AXIS I5304 Network Answering Unit

User manual

Table of Contents

Get started....4
Find devices on the network....4
Retrieve the current IP address using the device....4
Browser support....4
Open the device's web interface....4
Secure passwords....5
Upgrade the device software....5
Configure your device....6
Configure the IP address....6
Change the IP address mode using the RESET button....6
Upload user certificates....7
Set a custom language....7
Set up calls....7
Set up calls with an Axis intercom....7
Call over SIP proxy....8
Unlock a door using DTMF....9
Show video from an Axis camera....10
Connect a doorbell....10
Send HTTP commands from the device display....11
Add more unlock buttons....11
Create a time profile....11
The web interface....13
....13
State....13
Device....13
Services....13
Call logs....13
Events....14
Directory....15
Devices....15
Time profiles....17
Holidays....17
Calling....18
SIP....19
Local calls....23
Services....24
Unlocking....24
HTTP command....24
User sounds....24
Web server....26
Weather....28
Hardware....28
Audio....28
Camera....28
Display....30
Digital inputs....31
System....32
Network....32
Date & time....33
Features....34
Certificates....34
Auto provisioning....36
Diagnostics....37

Maintenance 39
The display interface 40
Home screen 40
Call log 40
Directory 40
Settings 41
Specifications 43
Product overview 43
Ports 43
Connectors 44
Network connector 44
Power and doorbell connector 44
Induction loop connector 44
Buttons 44
Reset button 44
Clean your device 46
Troubleshooting 47
Reset to factory default settings 47
Restart the device 47
Contact support 47

Get started

Find devices on the network

To find the device on the network and assign an IP address to it, use 2N® Network Scanner. The application is available to download from the 2N website, *2n.com*. Make sure to install Microsoft® .NET Framework 2.0 before you install the application.

1. Connect power and network to the answering unit.
2. Start 2N Network Scanner. All available devices on the network show up in the list automatically.
3. To access the device from a browser, right-click the device and select **Browse**.
4. To change the IP address of the device, select **Config** and enter the static IP address, or activate DHCP.

Note

- If the device is greyed out, you can't configure the IP address with 2N Network Scanner. Device discovery in the network scanner requires multicast support in the network.

Retrieve the current IP address using the device

You can retrieve the current IP address from the device itself, either through the device display or the RESET button.

Use the device display:

1. Tap **Settings**.
2. Tap **About**.

You can find the address under **IP ADDRESS**.

Use the RESET button:

1. Press and hold the RESET button.
2. When the red and green LEDs turn on simultaneously and you hear the acoustic signal , release the RESET button.
   This takes approximately 15 to 35 seconds.

When you release the button, the device announces the current IP address through the speaker.

Browser support

You can use the device with the following browsers:

	Chrome™	Firefox®	Edge™	Safari®
Windows®	recommended	recommended	✓	
macOS®	recommended	recommended	✓	✓
Linux®	recommended	recommended	✓	
Other operating systems	✓	✓	✓	✓*

Open the device's web interface

1. Open a browser and enter the IP address of the device.
2. Type the username and password. The default username and password is:
   - **Username**: Admin
   - **Password**: pass

If you access the device for the first time, you must change the password of the device.

For descriptions of all the controls and options in the device's web interface, see .

Secure passwords

Important

Use HTTPS (which is enabled by default) to set your password or other sensitive configurations over the network. HTTPS enables secure and encrypted network connections, thereby protecting sensitive data, such as passwords.

The device password is the primary protection for your data and services. Axis devices do not impose a password policy as they may be used in various types of installations.

To protect your data we strongly recommend that you:

- Use a password with at least 8 characters, preferably created by a password generator.
- Don't expose the password.
- Change the password at a recurring interval, at least once a year.

Upgrade the device software

We recommend that you upgrade the device software when you log in to the device for the first time. Download the latest version from *axis.com/support/device-software*.

1. Go to **System > Maintenance**.
2. Click **Upgrade Firmware** and select the file you downloaded.
3. Click **Upload**.

When you have uploaded the file and the upgrade is complete, the device restarts automatically.

Configure your device

This section covers all the important configurations that an installer needs to do to get the product up and running after the hardware installation has been completed.

Configure the IP address

The device is connected to the LAN and should be assigned a valid IP address or obtain the IP address from the LAN DHCP server. By default, the device is set to use a DHCP server to assign the IP address.

You can configure the IP address and DHCP in the web interface.

1. Go to **System > Network > Basic**.
2. To use a DHCP server to automatically assign the IP address, select **Use DHCP Server**.
3. To set a static IP address, first deselect **Use DHCP Server**. Then go to **Static IP Address Setting** to enter the **Static IP Address**, **Network Mask**, and **Default Gateway**.
4. To use manual DNS settings, go to **DNS Setting** and select **Always Use Manual Setting**.

Note

You can only select **Always Use Manual Setting** if you use a DHCP server. If you use static IP address, you always have to set the DNS server address.

5. Enter the **Primary DNS** and **Secondary DNS**.
6. Go to **Network Identification** and enter the **Hostname** and **Vendor Class Identifier** to identify the device.
7. To use VLAN, go to **VLAN Settings** and select **VLAN Enabled** and a **VLAN ID**. The VLAN ID must be a number between 1 and 4049.
8. Go to **Network Interface Settings** to select the **Required Port Mode** and **Advertised Modes**. **Current Port State** shows the current setting.
9. Click  to save your changes.

Change the IP address mode using the RESET button

You can turn on or off DHCP and change the IP address mode through the RESET button.

Turn off DHCP and turn on static IP address mode:

1. Press and hold the RESET button.
2. Wait for the following to occur before you release the button:
   - 2.1. The red and green LEDs turn on simultaneously and you hear the acoustic signal . This takes approximately 15 to 35 seconds.
   - 2.2. The red LED turns off and you hear the acoustic signal . This takes approximately another 3 seconds.
3. Release the RESET button.

Note

The device sets the networks parameters to default settings:

- IP address: `192.168.1.100`
- Network mask: `255.255.255.0`
- Default gateway: `192.168.1.1`

Turn on DHCP and turn off static IP address mode:

1. Press and hold the RESET button.

2. Wait for the following to occur before you release the button:

   2.1. The red and green LEDs turn on simultaneously and you hear the acoustic signal . This takes approximately 15 to 35 seconds.

   2.2. The red LED turns off and you hear the acoustic signal . This takes approximately another 3 seconds.

   2.3. The green LED turns off and you hear the acoustic signal . This takes approximately another 3 seconds.

3. Release the RESET button.

Upload user certificates

1. Go to **System** > **Certificates** > **User Certificates**.
2. Click  to upload a certificate or private key.
3. Enter a **Certificate ID**.
4. Upload a **User Certificate** or a **Private Key**.
5. If you upload a private key, enter the **Private Key Password**.
6. Click **Upload**.

Note

- If a certificate with a private RSA key longer than 2048 bits is rejected, the following message displays:
- For certificates based on elliptic curves, use only secp256r1 (also called, prime256v1 and NIST P-256) and secp384r1 (also called NIST P-384) curves.

Set a custom language

1. To set the language to a custom language, go to **Hardware** > **Display** > **User Localization**.
2. Click  to download the original language file.
3. In the downloaded file, replace the English text with the new language and save.
4. Click  to upload the translated language file.
5. Go to **Hardware** > **Display** > **Basic Settings**.
6. Select **Custom** in the **Language** drop-down menu.
7. Click  to save.
8. Go through the device display to make sure the translations are correct.

Set up calls

Set up calls with an Axis intercom

Connect the answering unit to an Axis intercom to be able to accept incoming calls and make outgoing calls, as well as control locks connected to the intercom.

Configure AXIS I5304
Enable SIP:

1. In the web interface, go to **Calling > SIP 1 > Configuration**.
2. Select **SIP Account Enabled**.

Add the intercom:

3. Go to **Directory** > **Devices**.
4. Click **Add device**.
5. In **Device Name**, enter a name for the intercom.
6. In the **Device Type** drop-down menu, select **Axis Door Station**.
7. In **Phone Number**, enter the IP address of the intercom in the format `sip:[ip-address]`.
8. Under **Display**, select **Display Device**.
9. Under **Unlock Button Function**, enter the DTMF code in the **UNLOCK CODE** column.
   The default DTMF code is 00.
10. Click  to save.

To be able to call the answering unit from an Axis intercom, you first need to set up SIP, then add the answering unit as a contact, and finally configure the call button. In this example we will set up the intercom for peer-to-peer communication.

Configure the Axis intercom

Set up SIP:

1. In the web interface of the intercom, go to **Communication** > **SIP Settings**.
2. Select **Enable SIP** and **Allow Incoming SIP calls**.
3. Click **Save**.

Add the network answering unit as a contact:

4. Go to **Communication > Contact list**.
5. Click **+ Add contact**.
6. Enter a name for the answering unit.
7. Enter the answering unit's IP address in the format `sip:[ip-address]`.
8. Select the SIP account to call from.

Note

Availability options are defined in **System** > **Events** > **Schedules**.

9. Choose the contact's **Availability**. If there's a call when the contact isn't available, the call gets canceled unless a there's a fallback contact.

Note

A fallback is a contact, to whom the call gets forwarded if the original contact doesn't reply or isn't available.

10. In **Fallback**, select a fallback contact if required.
11. Click **Save**.

Configure the intercom's call button:

12. Go to **Communication > Calls > Call button**.
13. Under **Recipients**, select the answering unit from the drop-down menu.

If you want to use the answering unit to unlock doors when someone calls from the intercom, see .
For more information about configuring Axis intercoms, see the user manual for your intercom at *help.axis.com*.

Call over SIP proxy

A SIP proxy is an IP network server responsible for call routing. The SIP proxy transfers calls to another entity closer to the destination. There can be more than one SIP proxy between users.

Note

In this example we will use the following parameters for illustration purposes:

- **SIP proxy and SIP registrar**: 192.168.50.252
- **Phone number (ID)**: 201 (for the answering unit), 203 (for the device you're calling to)
- **Port number**: 5060

1. Go to **Calling** > **SIP 1** > **Configuration** to register the device.
2. Select **SIP Account Enabled**.
3. Under **Device Identity**, enter the following information:
   - **Display Name**: The name of your device
   - **Phone Number (ID)**: 201
   - **Domain**: 192.168.50.252
4. Under **SIP Proxy** and **SIP Registrar**, enter the following information:
   - **Domain**: 192.168.50.252
   - **Port**: 5060
5. If your device requires authentication, enter **Authentication ID** and **Password**.
6. Go to **Directory** > **Devices** to add the device you want to make calls to.
7. Add a new user and enter the phone number, in this example 203.
8. Click  to save.

Unlock a door using DTMF

When someone calls the answering unit from an Axis intercom, you can use DTMF (Dual-Tone Multi-Frequency signaling) to unlock the door.

Before you start:

- Set up SIP calls with an Axis intercom, see .

Note

- DTMF is enabled by default in the answering unit. If you need to update your DTMF settings, go to **Calling > Audio > SIP 1**.
- The default DTMF code in the answering unit is 00. We will use the code to illustrate this example.

This example explains how to:

- Define the DTMF signal in the Axis intercom.
- Set up the intercom to unlock the door using the internal relay.

Configure the Axis intercom

Define the DTMF signal in the intercom:

1. Go to **Communication > SIP > DTMF**.
2. Click **+ Add sequence**.
3. In **Sequence**, enter 00.
4. In **Description**, enter Unlock door.
5. In **Accounts**, select the SIP account.
6. Click **Save**.

Set up the intercom to unlock the door using the internal relay:

7. Go to **System > Events > Rules** and add a rule.
8. In the **Name** field, enter DTMF unlock door.
9. From the list of conditions, under **Call**, select **DTMF** and **Unlock door**.
10. From the list of actions, under **I/O**, select **Toggle I/O once**.
11. From the list of ports, select **Relay 1**.

12. Change **Duration** to 00:00:07, which means that the door is open for 7 seconds.
13. Click **Save**.

When you receive a call from the Axis intercom, you can unlock the door connected to the intercom.

Show video from an Axis camera

You can connect an external Axis camera to the answering unit. When you receive a call from an intercom, you have the option to view the camera's video stream on the screen. The answering unit lets you use RTSP streams from standard IP video cameras with resolutions of up to 1280x720px at 30 fps using either the H.264 or MJPEG codec.

Requirements:

- We recommended to always use the latest firmware.
- A connected intercom. For more information, see .
- An Axis camera with support for RTSP streams that meets the requirements above.

Add the camera to the answering unit

Note

You can use the **External IP Camera Log** section to help you with the configuration. Here you can see basic communication with the external camera.

1. In the web interface of the answering unit, go to **Hardware** > **Camera** and select one of the numbered tabs.
2. Select **Camera Enabled**.
3. Under **Camera Assignment**, click **+** and select the connected intercom from the list.
4. Under **Settings**, enter a **Display Name** for the camera. This will show in the directory of the device.
5. Enter the **RTSP Stream Address** of the camera you want to use. Use following RTSP stream address format: `rtsp://[ip-address]/axis-media/media.amp?videocodec=h264&resolution=1280x720`.
6. Enter the **Username** and **Password** for the camera connection. This is only required if the camera uses authentication.
7. Enter the **Local RTP Port**.
8. Click  to save.

You can see a live view of the camera under **Camera Preview** in the answering unit if you configured everything correctly.

Connect a doorbell

With a doorbell button it's possible to call to the device directly without the use of any other devices. When you press the button the device starts to ring based on the configuration.

To do this configuration you need AXIS I5304, a doorbell (button), and 2-wires cable.

Connect the doorbell

1. Remove the answering unit from it's holder.
2. Put the device, face down, on a soft surface where you can't damage the display.
3. In the back, connect the 2-wire cable to the device.

Adjust the doorbell sound

- To change the ringtone, go to **Services** > **User sounds** > **Sound Mapping** and select a ringtone in the **Doorbell** drop-down menu.

- To set the volume, go to **Hardware** > **Audio**. Under **Phone Call Volume**, set the volume in dB for **Ringtone Volume**.

Send HTTP commands from the device display

You can configure the device to send HTTP commands by tapping a button on the display's home screen.

You can set up to three different HTTP commands for the home screen and configure a button for each command. When you tap the button, the device sends the command.

Note

HTTP commands are available in the HTTP API manual or in the HTTP API TESTool.

See *wiki.2n.com/hip/hapi/latest/en* for the HTTP API manual. To access the TESTool, enter the intercom's IP address and type `/apitest.html` at the end, for example `https://192.168.49.88/apitest.html`.

This example shows how to set commands for triggering Switch 1 and for holding Switch 2 open on a network intercom.

1. Go to **Services** > **HTTP Command**> **Home Screen HTTP Command Setting**.
2. In row 1, under **URL**, enter the HTTP command for switch 1: `https://[ip-address]/api/switch/ctrl?switch=1&action=on`.
   Replace `[ip-address]` with the address of the device.
3. In row 2, under **URL**, enter the HTTP command for switch 2: `https://[ip-address]/api/switch/ctrl?switch=2&action=hold`.
   Replace `[ip-address]` with the address of the device.
4. Select an icon for the display's home screen for each command.
5. Enter a name for each command.
6. Enter a username for each command. This is required in case the HTTP API account for authorization is set in the command receiving device.
7. Enter a password for the username for each command.
8. Click  to save.

Add more unlock buttons

1. On the display, set the activation codes for the IP intercom.
2. In the web interface, go to **Directory** > **Devices**.
3. To add the intercom, click **Add device**.
4. Fill in the desired information under **Basic settings**, **Cameras**, **Display**, **Call Button Function**, and **Alarm call**.
5. Under **Unlock Button Function**, add the switch activation codes under **Unlock code**. You can also give each button a unique name.
6. Click  to save.

Create a time profile

To use time profiles for **Do Not Disturb Mode With Time Profile**, set up the time profile before.

1. Go to **Directory** > **Time Profiles**
2. Select a number in the heading.
3. Under **Basic Settings**, enter a name for the profile.

4. Click on the timeline for the day you want to add to your schedule.
5. Adjust the times and click ✓ to save.
6. Click 💾 to save the time profile.

The web interface

To reach the device's web interface, type the device's IP address in a web browser.

Language: Click one of the language codes to set the language temporarily.

Log out: Click to sign out from the web interface.

 : Share your feedback.

 : Show tips and tricks for the configuration section.

State

Device

Device Info: Lists information about the device, such as its name and hardware version.

- **Factory Certificate Installed**: Specifies if a user certificate and private key are installed and can validate the right for the intercom to communicate with the auto configuration server (ACS).
- **Locate Device**: Click to start optical and acoustic signalling of a device. The control backlight on the device lights up and a sound starts. If the device doesn't have an integrated speaker, connect an external speaker to use acoustic signalling.

Services

Network Interface Status: Shows the status and information related to the network

Phone status (SIP1): Shows the status and information related to the phone over SIP 1.

Phone status (SIP2): Shows the status and information related to the phone over SIP 2.

Call logs

The list includes the last 20 records that are arranged from the latest call to the oldest one. Use the **Search** bar to search for a call record based on its name.

Search: Search for a call record based on its name.

Name: The name of the device that made or received the call.

Date and Time: The date and time the call was made or received.

Call Duration: The duration of the call, in seconds.

 : Indicates that the call was outgoing.

 : Indicates that it was a missed call.

 : Indicates that it was an incoming call.

 : Indicates that the call was answered elsewhere.

 : Deletes the call record on the selected row or all call records if you click on the icon in the header row.

Events

Shows the last 500 events captured by the device. Use the drop-down menu to filter bases on type of event.

TIME: Shows the time the event occurred.

EVENT TYPE: Shows the type of event that occurred. See the following list for more information about available event types.

- **ApiAccessRequested**: Generated whenever the request is sent to /api/accesspoint/grantaccess with the "success" : true result.
- **CallSessionStateChanged**: Describes the call direction/state, address, session number, and call sequence number.
- **CallStateChanged**: Indicates the call direction and opponent/SIP account identification at a call state change.
- **CapabilitiesChanged**: Describes a change in the list of available functions of the device.
- **ConfigurationChanged**: Describes a change in the device configuration.
- **DeviceState**: Describes a change in the device state, for example the startup of the device.
- **DtmfEntered**: The DTMF code received in-call or off-call locally.
- **DtmfSent**: The DTMF code sent in-call or off-call locally.
- **ExternalCameraStateChanged**: Describes a state change of the connected external camera.
- **InputChanged**: Describes a state change of the logic input.
- **KeyPressed**: Generated when a button is pressed (numeric keypad digits are 0, 1, 2..., 9 and quick dial buttons are %1, %2 ...).
- **KeyReleased**: Generated when a button is released (numeric keypad digits are 0, 1, 2..., 9 and quickdial buttons are %1, %2 ...).
- **LoginBlocked**: Generated after three incorrect login attempts to the web interface. Contains information about the IP address.
- **RegistrationStateChanged**: Describes a change of the SIP Proxy registration state.

DESCRIPTION: Shows the details for the event type.

Directory

Devices

Find Device: Click to find devices that are available on the local network.

Add Device: Click to add a new device.

: Download the list of existing contacts in .csv format from the directory

: Import a contact list in .csv format to the directory.

- **Replace Directory**: Select if you want to replace the existing directory with the imported file.
- **Import to Directory**: Select if you want to import the list of contacts and add it to the existing directory.

Search: Search for the device name or phone number.

Type: Indicates the type of device.

Name: The name of the device.

Phone Number: The device phone number.

Features: Shows the features of the device through the following icons:

- : The device is listed on the display.
- : The device sets an alarm call after you press the doorbell.
- : The device allows incoming calls.

To find or add a new device, click **Find Device** or **Add Device**. To edit an existing device, click ›. The configuration menu for adding or editing a device contains:

Basic Settings

- **Device Name**: Enter the device name for the selected contact. This parameter is optional and helps you find items in the directory more easily.
- **Displayed Icon**: Select if you want to show a standard icon or a reception desk icon.
- **Device Type**: Select the type of device you are adding.
- **Phone Number**: Enter the phone number of the station that the call should be routed to.
  - Enter `sip:[user_id@]domain[:port]` for Direct SIP calling, for example `sip:200@192.168.22.15` or `sip:name@yourcompany`.
  - Enter `device:device_name` to call 2N devices.
  - Set the device name in the mobile application. Enter /1 or /2 (account 1 or 2) behind the phone number to specify which SIP account to use for outgoing calls.
  - Enter /S or /N to force an encrypted or unencrypted call. The account and encryption selections can be combined into the suffix /1S, for example.
- **Individual Ringtone**: Set an individual ringtone for the contact.
- **Enable Viewing the Intercom's External Camera**: Enables switching from a stream of an external camera connected to the 2N intercom. If you select this option, the external camera button appears during calls and previews.
- **Face Zooming Button**: You can set whether the contact's terminal device can monitor faces during video calls. If you select this option, the face monitoring button appears during calls and call previews.
- : Click to edit the phone number details.
  - **Call Type**: set the scheme in the called destination URI. If you choose.
    - **[unspecified]**: The URI uses the data from the SIP account settings.
    - **sip**: Direct SIP call (`sip:`).
    - **device**: 2N local calls (`device:`).
    - **rava**: calls to Crestron devices (`rava:`).
    - **vms**: calls with a VMS, for example AXIS Camera Station (`vms:`).
  - **Destination**: Set the other parts of the called destination URI. As a rule, it contains the number, IP address, domain, port, or device identifier. Enter an asterisk (*) for calls to a VMS.
  - **Preferred SIP Account**: Select which SIP account to use for calling.
  - **Call Encryption**: Select if you want to use call encryption or no encryption.
  - **Door Opening**: Select to open doors via callbacks.

Cameras

- **Cameras Assigned to This Device**: Enter the cameras, numbers 1-16, separated by commas in the order they should appear during the calls with this device. Configure the cameras in **Hardware > Camera**.

Display

- **Display Device**: Select to display this device.
- **Display on Top**: Select to display this device in the top of the list.
- **Alternative Name**: Enter a name to display instead of the device name.

Call Button Function

- **Start Call on Short Press**: Select to be able to start a call to the selected device after a short press of the call button. If this is the only configured contact, a short press of the lock button opens the door.

Alarm Call

- **Start Call With Doorbell Button**: Select to start a phone call to this device after someone presses the alarm call button. Set the doorbell alarm call function in **Hardware > Digital inputs > Doorbell button**.

Unlock Button Function

- **Name**: Enter a name for the unlock button.
- **Lift**: Select to display the door lock/lift lock button icon.
- **Unlock Code**: The unlock code is used to remotely unlock a door. Make sure that the code includes at least two characters to unlock a door through an intercom keypad and at least one character to unlock the door through DTMF on a phone. The supported characters include * and #. We recommend to use at least four characters.

Time profiles

Set time profiles and assign them to the do not disturb mode to define when the mode is available.

1, 2, 3, 4... : The different profiles. Click to open a profile. You can create up to 20 profiles.

Basic settings

- **Profile name**: Enter the name of the profile.

Profile Time Sheet: Click and drag in the timeline to create blue bars that show when the do not disturb mode is allowed. If you have configured holidays, the **Holiday** row is applied regardless of the day in the week.

To set a time profile, go to **Calls > General settings > Incoming calls** and select the profile in **Do Not Disturb Mode With Time Profile**.

Holidays

Set the time span for holidays, such as Sundays and public holidays.

To set holidays for the next 10 years, select a year at the top of the screen. To select or deselect holidays, use the yearly calendar.

Fixed annual holidays are marked in green, and holidays that vary from year to year are blue. To manage holidays, click on a date once to add a fixed holiday, and click twice to add a variable one. To remove a holiday from your list, click three times.

Calling

General Settings

- **Call Time Limit**: Set a limit for the call in seconds. The device beeps 10 seconds before the call ends to signal that the call limit is approaching. To extend the call time during the call, enter any DTMF character. If the call time limit is set to 0 and SRTP isn't used, the call isn't time limited.

Incoming Calls

- **Call Answering Mode (SIP 1 and 2)**: Select how to handle incoming calls. You can set the call receiving mode for each SIP account separately. The following three options are available:
  - **Always Busy**: The device rejects incoming calls.
  - **Manual Pickup**: The device rings to signal incoming calls and the user can press a button to answer.
  - **Automatic**: The device automatically answers incoming calls.
- **Local Call Receiving Mode**: Select how to handle incoming local calls. The following three options are available:
  - **Always Busy**: The device rejects incoming calls.
  - **Manual Pickup**: The device rings to signal incoming calls and the user can press a button to answer.
  - **Automatic**: The device automatically answers incoming calls.
- **Voicemail Mode**: Select if you want to use voicemail or not when a is unanswered. The following three options are available:
  - **OFF**: The call is terminated if unanswered.
  - **Away Message Only**: The device plays a prerecorded message if the call is unanswered.
  - **Video Voicemail**: The device plays a prerecorded message and allows the caller to record a message for 20 seconds.
- **Pick Up In**: Enter the time in seconds before the device automatically picks up the call. This option is only available if you have selected **Automatic** as call answering or local call receiving mode.
- **Reject Calls in DND Mode**: Select to automatically reject calls in the do not disturb mode. You can use this option for immediate call redirection, for example to a mobile phone call.
- **Mute Doorbell in DND Mode**: Select to mute all calls from the doorbell.
- **Do Not Disturb Mode with Time Profile**: Select to use predefined time profiles, or manually select an individual time profile. Create time profiles in **Directory > Time profiles**.

Outgoing calls

- **Connection Time Limit**: Set the time, in seconds, for how long the device should try to connect to the network before it terminates the outgoing call. We recommend to set more than 20 seconds if you connect to the GSM network through GSM gateways.
- **Ring time limit**: Set the time, in seconds, before the device terminates an unanswered outgoing call. Set the time to more than 20 seconds if you connect to the GSM network through GSM gateways. Minimum value: 1 s, maximum value: 600 s. Set 0 to disable the time parameter.

Call Log

- **Save Image During Call**: Automatically takes one or more snapshots from each video call and save them into the call log.

Note

When you clear the **Save Image During Call** option, the system deletes all snapshots but keeps the call logs.

- **Automatic Image Count**: Select the amount of snapshots the device should take and save during a call.

Advanced Settings

- **Starting RTP Port**: Set the initial local RTP port in the range of 64 ports used for audio and video transmission. The default value is 4900 (which means the range will be 4900–4963). The parameter applies to both SIP accounts.
- **RTP Timeout**: Set the time, in seconds, to receive audio stream RTP packets during a call. If this limit is exceeded (no RTP packets are received), the device terminates the call. Enter 0 to disable this option. The option applies to both SIP accounts.
- **Extended SIP Logging**: Allow the syslog to record SIP telephony details for troubleshooting purposes.

SIP

Use SIP to set up, terminate, and forward calls between two SIP devices, for example an intercom and an answering unit. SIP devices can establish connections directly with each other, through direct SIP calls, or through one or more servers.

Configuration

You can configure two SIP accounts on this device; **SIP 1** and **SIP 2**.

SIP Accound Enabled: Select to be able to make outgoing calls and receive incoming calls from the device's SIP accounts.

Device Identity

- **Display Name**: The name that shows on the receiver's phone.
- **Phone Number (ID)**: Set your device phone number, or another unique ID that consists of characters or digits. Together with the domain, this number uniquely identifies the device in calls and registration.
- **Domain**: Set the domain name of the service with which the device is registered. Typically, it's the same as the SIP Proxy or Registrar address.
- **Test Call**: Make a test call to a selected phone number.

Authentication

- **Authentication ID**: Enter the alternative user ID for device authentication.
- **Password**: Set the device authentication password. If your PBX doesn't require authentication, the password will not be applied.

SIP Proxy

The IP network server responsible for call routing. There can be one or more SIP Proxy units between the users.

- **Proxy Address**: Set the SIP Proxy IP address or domain name.
- **Proxy Port**: Set the SIP Proxy port, typically 5060. Leave the field empty to use the default port.
- **Backup Proxy Address**: Set the backup SIP Proxy IP address or domain name. The address is used if the main proxy fails to respond to requests.
- **Backup Proxy Port**: Set the backup SIP Proxy port, typically 5060. Leave the field empty to use the default port.

SIP Registrar

The IP network server responsible for user registration in a certain network section. As a rule, SIP device registration is necessary for a user to be accessible to the others on a certain phone number. SIP Registrar and SIP Proxy are often installed on the same server.

- **Registration Enabled**: Enable to use device registration with the set SIP Registrar.
- **Registrar address**: Set the SIP Registrar IP address or domain name.
- **Registrar Port**: Set the SIP Registrar port, typically 5060. Leave the field empty to use the default port.
- **Backup Registrar Address**: Set the backup SIP Registrar IP address or domain name. The address is used if the main Registrar fails to respond to requests.
- **Backup Registrar Port**: Set the backup SIP registrar port, typically 5060. Leave the field empty to use the default port.
- **Registration Expiry**: Set the expiry time in seconds. The SIP Registrar can change the expiry time without letting you know.
- **Registration State**: Shows if the device is registered or not.
- **Failure Reason**: Shows the reason for the last failed registration attempt.

Advanced Settings

- **SIP Transport Protocol**: Set the SIP communication protocol. Choose between UDP (default), TCP, or TLS.
- **Lowest Allowed TLS Version**: Set the lowest TLS version that the device accepts for connection.
- **Verify Server Certificate**: Verifies the SIP server public certificate against the CA certificates in the device.

- **Client Certificate**: Specify the client certificate and private key used to verify the intercom's authority to communicate with the SIP server.
- **Local SIP Port**: Set the local port for the device for SIP signaling. If you change this value, it doesn't take effect until you restart the device. The default value is 5060.
- **PRACK Enabled**: Enable the PRACK method for reliable confirmation of SIP messages with codes 101–199.
- **REFER Enabled**: Enable the SIP REFER method for call transfer.
- **Send KeepAlive Packets**: Set if you want the device to send STUN/CRLF packets to the registrar at regular intervals and SIP OPTIONS during calls to keep the setup connection active.
- **IP Address Filter Enabled**: Blocks SIP packets from addresses other than a SIP Proxy and SIP Registrar, which helps to improve communication security and to prevent unauthorized phone calls.
- **Receive Encrypted Calls Only (SRTP)**: Set if you only want to receive SRTP-encrypted calls to this account, and reject unencrypted calls. For enhanced security, we recommend that you also use TLS as the SIP transport protocol.
- **Encrypted Outgoing Calls (SRTP)**: Set if you want the outgoing calls from this account to be SRTP encrypted. For enhanced security, we recommend that you also use TLS as the SIP transport protocol.
- **Use MKI in SRTP Packets**: Use MKI (Master Key Identifier) if your counterpart requires it for identifying the master key when multiple keys are rotated in the SRTP packets.
- **Adaptive Control of Video Quality**: Allow the use of the extended RTP profile for feedback via RTCP (RTP/AVPF), and the use of interactive video quality control according to RFC-4585. This lets you adapt the video data flow to match the current network connection quality.
- **Do Not Play Incoming Early Media**: Prevents the playing of the incoming audio stream from a PBX or other device before the call is picked up (early media). A standard local ringtone plays instead.
- **QoS DSCP Value**: Set the SIP packet priority in the network as a decimal value. This value is sent in the Type of Service (TOS) field in the IP packet header. If you change this value, it doesn't take effect until you restart the device.
- **STUN Enabled**: Allow the use of addresses and ports acquired from the configured STUN server in SIP headers and SDP media negotiation.
- **STUN server address**: Set the IP address of the STUN server used for this SIP account.
- **STUN server port**: Set the port of the STUN server used for this SIP account.
- **External IP Address**: Enter the public IP address or hostname of the router that your device is connected to. If your device has a public IP address, you can leave this field blank.
- **Compatibility With Broadsoft Devices**: Set the Broadsoft PBX compatibility mode. After you receive a re-invite from a PBX in this mode, the answering unit responds by repeating the last sent SDP with currently used codecs, instead of sending a complete offer.
- **Rotate SRV Records**: Allow SRV record rotation for SIP Proxy and Registrar. This is an alternative way to switch to backup servers if the main server fails or becomes unavailable.

Video

Video Codecs

- **Codec**: The name of the video codec.
- **Enabled**: Select to enable the video codec.
- **Priority**: Set the priority for the video codec.

Extended Codec Settings

- **Profile**: The available video codec profiles.
- **Enabled**: Enable the packetization mode. The payload type can be selected automatically in case it can't be set manually.
- **SDP Payload Type**: Set the payload type for video codec H.264 (packetization mode 1). Set a value between 96 and 127, or set to 0 to disable this codec type.

Audio

Audio Codecs

- **Codec**: The name of the audio codecs in the list.
- **Enabled**: Select to enable the audio codecs in the list.
- **Priority**: Set the priority for the audio codecs in the list.

DTMF Sending

This section helps you define how the device should send DTMF characters. Check the receiver's DTMF receiving options and settings to make sure DTMF sending works as expected.

- **In-Band (Audio)**: Use the classic method of sending DTMF in the audio band using standardized dual tones.
- **RTP (RFC-2833)**: Send DTMF through RTP according to RFC-2833.
- **SIP INFO (RFC-2976)**: Send DTMF through SIP INFO messages according to RFC-2976.

DTMF Receiving

This section helps you define how to receive DTMF characters from an intercom. Check the sender's DTMF sending options and settings to make sure the device can receive DTMF as expected.

- **In-Band (Audio)**: Use the classic DTMF dual tone receiving in the audio band.
- **RTP (RFC-2833)**: Use DTMF receiving via RTP according to RFC-2833.
- **SIP INFO (RFC-2976)**: Use DTMF receiving via SIP INFO messages according to RFC-2976.

Transmission Quality Settings

- **QoS DSCP Value**: Set the audio RTP packet priority in the network. The set value is sent in the TOS (Type of Service) field in the IP packet header.
- **Jitter Compensation**: Select the buffer length to compensate for uneven intervals in audio packet arrivals. Set a higher value to increase the receiving immunity at the cost of a higher sound delay.

Local calls

Configuration

Local Calls Enabled: Allows local calls between 2N devices and AXIS I5304 Network Answering Unit in the LAN. If you turn off local calls, the other devices in the LAN can't call the device using the format device:device_ID.

Network Identification

- **Device ID**: Set the device ID to be displayed in the LAN device list for other devices on the same LAN. To direct a call to this device, enter the user phone number as device:device_ID in those devices.
- **Test Call**: Make a test call to a selected phone number.

Connection to Intercoms

- **Access Key 1, 2**: Set the access key that 2N answering units, intercoms and AXIS I5304 Network Answering Unit share. Make sure the keys match. If they don't, the devices can't communicate.

Connection to Answering Units

- **Access Key**: Set the access key that 2N answering units, intercoms and AXIS I5304 Network Answering Unit share. Make sure the keys match. If they don't, the devices can't communicate.
- **Multicast Address**: Set network multicast address to which the answering unit messages will be sent.

LAN Devices

- **LAN Device Count**: Shows the number of local devices in the network.
- **Show LAN device List**: Click **Show** to show a detailed list of local devices in the network.

Audio

DTMF Sending

- **In-Band (Audio)**: Use the classic method of sending DTMF in the audio band using standardized dual tones.
- **RTP (RFC-2833)**: Send DTMF through RTP according to RFC-2833.
- **SIP INFO (RFC-2976)**: Send DTMF through SIP INFO messages according to RFC-2976.

DTMF Receiving

- **In-Band (Audio)**: Use the classic DTMF dual tone receiving in the audio band.
- **RTP (RFC-2833)**: Use DTMF receiving via RTP according to RFC-2833.
- **SIP INFO (RFC-2976)**: Use DTMF receiving via SIP INFO messages according to RFC-2976.

Transmission Quality Settings

- **Jitter Compensation**: Select the buffer length to compensate for uneven intervals in audio packet arrivals. Set a higher value to increase the receiving immunity at the cost of a higher sound delay.

Services

Unlocking

Unlocking Settings

- **Default Unlock Code**: Use the default code for calls with a device/phone number that isn't in the unit phone book.
- **Hang Up After Door Unlocking**: Ends the call after the door unlocking request has been sent successfully.
- **Hang-Up Delay**: Set a delay time for ending the call. When the unlocking request has been sent, the device ends the call after the set time.
- **Show Door Open Sensor**: Shows the state of the intercom's door open sensor.

HTTP command

Create buttons that appear on the display's home screen, during calls, and in the camera preview.

The HTTP command settings are the same for **home screen**, **in-call** and **external camera**.

- **Command**: You can set up to three commands for each button display.
- **URL**: Set the HTTP command to send to an external device when you press a button. The command format is http://ip-address/path, for example http://192.168.1.50/relay1=on. Set the parameter to 0 if you don't want to send the command.
- **Icon**: Select the HTTP command button icon.
- **Name**: Enter a name for the HTTP command.
- **Username**: Set the username for the HTTP commands sent during switch activation or deactivation. You only need to set this if authentication is required.
- **Password**: Set the password for the HTTP commands sent during switch activation or deactivation.

User sounds

Sound mapping

Sound message language: Select a language for spoken messages. If a translation is available for a mapped sound, the message plays in the specified language. Otherwise, it plays in English or as a language-neutral sound.

Sound mapping

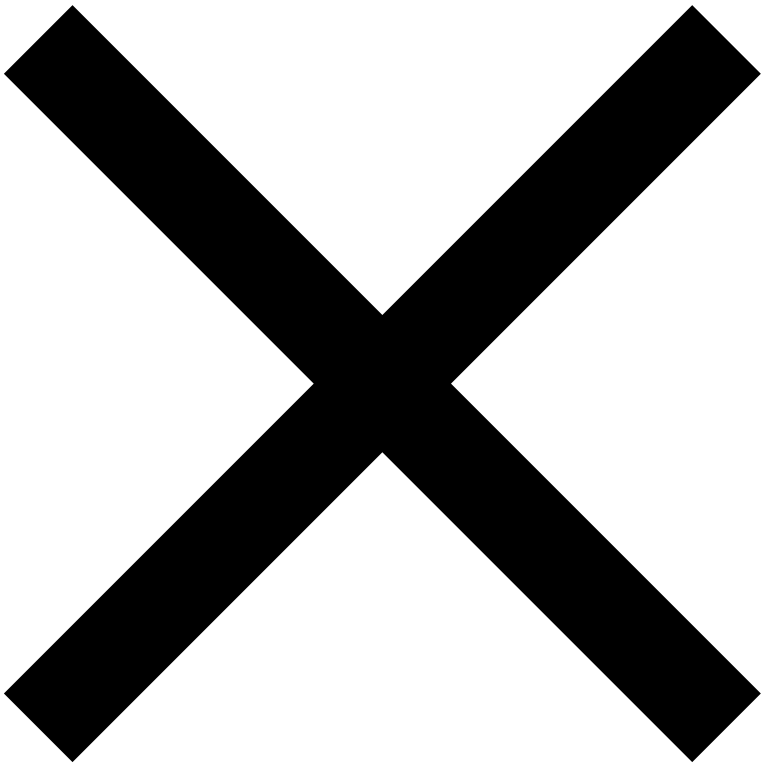
- **Busy Tone**: Select a tone to play when the called user is busy.
- **Call End Signaling**: Select a sound to play when a call ends.
- **Ringtone**: Select a ring-back tone to play when the called user is ringing.
- **Ringing Before Call Answering**: Select a ringtone sound to play before an incoming call is answered.
- **Doorbell**: Select a sound to play when someone presses the doorbell button.
- **Out-of-office message**: Select a message to play when a call is unanswered.
- ▷: Click to play the sound of your choice.

Sound upload

Sound upload

You can add up to 10 audio files to the device.

- **Name**: Add a name for the audio file to find it easier.
- **Size**: The size of the uploaded audio file.
- : Click to play an uploaded audio file locally on your PC.



- : Click to remove a file.
- : Click to record a sound that you can use in the **Sound Mapping** tab.
- : Click to upload an audio file to the device that you can use in the **Sound Mapping** tab.

Web server

Basic Settings

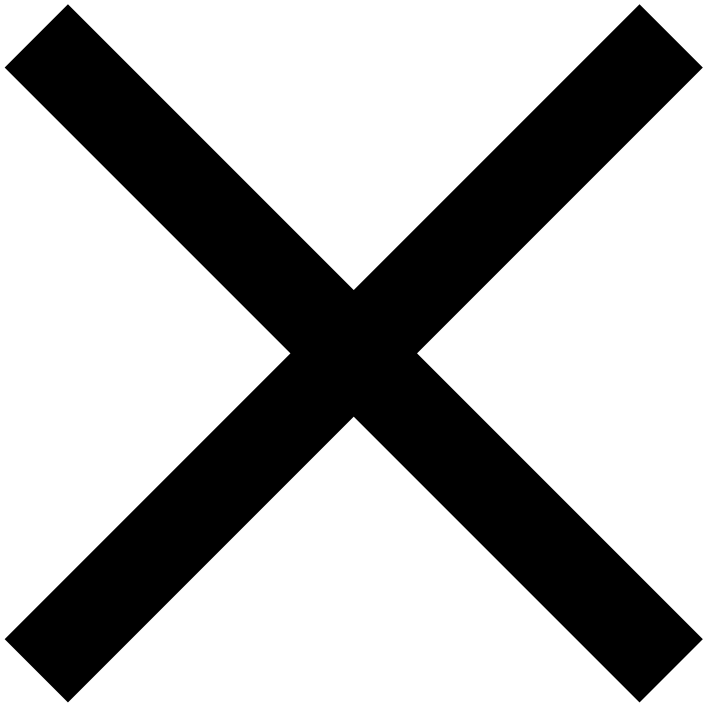
- **Device Name**: Set the name to display in the device web interface, login window, and in other applications.
- **Web Interface Language**: Set the default language for the administration web server login.
- **Password**: Set the device password. Click to change the password. The password must contain at least 8 characters, including one lowercase letter, one uppercase letter, and one digit.

Advanced Settings

- **HTTP Port**: Set the web server port for HTTP communication. If you change this value, it doesn't take effect until you restart the device.
- **HTTPS Port**: Set the web server port for HTTPS communication. If you change this value, it doesn't take effect until you restart the device.
- **Lowest Allowed TLS Version**: Set the lowest TLS version that your device accepts for connections.
- **HTTPS Server Certificate**: Select the server certificate and private key you want to use for encrypting the communication between your device's HTTPS server and the user's web browser.
- **Remote Access Enabled**: Enable remote access to your device's web server from off-LAN IP addresses.

User Localization

- **Original Language**: Click to download the original XML file from your device, which includes all user interface texts in English.
- **Custom Language**:

- Click 

  to remove custom language files including translations of the user interface texts.
- Click to download custom language files including translations of the user interface texts.
- Click to upload custom language files including translations of the user interface texts.

Weather

Settings

- **Show Weather**: Select to allow the device to show the current weather information on the display home screen.
- **Location**: Set the location of the device for the weather forecast. If you select **Show Weather** and leave **Location** empty, the weather for Prague is shown by default.
- **Location Shown**: Enter the name of the location you want to show with the weather information. If you leave it empty, the name of the location for the weather forecast is shown.
- **Temperature Units**: Select if you want to show the temperature in °C or °F.

Results

- **Last Update**: Shows the date of the last server data update.
- **Location Found**: Shows the weather forecast location found by the weather service.
- **Country**: Shows the country of the location you have entered, or the default location.

Hardware

Audio

Phone Call Volume

- **Call Volume**: Select the volume for phone calls.
- **Ringtone Volume**: Select the volume of the incoming call ringtone, which is relative to the master volume.
- **Call-Progress Tone Volume**: Select the volume levels for the dial tone, ringtone, and busy tone. However, if your PBX automatically generates call progress tones, this setting won't apply.

Signaling Volume

- **Warning Tone Volume**: Select the volume for warning and signaling tones, which is relative to the master volume.
- **Suppress Waning Tones**: Suppress signaling for the following operational states: **Internal application started**, **IP address received**, and **IP address lost**.
- **User Sounds Volume**: Select the volume for user sounds played by automation, which is relative to the master volume.

Camera

Note

You can configure up to 16 external cameras for video call streaming. The answering unit lets you use RTSP streams from standard IP video cameras that meet the following requirements:

- H.264 or MJPEG video codec
- Resolutions up to 1280x720
- Maximum frame rate of 30 fps for H.264, or 15 fps for MJPEG
- High profile with 5000 kbps for the H.264 codec

1, 2, 3, 4... : The configuration pages for the external IP cameras you can assign to devices in your network. You can assign up to 16 cameras. Click to open a page.

Camera Enabled: Allow the answering unit to use RTSP streams from external IP cameras.

Camera Assignment:

- Click + to open the device list, then select the devices you want to assign a camera to. During a call with one of those devices, you can show the selected camera's preview on the answering unit and switch between previews of other assigned and allowed cameras.
- Click ✕ to remove all devices you have assigned to the selected camera.

Settings

- **Display name**: Set the name you want to display at the camera preview in the directory of your device. If you leave this field empty, the default name for the selected language will appear instead.
- **RTSP Stream Address**: Enter the IP camera's RTSP stream IP address in the format rtsp://camera_ip_address/parameter1=value&parameter2=value. See the parameter table below for examples. The parameters are specific for the selected IP camera model.

Parameter	Description	Example/Values
audio	audio	– –
fps	frame rate	`fps=15`
vbr	video bitrate	`vbr=768` for 768 kbps
vcodec	video codec	`vcodec=h264` for H.264 `vcodec=mjpeg` for codec MJPEG
vres	video resolution	`vres=1920x1080` for FullHD
zipstream	zipstream	– – – – –

- **Username**: Enter the username for connecting to the external IP camera. This is only required if the camera needs authentication.
- **Password**: Enter the password for connecting to the external IP camera.
- **Local RTP Port**: Specify the local UTP port for receiving RTP streams.
- **State**: Shows the current connection status to the external IP camera.
- **Stream**: Shows the parameters of the received stream.

Camera Preview

Shows the current image from an external camera. If the camera is disconnected or not set up correctly, it displays **N/A** on a black background.

External IP Camera Log

Shows the RTSP communication with the selected external IP camera, including any failures or error states that may occur.

Display

Basic Settings

- **Language**: Select the language for the display. Choose from predefined languages or select a custom language from a language file that you have previously uploaded. For information about uploading a language file, see .
- **Date Format**: Select the date format for the display.
- **Time Format**: Select the time format for the display.
- **Enable Screen Lock**: Turn on the screen lock when the device is in idle mode.
- **Screen Lock PIN**: Set a four-digit code to unlock the screen. Use numbers from 1 to 9.
- **Advanced Settings Code**: Set an access code for the **Advanced Settings** on the display. If you don't enter a code, you won't be able to open the advanced settings on the device display.
- **Device mode**: Select the **Hotel** or **Normal** mode.
  - In **Hotel** mode, your device has a simpler user interface and some features work differently than they do in normal mode. Your device lets you call one preset contact and receive incoming calls. It also shows the time and weather. However, most other features are limited. You can't set the do not disturb mode from the device, and you can't access the directory, call log, or settings menus. Additionally, you won't have quick access to weather settings, and you won't see notifications about missed calls, door contact states, and more.
- **Display Setting Menu**: Show and access the **Setting** menu on the display. If you deactivate **Display Setting Menu**, you can only configure the device via the web and remote access.
- **Display Time In Idle Mode**: Select to allow the device to show time in idle mode.

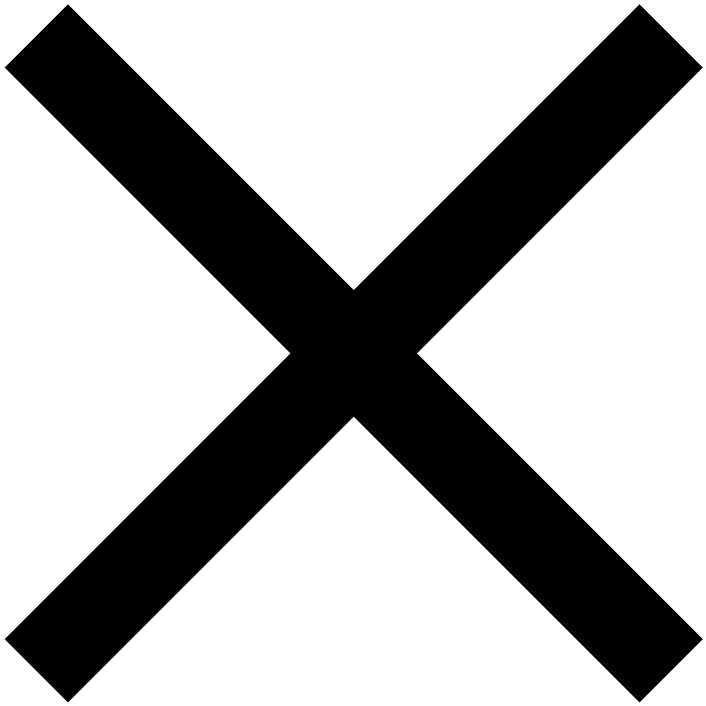
Backlight

- **Intensity in Active Mode**: Set the backlight brightness level. Select a value as a percentage of the maximum possible brightness.
- **Lower Intensity in Idle Mode To**: Set the level of reduction for the backlight intensity when the device goes into idle mode.
- **Go to Idle Mode In**: Set the inactivity timeout period after which your device switches to idle mode.

User Localization

- **Original Language**: Click  to download a localization file template, which is an XML file containing all the English texts to be displayed. Use the template when you create your own translation.
- **Custom Language**:

– Click



to remove your localization file.

– Click to download your localization file.

– Click to upload your localization file.

Digital inputs

Doorbell Button

- **Doorbell Button Function**: Select a doorbell function. The button is used either as a classical doorbell or for alarm call activation.
- **Camera Assigned to Doorbell**: Select the external camera to display when the doorbell rings. The camera preview will not interrupt an active call or ringing. To return to the call or ringing, tap the green bar at the top of the display. If you don't confirm the doorbell, a warning will appear on your device and a record will be added to the call log.

System

Network

Basic

Use DHCP server: Select to automatically obtain the IP address from the LAN DHCP server. If no DHCP server exists or is available in the network, set the network manually.

Static IP Address Setting

- **Static IP Address**: Enter the static IP address of the device.
- **Network Mask**: Enter the network mask (also known as a subnet mask).
- **Default Gateway**: Enter the default gateway address for off-LAN communication.

DNS Setting

- **Always Use Manual Setting**: Select to manually set the DNS server addresses.
- **Primary DNS**: Enter a primary DNS server address for the translation of domain names to IP addresses.
- **Secondary DNS**: Enter a secondary DNS address to use if the primary DNS is unavailable.

Network Identification

- **Hostname**: Set the device LAN identification.
- **Vendor Class Identifier**: Set the manufacturer identifier as a character string for DHCP Option 60.

VLAN Settings

- **VLAN Enabled**: Select if you want to use virtual network support (VLAN according to 802.1q). Remember to also set the VLAN ID.
- **VLAN ID**: Enter a VLAN ID from the range of 1–4094. The device can only receive packets with the set ID. Be aware that an incorrect setting can cause a connection loss.

Network Interface Settings

- **Required Port Mode**: Select the preferred network interface port mode; **Automatically** or **Half Duplex – 10 Mbps**. If the available LAN cabling isn't reliable enough for 100 Mbps traffic, the bit rate is reduced to 10 Mbps.
- **Advertised Modes**: Select the modes to advertise during auto-negotiation.
- **Current Port State**: Shows the current LAN port state.

802.1x

Device Identity

- **Device identity**: Enter the username for authentication through EAP-MD5 and EAP-TLS.

MD5 Authentication

- **Authentication enabled**: Use the 802.1x EAP-MD5 protocol for network device authentication. If the network doesn't support 802.1x and you select this option, your device will become unavailable.
- **Password**: Enter the access password for EAP-MD5 authentication.

TLS Authentication

- **Authentication enabled**: Use the 802.1x EAP-TLS protocol for network device authentication. If the network doesn't support 802.1x and you select this option, your device will become unavailable.
- **Trusted Certificate**: Select a trusted certificate to verify the validity of the RADIUS server's public certificate. If you don't include a trusted certificate, the RADIUS public certificate won't be verified.
- **Client certificate**: Select a user certificate and private key to verify the answering unit authorization to communicate through the 802.1x-secured network element port in the LAN.

PEAP MSCHAPv2 authentication

- **Authentication Allowed**: Use the 802.1x PEAP MSCHAPv2 protocol for network device authentication. If the network doesn't support 802.1x and you select this option, your device will become unavailable.
- **Trusted Certificate**: Select a trusted certificate to verify the validity of the RADIUS server's public certificate. If you don't include a trusted certificate, the RADIUS public certificate won't be verified.
- **Password**: Enter the access password for PEAP-MSCHAPv2 authentication.

Date & time

The answering unit is equipped with a real time clock without power outage backup.

Note

Your device doesn't require the current date and time values for its basic functionality. However, having accurate date and time values is crucial for features like time profiles and ensuring correct event timestamps in logs, such as those from Syslog, card entries, and logs retrieved through the HTTP API.

Current Time

- **Use Time From the Internet**: Select to synchronize the device time with the Internet.

Important

We recommend that you select **Use time from Internet** for maximum accuracy and reliability. The device time error can be up to ±2 minutes per month under normal operation conditions.

- **Current Device Time**: The current time of the device.
- **Synchronize With Browser**: Click to synchronize the time with your current PC time.

Time Zone

- **Automatic Detection**: Select if you want to automatically detect the time zone from My2N. If you turn off this option, use the manual selection option to select a time zone manually or apply your own custom rule.
- **Detected Time Zone**: Shows the automatically detected time zone. If the function is unavailable or turned off, **N/A** appears.
- **Manual Selection**: Select your local time zone to define time shifts and the transition to and from daylight saving time.
- **Custom Rule**: Set a custom rule if your device is installed at a location that isn't listed in **Manual Selection**. Make sure to select **Custom Rule** from the **Manual Selection** drop-down menu..

NTP Server

- **NTP Server Address**: Enter the IP address or domain name of the NTP server that you want to use to synchronize your device's internal clock.
- **NTP Time Status**: Shows the stauts of the last local time synchronization attempt via NTP.

Features

Beta Features

The list contains published beta functions designed for user testing.

Important

The test functions are not warranted and Axis can't be held liable for any functionality limitations and damage incurred as a result of functionality limitations of the beta functions. The beta functions are provided for testing purposes exclusively.

- **Name**: The name of the function.
- **State**: The function status (started/stopped)
- **Action**: The event that starts/stops the function

The function status changes when you restart the device. Use the **Cancel** action before the device is restarted to cancel the status change request.

Certificates

Some LAN services use the TLS protocol to communicate securely with other LAN devices. This protocol protects against eavesdropping on, or modification of call content. TLS is based on one-way or two-way authentication, which requires certificates and private keys.

The following device services use TLS protocol:

- Web server (HTTPS)
- 802.1x (EAP-TLS)
- SIP

When powered up for the first time, your device automatically creates a self-signed certificate and private key for the web server and services, without forcing you to upload your own. You can upload up to three sets of certificates from certification authorities to authenticate communicating devices, and up to three user certificates and private keys for encryption purposes.

Each certificate requiring service can be assigned one certificate set and the certificates can be shared by the services. The device supports the DER (ASN1) and PEM certificate formats.

Note

If you use the self-signed certificate to encrypt the device's web server and browser communication, the communication is secure, but your browser will warn you that it can't verify the validity of the device certificate.

CA certificates

CA Certificates

- + : Click to upload a certificate stored on your local PC.
  - **Certificate ID**: Enter the certificate ID used for identification when selecting, modifying, or deleting certificates.
  - **Select File...**: Click to browse and select a file from your PC.
  - **Upload**: Click to upload the certificate.
- : Click to delete one or more of the certificates from the device.
- : Click to read more about the selected certificate in the list.

User certificates

User Certificates

- + : Click to upload a certificate stored on your local PC.
  - **Certificate ID**: Enter the certificate ID used for identification when selecting, modifying, or deleting certificates.
  - **User Certificate**
    - **Select File...**: Click to browse and select a file from your PC.
  - **Private Key**
    - **Select File...**: Click to browse and select a file from your PC.
  - **Private Key Password**: Enter the password if this is required for authentication of the private key.
  - **Upload**: Click to upload the certificate and private key.
- : Click to delete one or more of the certificates from the device.
- : Click to read more about the selected certificate in the list.

Auto provisioning

My2N

My2N Enabled: Enable connection to My2N. You can use the My2N cloud platform to access the device's web interface remotely and to remotely administer and configure 2N IP devices.

My2N Security Code

- **Serial Number**: Shows the serial number of the device that the valid My2N code applies to.
- **My2N Security Code**: Shows the code for adding the device to My2N.
- **Generate New**: Click to make the current My2N security code inactive, and generate a new one.

Connection State

Shows status messages for the connection to My2N.

- **My2N ID**: Shows the unique identifier of the company created in the My2N portal.

TR069

Use this tab to enable and configure remote device management through the TR-069 protocol.

My2N / TR069 Enabled: Enable this option to connect to My2N or another auto configuration server (ACS).

General Settings

- **Active Profile**: Select a pre-defined profile, or select **Custom Setting** and configure the auto configuration server (ACS) connection manually.
- **Next Synchronization In**: Shows the time for the next synchronization with the remote ACS.
- **Connection State**: Shows the current status of the connection to the ACS.
- **Communication Status Detail**: Shows the server communication error code or HTTP status code.
- **Connection test**: Click to test the TR069 connection according to the set profile. You can see the result of the test in **Connection State**.

Diagnostics

Diagnostics Package

Shows information about packet and syslog capture, such as status, packet size,

- **Packet Capture Status**: Shows if packet capture has been started in the **Packet Capture** tab.
- **Size of Captured Packets**: Shows the size of the captured packets.
- **Syslog Capture State**: Shows if Syslog message capture has been started in the **Syslog** tab.
- **Duration of Captured Syslogs**: Shows how long Syslog messages are captured in the **Syslog** tab.
- **Size of Captured Syslogs**: Shows the size of the captured Syslog messages.
- **Stop Syslog Capture**: Set the packet capture time.
- **Diagnostics Package Control**
  - : Start to capture diagnostic data. Restarts packet capture if already running.
  - : Download a zip file of the captured diagnostics data.

Tools

- **Ping**: Click and enter the IP address in the **Address** field. Click **Ping** again to send test data to the IP address.

Packet capture

Local Packet Capture

- **Current State**: Shows if the local packet capture has been started or stopped.
- **Buffer size**: Shows the size of the available buffer.
- **Buffer Utilization**: Shows how much of the buffer you use.
- **Number of Captured Packets**: Shows the amount of captured packets.
- **Packet Capture Control**
  - : Click to start local packet capturing. If already running, it restarts packet capturing.
  - : Click to stop capturing.
  - : Click to download the packet capture file.

Remote Packet Capture

- **Current State**: Shows if the remote packet capture has been started or stopped.
- **Count of Sent Packets**: Shows the amount of sent packets.
- **Count of Sent Bytes**: Shows the size of the sent packets.
- **Remaining Time**: Shows the remaining capture time.
- **Packet Capture Control**
  - : Click to start remote packet capturing. In the dialog, set the incoming/outgoing packet capturing time (in seconds). Click **OK** to start capturing.
  - : Stop capturing.

Syslog

Syslog Server Settings

- **Send Syslog Messages**: Select to send syslog messages to the Syslog server. Make sure that the server address is valid.
- **Server Address**: Enter the IP or MAC address of the server that runs the Syslog application.
- **Severity Level**: Select the severity level of the messages to be sent. The **Debug 1–3** setting is only recommended to facilitate troubleshooting for the Technical Support department.

Local Syslog Messages

Shows a general status overview of the local Syslog messages, such as if messages are being saved, and the size of the Syslog messages.

- **Required Saving Time**: Select how long the Syslog messages should be saved.
- **Syslog Messages Saving Control**
  - : Click to start saving Syslog messages.
  - : Click to stop saving Syslog messages.
  - : Click to download Syslog messages.
  - : Click to delete the locally saved Syslog messages in the device.

Maintenance

Configuration

- **Upload Configuration File to Device**: Click **Restore Configuration** to restore the configuration from a previous backup. In the dialog that opens, select a configuration file and upload it to your device. Before uploading, decide whether to apply the LAN settings and SIP PBX connection settings.

Important

The login password is stored in the configuration file. If the password isn't encoded in the file, or if you use the default password (2n), only the valid parts of the configuration will be uploaded and your password won't change.

- **Download Configuration File from Device**: Click **Back Up Configuration** to back up your device's complete current configuration. This downloads the entire configuration to your storage.

Note

Handle the configuration file with care, as it might contain sensitive information like user phone numbers and access passwords.

- **Reset Configuration to Default State**: Click **Reset Configuration** to reset all settings in the device, except for the LAN settings. For a full reset, including the LAN settings, reset the device using the RESET button. For more information, see .

System

Shows a general overview of the device software, such as version and the date for the build.

- **Upgrade Device Firmware**: Click **Upgrade Firmware** and select a firmware file to upload in the dialog that appears. Once the upload is successful, the device restarts automatically. The process typically takes less than a minute and doesn't affect the configuration.
  You can find the latest firmware version for your device on *axis.com/support/device-software*. The device checks the firmware file, and prevents you from uploading an incorrect or corrupt file.
- **Firmware Status**: Shows whether a newer firmware version is available. If a new version is available, click **Upgrade Now** to upgrade. If the device can't find a new version, click **Check Now** to check for new versions.
- **Notify of Beta Versions**: Select this option to monitor and download the latest firmware beta version.
- **Restart Device**: Click to restart the device, which takes approximately 30 seconds. Once the restart is complete and the device has been assigned an IP address, the login window appears automatically.
- **Third Party Library License**: Click **Show** to view a dialog listing the used licenses and third-party libraries, along with a link to the End User License Agreement (EULA).

Usage Statistics

- **Send Anonymous Statistics Data**: Enable the sending of anonymous statistics on device usage to the manufacturer. Sensitive information, like passwords, access codes, or phone numbers, is not included. By sharing this data, you're helping the manufacturer to improve the quality, reliability, and performance of the software. Your participation is voluntary, and you can opt out of sending statistics at any time.

The display interface

Home screen

The home screen is the start screen of the device. If there's no activity, your device will automatically switch to idle mode after a set time.

Date and time: Shows the date and time for the given location.

: Shows the weather conditions in the given location.

: Do not disturb mode is active. The ringtone for incoming calls is silenced. Toggle to turn off.

: Do not disturb mode is inactive. Toggle to turn on.

CALL LOG : Tap to show the call log, which include all calls to and from the device. See for more information.

: Tap to go to your list of contacts and connected external cameras. See for more information.

SETTINGS: Tap to access the settings for the device, such as language and sounds. See for more information.

Call log

: Shows an outgoing call with information about date, time, and the receiver of the call.

: Shows an incoming call, with information about date, time, and the caller.

: Shows a missed call with information about date, time, and the caller.

: Click to show more information about the call, and if available, a camera preview.

DELETE ALL : Click to delete all calls in the log.

Directory

: Tap to call the selected contact.

: Tap to send a configured unlock code to the selected device. If the code is compatible with the selected device, its lock opens. If no unlock code is set, the default unlock code will be sent to the selected device.

: Tap to preview the selected device's video, if available.

: Tap to show your contacts in a row.

: Tap to show your contacts in a list.

Settings

Display: Tap to change the following settings:

- **Brightness**: Set the display backlight.
- **Screen timeout**: Set the time before the screen changes to idle mode.
- **Screen lock**: Turn the screen lock on or off. When you turn on the screen lock, you need to select a 4-digit pin code.

Sound: Tap to change the following settings:

- **Ringing volume**: Set the ringtone volume for incoming calls..
- **Call volume**: Set the speaker volume for incoming calls.
- **Ringtone**: Select a ringtone for incoming calls.
- **Doorbell tone**: Select a tone for the doorbell.
- **Voicemail**: Set your voicemail message directly in the device.
  - **Voicemail**: Turn off if you don't want to play a voicemail message. Unanswered calls will be terminated.
  - **Select recording**: Select a recording. You can either select a default voicemail message, or record a customized message.
  - **Default Recording Language**: If you have selected the default recording, which is a default voicemail message, set the language for the message.
  - **Enable visitor to leave message**: Turn on to allow callers to record a message that's stored in the device. After the voicemail message plays, a tone sounds, and recording begins for up to 20 seconds. The message captures both audio and video, depending on the capabilities of the calling device.
  - **Ring Time Before Voicemail Activation**: Set the timeout for incoming calls, after which the voicemail message plays.

Date and time: Tap to change the following settings:

- **Automatic date and time**: Turn on to retrieve date and time automatically from the network.
- **Set time zone**: Set your local time zone to define time shifts and the transition to and from daylight saving time.
- **Set date**: Set the date manually.
- **Set time**: Set the time manually.
- **Time format**: Select if you want to show a 12-hour clock or a 24-hour clock on the home screen.
- **Date format**: Set the format for the date you want to show on the home screen.

Language: Tap to select a language for the display interface. You can select one of eight predefined languages.

- **Custom language**: Tap to set a custom language from a language file that you have previously uploaded. For information about uploading a language file, see .

Do Not Disturb mode: Tap to change the following settings:

- **Do Not Disturb Mode**: Turn the do not disturb mode on or off. When turned on, incoming calls will be silenced. Per default, the doorbell tone will ring even if the do not disturb mode is turned on.
- **Reject Calls in DND Mode**: Turn on to reject incoming calls when the device is set to do not disturb mode.

- **Mute Doorbell in DND Mode**: Turn on to silence the doorbell when the device is set to do not disturb mode.

Weather: Tap to change the following settings:

- **Show Weather**: Turn on to show information about the weather on the home screen.
- **Location**: Set the location for the weather forecast.
- **Units**: Select if you want to show the temperature in °C or °F.

Advanced settings: Enter your access code to open the advanced settings. Set or change the access code in the device's web interface. For more information, see .

- **Network Settings**
  - **Use DHCP Server**: Turn on to allow the DHCP server to assign an IP address.
  - **Static IP Address Setting**: Set the static IP address, network mask and default gateway.
  - **Required Port Mode**: Select the preferred network interface port mode.
  - **Advertised Modes**: Select the modes to be advertised in auto-negotiation.

For more information about the network settings, see .

- **Restart device**: Tap to restart the device.

About: Tap to show the following details about the device:

- serial number
- software version
- MAC address
- IP address

Specifications

Product overview

Ports

Service	Port	Protocol	Direction	On by default	Configurable	Settings
802.1x	–	–	In/out	–	–	–
DHCP	68	UDP	In/out	x	–	–
DNS	53	TCP/UDP	In/out	x	–	–
Echo (device recovery)	8002	UDP	In/out	x	–	–
HTTP	80	TCP	In/out	x	x	
HTTPS	443	TCP	In/out	x	x	
Multicast audio for ICU protocol	8006	UDP	In	x	–	–
Multicast video for ICU protocol	8008	UDP	In	x	–	–
Multicast video (wide) for ICU protocol	8016	UDP	In	x	–	–
NTP client	123	UDP	In	x	–	–
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/out	–	x	
RTP+RTCP ports (external camera)	4800+ (range of 64 ports)	UDP	In/out	–	–	–
RTSP client	554	UDP	In/out	–	x	
SLP	427	UDP	In/out	x	–	–
SIP	5060, 5062	TCP/UDP	In/out	–	x	
SIPS	6061	TCP	In/out	–	x	
Syslog	514	UDP	Out	–	–	–
My2N Knocker	443	TCP	Out	x	–	–
My2N Tribble Tunnel	10080	TCP	Out	x	–	–
Unitchannel	8011	UDP	In/out	x	–	–

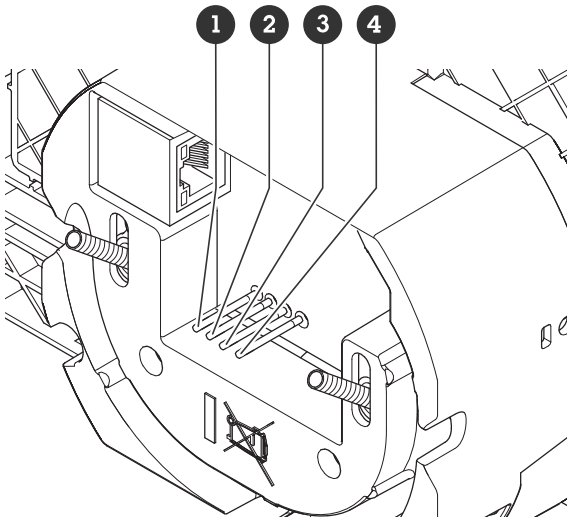
Service	Port	Protocol	Direction	On by default	Configurable	Settings
Sitechannel (ICU protocol)	8004	UDP	In/out	x	–	–
CWMP Stun	3478	UDP	Out	–	x	

Connectors

Network connector

RJ45 Ethernet connector with Power over Ethernet (PoE).

Power and doorbell connector



Function	Pin	Notes	Specification
0 V DC (-)	1	DC input	
12 V DC	2		1 A
Doorbell input	3	Switching contact (button/relay), normally open	
Doorbell input	4		

Induction loop connector

Line output for induction loop, 600 mV RMS.

Buttons

Reset button

The reset button has multiple functions. For more information, see:

-
-

-
-

Clean your device

You can clean your device with lukewarm water.

NOTICE

- Harsh chemicals can damage the device. Don't use chemicals such as window cleaner or acetone to clean your device.
- Avoid cleaning in direct sunlight or elevated temperatures, since this can cause stains.

1. Use a can of compressed air to remove dust and loose dirt from the device.
2. If necessary, clean the device with a soft microfiber cloth dampened with lukewarm water.
3. To avoid stains, dry the device with a clean, nonabrasive cloth.

Troubleshooting

Reset to factory default settings

You can reset the device to factory default settings through the web interface, or using the RESET button.

Important

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

Use the web interface:

1. Go to **System > Maintenance**.
2. Click **Reset Configuration**.

Use the RESET button:

1. Press and hold the RESET button.
2. Wait for the following to occur before you release the button.
   - 2.1. The red and green LEDs turn on at the same time and you hear the acoustic signal . This takes approximately 15 to 35 seconds.
   - 2.2. The red LED turns off and you hear the acoustic signal . This takes approximately another 3 seconds.
   - 2.3. The green LED turns off and the red LED turns on again, and you hear the acoustic signal  . This takes approximately another 3 seconds.
   - 2.4. The red LED turns off and you hear the acoustic signal . This takes approximately another 3 seconds.
3. Release the RESET button.

Restart the device

You can restart the device without changing the configuration in three different ways:

Use the web interface:

1. Go to **System > Maintenance > System**.
2. Click **Restart Device**.

The restart can take some time. When complete, the device shows the home screen on the display.

Use the device display:

1. Go to **Settings > Advanced settings**.
2. Enter your code to access the advanced settings.
   You can set the access code for the advanced settings in the device's web interface. For more information, see .
3. Tap **Restart Device**.
4. To confirm, tap **RESTART**.

Use the reset button:

1. Press the RESET button shortly, approximately 1 second.

Contact support

If you need more help, go to *axis.com/support*.

T10212854

2025-11 (M2.2)

© 2025 Axis Communications AB