignal(2)
AXIS-VIDEO-MIB::videoSignalStatus.4 = INTEGER: noSignal(2)
AXIS-VIDEO-MIB::storageName.1 = STRING: SD_DISK
AXIS-VIDEO-MIB::storageName.2 = STRING: NetworkShare
AXIS-VIDEO-MIB::storageDisruptionDetected.1 = INTEGER: no(1)
AXIS-VIDEO-MIB::storageDisruptionDetected.2 = INTEGER: yes(2)
```

9.3 Net-SNMP get

```
$ snmpget -v 2c -c public 192.168.0.90 storageName.1
AXIS-VIDEO-MIB::storageName.1 = STRING: SD_DISK
```


User Manual

AXIS SNMP MIB

© Axis Communications AB, 2014

Rev. 1.0

Printed: February 2014

Part No. 56175