www.use-ip.co.uk
01304 827609

AXIS Camera Station S20 Appliance Series

AXIS Camera Station S2008 Appliance

AXIS Camera Station S2016 Appliance

AXIS Camera Station S2024 Appliance

User Manual

About this Document

This manual is intended for administrators and users of AXIS Camera Station S20 Appliance Series. It includes instructions for using and managing the product on your network. Previous experience of networking will be of use when using this product. Some knowledge of UNIX or Linux-based systems may also be useful when developing shell scripts and applications. Later versions of this document will be posted at *www.axis.com*.

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 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 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/*

Equipment Modifications

This equipment must be installed and used in strict accordance with the instructions given in the user documentation. This equipment contains no user-serviceable components. Unauthorized equipment changes or modifications will invalidate all applicable regulatory certifications and approvals.

Copyright and Trademark Acknowledgments

©2015 Axis Communications AB, © 2014 Dell Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. AXIS COMMUNICATIONS, AXIS, ETRAX, ARTPEC and VAPIX 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. We reserve the right to introduce modifications without notice.

Dell™ is a trademark of Dell Inc. Ethernet, Internet Explorer, WWW are registered trademarks of the respective holders. Microsoft®, Windows®, MS-DOS®, Windows Vista®, the Windows Vista start button, and Office Outlook® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Regulatory Information

Europe

CE This product complies with the applicable CE marking directives and harmonized standards:

- Electromagnetic Compatibility (EMC) Directive 2014/30/EU. See *Electromagnetic Compatibility (EMC) on page 2*.
- Low Voltage (LVD) Directive 2014/35/EU. See *Safety on page 2*.
- Restrictions of Hazardous Substances (RoHS) Directive 2011/65/EU. See *Disposal and Recycling on page 2*.

A copy of the original declaration of conformity may be obtained from Axis Communications AB. See *Contact Information on page 3*.

Electromagnetic Compatibility (EMC)

This equipment has been designed and tested to fulfill applicable standards for:

- Radio frequency emission when installed according to the instructions and used in its intended environment.
- Immunity to electrical and electromagnetic phenomena when installed according to the instructions and used in its intended environment.

USA

This equipment has been tested using a shielded network cable (STP) and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.The product shall be connected using a shielded network cable (STP) that is properly grounded.

Canada

This digital apparatus complies with CAN ICES-3 (Class A). The product shall be connected using a shielded network cable (STP) that is properly grounded. Cet appareil numérique est conforme à la norme NMB ICES-3 (classe A). Le produit doit être connecté à l'aide d'un câble réseau blindé (STP) qui est correctement mis à la terre.

Europe

This digital equipment fulfills the requirements for RF emission according to the Class A limit of EN 55022. The product shall be connected using a shielded network cable (STP) that is properly grounded. Notice! This is a Class A product. In a domestic environment this product may cause RF interference, in which case the user may be required to take adequate measures.

This product fulfills the requirements for immunity according to EN 55024 office and commercial environments.

Australia/New Zealand

This digital equipment fulfills the requirements for RF emission according to the Class A limit of AS/NZS CISPR 22. The product shall be connected using a shielded network cable (STP) that is properly grounded. Notice! This is a Class A product. In a domestic environment this product may cause RF interference, in which case the user may be required to take adequate measures.

Japan

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害 を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求され ることがあります。 本製品は、シールドネットワークケーブル(STP)を使用して接続してください。また適切に接地してください。

Safety

This product complies with IEC/EN 60950-1, Safety of Information Technology Equipment.

Disposal and Recycling

When this product has reached the end of its useful life, dispose of it according to local laws and regulations. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. In accordance with local legislation, penalties may be applicable for incorrect disposal of this waste.

Europe

This symbol means that the product shall not be disposed of together with household or commercial waste. Directive 2012/19/EU on waste electrical and electronic equipment (WEEE) is applicable in the European Union member states. To prevent potential harm to human health and the environment, the product must be disposed of in an approved and environmentally safe recycling process. For information about your nearest designated collection point, contact your local authority responsible for waste disposal. Businesses should

contact the product supplier for information about how to dispose of this product correctly.

This product complies with the requirements of Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS).

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/*

Warranty Information

For information about Axis' product warranty and thereto related information, see *www.axis.com/warranty/*

Learn More!

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

Table of Contents

Switch Management 5
Access the Built-in PoE Switch 5
Navigation Bar 5
Overview 6
System Information 6
Resource Usage 6
Port Status 6
PoE 8
PoE Status 8
PoE Administration 8
ACL (Access Control List) 10
Access Control List Status 10
Access Control List Administration 10
Network 11
Switch Configuration 11
DHCP Server 11
Admin 13
Security 13
Maintenance 13
Settings 13
Firmware 13

Switch Management

This manual covers switch features, functionality, and operations that are accessible via the switch's build-in web server.

The switch function offers an easy-to-use interface that lets you configure and manage your product and review current system conditions.

Access the Built-in PoE Switch

From the desktop, open the **Get Started Application** and go to the **Information & Support** tab or point your browser to the switch IP address 192.168.50.1

Log in with user name **admin** and password **system**.

It is recommended to change the password the first time you access the switch.

Navigation Bar

Features of the navigation bar are:

- Tabs
  - Overview
  - PoE
  - ACL
  - Network
  - Admin
- Language selection

  The drop down list displays language selections available on your product. When you select a language, all user interfaces will be displayed in that language.

Overview

Overview

The Overview contains three panes where you can find product information and status:

- System Information
- Resource Usage
- Port Status

System Information

This pane provides basic identity information about your switch.

Model – The device's model name.

Serial Number – The device serial number is useful for maintenance or when tracking the individual device.

Firmware Version – See which firmware that are installed to determine whether you need to upgrade the switch firmware.

Port Counter – A count on the number of network ports the device supports, including a corporate uplink port.

Max PoE – The total power available for power over ethernet (PoE) devices.

Resource Usage

This pane tells you how key switch resources are being used.

Total PoE Usage – The Total PoE bar graph shows how much power (in watts) is being consumed by PoE devices attached to the switch. Once the maximum power has been reached, the devices cannot provide any further power.

PoE Status – PoE Status indicates whether PoE is enabled and how many ports have been enabled to support PoE.

ACL Status – Indicates whether ACL (Access Control List) is enabled and how many ports are enabled with this added security feature. ACL binds a specific MAC address to a port, preventing traffic (sent or received) from devices with other MAC addresses.

Port Status

Port Status displays operational details for each switch port and U1. This area is helpful when you want to know all the key operational parameters of each port. From this pane you can disable individual switch ports and improving security for unused ports.

Port # – The port number to which the selected device is connected.

Link State –

- **Up** indicates that a device is connected to this port
- **Down** indicates that no device is connected

Link Speed – The current negotiated link speed for each port.

Transmit Rate/Receive Rate – An overview of traffic load on each port showing the average data rate in megabits per second for outbound and inbound data on the port.

Power Draw – The average power (in watts) being drawn via PoE by the device attached to the port.

PoE Enabled/ACL Enabled – Enabled/disabled status of each port. To improve security, it is recommended to only enable PoE for those ports with active PoE devices. ACL should be used to prevent unauthorized devices from being placed on the network.

Overview

Port Enabled/Disabled – Allows you to view and change Enabled/Disabled port status (the port's ability to receive or send data). This is separate from the link status and PoE. A disabled port may or may not still be providing power to a PoE device, and it may still be physically connected to device, but it cannot be used to send or receive data, even though its link status may still be **Up** and the attached device is still drawing power. Disabling the port prevents any device from accessing the switch or network. Ports that are not in use should be disabled for increased security.

Uplink 1 – If U1 or SFP1 contains an active connection it will display **Up**; otherwise, it will show **Down**. The maximum link speed and average transmit/receive data in megabits per second help you understand traffic patterns and verify operational status of associated applications.

PoE

PoE

The PoE/Cable page displays detailed information about the setup and status of power over Ethernet for each port and for the PoE device as a whole. This data will be useful for setting, enabling, disabling, and managing the switch's power budget.

The PoE page contains two panes:

- PoE Status
- PoE Administration

PoE Status

This pane displays the power over Ethernet status parameters.

Port # – The appliance port number to which the selected device is connected.

Link State – Up indicates that a device is connected to this port; **Down** indicates that no device is connected.

PoE Mode/PoE Class – Type of device the switch has detected. This is not configurable, rather the values assigned by the switch based on its interaction and power draw of the attached device.

- PoE Mode values will be either AT or AF referring to the IEEE 802.3at or IEEE 802.3af standards.
- PoE Class values range from 0 to 4 and correspond to the following properties as defined in the IEEE standard and as shown in the table below:

Class	Usage	Classification Current (mA)	Power Range (watts)	Class Description
0	Default	0-4	0.44-12.94	Classification unimplemented
1	Optional	9-12	0.44-3.84	Very low power
2	Optional	17-20	3.84-6.49	Low power
3	Optional	26-30	6.49-12.95	Mid power
4	Valid for 802.3at (Type 2) devices; not allowed for 802.3af devices	36-44	12.95-25.50	High power

Power Draw – The average number of watts the attached device is consuming.

Power Limit – This displays a default limit based on the PoE mode and class.

PoE Enabled/Disabled – Allows you to view and change the PoE Enabled/Disabled status to turn the PoE to the device on or off for devices. Devices requiring PoE will be turned off when disabled and the link state will change to **Down**.

PoE Administration

This pane summarizes the switch's current total power consumption and power availability information. It also provides a general PoE control.

(Watts Scale) and Total PoE Usage – Shows the amount of power (in watts) being drawn by all devices currently attached to the switch along with the total power consumed (in watts and percentages) by all attached devices. This is helpful when installing devices and verifying your power budget.

PoE Port Active – Shows the number of ports that are currently enabled for data providing power over Ethernet.

Master PoE (Enable All / Disable All) – Allows you to enable or disable PoE for all the ports in one command. You can toggle all PoE on or off for all ports.

PoE

PoE Power Management

Each port reserves power according to the connected powered device's PoE class.

If the actual power consumption for a given port exceeds the reserved power for that port it will shut down.

Ports will also shut down when the actual power consumption for all ports exceeds the total amount of power that the power supply can deliver. The ports are then shut down according to the ports priority where a lower port number means higher priority.

ACL (Access Control List)

This page allows you to lock a MAC address to a port so that only traffic coming from that MAC address will be passed. This dramatically improves security and prevents unauthorized users from attaching a laptop or other devices to the security network.

The ACL page contains two panes:

- Access Control List Status
- Access Control List Administration

Access Control List Status

This pane shows the status of the ACL functionality and provides controls to enable/disable ACL on individual ports.

The access control list status features are:

Port # – The port number to which the selected device is connected.

Link State – Up indicates that a device is connected to this port; **Down** indicates that no device is connected.

Discovered MAC Address – Data traffic will only be allowed to/from this MAC address. The switch automatically detects the MAC address of any device attached to the port and displays it here.

Bound MAC Address – Enabling ACL will bind the port to the discovered MAC address. No other device will be able to communicate on this port. When you enable ACL, if there is a **Discovered MAC Address**, it will move to the **Bound MAC Address** column, binding it to this port.

PoE Enabled/Disabled – Displays the current PoE Enabled/Disabled status.

ACL Enabled/Disabled – When you enable ACL, if there is a **Discovered MAC Address** it will move to the **Bound MAC Address** column, binding it to this port. Disabling ACL clears the **Bound MAC Address** value so you may bind a different device to this port.

Access Control List Administration

This shows you an overview of ACL status and allows you to enable or disable ACL for all devices attached to the switch.

ACL Ports Active – The number of ports bound to a specific MAC address using ACL.

Master ACL – This feature will enable or disable ACL for all ports with a bounded MAC address. Only ports with a discovered MAC address or bounded address will be affected.

Network

The network page allows you to configure the IP address of the switch and to manage the built-in DHCP server controlling the assignment of IP addresses of cameras or other devices attached to the switch's ports.

The Network screen contains two panes:

- Switch Configuration
- Switch DHCP Server

Switch Configuration

The switch configuration allows you to manage the IP assignment of the switch, its subnet mask, gateway, and DNS.

The factory default setting is a Static IP connection type with an address of 192.168.50.1 and a subnet mask of 255.255.255.0.

You can enter a different address through this pane, but for most camera installations we recommend you to use default settings. The reason is that this network will normally be isolated from the corporate LAN and will only be used for managing and collecting camera and related security application data by the video management software (VMS) residing on the server.

If an installation requires that other applications (not residing on the AXIS S20xx Server) are able to access devices on the switch, the traffic must pass through a physical connection to the U1 port. However, in most instances this is undesirable, and not recommended, since it would introduce traffic from cameras to the corporate LAN.

If direct access to devices on the switch from external applications is required, then you should set the Gateway, DNS 1, and DNS 2 for allowing traffic to pass from the switch to other subnets and to resolve domain names to IP addresses.

Features of this pane are:

Connection Type – The default setting is Static IP.

IP Address – The IP address of the U1 switch connection. The switch web-interface can be accessed through this address.

Subnet Mask – The subnet mask of the U1 switch connection.

Gateway – The gateway for accessing the U1 switch connection.

DNS 1 – The primary domain name server used by the switch.

DNS 2 – An alternate domain name server used by the switch.

Reset – Clears all the entries allowing you to start again.

Save – Saves the changes made in any of the network settings. For these changes to take effect, you must reboot the switch.

DHCP Server

From the Switch DHPC Server pane you can configure the switch to use its internal DHCP server for assigning IP addresses to attached devices. You can also set the dynamic IP address lease length for renewal with a minimum setting of 60 minutes.

When using the U1 connection for allowing devices to access or being accessed by external applications the gateway and DNS addresses must be specified.

The Intel I211 Network Interface connects the server to the built-in switch and should always be set to use DHCP.

Important

If the switch's DHCP is enabled and the server is connected to an external network via the U1 network connector, no other DHCP hosts can be in use on the external network, otherwise there will be IP address conflicts.

Network

The features of this pane are:

Status Enable/Disable – When the DHCP server is set to disable you must assign IP addresses manually to the cameras or use an external DHCP server accessible via the U1 network connection for IP assignment.

Start/End IP Addresses – When DHCP is enabled, you can choose a Start and End IP address range for assignment of attached devices.

Subnet Mask – The subnet mask of the U1 switch connection.

Gateway – The gateway that could be used to access the U1 switch connection.

DNS 1 – The primary domain name server used by the switch.

DNS 2 – An alternate domain name server used by the switch.

Lease Length – The suggested length of time in minutes that the DHCP server will use for potentially reassigning its pool of dynamic IP addresses. A minimum of 60 minutes is enforced.

Reset – Clears all the entries allowing you to start again.

Save – Saves the changes made in any of the network settings. For these changes to take effect, you must reboot the switch.

Admin

Admin

From this page you can perform basic administrative functions. The Admin screen contains four operational panes:

- Security
- Maintenance
- Settings
- Firmware

Security

This pane allows you to set the password for the switch administrator. The appliance's switch only has one user named **admin** whose factory default password is **system**.

Maintenance

You will use this pane to reset the switch to its factory default, or to reboot after making network settings or other significant configuration changes.

You must reboot the switch to commit changes to the switch's IP address assignments or to enable/disable changes in DHCP/Static IP assignment behavior.

Rebooting the switch causes all devices to temporarily lose connection with the switch (including PoE).

Settings

You can set the switch's hostname and domain when you want to locate and access the switch using a logical name rather than a physical IP address. This makes it easier to locate specific devices using network discovery tools.

The factory default settings for hostname is the appliance's serial number with a domain of **local**.

Firmware

This pane shows the current installed firmware version of the switch and allows you to change it.

To update the firmware, browse on the host device of the browser to find the new firmware. Select the appropriate firmware file, and click **Update**, the switch will begin the upgrade process. This process will take several minutes, do not remove power or exercise other features of the switch during the upgrade process. All devices connected to the switch will temporarily lose connection with the switch as it reboots.

Changing the firmware does not change the settings of the switch, it only changes the firmware and any associated changes in behavior that come with the new version.

User Manual
AXIS Camera Station S20 Appliance Series
© Axis Communications AB, 2016
Ver. M1.8
Date: August 2016
Part No. 1637679