

AXIS C3003-E Network Speaker

User Manual

About this Document

This manual is intended for administrators and users of AXIS C3003-E Network Speaker, and is applicable to firmware 1.15 and later. 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. See also the product's online help, available through the web-based interface.

Legal Considerations

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.

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.

Trademark Acknowledgments

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.

Regulatory Information

Europe

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

- Electromagnetic Compatibility (EMC) Directive 2004/108/EC. See *Electromagnetic Compatibility (EMC)* on page 2.
- Low Voltage (LVD) Directive 2006/95/EC. 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 B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a

residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and receiver.
 - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
 - Consult the dealer or an experienced radio/TV technician for help.
- 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 B). The product shall be connected using a shielded network cable (STP) that is properly grounded.

Cet appareil numérique est conforme à la norme CAN NMB-3 (classe B). 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 B limit of EN 55022. The product shall be connected using a shielded network cable (STP) that is properly grounded.

This product fulfills the requirements for immunity according to EN 61000-6-1 residential, commercial and light-industrial environments.

This product fulfills the requirements for immunity according to EN 61000-6-2 industrial environments.

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 B limit of AS/NZS CISPR 22. The product shall be connected using a shielded network cable (STP) that is properly grounded.

Japan

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。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。

Korea

이 기기는 가정용(B급) 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다. 적절히 접지된 STP (shielded twisted pair) 케이블을 사용하여 제품을 연결 하십시오.

Safety

This product complies with IEC/EN/UL 60950-1 and IEC/EN/UL 60950-22, Safety of Information Technology Equipment. The product shall be grounded either through a shielded network cable (STP) or other appropriate method.

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).

China



This product complies with the requirements of the legislative act Administration on the Control of Pollution Caused by Electronic Information Products (ACPEIP).

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/

Learn More!

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

AXIS C3003-E Network Speaker

Safety Information

Safety Information

Hazard Levels

▲DANGER	Indicates a hazardous situation which, if not avoided, will result in death or serious injury.
▲WARNING	Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
▲CAUTION	Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a situation which, if not avoided, could result in damage to property.

Other Message Levels

Important	Indicates significant information which is essential for the product to function correctly.
Note	Indicates useful information which helps in getting the most out of the product.

AXIS C3003-E Network Speaker

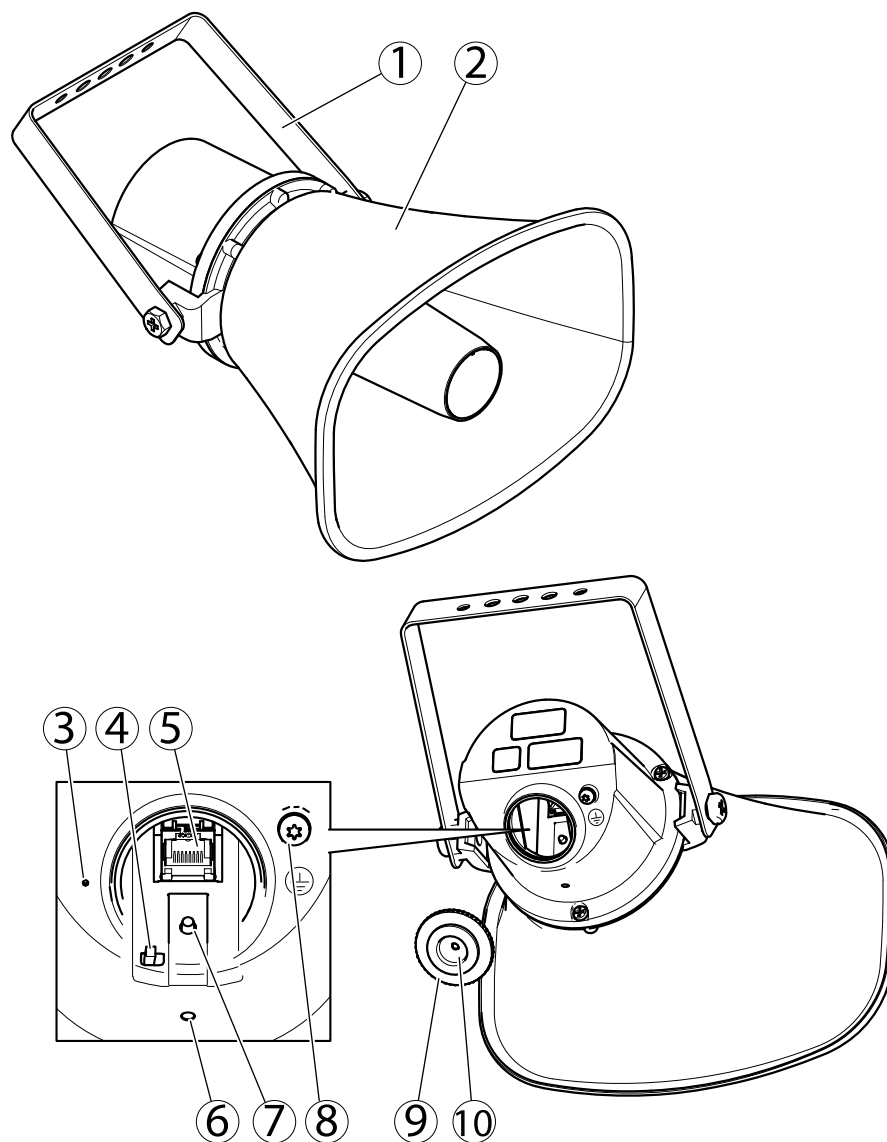
Table of Contents

Safety Information	4
Hazard Levels	4
Other Message Levels	4
Hardware Overview	6
Connectors and Buttons	7
LED Indicators	7
Access the Product	8
Access from a Browser	8
Access from the Internet	8
Set the Root Password	8
Set Up the Product	9
Basic Setup	9
Audio	10
Set Up Audio	10
Audio Clips	11
Voice over IP (VoIP)	12
The VoIP Overview Page	12
Configure the SIP Settings	12
The Account Settings Page	14
Events	18
Set Up Action Rules	18
Add Recipients	19
Create Schedules	20
Set Up Recurrences	20
Languages	21
System Options	22
Security	22
Date & Time	24
Network	24
Ports & Devices	29
Maintenance	29
Support	29
Advanced	30
Reset to Factory Default Settings	30
Troubleshooting	31
Check the Firmware	31
Upgrade the Firmware	31
Symptoms, Possible Causes and Remedial Actions	31
Technical Specifications	33

AXIS C3003-E Network Speaker

Hardware Overview

Hardware Overview



- 1 Bracket
- 2 Horn
- 3 Microphone
- 4 Microphone disable switch
- 5 Network connector
- 6 Status LED indicator
- 7 Control button
- 8 Protective earth terminal
- 9 Cap
- 10 Gasket

AXIS C3003-E Network Speaker

Hardware Overview

Connectors and Buttons

For technical specifications, see *page 33*.

Protective Earth Terminal

⚠ DANGER

Risk of electric shock. The product shall be grounded using a grounding wire. Make sure both ends of the grounding wire are in contact with their respective grounding surfaces.

Make sure the grounding wire is as short as possible to make the current path as short as possible.

Network Connector

NOTICE

The product shall be connected using a shielded network cable (STP). All cables connecting the product to the network shall be intended for their specific use. Make sure that the network devices are installed in accordance with the manufacturer's instructions. For information about regulatory requirements, see *Electromagnetic Compatibility (EMC) on page 2*.

Control Button

For location of the control button, see *Hardware Overview on page 6*.

The control button is used for:

- Sending out a test tone that calibrates the Auto Speaker Test. Press and release the control button.
- Resetting the product to factory default settings. See *page 30*.
- Connecting to an AXIS Video Hosting System service. See *page 25*. To connect, press and hold the button for about 3 seconds until the Status LED flashes green.
- Connecting to AXIS Internet Dynamic DNS Service. See *page 25*. To connect, press and hold the button for about 3 seconds.

Microphone Disable Switch

For location of the microphone disable switch, see *Hardware Overview on page 6*.

The microphone disable switch is used to mechanically turn the microphone **ON** or **OFF**. The factory default setting for this switch is **ON**.

LED Indicators

Status LED	Indication
Unlit	Unlit for normal operation (can be useful in making the Axis product less noticeable).
Green	Steady green for normal operation.
Amber	Steady during startup and when restoring settings.
Red	Slow flash for failed upgrade.

AXIS C3003-E Network Speaker

Access the Product

Access the Product

To install the Axis product, see the Installation Guide supplied with the product.

Access from a Browser

1. Start a browser (Chrome, Internet Explorer, Firefox, Safari).
2. Enter the IP address or host name of the Axis product in the browser's Location/Address field.

To access the product from a Mac computer (OS X), go to Safari, click on Bonjour and select the product from the drop-down list.

Note

To show Bonjour as a browser bookmark, go to **Safari > Preferences**.

3. Enter your user name and password. If this is the first time the product is accessed, the root password must first be configured. For instructions, see *Set the Root Password on page 8*.

Access from the Internet

Once connected, the Axis product is accessible on your local network (LAN). To access the product from the Internet you must configure your network router to allow incoming data traffic to the product. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the product. This is enabled from .

For more information, see *NAT traversal (port mapping) for IPv4 on page 27*. See also AXIS Internet Dynamic DNS Service at www.axiscam.net

For Technical notes on this and other topics, visit the Axis Support web at www.axis.com/techsup

Set the Root Password

To access the Axis product, you must set the password for the default administrator user **root**. This is done in the **Configure Root Password** dialog, which opens when the product is accessed for the first time.

To prevent network eavesdropping, the root password can be set via an encrypted HTTPS connection, which requires an HTTPS certificate. HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt traffic between web browsers and servers. The HTTPS certificate ensures encrypted exchange of information. See *HTTPS on page 22*.

The default administrator user name **root** is permanent and cannot be deleted. If the password for root is lost, the product must be reset to the factory default settings. See *Reset to Factory Default Settings on page 30*.

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

To set the password via an encrypted HTTPS connection, follow these steps:

1. Click **Use HTTPS**.
A temporary certificate (valid for one year) is created, enabling encryption of all traffic to and from the product, and the password can now be set securely.
2. Enter a password and then re-enter it to confirm the spelling.
3. Click **OK**. The password has now been configured.

AXIS C3003-E Network Speaker

Set Up the Product

Set Up the Product

The Axis product can be configured by users with administrator rights. Go to **Setup > Basic Setup > 1 Users** to administer users.

- **Administrators** have unrestricted access to all settings.

See also the online help .

Basic Setup

Basic Setup provides shortcuts to the settings that should be made before using the Axis product:

1. Users. See *page 22*.
2. TCP/IP. See *page 24*.
3. Date & Time. See *page 24*.
4. VoIP Settings. See *page 12*.

AXIS C3003-E Network Speaker

Audio

Audio

The audio settings can be used to audio quality. You can configure the following:

- Audio settings. See *page 10*.
- Audio clips. See *page 11*.

Set Up Audio

To set up the Axis product, go to **Audio > Audio Settings**.

Auto Speaker Test

The Auto Speaker Test is a way to verify that the speaker is working from a remote location. A test tone is played in the speaker and the test tone is measured by the onboard microphone to ensure that the speaker sounds as intended.

The Auto Speaker Test must be calibrated during first time use. To calibrate the Axis product and run an Auto Speaker Test, follow the instructions below:

1. Go to **Setup > Audio > Audio Settings**.
2. Click **Calibrate** to calibrate Axis product and run the first Auto Speaker Test.

It is also possible to run the Auto Speaker Test by pressing the control button. See *Hardware Overview on page 6*.

Once the Axis product is calibrated, the Auto Speaker Test can be run at any time:

1. Go to **Setup > Audio > Audio Settings**.
2. Click **Test** to run the Auto Speaker Test.

To set up the Auto Speaker Test as an action rule, see *Set Up Action Rules on page 18*.

Audio Modes

The Axis product supports the following audio modes:

Full duplex – Simultaneous two-way audio allowing the Axis product to transmit and receive audio at the same time. There is no echo cancellation.

Half-duplex – Audio can be transmitted to and from the Axis product but only in one direction at a time.

Simplex – Speaker only – Audio is transmitted from a client to the Axis product. This is the default audio mode.

Simplex – Microphone only – Audio captured by the product microphone is transmitted from the Axis product to one or more clients.

To set the audio mode, go to **Audio > Audio Settings** and select the desired mode from the **Audio mode** drop-down list.

Audio Output

Configure the audio output settings under **Audio > Audio Settings**.

Output gain – Move the slider to adjust the volume of the audio output. To mute the sound, move the slider to the left end of the slider.

Audio Input

Configure the audio input settings under **Audio > Audio Settings**.

AXIS C3003-E Network Speaker

Audio

Source lists the built-in microphone.

Use the **Input gain** to control the volume (dB Full Scale) of the audio input. If the sound is too low, choose a higher dB, to amplify the sound. If the sound is too high, choose a lower dB. The **Level** bar gives a visual representation of the audio signal level in dB relative to the full-scale input level.

- Green — the signal is at a good level.
- Yellow — the signal is becoming distorted.
- Red — the signal is distorted.

Use the **Encoding** option to select digital audio encoding format.

- **AAC** is used for encoding only in the Axis product. For decoding, no license is included in the Axis product.
- **G711** is an unlicensed standard codec that is useful when integrating audio into a VoIP system
- **G726** is an unlicensed speech codec that is most commonly used within the security industry.

The **Sample rate** defines the number of times per second the sound is sampled. A higher sample rate will provide better audio quality, but also requires a greater bandwidth.

Set the required **Bit rate** depending on the selected encoding. A higher bit rate will give better audio quality. A lower bit rate may have latency or delay, but will require less bandwidth.

For more information about these settings, please see the online help .

Audio Clips

Audio clips can be played when an event occurs. Audio clips are created by uploading a sound file to the Axis product. To add, play, download, modify or remove audio clips, go to **Audio > Audio Clips**. For more information see the online help .

- **Add** – To add an audio clip, click **Add**, select the **Upload** radio button and click **Browse**. Navigate to the desired file and click **Upload** to upload the audio clip.
 - The following audio formats are supported: .au G.711 u-law, 8-bit, mono (8, 16 kHz) and .wav PCM, 16-bit, mono (8, 16, 32 kHz)
 - The maximum file size per audio clip is 1.5 MB and a maximum amount of 20 audio clips can be uploaded.
- **Play** – To play an audio clip, select an audio clip in the **Audio Clip List** and click **Play**. Audio clips can only be played if the speaker is not streaming audio or playing another clip.
- **Download** – To download a recording to a hard drive or network disk, select it and click **Download**.
- **Modify** – To change the name of the audio clip, select it and click **Modify**.
- **Remove** – To remove an audio clip, select it and click **Remove**.

To configure the Axis product to play audio clips when an event occurs, an action rule must be set up. For more information, see *Events on page 18*.

AXIS C3003-E Network Speaker

Voice over IP (VoIP)

Voice over IP (VoIP)

Voice over IP (VoIP) is a group of technologies that enables voice communication and multimedia sessions over IP networks. In the Axis product, VoIP is enabled through the Session Initiation Protocol (SIP) and Dual-Tone Multi-Frequency (DTMF) signaling.

To open the product's VoIP pages, go to **Setup > VoIP**.

The VoIP settings include the following pages:

- **VoIP Overview.** See *The VoIP Overview Page on page 12*.
- **SIP Settings.** See *Configure the SIP Settings on page 12*.
- **Account Settings.** See *Create or Edit Accounts on page 14*.

The VoIP settings can be configured by users with administrator rights.

The VoIP Overview Page

The VoIP Overview page shows basic information about the SIP, VoIP action rule, and account settings.

- **SIP Settings** – Shows the basic Session Initiation Protocol (SIP) settings, such as whether SIP is enabled and allows incoming calls or not.

To change the settings, click **Configure** or go to **VoIP > SIP Settings**. For more information, see *Configure the SIP Settings on page 12*.

- **Account Settings** – Shows an overview of the SIP account settings. See also *The Account Settings Page on page 14*.

To create a new account, test an account, or change the account settings, click **Configure** or go to **VoIP > Account Settings**. For more information, see *Create or Edit Accounts*.

Configure the SIP Settings

Session Initiation Protocol (SIP) is a text-based protocol, similar to HTTP and SMTP, for interactive communication sessions between users. The sessions can include voice, video, and chat elements. For information, see *About SIP Addresses on page 16*.

Before the Axis product can be used to make and receive calls, you need to configure the SIP settings. This includes enabling SIP, configuring the ports, and setting the rules for Network Address Translation (NAT) traversal.

To configure the SIP settings:

1. Go to **Setup > VoIP > SIP Settings**.
2. Select **Enable SIP**.
3. To make a test call to an account on another device, enter a valid SIP address for the other device and click **Test call**. For more information, see *Make Test Calls on page 16*.
4. To allow the Axis product to receive calls, select **Allow incoming calls**.
5. Enter the **SIP port number** and the **SIP TLS port number**. For more information, see *Port Settings on page 13*.
6. Select the protocols you want to enable for NAT traversal. See *Network Address Translation (NAT) Traversal (port forwarding) on page 13*.
7. Click **Save**.

Note

Even if you choose to not enable SIP, you can configure the SIP settings. But remember that when SIP is disabled, you cannot make or receive calls.

AXIS C3003-E Network Speaker

Voice over IP (VoIP)

Port Settings

- **SIP port** – Enter the port used for SIP sessions. The signalling traffic through this port will be non-encrypted. The default port number is 5060.
- **SIP TLS port** – Enter the port used for SIPS sessions and TLS-secured SIP sessions. The signalling traffic through this port will be encrypted using Transport Layer Security (TLS). The default port number is 5061.

Network Address Translation (NAT) Traversal (port forwarding)

Use NAT traversal when the Axis product is connected to the network behind a NAT router or firewall device.

VoIP services require clients to be servers as well, and many VoIP services carry IP address and port information in the application data. Therefore, Axis products behind Network Address Translation (NAT) devices such as network routers need to use special protocols for NAT traversal (port forwarding) so that incoming calls can be linked to the correct host.

Without SIP-specific port forwarding, users of clients within the same private network would be able to talk to each other (peer-to-peer communication) but users of clients in different networks would not.

The following NAT traversal settings are available:

- **ICE** – Interactive Connectivity Establishment (ICE). See *page 13*.
- **STUN** – Session Traversal Utilities for NAT (STUN). See *page 13*.
- **TURN** – Traversal Using Relays around NAT (TURN). See *page 13*.

Each NAT traversal protocol has its benefits and flaws. The flaws can be reduced by making sure that the network and its connected devices support all these protocols.

For more information about the product's general NAT traversal settings, see *NAT traversal (port mapping) for IPv4 on page 27*.

Interactive Connectivity Establishment (ICE)

Interactive Connectivity Establishment (ICE) enables the product to send a request that includes multiple addresses to the receiving device. In its response, the receiving device also includes multiple addresses. Through a process of connectivity checks, also called handshakes, the channel for communication is established.

ICE increases the chances of finding the most efficient path to successful communication between peer devices. If you also enable STUN and TURN, you improve the ICE protocol's chances of finding the most efficient path to successful communication, not just between peers but between all devices on either side of the NAT device.

To use the ICE protocol for NAT traversal, select **Enable ICE**.

Session Traversal Utilities for NAT (STUN)

Session Traversal Utilities for NAT (STUN) is a client-server network protocol that enables the product to ask a STUN server on the Internet for a mapped public IP address. The STUN server response includes this IP address and port so that the client can use them in its SIP messages to other hosts and clients.

Like TURN, STUN can be used in full-cone, address-restricted cone, and port-restricted cone NAT setups. STUN is fast because it is lightweight. However, STUN does not allow incoming messages from symmetric NATs, and it cannot communicate with a peer behind the same NAT device.

To use the STUN protocol for NAT traversal, select **Enable STUN**. Then enter the address of the STUN server.

Traversal Using Relays around NAT (TURN)

Traversal Using Relays around NAT (TURN) is a client-server network protocol that enables the product to ask a TURN server for a mapped IP address. The TURN server responds with its IP address and port so that the client can use them in its SIP messages.

AXIS C3003-E Network Speaker

Voice over IP (VoIP)

TURN is primarily used in symmetric NAT setups. Like STUN, TURN can also be used in full-cone, address-restricted cone, and port-restricted cone NAT setups. But because the IP address and port provided by the TURN server are those of the TURN server itself, it works like a carrier that forwards information to and from the client. This means that while TURN servers are reliable, they sometimes cause a bit of latency.

To use the TURN protocol for NAT traversal, select **Enable TURN**. Then the address of the TURN server, the username and password.

The Account Settings Page

The Account Settings page allows you to set up and manage SIP accounts. See *Create or Edit Accounts on page 14*.

The Account Settings page also includes an account list that shows an overview of the SIP account settings, including:

- Name. See also *Account Information on page 15*.
- SIP address. See also *About SIP Addresses on page 16*.
- Transport mode. See also *Transport Settings on page 15*.
- Default. See also *Account Information on page 15*.
- Registration status. See *Registration Status on page 14*.

Registration Status

The account status is indicated with dots in different colors. For more detailed information about an account's status, hover the mouse pointer over the status dot or select the account in the account list and click **Modify**.

-  **SIP disabled** – SIP is disabled.
Account not registered – The SIP account is not registered with a PBX.
-  **Provisional** – The product is trying to register the account.
Redirection – The account or address needs to be redirected.
-  **Successful** – The account has successfully registered with the SIP registrar.
-  **Failure** – There is a problem with the account, such as the account credentials are wrong, authorization failed, or the request was bad.

Create or Edit Accounts

To set up a SIP account:

1. Go to **Setup > VoIP > Account Settings**.
2. Click **Add**.
3. Enter the account details.
 - See *Account Information on page 15*.
 - See *Account Credentials on page 15*.
 - See *SIP Server Settings on page 15*.
 - See *Transport Settings on page 15*.
 - See *Proxy Settings on page 16*.
4. Click **OK**.

To edit an account, select the account in the account list and click **Modify**.

AXIS C3003-E Network Speaker

Voice over IP (VoIP)

To remove an account, select the account in the account list and click **Remove**.

Account Information

- **Name** – Enter a descriptive name. This can for example be a first and last name, a role, or a location. The name is used as an alias and is especially useful when several accounts have the same user ID.
- **Default account** – Select to make this the default account. Only one account can be the default account.

At startup, the first time the product is accessed or after a reset, a peer account is created automatically and set to be the default account. This peer account can only be removed if at least one more account has been added to the list.

The default account will be used to make triggered calls and to make test calls on the SIP Settings page. For more information about triggers and actions, see *Events on page 18*.

Account Credentials

- **User ID (required)** – Enter the name or PBX extension that shall be shown when calling other accounts. A private branch exchange (PBX) is a telephone switching system that connects telephone extensions to each other and to other telephone networks. Each PBX-connected device has its own extension number.
- **Authentication ID** – Some PBXs require that the account verifies itself with the SIP registrar to allow access to the PBX. For more information, see the PBX's and service provider's instructions. By default the Authentication ID is identical to the User ID. To enable an Authentication ID that is different from the User ID, clear the **Use User ID as Authentication ID** check box.
- **Password** – Enter the password for the account. A password is not required for peer-to-peer accounts.
- **Confirm password** – Repeat the password. A password is not required for peer-to-peer accounts.
- **Caller ID** – Enter the name or phone number that you want the recipient to see when you make the call.

If you only enter a user ID, the account will be used as a peer-to-peer account. This means that unless the devices are connected to NATs with SIP-specific port forwarding such as STUN or TURN, the account will only be able to communicate with devices that are connected to the same private network. For more information, see *Network Address Translation (NAT) Traversal (port forwarding) on page 13*.

To create an account that is registered with a PBX or a service provider, enter the user ID, password, and the registrar address or domain name. See *SIP Server Settings* below.

SIP Server Settings

- **Domain name** – If available, enter the public domain name. The domain name will be shown as part of the SIP address when calling other accounts. For more information, see *About SIP Addresses on page 16*.
- **Registrar address** – Enter the SIP server's registrar address. This is to point out the SIP registrar with which the account should register itself. The SIP registrar is the part of the PBX that keeps track of all the extensions.

Important

The registrar address should be an IPv4 address. The product's VoIP capabilities currently do not include support for IPv6.

Transport Settings

- **Enable SIPS** – Select to use Secure Session Initiation Protocol (SIPS). SIPS uses the TLS transport mode to encrypt the traffic. If you enable SIPS, you cannot select any other transport mode than TLS.
- **Transport mode** – Select the SIP transport mode for the account: UDP, TCP, or TLS.
- **Allow port update messages through MWI** – Message waiting indicator (MWI) notifies the user of changes in the port settings.

The difference between SIPS (**Enable SIPS**) and SIP over TLS (**Transport mode – TLS**) is that SIPS ensures that each message transfer is encrypted, while SIP over TLS only has to make a best effort.

AXIS C3003-E Network Speaker

Voice over IP (VoIP)

SIP over UDP Transport mode – UDP means that the message will be sent without delay but also without the handshakes that SIPs, SIP over TLS, and SIP over TCP Transport mode – TCP offer.

Proxy Settings

A SIP proxy manages registration and routing requests from calling devices. The SIP proxy communicates with the private branch exchange (PBX) in order to find a route that a call has to take to reach a device that is set in a different location or site.

Address – Enter the SIP proxy server's address.

Username – Enter a user name for the SIP proxy server if required.

Password – Enter a password for the SIP proxy server if required.

Make Test Calls

To make sure that calls can be made from the Axis product, you can make a test call:

1. Go to **Setup > VoIP > SIP Settings** or **Setup > VoIP > Account Settings**.
2. In the test call field, enter a valid SIP address to the other device. Use the format `sip:<extension>@<domain>` or `sips:<extension>@<domain>`. For more information and examples, see *About SIP Addresses on page 16*.
3. Click **Test call**. The test call is made from the default account. For more information, see *Transport Settings on page 15*.
The call status shows below the button. For more information, see *Call Status on page 17*.
4. To end the call, click **End call**.

About SIP Addresses

SIP addresses are used to identify users within a network just like you would use a phone number or an email address to contact a friend or colleague. One of the major differences between phone calls, emails, and SIP calls is that they use different protocols to start and end conversations.

Like email addresses, SIP addresses are a type of uniform resource identifier (URI) that includes two user-specific parts, a user ID or extension and a domain or IP address. Together with a prefix and the @ symbol, they make up a unique address. For example, if Caesar of ancient Rome had both an email address and a SIP address, they would be `mailto:caesar@ancientrome.it` and `sip:caesar@ancientrome.it` respectively. For more examples and descriptions, see below.

SIP addresses are also known as SIP URIs or, in some cases, SIP numbers. For more information, see the PBX's and service provider's instructions.

Example

```
sip:3468@172.25.33.142  
sip:3468@voipprovider.com
```

Description

<code>sip:</code>	Prefix that tells the system that a SIP session is being started.
<code>sips:</code>	Prefix that tells the system that a SIPs session is being started.
<code><extension></code>	The user ID or extension of the recipient of the call. Or, if it is a peer-to-peer call, the IP address of the receiving device.
<code>@<domain></code>	The domain name or registrar address (IPv4 address) of the receiving device.

Important

The Axis product's VoIP functionality does not include support for IPv6.

AXIS C3003-E Network Speaker

Voice over IP (VoIP)

For more information about SIP, SIPS, and TLS, see *Port Settings on page 13* and *Transport Settings on page 15*.

For more information about registrar addresses and domains, see *Account Credentials on page 15*.

Call Status

The call status is indicated with dots in different colors. More information about the call status is shown next to the status dot.



Idle – No active calls or the extension is busy.

Terminated – The call was denied or ended, there was no answer, or the connection failed.



Calling – Calling and waiting for an answer.



Active – The call has been answered and is ongoing.

AXIS C3003-E Network Speaker

Events

Events

The Event pages allow you to configure the Axis product to perform actions when different events occur. For example, the product can play an audio clip according to a schedule or when a call is received. The set of conditions that defines how and when the action is triggered is called an action rule.

Set Up Action Rules

An action rule defines the conditions that must be met for the product to perform an action, for example play an audio clip or send a notification message. If multiple conditions are defined, all of them must be met to trigger the action.

For more information about available triggers and actions, see *Triggers on page 18* and *Actions on page 19*.

The following example describes how to set up an action rule to play an audio file when the Axis product receives an input signal from a video management system.

1. Go to **Events > Action Rules** and click **Add**.
2. Select **Enable** rule and enter a descriptive name for the rule.
3. Select **Input Signal** from the **Trigger** drop-down list.
4. Select **Virtual Inputs** from the second drop-down list.
5. Select **1** from the third drop-down list.
6. Select **Yes** in the **Active** list.
7. Optionally, select a **Schedule** and **Additional conditions**. See below.
8. Under **Actions**, select **Play Audio Clip** from the **Type** drop-down list.
9. Select the desired audio file from the **Play** drop-down list.
10. Click **OK**.

To use more than one trigger for the action rule, select **Additional conditions** and click **Add** to add additional triggers. When using additional conditions, all conditions must be met to trigger the action.

To prevent an action from being triggered repeatedly, a **Wait at least** time can be set. Enter the time in hours, minutes and seconds, during which the trigger should be ignored before the action rule can be activated again.

For more information, see the online help .

Triggers

Available action rule **triggers** and **conditions** include:

- **Call**
 - **State** – Triggers the action rule when a call service state changes to active, calling or idle. This trigger can, for example, be used to play a dial tone when a call is connecting.
 - **State Change** – Triggers the action rule when a call state changes. This trigger can for example, be used to play a busy tone when a call is busy or call another specified SIP account if the call is busy.
- **Hardware**
 - **Network** – Triggers the action rule when the network connection is lost. Select **Yes** to trigger the action rule when the network connection is lost. Select **No** to trigger the action rule when the network connection is restored.

AXIS C3003-E Network Speaker

Events

- **Input Signal**
 - **Speaker Test Performed** – Triggers an action rule after an Auto Speaker Test has been performed. It can be used to, for example, send a notification to an operator when a speaker test has been performed after the product has restarted.
 - **Virtual Inputs** – Triggers the action rule when one of the virtual inputs changes states. It can be used by a client such as an access management system, through the VAPIX® application programming interface, to trigger actions. Virtual inputs can, for example, be connected to buttons in the management system's user interface.
- **System**
 - **System Ready** – Triggers the action rule when the system is in state ready. For example, the Axis product can detect the system state and send a notification when the system has started.

Select **Yes** to trigger the action rule when the product is in state ready. Note that the rule will only trigger when all necessary services, such as the event system, has started.
- **Time**
 - **Recurrence** – Triggers the action rule by monitoring the recurrences that you have created. You can use this trigger to initiate recurring actions such as sending notifications every hour. Select a recurrence pattern or create a new one. For more information about setting up a recurrence pattern, see *Set Up Recurrences on page 20*.
 - **Use Schedule** – Trigger the rule according to the selected schedule. See *Create Schedules on page 20*.

Actions

Available actions include:

- **Play Audio Clip** – Plays an audio clip when the action rule is triggered. From the **Play** drop-down list, select an audio clip to play when the action rule is triggered. To add new audio clips go to **Audio > Audio Clips**.
- **Run Auto Speaker Test** – Sends an Auto Speaker Test signal when the action Rule is triggered.
- **Send Notification** – Send a notification message to a recipient.
- **Status LED** – The status LED can be set to flash for the duration of the action rule or for a set number of seconds. The status LED can be used during installation and configuration to visually validate if the trigger settings work correctly. To set the status LED flash color, select a **LED Color** from the drop-down list.

Add Recipients

The product can send messages to notify administrators about events and alarms. But before the product can send notification messages, you must define one or more recipients. For information about available options, see *Recipient Types on page 19*.

To add a recipient:

1. Go to **Events > Recipients** and click **Add**.
2. Enter a descriptive name.
3. Select a recipient **Type**.
4. Enter the information needed for the recipient type.
5. Click **Test** to test the connection to the recipient.
6. Click **OK**.

Recipient Types

The following recipients are available:

AXIS C3003-E Network Speaker

Events

- HTTP
- HTTPS
- Email
- TCP

Set Up Email Recipients

Email recipients can be configured by selecting one of the listed email providers, or by specifying the SMTP server, port and authentication used by, for example, a corporate email server.

Note

Some email providers have security filters that prevent users from receiving or viewing large amount of attachments, from receiving scheduled emails and similar. Check the email provider's security policy to avoid delivery problems and locked email accounts.

To set up an email recipient using one of the listed providers:

1. Go to **Events > Recipients** and click **Add**.
2. Enter a **Name** and select **Email** from the **Type** list.
3. Enter the email addresses to send emails to in the **To** field. Use commas to separate multiple addresses.
4. Select the email provider from the **Provider** list.
5. Enter the user ID and password for the email account.
6. Click **Test** to send a test email.

To set up an email recipient using for example a corporate email server, follow the instructions above but select **User defined as Provider**. Enter the email address to appear as sender in the **From** field. Select **Advanced settings** and specify the SMTP server address, port and authentication method. Optionally, select **Use encryption** to send emails over an encrypted connection. The server certificate can be validated using the certificates available in the Axis product. For information on how to upload certificates, see *Certificates on page 23*.

Create Schedules

To create a new schedule:

To use the schedule in an action rule, select the schedule from the **Schedule** drop-down list in the Action Rule Setup page.

Set Up Recurrences

Recurrences are used to trigger action rules repeatedly, for example every 5 minutes or every hour.

To set up a recurrence:

1. Go to **Events > Recurrences** and click **Add**.
2. Enter a descriptive name and recurrence pattern.
3. Click **OK**.

To use the recurrence in an action rule, first select **Time** from the **Trigger** drop-down list in the Action Rule Setup page and then select the recurrence from the second drop-down list.

To modify or remove recurrences, select the recurrence in the **Recurrences List** and click **Modify** or **Remove**.

AXIS C3003-E Network Speaker

Languages

Languages

Multiple languages can be installed in the Axis product. All web pages including the online help will be displayed in the selected language. To switch languages, go to **Setup > Languages** and first upload the new language file. Browse and locate the file and click the **Upload Language** button. Select the new language from the list and click **Save**.

Note

- Resetting the product to factory default settings will erase any uploaded language files and reset the product language to English.
- Clicking the **Restore** button on the Maintenance page will not affect the language.
- A firmware upgrade will not affect the language used. However if you have uploaded a new language to the product and later upgrade the firmware, it may happen that the translation no longer matches the product's web pages. In this case, upload an updated language file.
- A language already installed in the product will be replaced when a current or a later version of the language file is uploaded.

AXIS C3003-E Network Speaker

System Options

System Options

Security

Users

The user list displays authorized users and user groups (access levels):

Administrator – Unrestricted access to all settings; can add, modify and remove other users.

Under **HTTP/RTSP Password Settings**, select the type of password to allow. You may need to allow unencrypted passwords if there are viewing clients that do not support encryption, or if you upgraded the firmware and existing clients support encryption but need to log in again and be configured to use this functionality.

Deselect the **Enable Basic Setup** option to hide the Basic Setup menu. Basic Setup provides quick access to settings that should be made before using the Axis product.

IP Address Filter

IP address filtering is enabled on the page. Once enabled, the listed IP address are allowed or denied access to the Axis product. Select **Allow** or **Deny** from the list and click **Apply** to enable IP address filtering.

The administrator can add up to 256 IP address entries to the list (a single entry can contain multiple IP addresses).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol providing encrypted browsing. HTTPS can also be used by users and clients to verify that the correct device is being accessed. The security level provided by HTTPS is considered adequate for most commercial exchanges.

To use HTTPS, an HTTPS certificate must first be installed. Go to **System Options > Security > Certificates** to install and manage certificates. See *Certificates on page 23*.

To enable HTTPS on the Axis product:

1. Go to **System Options > Security > HTTPS**
2. Select an HTTPS certificate from the list of installed certificates.
3. Optionally, click **Ciphers** and select the encryption algorithms to use for SSL.
4. Set the **HTTPS Connection Policy** for the different user groups.
5. Click **Save** to enable the settings.

To access the Axis product via the desired protocol, in the address field in a browser, enter `https://` for the HTTPS protocol and `http://` for the HTTP protocol.

The HTTPS port can be changed on the **System Options > Network > TCP/IP > Advanced** page.

IEEE 802.1X

IEEE 802.1X is a standard for port-based Network Admission Control providing secure authentication of wired and wireless network devices. IEEE 802.1X is based on EAP (Extensible Authentication Protocol).

To access a network protected by IEEE 802.1X, devices must be authenticated. The authentication is performed by an authentication server, typically a **RADIUS** server, examples of which are FreeRADIUS and Microsoft Internet Authentication Service.

AXIS C3003-E Network Speaker

System Options

In Axis implementation, the Axis product and the authentication server identify themselves with digital certificates using EAP-TLS (Extensible Authentication Protocol – Transport Layer Security). The certificates are provided by a **Certification Authority (CA)**. You need:

- a CA certificate to authenticate the authentication server.
- a CA-signed client certificate to authenticate the Axis product.

To create and install certificates, go to **System Options > Security > Certificates**. See *Certificates on page 23*. Many CA certificates are preinstalled.

To allow the product to access a network protected by IEEE 802.1X:

1. Go to **System Options > Security > IEEE 802.1X**.
2. Select a **CA Certificate** and a **Client Certificate** from the lists of installed certificates.
3. Under **Settings**, select the EAPOL version and provide the EAP identity associated with the client certificate.
4. Check the box to enable IEEE 802.1X and click **Save**.

Note

For authentication to work properly, the date and time settings in the Axis product should be synchronized with an NTP server. See *Date & Time on page 24*.

Certificates

Note

Installed certificates, except preinstalled CA certificates, will be deleted if the product is reset to factory default. Preinstalled CA certificates that have been deleted will be reinstalled.

A **Server/Client** certificate can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection and can be used before a CA-issued certificate has been obtained.

To install a self-signed certificate:

1. Go to **Setup > System Options > Security > Certificates**.
2. Click **Create self-signed certificate** and provide the requested information.

To create and install a CA-signed certificate:

1. Create a self-signed certificate as described above.
2. Go to **Setup > System Options > Security > Certificates**.
3. Click **Create certificate signing request** and provide the requested information.
4. Copy the PEM-formatted request and send to the CA of your choice.
5. When the signed certificate is returned, click **Install certificate** and upload the certificate.

Server/Client certificates can be installed as **Certificate from signing request** or as **Certificate and private key**. Select **Certificate and private key** if the private key is to be upload as a separate file or if the certificate is in PKCS#12 format.

The Axis product is shipped with several preinstalled CA certificates. If required, additional CA certificates can be installed:

1. Go to **Setup > System Options > Security > Certificates**.
2. Click **Install certificate** and upload the certificate.

AXIS C3003-E Network Speaker

System Options

Date & Time

The Axis product's date and time settings are configured under **System Options > Date & Time**.

To change the date and time settings, select the preferred **Time mode** under **New Server Time**:

- **Synchronize with computer time** – Sets date and time according to the computer's clock. With this option, date and time are set once and will not be updated automatically.
- **Synchronize with NTP Server** – Obtains date and time from an NTP server. With this option, date and time settings are updated continuously. For information on NTP settings, see *NTP Configuration on page 26*.

If using a host name for the NTP server, a DNS server must be configured. See *DNS Configuration on page 26*.

- **Set manually** – Allows you to manually set date and time.

If using an NTP server, select your **Time zone** from the drop-down list. If required, check **Automatically adjust for daylight saving time changes**.

Network

Basic TCP/IP Settings

Network Interface Mode

The network interface to the AXIS product can be wired or wireless. Different settings can be used for each network interface, but only one can be used at a time. In **Auto** mode the product will use a wireless network unless a network cable is connected, in which case it will use the wired network. In **Wired** mode the product will require a network cable to connect to the network.

IPv4 Address Configuration

By default, the Axis product is set to use IPv4 (IP version 4) and to obtain the IP address automatically via DHCP. The IPv4 settings are configured under **System Options > Network > TCP/IP > Basic**.

DHCP (Dynamic Host Configuration Protocol) allows network administrators to centrally manage and automate the assignment of IP addresses. DHCP should only be enabled if using dynamic IP address notification, or if the DHCP can update a DNS server. It is then possible to access the Axis product by name (host name).

If DHCP is enabled and the product cannot be accessed, run **AXIS IP Utility** to search the network for connected Axis products, or reset the product to the factory default settings (see *page 30*) and then perform the installation again.

To use a static IP address, check **Use the following IP address** and specify the IP address, subnet mask and default router.

IPv6 Address Configuration

If IPv6 (IP version 6) is enabled, the Axis product will receive an IP address according to the configuration in the network router.

To enable IPv6, go to **System Options > Network > TCP/IP > Basic**. Other settings for IPv6 should be configured in the network router.

ARP/Ping

The product's IP address can be assigned using ARP and Ping. For instructions, see *Assign IP Address Using ARP/Ping on page 25*.

The ARP/Ping service is enabled by default but is automatically disabled two minutes after the product is started, or as soon as an IP address is assigned. To re-assign IP address using ARP/Ping, the product must be restarted to enable ARP/Ping for an additional two minutes.

To disable the service, go to and clear the option **Enable ARP/Ping setting of IP address**.

Pinging the product is still possible when the service is disabled.

AXIS C3003-E Network Speaker

System Options

Assign IP Address Using ARP/Ping

The product's IP address can be assigned using ARP/Ping. The command must be issued within 2 minutes of connecting power.

1. Acquire a free static IP address on the same network segment as the computer.
2. Locate the serial number (S/N) on the product label.
3. Open a command prompt and enter the following commands:

Linux/Unix syntax

```
arp -s <IP address> <serial number> temp  
ping -s 408 <IP address>
```

Linux/Unix example

```
arp -s 192.168.0.125 00:40:8c:18:10:00 temp  
ping -s 408 192.168.0.125
```

Windows syntax (this may require that you run the command prompt as an administrator)

```
arp -s <IP address> <serial number>  
ping -l 408 -t <IP address>
```

Windows example (this may require that you run the command prompt as an administrator)

```
arp -s 192.168.0.125 00-40-8c-18-10-00  
ping -l 408 -t 192.168.0.125
```

4. Check that the network cable is connected and then restart the product by disconnecting and reconnecting power.
5. Close the command prompt when the product responds with `Reply from 192.168.0.125:...` or similar.
6. Open a browser and type `http://<IP address>` in the Location/Address field.

Note

- To open a command prompt in Windows, open the **Start menu** and type `cmd` in the **Run/Search** field.
- To use the ARP command in Windows 8/Windows 7/Windows Vista, right-click the command prompt icon and select **Run as administrator**.
- To open a command prompt in Mac OS X, open the **Terminal** utility from **Application > Utilities**.

AXIS Video Hosting System (AVHS)

The AVHS settings are configured under **System Options > Network > TCP/IP > Basic**. The possibility to connect to an AVHS service is enabled by default. To disable, clear the **Enable AVHS** box.

One-click enabled – Press and hold the product's control button (see *Hardware Overview on page 6*) for about 3 seconds to connect to an AVHS service over the Internet. Once registered, **Always** will be enabled and the Axis product stays connected to the AVHS service. If the product is not registered within 24 hours from when the button is pressed, the product will disconnect from the AVHS service.

Always – The Axis product will constantly attempt to connect to the AVHS service over the Internet. Once registered the product will stay connected to the service. This option can be used when the product is already installed and it is not convenient to use the one-click installation.

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Service assigns a host name for easy access to the product. For more information, see www.axiscam.net

To register the Axis product with AXIS Internet Dynamic DNS Service, go to **System Options > Network > TCP/IP > Basic**. Under **Services**, click the **AXIS Internet Dynamic DNS Service Settings** button (requires access to the Internet). The domain name currently registered at AXIS Internet Dynamic DNS service for the product can at any time be removed.

AXIS C3003-E Network Speaker

System Options

Note

AXIS Internet Dynamic DNS Service requires IPv4.

Advanced TCP/IP Settings

DNS Configuration

DNS (Domain Name Service) provides the translation of host names to IP addresses. The DNS settings are configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain DNS server address via DHCP** to use the DNS settings provided by the DHCP server.

To make manual settings, select **Use the following DNS server address** and specify the following:

Domain name – 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.

Primary/Secondary DNS server – Enter the IP addresses of the primary and secondary DNS servers. The secondary DNS server is optional and will be used if the primary is unavailable.

NTP Configuration

NTP (Network Time Protocol) is used to synchronize the clock times of devices in a network. The NTP settings are configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain NTP server address via DHCP** to use the NTP settings provided by the DHCP server.

To make manual settings, select **Use the following NTP server address** and enter the host name or IP address of the NTP server.

Host Name Configuration

The Axis product can be accessed using a host name instead of an IP address. The host name is usually the same as the assigned DNS name. The host name is configured under **System Options > Network > TCP/IP > Advanced**.

Select **Obtain host name via IPv4 DHCP** to use host name provided by the DHCP server running on IPv4.

Select **Use the host name** to set the host name manually.

Select **Enable dynamic DNS updates** to dynamically update local DNS servers whenever the Axis product's IP address changes.

For more information, see the online help .

Link-Local IPv4 Address

Link-Local Address is enabled by default and assigns the Axis product an additional IP address which can be used to access the product from other hosts on the same segment on the local network. The product can have a Link-Local IP and a static or DHCP-supplied IP address at the same time.

This function can be disabled under **System Options > Network > TCP/IP > Advanced**.

HTTP

The HTTP port used by the Axis product can be changed under **System Options > Network > TCP/IP > Advanced**. In addition to the default setting, which is 80, any port in the range 1024–65535 can be used.

AXIS C3003-E Network Speaker

System Options

HTTPS

NAT traversal (port mapping) for IPv4

A network router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the "outside", that is, the Internet. Security on the private network (LAN) is increased since most routers are pre-configured to stop attempts to access the private network (LAN) from the public network (Internet).

Use **NAT traversal** when the Axis product is located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the product.

NAT traversal is configured under **System Options > Network > TCP/IP > Advanced**.

Note

- For NAT traversal to work, this must be supported by the router. The router must also support UPnP™.
- In this context, router refers to any network routing device such as a NAT router, Network router, Internet Gateway, Broadband router, Broadband sharing device, or a software such as a firewall.

Enable/Disable – When enabled, the Axis product attempts to configure port mapping in a NAT router on your network, using UPnP™. Note that UPnP™ must be enabled in the product (see).

Use manually selected NAT router – Select this option to manually select a NAT router and enter the IP address for the router in the field. If no router is specified, the product automatically searches for NAT routers on your network. If more than one router is found, the default router is selected.

Alternative HTTP port – Select this option to manually define an external HTTP port. Enter a port in the range 1024–65535. If the port field is empty or contains the default setting, which is 0, a port number is automatically selected when enabling NAT traversal.

Note

- An alternative HTTP port can be used or be active even if NAT traversal is disabled. This is useful if your NAT router does not support UPnP and you need to manually configure port forwarding in the NAT router.
- If you attempt to manually enter a port that is already in use, another available port is automatically selected.
- When the port is selected automatically it is displayed in this field. To change this, enter a new port number and click **Save**.

FTP

The FTP server running in the Axis product enables upload of new firmware, user applications, etc. The FTP server can be disabled under **System Options > Network > TCP/IP > Advanced**.

RTSP

The RTSP server running in the Axis product allows a connecting client to start an audio stream from the Axis product. The RTSP port number can be changed under **System Options > Network > TCP/IP > Advanced**. The default port is 554.

Note

Audio streams will not be available if the RTSP server is disabled.

SOCKS

SOCKS is a networking proxy protocol. The Axis product can be configured to use a SOCKS server to reach networks on the other side of a firewall or proxy server. This functionality is useful if the Axis product is located on a local network behind a firewall, and notifications, uploads, alarms, etc need to be sent to a destination outside the local network (for example the Internet).

SOCKS is configured under **System Options > Network > SOCKS**. For more information, see the online help .

AXIS C3003-E Network Speaker

System Options

QoS (Quality of Service)

QoS (Quality of Service) guarantees a certain level of a specified resource to selected traffic on a network. A QoS-aware network prioritizes network traffic and provides a greater network reliability by controlling the amount of bandwidth an application may use.

SNMP

The Simple Network Management Protocol (SNMP) allows remote management of network devices. An SNMP community is the group of devices and management station running SNMP. Community names are used to identify groups.

To enable and configure SNMP in the Axis product, go to the **System Options > Network > SNMP** page.

Depending on the level of security required, select the version on SNMP to use.

Traps are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

Note

If HTTPS is enabled, SNMP v1 and SNMP v2c should be disabled.

Traps for SNMP v1/v2 are used by the Axis product to send messages to a management system on important events and status changes. Check **Enable traps** and enter the IP address where the trap message should be sent and the **Trap community** that should receive the message.

The following traps are available:

- Cold start
- Warm start
- Link up
- Authentication failed

SNMP v3 provides encryption and secure passwords. To use traps with SNMP v3, an SNMP v3 management application is required.

To use SNMP v3, HTTPS must be enabled, see *HTTPS* on page 22. To enable SNMP v3, check the box and provide the initial user password.

Note

The initial password can only be set once. If the password is lost, the Axis product must be reset to factory default, see *Reset to Factory Default Settings* on page 30.

UPnP™

The Axis product includes support for UPnP™. UPnP™ is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

UPnP™ can be disabled under **System Options > Network > UPnP**

Bonjour

The Axis product includes support for Bonjour. Bonjour is enabled by default and the product is automatically detected by operating systems and clients that support this protocol.

Bonjour can be disabled under **System Options > Network > Bonjour**.

AXIS C3003-E Network Speaker

System Options

Ports & Devices

LED Settings

The Status LED can be configured to be unlit during normal operation. To configure, go to **Setup > System Options > Ports & Devices > LED**.

The available options for the Status Indicator LED are:

- **Normal:** The status LED shows steady green during normal operation. This is the default setting.
- **Off:** The status LED is off during normal operation. This can be useful in making the Axis product less noticeable.

Maintenance

The Axis product provides several maintenance functions. These are available under **System Options > Maintenance**.

Click **Restart** to perform a correct restart if the Axis product is not behaving as expected. This will not affect any of the current settings.

Note

A restart clears all entries in the Server Report.

Click **Restore** to reset most settings to the factory default values. The following settings are not affected:

- the boot protocol (DHCP or static)
- the static IP address
- the default router
- the subnet mask
- the system time

Click **Default** to reset all settings, including the IP address, to the factory default values. This button should be used with caution. The Axis product can also be reset to factory default using the control button, see *Reset to Factory Default Settings on page 30*.

For information about firmware upgrade, see *Upgrade the Firmware on page 31*.

Support

Support Overview

The page provides information on troubleshooting and contact information, should you require technical assistance.

See also *Troubleshooting on page 31*.

System Overview

Logs & Reports

The page generates logs and reports useful for system analysis and troubleshooting. If contacting Axis Support, please provide a valid Server Report with your query.

System Log – Provides information about system events.

Access Log – Lists all failed attempts to access the product. The Access Log can also be configured to list all connections to the product (see below).

AXIS C3003-E Network Speaker

System Options

Server Report – Provides information about the product status in a pop-up window. The Access Log is automatically included in the Server Report.

Parameter List – Shows the product's parameters and their current settings. This may prove useful when troubleshooting or when contacting Axis Support.

Connection List – Lists all clients that are currently accessing media streams.

Crash Report – Generates an archive with debugging information. The report takes several minutes to generate.

Advanced

Scripting

Scripting allows experienced users to customize and use their own scripts.

NOTICE

Improper use may cause unexpected behavior and loss of contact with the Axis product.

Axis strongly recommends that you do not use this function unless you understand the consequences. Axis Support does not provide assistance for problems with customized scripts.

To open the Script Editor, go to **System Options > Advanced > Scripting**. If a script causes problems, reset the product to its factory default settings, see *page 30*.

For more information, see www.axis.com/developer

Plain Config

Plain Config is for advanced users with experience of Axis product configuration. Most parameters can be set and modified from this page.

To open Plain Config, go to **System Options > Advanced > Plain Config**. Axis Support does not provide assistance.

Reset to Factory Default Settings

Important

Reset to factory default should be used with caution. A reset to factory default will reset all settings, including the IP address, to the factory default values.

To reset the product to the factory default settings:

1. Disconnect power from the product.
2. Press and hold the control button and reconnect power. See *Hardware Overview on page 6*.
3. Keep the control button pressed for about 10 seconds until the status LED indicator turns amber for the second time.
4. Release the control button. The process is complete when the status LED indicator turns green. The product has been reset to the factory default settings. If no DHCP server is available on the network, the default IP address is 192.168.0.90
5. Using the installation and management software tools, assign an IP address, set the password, and access the product.

It is also possible to reset parameters to factory default via the web interface. Go to **Setup > System Options > Maintenance**.

AXIS C3003-E Network Speaker

Troubleshooting

Troubleshooting

Check the Firmware

Firmware is software that determines the functionality of network devices. One of your first actions when troubleshooting a problem should be to check the current firmware version. The latest version may contain a correction that fixes your particular problem. The current firmware version in the Axis product is displayed in the page **Setup > Basic Setup** and in **Setup > About**.

Upgrade the Firmware

Important

- Your dealer reserves the right to charge for any repair attributable to faulty upgrade by the user.
- Preconfigured and customized settings are saved when the firmware is upgraded (providing the features are available in the new firmware) although this is not guaranteed by Axis Communications AB.

Note

- When you upgrade the Axis product with the latest firmware from Axis website, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before upgrading the firmware.

Symptoms, Possible Causes and Remedial Actions

Problems setting the IP address

When using ARP/Ping

The product is located on a different subnet	If the IP address intended for the product and the IP address of the computer used to access the product are located on different subnets, you will not be able to set the IP address. Contact your network administrator to obtain an IP address.
The IP address is being used by another device	Disconnect the Axis product from the network. Run the Ping command (in a Command/DOS window, type <code>ping</code> and the IP address of the product): • If you receive: <code>Reply from <IP address>: bytes=32; time=10...</code> this means that the IP address may already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the product. • If you receive: <code>Request timed out</code>, this means that the IP address is available for use with the Axis product. Check all cabling and reinstall the product.
Possible IP address conflict with another device on the same subnet.	The static IP address in the Axis product is used before the DHCP server sets a dynamic address. This means that if the same default static IP address is also used by another device, there may be problems accessing the product.

The product cannot be accessed from a browser

Cannot log in	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used when attempting to log in. You may need to manually type <code>http</code> or <code>https</code> in the browser's address field. If the password for the user <code>root</code> is lost, the product must be reset to the factory default settings. See <i>Reset to Factory Default Settings</i> on page 30.
The IP address has been changed by DHCP	

AXIS C3003-E Network Speaker

Troubleshooting

The product is accessible locally but not externally

Router configuration	To configure your router to allow incoming data traffic to the Axis product, enable the NAT-traversal feature which will attempt to automatically configure the router to allow access to the Axis product, see <i>NAT traversal (port mapping) for IPv4 on page 27</i> . The router must support UPnP™.
Firewall protection	Check the Internet firewall with your network administrator.
Default routers required	

AXIS C3003-E Network Speaker

Technical Specifications

Technical Specifications

Function/group	Item	Specifications
Audio	Models	AXIS C3003-E
	Audio streaming	One-way/two-way (mono)
	Audio compression	G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, Axis μ -law 16 kHz, Configurable bit rate
	Audio input/output	Built-in microphone (can be disabled mechanically)
	Built-in microphone specification	50 Hz - 16 kHz
Speaker	Max sound pressure level	>121 dB
	Frequency response	280 Hz - 12.5 kHz
Amplifier	Amplifier description	Built-in 7 W Class D amplifier
Network	Security	Password protection, IP address filtering, HTTPS * encryption, IEEE 802.1X* network access control, Digest authentication, User access log
	Supported protocols	IPv4/v6, HTTP, HTTPS*, SIP, SSL/TLS*, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMP v1/v2c/v3(MIB-II), DNS, DynDNS, NTP, TCP, UDP, IGMP, ICMP, DHCP, ARP, SOCKS
		* This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (www.openssl.org), and cryptographic software written by Eric Young (eay@cryptsoft.com).
System Integration	Application Programming Interface	Open API for software integration, including VAPIX®; specifications at www.axis.com AXIS Video Hosting System (AVHS) with One-click Connection
	Intelligent audio	Auto Speaker Test
	Event triggers	Call: State, State Change Hardware: Network Input Signal: Speaker Test Performed, Virtual Inputs System: System Ready Time: Recurrence, Use Schedule
	Event actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP Play Audio Clip Run Auto Speaker Test Send SNMP Trap Status LED
	Built-in installation aids	Test tone
	Functional monitoring	Auto Speaker Test, Connection verification, Built-in system logging

AXIS C3003-E Network Speaker

Technical Specifications

Function/group	Item	Specifications
General	Casing	Impact-resistant aluminum, IP66-, IP67- and NEMA 4X-rated. For repainting instructions and impact on warranty, contact your Axis partner
	Memory	256 MB RAM, 256 MB Flash
	Power	Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3 (max 12.95 W)
	Connectors	RJ45 10BASE-T/100BASE-TX PoE
	Operating conditions	-20°C to 50 °C (-4 °F to 122 °F) Humidity 10–100% RH (condensing)
	Approvals	EN 55022 Class B, EN 61000-6-1, EN 61000-6-2, EN 55024, EN 50121-4, IEC 62236-4, FCC Part 15 Subpart B Class B, ICES-003 Class B, VCCI Class B, C-tick AS/NZS CISPR 22 Class B, KCC KN22 Class B, KN24, IEC/EN/UL 60950-1, IEC/EN/UL 60950-22, IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-64, IEC 60068-2-78, IEC/EN 60529 IP66, IEC/EN 60529 IP67, NEMA 250 Type 4X
	Dimensions	Without bracket: 164 x 225 x 250 mm (6 1/2 x 8 7/8 x 9 7/8 in.) With bracket: 164 x 225 x 305 mm (6 1/2 x 8 7/8 x 12 in.)
	Weight	1.3 kg (2.9 lb.)
	Included accessories	Installation Guide, AVHS Authentication Key, AXIS Connector Guard A, Cable shoe
	Optional accessories	AXIS T91A47 Pole Mount, AXIS T91C67 Pole Mount, Cable Gland M20 x 1, RJ45, Cable Gland A M20, AXIS Power over Ethernet Midspans
	Warranty	Axis 3-year warranty and AXIS Extended Warranty option, see www.axis.com/warranty

