AXIS Device Manager

User manual

Table of Contents

About AXIS Device Manager

AXIS Device Manager is a installation and management software for Axis products. The software can automatically search the network for devices, assign IP addresses, set passwords, show connection status, manage firmware upgrades, certificates and configuration of multiple devices.

AXIS Device Manager is comprised of:

- AXIS Device Manager Service Control - the server that handles all communication with Axis products
- AXIS Device Manager Client - the front end user interface that enables remote management from the Internet or corporate network

Several clients can be connected to the same server. A client can be connected to multiple servers at the same time.

Solution overview

Prerequisites

Compatible operating systems:

Required: 64-bit Operating System Microsoft .NET version 4.8

Supported OS: Windows 10 Pro, Windows 11 Pro, Windows Server 2016, Windows Server 2019, Windows Server 2022

Recommendations: Latest OS Service Packs.

Minimum system recommendation:

- Minimum (up to 500 devices): Intel core i5 or equivalent, 4GB RAM, 100 Mbits/s across the network infrastructure
- Recommended (between 500 to 2,000 devices): Intel core i7 or equivalent, 8GB RAM, 1000 Mbits/s across the network infrastructure
- More than 2,000 devices per server is not recommended.
- Make sure Axis devices run the latest available AXIS OS.

Note

We always support the two preceding version of the latest release. Check the latest release notes to see which specific versions that are supported.

Supported devices:

AXIS products with AXIS OS versions 4.40 or higher. (Note that the exact functionality supported varies depending on a particular product model and firmware)

Languages:

UI + help files: English, French, German, Italian

UI only: Arabic, Czech, Chinese (Simplified), Chinese (Traditional), Dutch, Finnish, Japanese, Korean, Persian, Polish, Portuguese (Brazil), Russian, Spanish , Swedish, Thai, Turkish and Vietnamese.

Get started

Install software

To install AXIS Device Manager 5, make sure you have full administrator rights on the computer you install on, then do the following:

1. *Go to the product page on axis.com and download AXIS Device Manager desktop app*
2. Run the installer and follow the on screen instructions.

Note

If not already installed, Microsoft .NET 4.8 framework will be installed (included in installation file). This will take a few minutes. Microsoft .NET 4.8 framework can also be installed via Windows Update prior to installation of AXIS Device Manager.

Connect to a server

When you start AXIS Device Manager for the first time, you will be asked to connect to a server. The server can be run on the local machine or a remote server.

To log in as a local Windows user:

1. Select **This computer**.
2. Check **Log on as current user** to log in using you current credentials.

To log in as another user on the server or the domain:

- Select **Other user**.
- Under **Other user**, enter the credentials for that account.
- Check **Remember me** to skip this step the next time you run the client.
- Click **Log on**.

Note

To clear the saved credentials for all servers, go to the logon screen and select **Delete saved passwords**.

To log in to a remote server:

1. Select **Remote server**.
2. Select a server from the drop-down list or enter the IP or DNS address in the field.
3. Enter your credentials
4. Click **Log on**.

Note

This option can't be used to log in to a remote server from a computer that is not part of a Windows domain.

Connect to multiple servers

You can connect to multiple servers with AXIS Device Manager. Once you've successfully logged in to a server, you can then switch between servers in the main menu.

1. Go to the main menu > Servers > New connection
2. Choose to connect to either you computer or a remote server as described above.

Initial configuration

To get started, you need to do these things:

- Add devices and create user accounts, see:

- Provide cyber security hardening to your system. See

Manage devices

Add devices

AXIS Device Manager automatically searches the network for connected devices and tries to log in to all devices. The list of found devices shows the device address (IP address or host name), serial number, model and status. The serial number (S/N) is printed on the product label.

To add devices from the list:

1. Select the devices to add and click **Next**.
2. Select **Use host name when possible**. If a device is added using its host name, the host name will be used for all further communication with the device. If a host name isn't available, the IP address will be used.
3. Set password for devices without a password. If a password should not be set, select **Skip**.
4. Click **Next**.

The "Ready to add devices" page shows the devices to be added.

5. Click **Finish** to add the devices.

Remove devices

To remove devices from the list:

1. Go to **Device management**.
2. Select the devices.
3. Right click and select **Remove**.
4. Click **Yes**.

Replace devices

To replace a device in AXIS Device Manager, connect a new device and reuse the configuration from the existing device. The replaced device will be deleted if the operation is successful. There must be at least one restore point available for that device, see . No restore points will be moved to the new device.

1. Go to **Device management**.
2. Go to the tool bar and click on the replace device icon.
3. Select a device to replace and click **OK**.
4. Select the device you want to replace it with and click **OK**.
5. Click **Next** to retrieve a device configuration from the latest restore point.
6. Go to **Parameters > Additional Settings** and select the parameters and settings to apply.
7. Click **Next**.
8. Click **Finish** to apply your settings.

Restore devices

It is possible to restore one or several devices to previously created restore points. To restore devices, each device must have at least one restore point available. By default, automatic restore points are created and continuously removed every night for all devices on the selected server. A set number of the latest automatic restore points are kept for restore purposes.

Restore devices to a previous restore point:

1. Go to the **Device management** workspace.
2. Select one or several devices to restore.

3. Right-click and select **Backup / Restore > Restore to a Previous Time** from the drop-down menu.
4. Select a restore point in the list of the most recent restore points available and click **Next**.
5. Review the settings for each device and click **Finish**.

Configuration

Create restore point

To create a manual restore point:

- Go to the **Device management** workspace.
- Select one or several devices to restore.
- Right-click and select **Backup / Restore > Create Restore Points**.
- Type a description that identifies the restore point.
- Click **OK**.

Note

Manually created restore points are not removed automatically.

Create automatic restore points

If you have more than one server, select the server to configure from the server list.

- Go to **Options > Restore point settings**.
- Select **Create restore points automatically** to enable automatic creation of restore points.
- Enter the number of automatic restore points to be saved and click **OK**.

Manage multiple credentials

This functionality provides AXIS Device Manager with credentials for an administrator account of the devices.

Type device credentials manually

If you choose to enter device credentials manually, the credentials will be updated in AXIS Device Manager for the selected devices.

- Select one or more devices
- Right-click and select **Advanced -> Enter Device Credentials** from the drop-down menu.

Note

Credentials that cannot be verified to work for the device will not be updated. The same password and username have to be used for all devices participating in such an operation.

Use a CSV-file for different credentials

By using a CSV-file, you can use separate passwords and separate usernames for each device. MAC address, IP address or host address is used to map the rows of the CSV-file to the corresponding devices in the Axis Device Manager database.

When using a CSV-file, the user interface asks you to specify how to interpret the columns of the CSV-file.

Note

How to specify to which device a row in the CSV-file belongs.

One column in the CSV-file needs to contain either MAC addresses, IP addresses or host addresses, so either specify a column in the CSV-file to be interpreted as MAC address or as IP or host address. This is needed to specify to which device the data in a row in the CSV-file belongs. Additionally, a column can be specified to be interpreted as Server name. In such a way, rows in the CSV-file targeting devices at different Axis Device Manager servers but with the same IP address or host address, can be distinguished. If no such distinction is needed, there is no use having a column to be interpreted as Server name. In a setup where a server uses the same IP address or host address for several devices, but uses ports to distinguish them from each other, a column can be specified to be interpreted as Port. If no distinction on port is needed, there is usually no reason to interpret a column as Port. An option to provide the port in a dedicated column is to give the port along with the IP address or the host address. The IP address or the host address should then be followed by a colon and the port number.

Install certificates

About certificates

AXIS Device Manager provides the settings for managing server/client certificates. Client certificates are used for IEEE 802.1X and server certificates are used for HTTPS. To implement any changes, select the appropriate devices in Device management and then select Enable/update in the context menu.

Create a Certificate Authority (CA)

A CA will allow you to enable HTTPS and IEEE 802.1X on devices without any server/client certificates in place. The CA instructs the devices to create certificates using their own private keys, sign them and then install them

To create a Certificate Authority:

- Go to the **Configuration** tab.
- Go to **Security > Certificates**
- Under **Certificate authority**, click **Generate...**
- Type a passphrase and conform it.
- Click **OK**.

The CA will now be generated and ready for use.

Note

> Your self-signed root certificate and private key which is protected by a passphrase of your choice. A certificate generated by AXIS Device Manager will last for 3 years. . If you want AXIS Device Manager to renew server/client certificates automatically, you have to check the box titled **Remember passphrase**. If a CA is not set up, you will have to create server/client certificates outside of AXIS Device Manager. You will then lose the advantages of automatic certificate management.

Import - Using the Import feature, you can import an existing CA consisting of a public certificate and a private key. You will have to provide a passphrase.

Save to file - Save the public certificate of the CA in .cer or .crt formats. The file will not contain the private key and will therefore not be encrypted.

Backup - A backup of a CA is recommended if a hardware failure were to happen. If selected, a backup of both the certificate and the private key of the CA used by Axis Device Manager will be made. The backed up data will be protected by the passphrase used to generate the CA.

Certificate expiration warning A system notification will be created if a certificate is expired or is about to be expire. It applies to all certificates installed on connected devices, except CAs installed outside of AXIS Device Manager. The warning will appear as a system alarm, in the status column in Device management, as icons in the "View installed certificates" dialogue, and in the Configuration workspace.

Specify how early you want AXIS Device Manager to notify you when certificates are approaching their expiration date. By default, AXIS Device Manager-generated server and client certificates will be automatically renewed seven days before the expiration warning is set to appear. To receive notification for when the CA is set to expire "remember passphrase" needs to be checked.

Enable HTTPS

To enable HTTPS, a server certificate must be present on each device. AXIS Device Manager can use a Certificate Authority (CA) to sign and install server certificates for devices.

You can also do it manually:

1. Go to the **Device manager** tab
2. Right click the devices and choose **Install server certificates** for each device in the context menu.

There can be only one server certificate present on each device before enabling HTTPS. Excess certificates can be deleted from the context menu.

3. After installing the certificates, you can enable HTTPS in the context menu.

Note

A connection can be made using HTTP if a secure connection (HTTPS) is unavailable. This is done in order to be able to configure devices that are not yet secure.

Ignore certificate validation

AXIS Device Manager won't connect to a device if its certificate isn't validated. The server certificate needs to be signed by the active CA in AXIS Device manager or validated through Windows Certificate Store. By selecting Ignore certificate validation, AXIS Device Manager will not validate if the certificate sent by the device is trusted or not.

To make AXIS Device Manager ignore certificate validation.

- Go to the **Configuration** tab.
- Under **HTTPS**, enable **Ignore certificate validation**.

Enable 802.1X

To enable IEEE 802.1X, a client certificate must be present on each device. AXIS Device Manager can use a Certificate Authority (CA) to sign and install client certificates for devices.

You can also do it manually in Device management if you right click the devices and choose install client certificates for each device in the context menu. There can be only one client certificate present on each device before enabling IEEE 802.1X. Excess certificates can be deleted from the context menu. After installing the certificates, you can enable IEEE 802.1X in the context menu.

You also need an IEEE 802.1X authentication CA certificate in order to use the IEEE 802.1X protocol.

EAPOL Version - Select what version of Extensible Authentication Protocol (EAP) you want to use.

EAP identity - Enter either the device's MAC address, the device host name or custom text.

Custom - Enter any text that will function as the EAP identity.

IEEE 802.1X authentication CA certificate - In addition to the client certificate, an IEEE 802.1X authentication CA certificate has to be installed. To activate IEEE 802.1X, only the public certificate is needed and not the private key, so no need for any passphrase. The IEEE 802.1X authentication CA certificate will be installed when enabling or updating IEEE 802.1X..

Import - Select a CA certificate that will be installed on the devices and used to validate the authentication server. The CA certificate can either created by the CA in AXIS Device Manager or come from an external source.

View - Details of the CA certificate used during the IEEE 802.1X authentication process.

Common name - Select either Device EAP identity or Device IP address. If the custom field is left empty, the host name will be selected. If there is an issue with the host name, the IP address will be used as the common name.

Manage SIP accounts

Manage device software

AXIS OS updates

New AXIS OS versions can be obtained in two ways:

- Downloaded using AXIS Device Manager (requires Internet access)
- Imported from a file (e.g. on a hard drive or memory stick).

Manual upgrade of AXIS OS

1. Select the devices that you want to upgrade with a new AXIS OS version, right-click and select **Upgrade AXIS OS**.
2. In the **Upgrade firmware** dialogue: To update the list of firmware versions available for download and click the **Check for Updates** button.
3. To browse for one or more AXIS OS version files stored on the local client, click the **Browse** button.
4. To factory default the selected devices during AXIS OS upgrade, click the **Factory default checkbox**. This is a requirement when downgrading for some AXIS OS versions.
5. Select the devices and the AXIS OS versions that you want to upgrade and click **OK** to start upgrading the selected devices in the list.

Note

By default, AXIS OS updates are done for all the selected devices at the same time. The update order can be changed in **Configuration > Connected Services > Firmware upgrade settings**.

Automatic updates

AXIS Device Manager 5 default setting is to not check for any AXIS OS updates, but it can be set up to automatically check if AXIS OS updates are available on the server or axis.com.

To manually check for AXIS OS updates, press the **Check now** button in the action menu.

AXIS OS upgrade order

AXIS OS updates can be done on all devices at the same time, or one device after the other.

- To update all devices at once, select **Parallel** upgrade order
- To upgrade devices one after the other, select **Sequential**. This option will take longer, but the devices won't be offline at the same time. You can also choose to stop a sequential upgrade if there is an issue by checking the **Cancel all remaining upgrades if one device fails** box.

Troubleshooting

Contact support

When you contact support, first create a ticket and include a system report file to make it easier to troubleshoot your particular issue:

1. Go to the main menu.
2. Go to **Help > System Report...**
3. Save the report file in a chosen folder.
4. Go to *axis.com/support*.
5. Create a support ticket.
6. Attach the file to your support ticket.

Note

To create a system report from a unresponsive system:

1. Go to `C:\ProgramData\Axis Communications\`
2. Archive the contents of the folder to a .zip file and attach it to the support ticket.

Escalation process

When you have issues that can't be solved using this guide, escalate the issue to Axis online helpdesk, see *Axis online helpdesk*. For our support team to understand your issue and be able to solve it, you must include the following information:

- A clear description on how to reproduce the issue or under what circumstances the issue happen.
- The time and the concerned device's name or IP address where the issue happens.
- AXIS Device Manager system report generated directly after the issue happens. The system report must be generated from the client or server where the issue was reproduced.
- Optional screenshots or recordings that show the issue.
- If necessary, include the database files. Exclude these to make the upload go faster.

Some issues require additional information that the support team requests if necessary.

Note

If the file is larger than 100 MB, for example a network trace or database file, use a secure file sharing service that you trust to send the file.

Additional information	
Debug level logs	Sometimes we use debug level logging to collect more information. This is only done by request from an Axis support engineer. You can find Instructions on *Axis online helpdesk*.
Network trace	If requested by the support engineer, generate network traces when you create the system report. Take the network traces during the time when the issue happens if it's reproducible. This includes: • A 60 sec Network trace taken on the camera (only applicable for firmware 5.20 and later) Use the following VAPIX command to change the login, IP address, and duration (in seconds) if necessary: `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • A 10-30 sec Network trace taken on the server that shows communication between the server and the camera.

Additional information	
Database files	In cases where we have to examine or manually repair the database. Select **Include database in the report** before you generate the system report.
Screenshots	Use screenshots when it's a live view issue, related to UI. For example, when you want to show a timeline for recordings or when it's difficult to describe.
Screen recordings	Use screen recordings when it's difficult to describe the problem in words, for example when there are many UI interactions involved to reproduce the issue.

T10211981

2025-03 (M1.9)