AXIS A4611 Network Reader

User manual

Table of Contents

Installation

The following video shows an example of how you can install an AXIS A46 Network Reader Series.

For complete instructions on all installation scenarios and important safety information, see the installation guide for:

- AXIS A4610 on *axis.com/products/axis-a4610/support*
- AXIS A4611 on *axis.com/products/axis-a4611/support*
- AXIS A4612 on *axis.com/products/axis-a4612/support*

Get started

Find the device on the network

To find Axis devices on the network and assign them IP addresses in Windows®, use AXIS IP Utility. The application is free and can be downloaded from *axis.com/support*.

Note

The computer running AXIS IP Utility must be on the same network segment (physical subnet) as the Axis device.

1. Connect power and network to the Axis device.
2. Start AXIS IP Utility. All available devices on the network show up in the list automatically.
3. To access the device from a browser, double-click the name in the list.

Browser support

You can use the device with the following browsers:

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

✓: Recommended

*: Supported with limitations

Open the device's web interface

1. Open a browser and type the IP address or host name of the Axis device.
   If you do not know the IP address, use AXIS IP Utility to find the device on the network.
2. Type the default username `root` and password `pass`. If you access the device for the first time, you will be prompted to change the password and device name. See *The web interface, on page 7*.

For descriptions of all the controls and options in the device's web interface, see *The web interface, on page 7*.

Configure your device

The device works as a standard reader out-of-the-box. 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 must be assigned a valid IP address or obtain the IP address from the LAN DCHP server. Configure the IP address and DHCP in the web interface.

To manually configure the IP address:

1. Go to **System** > **Network connection** > **Basic configuration**
2. Under **IP address settings**, turn on **Use DHCP Server** to automatically get the IP address from the LAN DHCP server.
3. Enter the **IP address**, **Network mask** and **Default gateway**.
4. Turn on **Always use manual DNS settings** to use manual DNS settings.
5. Enter the **Primary DNS** and **Secondary DNS**.
6. Enter the **Hostname** and **Vendor Class Identifier** to identify the device.
7. Select an option for **Required port mode**.

To find your current IP address:

Note

- The configuration remains the same when you restart your device.

1. Open your device and press the control button for approximately 15 seconds until the back LED indicator turn red and green simultaneously and you hear one short beep.
2. Release the control button and the device announces the current IP address through the speaker.

Upgrade the device software

We recommend that you upgrade the device software when you login to the device for the first time. Download the latest version for your device from *axis.com/support*. To upload the new version:

1. Go to **System** > **Maintenance**.
2. Click **Firmware upload** and select the software version you downloaded.
3. Click **Upload**.

Note

The device restarts after the upload to complete the upgrade.

Upload CA and user certificates

Note

- The certificate ID shouldn't be longer than 40 characters and should contain only small and capital letters, numbers, and the _ and – characters.
- 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.

To upload a CA certificate:

1. Go to **System** > **Certificates** > **CA Certificates**.
2. Click + **Upload**.

3. Enter a **Certificate ID**.
4. Click **Select file** to upload a CA certificate.
5. Click **Upload**.

To upload a user certificate:

1. Go to **System** > **Certificates** > **User Certificates**.
2. Click + **Upload** to upload a certificate or private key.
3. Enter a **Certificate ID**.
4. Click **Select file** to upload a user certificate and a private key..
5. If you upload a private key, enter the **Default Key Password** if there is one.
6. Click **Upload**.

Note

You need to connect the reader in the door controller's web interface. See the door controller's user manual.

The web interface

Note

Support for the features and settings described in this section varies between devices. This icon indicates that the feature or setting is only available in some devices.

Access the device's new notifications.

The user menu contains:

- **Device time**: Current time on the device.
- **Change language**: Change the language.
- **Change password**: Change the password required to log in to the device.
- **Help**: Access the product help.
- **About**: View product information, including firmware version and serial number.
- **Log out**: Log out from the current account.

Dashboard

The context menu contains:

- **Rename device**: Change the device name.

Locate: Plays a sound that helps you identify your reader.

Serial number: Device serial number.

Firmware version: The software version currently running on the device.

MAC address: Device unique identifier number.

Uptime: Shows how long the device has been working.

Hardware version: The hardware version currently running on the device.

Power source: The current power source.

Modules : Click → to view and update module information for your card and reader.

Modules

The context menu contains:

- **Module details**: Shows the card reader name, module type, board type, assembly version, application version, and bootloader version.
- **Locate**: Click to search for connected modules.

Touch keypad

Module name: Enter a module name for your device keypad.

Flash when button is pressed: Select an option for when someone presses the keypad.

- **No**: The light on the keypad stays off.
- **Yes**: The light on the keypad flashes when someone presses a button.

13.56 MHz Card Reader

Module name: Enter a module name for the input and output specification.

Allowed card types: Select the card types the card reader should accept from the drop-down list.

I/O

Active output

Logical state: Shows the status of your door. Logical state is off when the system does not receive a request to open the door and on when it receives a request to open the door.

Output state: Shows the actual state of the physical output. Output state corresponds to logical state when in normal mode. In inverted and security mode, logical state and output state are reversed.

Mode: Select a mode from the drop-down menu.

- **Normal**: The output is always off but gets activated when there is a request to open the door.
- **Security**: The output is in the mode to connect with a security relay. In this mode, the output is on all the time and when the door opening is requested, a code is sent to the security relay through the output wires. The relay verifies if the code is correct.
- **Inverted**: The output is always on but gets deactivated when there is a request to open the door.

Test: Click to check if your I/O's active output is working.

Relay

Relay state: Shows the physical relay state.

Test: Click to check if the relay is working.

Customization

Signaling volume

Signaling volume is the level of sound the device produces when there is a form of communication within the access control system, for example, the beep the device makes when it reads a card or grants access.

Key beep volume: Set the sound volume.

Warning tone volume: Set the volume for warnings and signals when the device operational status switches, for example, from power on to cable connection.

Backlight

Signaling LEDs intensity: Set the LED brightness.

Backlight enabled : Turn on to enable backlight.

Intensity: Set the backlight intensity level.

System

System dashboard

Download diagnostic package : Click to download the diagnostics package as a file.

Network connection : Click → to edit network settings.

- **Network overview**: Shows the network settings that are currently configured on the device.

Date & time: Shows the current date and time on the device. Click → to edit date and time.

Maintenance: Shows the current software version on the device. Click → to go to the maintenance web page.

- **Download backup**: Click to download the device configuration file to your computer.
- **Restore configuration**: Click to upload a configuration file and select import settings in the dialogue.

Network connection

Local network

The device can connect to a local area network with the Ethernet cable.

IP address settings

Use DHCP server: Turn on to automatically get the IP address from the LAN DHCP server. We recommend automatic DNS (DHCP) for most networks.

IP address: Enter a unique IP address for the device. Static IP addresses can be assigned at random within isolated networks, provided that each address is unique. To avoid conflicts, we recommend you contact your network administrator before you assign a static IP address.

Network mask: Enter the network mask to define what addresses are inside the local area network.

Default gateway: Enter the address of the default gateway, which provides communication with off-LAN equipment.

Current IP address settings: Shows the IP address settings you currently have on the device.

DNS settings

Always use manual DNS settings: Turn on to set DNS settings manually.

Primary DNS: Enter the primary DNS server address for translating domain names to IP addresses. The primary DNS value is 8.8.8.8 after a factory reset.

Secondary DNS: Enter the secondary DNS server address, as an alternative when the primary DNS is inaccessible. The secondary DNS value is 8.8.4.4 after factory reset.

Current DNS settings: Shows the DNS settings you currently have on the device.

Advanced configuration

Hostname: Enter the IP network identification. Allowed characters are A–Z, a–z, 0–9 and -.

Vendor class identifier: Enter the vendor class identifier as a string of characters for DHCP Option 60.

Required port mode: Select the preferred network interface port mode: Automatic or Half Duplex – 10 mbps. The lower bit rate of 10 mbps may be necessary if the used network cabling is not reliable for the 100 mbps traffic.

Current port state: Shows the current network interface port state (Half or Full Duplex – 10 mbps or 100 mbps).

Web server

You can configure your device in a standard web browser with access to the integrated web server. The HTTPS protocol enables secured communication between the device and the web browser.

HTTP port: Enter the HTTP port to use.

HTTPS port: Enter the HTTPS port to use.

Minimum allowed TLS version: Select the lowest TLS version to connect to the device.

HTTPS user certificate: Select the user certificate and private key for the HTTP server. If there is no selection, the device uses the self-signed certificate.

Enable remote access: Turn on to enable remote access to the intercom web server from off-LAN IP addresses.

Firewall

Firewall protects your device and ensures only authorized users gain access to your network.

Disabled: Use the toggle to enable or disable firewall.

Date and time

Note

We recommend that you synchronize the device's date and time with an NTP server.

Time synchronization settings

Automatic time from NTP or internet: Use the toggle to enable or disable time synchronization with an NTP server or internet.

NTP server address: Enter an NTP server address for the synchronization.

Synchronize with browser: Click to synchronize the time on your device with the time on your computer.

Time zone:

Manual selection: Select a time zone for your device.

Custom rule: Enter a time zone manually.

Certificates

Certificates are used to authenticate devices on a network. Your device supports these certificate and private key formats:

- PEM
- CER
- PFX
- DER

CA Certificates: You can use CA certificate to authenticate peer certificate. It validates the identity of an authentication server when a device connects to the network.

Important

If you reset the device to factory default, all certificates are deleted.

CA certificates: Select a certificate for device identity verification.

Upload: Click to upload a CA certificate and enter the certificate ID.

Search: Enter a certificate ID to find it in the list of CA certificates.

: Click to delete the certificate from the device.

: Click to view the certificate information.

User certificates: A user certificate validates users' identity. It can be self-signed or issued by a Certificate Authority (CA). A self-signed certificate offers limited protection which you can use before obtaining a CA-issued certificate.

User certificates: Select the certificate and private key to use for identity verification.

Upload: Click to upload a user certificate and private key and enter the key password if there is one.

Search: Enter a certificate ID to find it in the list of user certificates.

: Click to delete the certificate from the device.

: Click to view the certificate information.

Diagnostics

The diagnostic logs help to identify and solve reported problems. You can use diagnostics to capture diagnostic logs for subsequent download and for technical support.

Ping: To send test data to the IP address:

- Click **Ping**
- Enter an IP address or URL.
- Click **Ping**.

Close: Click to close the dialogue.

Diagnostics package

Diagnostics package is a ZIP file that includes network packets and syslog messages. It contains information about the device, its configuration, network traffic, crash log, and memory statistics. It also shows the number of network packets and the size of syslog messages captured by the device.

Restart capture: Click to restart packet capturing.

Download: Click to download the diagnostics package as a file.

On-device network packet capture

Download: Click to download the captured network packets.

Start: Click to start capturing incoming and outgoing packets on the network.

Note

Previously captured packets will be deleted when you click start.

Stop: Click to stop capturing incoming and outgoing packets on the network.

Syslog capture: Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, which indicates the software type generating the message, and assigned a severity level.

The context menu contains:

- **Delete captured messages**: Click to delete syslog messages.

Download: Click to download syslog messages.

Start: Click to start capturing data.

Stop: Click to stop capturing data.

Network packet capture download

With this, you can capture and download incoming and outgoing packets on the device network interface to your computer.

Start: Click to start capturing data.

Time to capture: Set a duration for the capture.

Stop: Click to stop capturing data.

Sending syslog to remote server: Use the toggle to enable or disable syslog. This allows you to send syslog messages to a syslog server for record keeping and for further device analysis.

Server address: Enter the IP or MAC address of the server on which syslog application is running.

Severity level: Select the severity of messages to send when triggered.

Maintenance

Reset to default: Click to reset the device to its factory default configuration.

- Select **Keep network settings and certificates** to keep the settings you configured for your network and certificates.
- Select **Reset everything** to reset all device settings.
- **Reset**: Click to reset.

Restart device: Click to restart the device.

Download backup: Click to download the device configuration file to your computer.

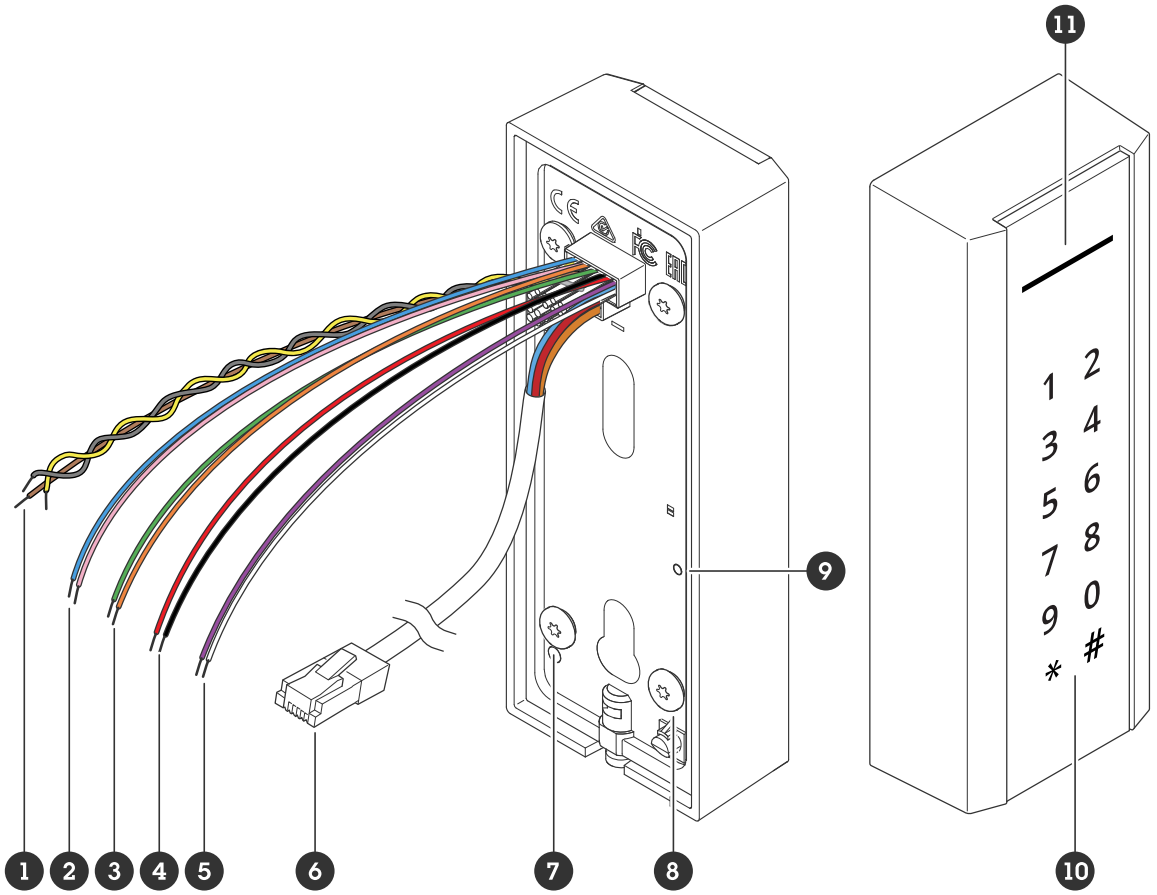
Restore configuration: Click to upload a configuration file and select import settings in the dialogue.

Firmware: Shows an overview of the software version currently running on your device, the minimum software version available for the device, bootloader version, software build type, date, and time.

Firmware upload: Click to upload a software file and upgrade the device software.

Specifications

Product overview



1 *Relay cable*
2 *Input cable 1*
3 *Input cable 2*
4 *External power*
5 *Active output*
6 *Network connector (PoE)*
7 *Control button*
8 *Tamper switch*
9 *Back LED indicator*
10 *Keypad*
11 *Front reader indicator stripe*

Signaling LED

Status LED	Indication
White	Locates device.
Green	Valid authentication.
Red	Steady while waiting for card. Flashes for invalid authentication.

Note

To set the backlight and brightness level, see *Customization, on page 8*.

Buttons

Control button

The control button is used for:

- Finding current IP address. Press the button for approximately 15 seconds until the back LED indicator turn red and green simultaneously and you hear one short beep.
- Resetting the product to factory default settings. See *Reset to factory default settings, on page 18*.
- Restarting the device. Press the button for less than 1 second to restart the device.
- Switching to a static IP address (192.168.1.100):
  - Press and hold the button for approximately 15 seconds until the LED indicators on the back of the device turn red and green simultaneously and you hear a beep.
  - Release the button after the red LED goes off and you hear two beeps.
- Switching to a DHCP server:
  - Press and hold the button for 15 seconds until the back LED indicator turn red and green simultaneously and you hear a beep.
  - Keep the button pressed for 3 seconds while the red LED goes off and you hear two beeps.
  - Release the button after the green LED goes off, red LED goes on again and you hear three beeps.

Cables

External power

The device has a cable to connect to external power supply.

Function	Color	Specifications
DC +	Red	12 V DC, max 12.0 W Cable length: 350 mm
DC -	Black	

Network connector

Function	Color	Specifications
Ethernet and PoE	Black	RJ45 Cable length: 2,900 mm

Power priority

This device can be powered by either PoE or DC input. See *Network connector, on page 15*.

- When PoE and DC are both connected, DC is used for powering.
- PoE and DC are both connected and DC is currently powering. When DC is lost, the device uses PoE for powering.
- When PoE is used during startup and DC is connected after the device has started, DC is used for powering.

Active output

The active output cable is used to connect to a security relay or an electric lock.

Note

For additional security, add *2N Security Relay* between the reader and the lock.

Function	Color	Specifications
DC +	White	9.8 to 13.8 V DC according to power supply, up to 600 mA. PoE: 11.6 V DC: source voltage -0.4 V Cable length: 350 mm
DC -	Violet	

Relay cable

A relay cable to manage access locks and sensors.

Function	Color	Note	Specifications
NO	Yellow	Normally open for fail secure lock.	Max 1 A 30 V DC Cable length: 350 mm
COM	Grey	Common	
NC	Brown	Normally closed for fail safe lock.	

Input cable

The input cable is used for connecting to an external input device while enabling good communication between the device control panel and the input device. The device has 2 input connectors, input 1 and input 2 which you can use to connect a door position sensor and REX button.

Cable	Color	Specifications
Input 1+	Pink	0 to 30 V DC
Input 1-	Blue	
Input 2+	Orange	
Input 2-	Green	

Clean your device

Note

- 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

Note

- A reset to factory default changes all settings back to the factory default values.

1. Open your device.
2. Press and hold the button for approximately 24 seconds until the back LED indicator turns red, green, and off.

Note

You will hear one beep, two beeps, three beeps, and then four beeps at different intervals.

3. Release the control button after the fourth beep. The process is complete and the product has been reset to the factory default settings.
4. Use the installation and management software tools, set the password, and access the product.
   The installation and management software tools are available from the support pages on *axis.com/support*.

You can also reset parameters to factory default through the device's web interface. Go to **System** > **Maintenance** > **Reset to default**.

Check the current software version

The device software determines the device functionality. When you troubleshoot a problem, we recommend that you to start by checking the current software version. The latest version might contain a correction that fixes your particular problem.

You can check the current software version in two ways:

- Go to the device's web interface:
  - Go to **Dashboard**.
  - Go to **Firmware**, see *Maintenance, on page 13*.

Upgrade software

Important

- Preconfigured and customized settings are saved when you upgrade the device software (provided that the features are available in the new firmware version) although this is not guaranteed by Axis Communications AB.
- Make sure the device remains connected to the power source throughout the upgrade process.

Note

When you upgrade the device with the latest software version, the product receives the latest functionality available. Always read the upgrade instructions and release notes available with each new release before you upgrade. To find the latest software version and the release notes, go to *axis.com/support/device-software*.

1. Download the software file to your computer, available free of charge at *axis.com/support/device-software*.
2. Log in to the device page.
3. Go to **System** > **Maintenance** and click **Firmware upload**.
4. Select the software file and click **Upload**.

When the upgrade has finished, the product restarts automatically.

Technical problems and possible solutions

Problems setting the IP address

- If the IP address intended for the device and the IP address of the computer used to access the device are located on different subnets, you cannot set the IP address. Contact your network administrator to obtain an IP address.
- If the IP address is being used by another device:
  1. Disconnect the Axis device from the network.
  2. In a Command/DOS window, type `ping` and the IP address of the device.
  3. If you receive: `Reply from <IP address>: bytes=32; time=10...` this means that the IP address might already be in use by another device on the network. Obtain a new IP address from the network administrator and reinstall the device.
  4. If you receive: `Request timed out`, this means that the IP address is available for use with the Axis device. Check all cabling and reinstall the device.

Problems accessing the device

Can't 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 `http` or `https` in the browser's address field.

If the password for the account is lost, the device must be reset to the factory default settings. See *Reset to factory default settings, on page 18*.

The IP address has been changed by DHCP

IP addresses obtained from a DHCP server are dynamic and may change. If the IP address has been changed, use AXIS IP Utility to locate the device on the network. Identify the device using its model or serial number, or by the DNS name (if the name has been configured).

Certificate warning `NET::ERR_CERT_AUTHORITY_INVALID`

The certificate warning is a standard procedure for OS devices. Click **Advanced** and then click **Proceed to *IP address* (unsafe)** to access the device login webpage. There are few options:

- Use a different browser or device.
- Click anywhere on the certificate warning page and type thisisunsafe.

When you get to the webpage, go to **System** > **Maintenance** > **Firmware upload** to update to the latest device software.

If you can't find what you're looking for here, try the troubleshooting section at *axis.com/support*.

Performance considerations

The most important factors to consider:

- Heavy network utilization due to poor infrastructure affects the bandwidth.

Contact support

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

T10237046

2026-07 (M2.3)