AXIS Device Manager Pro Beta

User manual

Table of Contents

About AXIS Device Manager Pro 4
Solution overview 5
Get started 7
    Install software 7
    Connect to a server 7
    Connect to multiple servers 7
    Configure the server 7
    Configure firewall settings 8
    Initial configuration 9
Manage devices 10
    Add devices 10
    Remove devices 10
    Replace devices 10
    Restore devices 10
    Install apps 11
Configuration 12
    Manage restore points 12
        Create restore point 12
        Create automatic restore points 12
    Manage credentials on multiple devices 12
        Enter device credentials manually 12
        Use a CSV-file for different credentials 12
    Configure certificates 13
        About certificates 13
        Create a Certificate Authority (CA) 13
        Configure HTTPS 15
        Configure IEEE 802.1X 15
        Device certificate expiration warning 15
        Manage certificates 15
    Configure SIP settings 17
    Manage SIP accounts 18
        Add SIP accounts 18
        Remove SIP accounts 19
    Enable metadata on devices 20
    View warranty 20
    Update warranty information 20
Manage device software 22
    AXIS OS upgrades 22
Troubleshooting 23
    Software Bill Of Material 23
    Contact support 23
    Escalation process 23
    Use command line to install AXIS Device Manager Pro 24

Note

AXIS Device Manager Pro Beta supports device software upgrades to AXIS OS 13 and improved certificate management. Axis will continually improve and evaluate AXIS Device Manager Beta during the beta test period. All feedback is welcome.

About AXIS Device Manager Pro

AXIS Device Manager Pro is an installation and management software application 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.

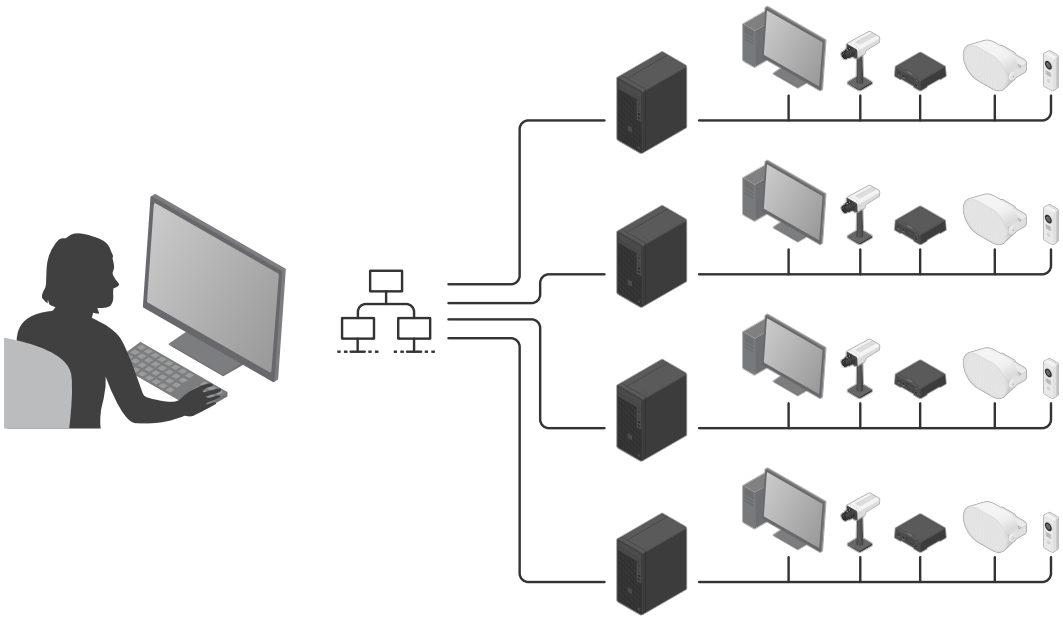
AXIS Device Manager Pro is comprised of:

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

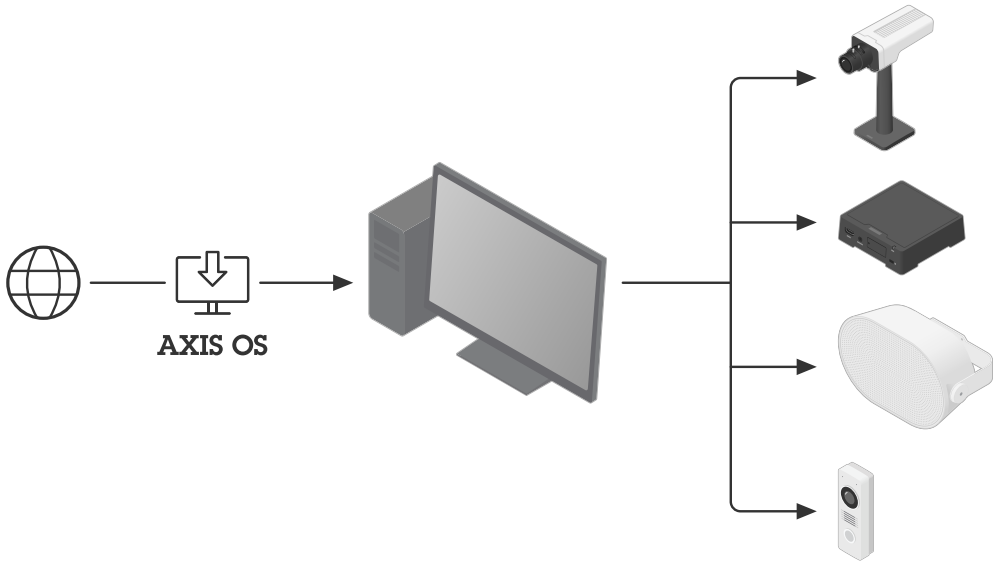
Several clients can be connected to the same server. A client can be connected to multiple servers at the same time.

AXIS Device Manager Pro is also very useful for hardening your system and increasing security. For more information, see the *AXIS Device Manager Pro Security Guide*.

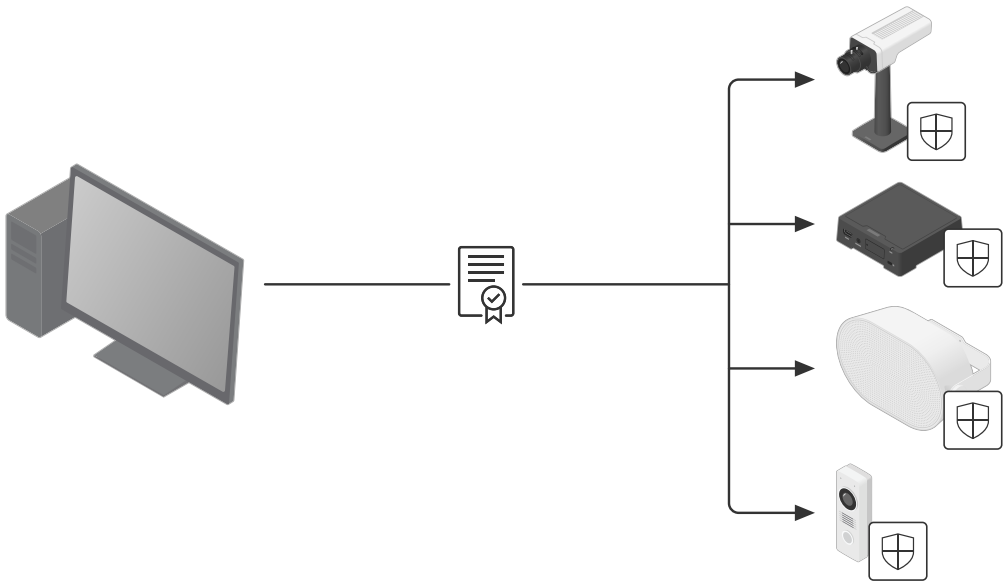
Solution overview



Multi-site management



AXIS OS upgrades



Certificate management

Get started

Install software

To install AXIS Device Manager Pro, 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 Pro installer*
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 Pro.

Connect to a server

When you start AXIS Device Manager Pro 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 Pro. 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 your computer or a remote server as described above.

Configure the server

Once AXIS Device Manager Pro Server has been installed on your computer, the Service Control allows you to start and stop the server as well as modify server settings.

To configure the server:

1. Double-click the icon to open the **AXIS Device Manager Pro Service Control**
2. Check the **Modify settings** check box
3. Name the server. The Server name identifies the server and is displayed in AXIS Device Manager Pro client when the client is connected to more than one server. The default name is that of the computer where the software was installed.
4. Type the HTTP port. The default HTTP port number is: 55762
5. Type the TCP port. The default TCP port number is: 55764

Note

The server port number must be between 1024-65533. The TCP port number will always be the server port number + 2. For example, if the server port number is 55765 the TCP port number will be 55767.

Information about the ports used by AXIS Device Manager Pro at axis.com.

For larger installations, we recommend AXIS Device Manager Pro Service Administration. It is a console application that can be used from the command prompt or from a batch script to start and stop the service, backup the database, etc. The console application "AdmAdminConsole.exe" is located in the server installation directory.

Configure firewall settings

In order for AXIS Device Manager Pro server and client to work correctly, add the following IP addresses and ports to the allow list of the organization's firewall:

The **Direction** data is always indicated from AXIS Device Manager Pro server point of view.

Port	Protocol	Direction	Used	Comments
80	HTTP	Outbound	From AXIS Device Manager Pro server and devices to the network.	AXIS Device Manager Pro server can use the port to check for firmware updates and download the firmware from Axis servers. Devices can use the port to use services and API, or to send HTTP/HTTPS notifications if that's configured in the firmware. AXIS Device Manager Pro can use APIs toward the device (from both server and client to device).
443	HTTPS			
5353	UDP	Outbound	From ADM Pro server and devices to the network.	mDNS Discovery (Bonjour) search for devices. Multicast on address 224.0.0.251 is used.
1900	UDP	Outbound	From AXIS Device Manager Pro server and devices to the network.	SSDP Discovery UPNP search for devices. Multicast on address

				239.255.255.250 is used.
15157	UDP	Outbound	From AXIS Device Manager Pro server to server-control applet.	Broadcast messages from server to service control, for example progress of database upgrade during installation.
52365	TCP	Internal	Used only internally by ADM Pro components.	This port is used by an internal API to communicate between AXIS Device Manager Pro services inside the server machine.
55762	HTTP	Inbound	Between AXIS Device Manager Pro client and server.	Channel to exchange application data if TCP on 55764 is not available/fails (Backup port and protocol, see below).
55764	TCP	Inbound	Between AXIS Device Manager Pro client and server.	TLS-encrypted application data.
55765	TCP	Inbound	Between AXIS Device Manager Pro client and server.	Used from the client to detect available servers via SSDP/UPNP.

To get warranty information and for updates of AXIS OS, you will have to allow all Axis URLs in your firewall: *axis.com.

Initial configuration

To get started, you need to do these things:

- Add devices and create user accounts, see: *Add devices, on page 10*
- Provide cyber security hardening to your system. See

Manage devices

Add devices

AXIS Device Manager Pro 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 Pro, 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 *Create restore point, on page 12*. 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**.

Install apps

An app is software that can be uploaded to and installed on Axis devices. Apps can be installed on devices with support for AXIS Camera Application Platform. They add functionality to the device, for example detection, recognition, tracking or counting capabilities. Apps must first be downloaded from *axis.com* or from the app vendor's website. Some applications also require a specific AXIS OS version or device model. If the app requires a license, the license key file can be installed at the same time as the app or it can be installed later using the devices' setup pages. If an app can't be installed, go to *axis.com* and check if the device model and AXIS OS version support AXIS Camera Application Platform.

To install an app:

1. Go to *axis.com* and download the app.
2. Go to **Browse to Application**.
3. Click **Browse** and go to you downloads folder.
4. Select the app and click **Next**.

If the app requires a license to be started you have to have a license file already downloaded, if no click **No** and continue on step 8:

5. Select **Yes** and click **Next**.
6. Click **Browse** and select the license file.
7. Click **Next**.
8. Select the kind of installation you'd like:
   - **Application downgrade** installs a previous version of the applications.
   - **Application overwrite** reinstalls the applications.

Note

Downgrade or overwrite the application resets the application settings on the devices.

Ready to install
Listed are the devices on which the apps will be installed. If the apps are already installed on some devices, the existing apps will be overwritten. Overwriting removes all app settings.

9. Click **Finish**.

Configuration

Manage restore points

A restore point is a saved device configuration that can be used to backup and restore device settings. Automatic restore points are created every night for all reconfigured devices on a server. If no settings have been changed on a device since the last restore point, no new restore point will be created. To maximize storage capacity, the oldest restore points are automatically removed. A set number of the latest automatic restore points are kept for restore purposes.

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 credentials on multiple devices

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

Enter 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 Pro database.

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

Create the CSV file

Your CSV file needs at least one column with device addresses (MAC addresses or IP/host addresses) so AXIS Device Manager knows which device each row applies to.

You can also include columns for:

- **Passwords** – set a different password per device if needed
- **Users** – specify usernames to add or remove
- **Server name** – useful if multiple devices share the same IP address across different Axis Device Management Pro servers
- **Port** – use this if your setup uses ports to distinguish devices, or combine the port with the address in the format **IP:PORT**

The order of columns doesn't matter. You'll assign meaning to each column in AXIS Device Manager Pro.

Add users on multiple devices

1. In the device list, right-click one or more devices.
2. Go to **Security > User Management**.
3. Select **Use CSV file** as the method, then select **Add user** as the operation.
4. Browse to your CSV file and click **Next**.
5. Assign a meaning to each column. If your file has a header row, exclude it.
6. Click **Next** to preview the actions.
7. Select the role and PTZ options for the new users.
8. If you want to limit the changes to only the devices you selected, check that option.
9. Click **Finish**.

You can follow the progress in the Task pane.

Set passwords on multiple devices

1. In the device list, right-click one or more devices.
2. Go to **Security > User Management**.
3. Select **Use CSV file** as the method.
4. Browse to your CSV file and click **Next**.
5. Assign a meaning to each column and exclude the header row if needed.
6. Click **Next** to preview the actions.
7. Click **Finish**.

Note

If you change passwords on multiple devices at once, that can disconnect them from other services or hardware. We recommend testing on a small group of devices first before rolling out the change more broadly

Configure certificates

About certificates

AXIS Device Manager Pro provides the settings for managing server/client certificates and certificate authorities (CAs). Client certificates are used for IEEE 802.1X network authentication and server certificates are used for HTTPS.

Create a Certificate Authority (CA)

A CA will allow you to enable, disable, or renew HTTPS and IEEE 802.1X. The CA instructs the devices to create certificate signing requests and sign them. Multiple CAs can be used as verification for network authentication servers (NAS).

When a CA is used with AXIS Device Manager Pro, for each device selected, the software:

- Instructs the device to create and fetch a certificate signing request.
- Signs the request with the CA to create the final certificate.
- Uploads the certificate to the device.
- Enables the HTTPS, IEEE 802.1X, or RTSPS that you've selected for each of the devices.

CAs can be managed from the **Certificate authority inventory**. From the inventory you can see a list of active CAs and their chains of trust, as well as:

- – The key icon confirms whether a private key was properly imported for the CA.
- – A certificate authority expiration warning is displayed if a CA is expired or set to expire within one year.

To import an existing CA:

1. Go to the **Configuration** tab.
2. Go to **Security > Certificates**.
3. Under **Certificate authority inventory**, click **Import**.
4. Browse to an existing CA file. Import supports .pem, .pfx, .p12, .crt, .cer, and .der formats that contain a public certificate and private key.
5. Click **OK**.
6. If the private key is encrypted, you will be prompted to provide a password and click **OK.**

To generate a new CA:

1. Go to the **Configuration** tab.
2. Go to **Security > Certificates**.
3. Under **Certificate authority inventory**, click **Generate...**
4. Fill in the certificate properties and click **Next**.
5. Select your encryption method and click **Next**.
6. Check the summary and click **Finish**.

The CA will now be generated in the **Certificate authority inventory** and ready for use.

To use or revise an existing CA in the list, right click the CA. From the right-click menu, you can:

- **View** – View information about the CA and its expiration date.
- **Save to file** - Save the public certificate of the CA in .pem and .der formats. The file will not contain the private key and will therefore not be encrypted.
- **Backup** - A backup of a CA is recommended in case of a hardware failure or to distribute the CA to other certification authorities. If selected, a backup of the CA certificate and private key used by AXIS Device Manager Pro will be created. Backup files can be saved in .pem, .p12, and .pfx formats.
- **Remove** – Delete the selected CA certificate from your **Certificate authority inventory**. The whole chain of trust connected to your selected CA will be removed as well.
- **Designation options** – Set the scope of the CA by selecting one or more of the following:
  - Set as HTTPS signing
  - Set as IEEE 802.1X signing
  - Set as IEEE 802.1X verification
  - Remove IEEE 802.1X verification

Note

Multiple certificate authorities can be selected to be used for IEEE 802.1X verification. The chosen CAs will be used by the devices to trust the Network Authentication Server (NAS). If no listed CAs are selected for

verification, the device will trust any authentication server in the network when performing IEEE 802.1X authentication steps.

Configure HTTPS

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

Skip certificate validation – When this setting is turned off, AXIS Device Manager Pro won't connect to a device if its certificate isn't validated. If you turn on **Skip certificate validation**, AXIS Device Manager Pro will trust the certificate that is preinstalled on the device without certificate validation. Your connection is less secure when this setting is turned on.

Common name – You can choose to use either the device IP address or the device host name to identify your certificate.

Validity of the certificate – You can set the number of days that your certificate is valid for HTTPS. When you change the number of days, the depicted expiration date will update automatically. If you extend the validity timeframe beyond the CA's expiration date, the expiration date will stop at the CA's actual expiration date.

Configure IEEE 802.1X

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

EAPOL Version - Select which version of the Extensible Authentication Protocol over Lan (EAPOL) you want to use.

EAP identity - Configure the device identify by choosing between the device's MAC address, the device host name, or custom text.

Validity of the certificate – You can set the number of days that your certificate is valid for IEEE 802.1X. When you change the number of days, the depicted expiration date will update automatically. If you extend the validity timeframe beyond the CA's expiration date, the expiration date will stop at the CA's actual expiration date.

Device certificate expiration warning

AXIS Device Manager Pro allows you to set a warning before your device certificates expire. The warning will appear in the HTTPS and IEEE 802.1X columns of the **Device inventory** under the **Device management** tab.

Approximately 15 days before a certificate expires, AXIS Device Manager Pro will attempt to automatically update your device's certificates if a CA has been assigned to HTTPS signing.

Manage certificates

Enable and disable certificates

To enable or disable certificates on your devices:

1. Select the device or devices you wish to update in **Device manager**.
2. Right click on the device and then select **Security** > **Secure communication** > **Enable/disable**.
3. In the dialogue box that appears, choose which certificate signing and validation options to enable and disable. **Note:** RTSPS can only be enabled when HTTPS signing is enabled.
4. Click **Next**.
5. Choose a certificate to use for HTTPS. You can use either an AXIS Device Manager Pro certificate authority or select your own HTTPS certificate authority.
6. Click **Next**.

7. If you not choose to use your own HTTPS certificate authority, browse for the correct files. You can choose multiple certificate files and they will be matched to the correct devices via IP address or MAC address. If you select multiple files, every file must have the same password to continue.
8. Review the summary and click **Finish**.

View certificates

To view certificates on your devices:

1. Select the device or devices you wish to view in **Device manager**.
2. Right click on the device and then select **Security** > **Secure communication** > **View**.
3. Double click on each entry for additional information.

Delete internal certificates

To delete certificates that are managed by AXIS Device Manager Pro:

1. Select the device or devices with certificates you wish to delete in **Device manager**.
2. Right click on the device and then select **Security** > **Secure communication** > **Delete certs.**
3. Click **Continue**.
4. Expand the categories and select the certificates you wish to delete.
5. Click **Delete**.

Delete external device certificates

Note

Before you start, you need to make sure the certificate isn't currently in use by any function on the devices, such as HTTPS, RTSPS, IEEE 802.1X, or Syslog. You can verify this in Plain config on each device.

To remove a device certificate that is not managed by AXIS Device Manager Pro, use Advanced configuration.

1. Go to the **Device management** tab.
2. Select the devices you'd like to remove the certificate from.
3. Right click and select **Configure** > **Advanced** > **Set configuration**.
4. In the **Set configuration** dialogue box:
   - Select your task from the **Example** dropdown menu
   - Set **Uri** to **Post**
   - Set **url** to `vapix/services`
   - Update **Content-type** to `text/xml`
   - Replace the XML content with the following

   ```
   <?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:xsi=
   "http://www.w3.org/2003/05/soap-envelope" xmlns:tds="http://www.
   onvif.org/ver10/device/wsdl" <soap:Body> <tds:DeleteCertificates>
   <CertificateID>CertificateNameHere</tds:CertificateID> </tds:
   DeleteCertificates> </soap:Body></soap:Envelope></xml>
   ```

5. Replace `CertificateNameHere` with your certificate name. Your certificate name can be found in the device web interface, under **System** > **Security** > **Certificates** > **Name**.
6. Click **Send** and check the task list to confirm the results.

Note

Match the ID exactly, including capitalization, spaces, punctuation, and any content inside parentheses. For example:

Default (self-signed)

Cybertrust Global Root

Set advanced configuration

You can use AXIS APIs to perform a bulk configuration function.

1. Go to **Device manager** and select the device or devices you want to configure.
2. Right click on the device and then select **Configure devices** > **Advanced** > **Set configuration**.
3. Choose from the available examples or write your own content based on your documentation.
4. Set method and uri.
5. Enter the content and content type based on your documentation.
6. Click **Send**.

Note

AXIS Device Manager Pro doesn't support text responses from the API. However, you can confirm that the configuration was successful in the task list.

Configure SIP settings

To configure the SIP and port settings on selected devices, use the setup assistant. The setup assistant lets you to keep the value that is already in the device or enter a value to be applied to all the selected devices. You can also load values from a CSV-file to apply device–specific values to selected devices.

Use one row in the CSV-file for each device, and one column for each parameter to be set. The setup assistant lets you specify which values to be fetched.

To use a CSV file for device–specific settings for multiple devices:

1. Go to the **Device management** workspace.
2. Select the devices you want to configure.
3. Right-click and select **Configure devices > Advanced > SIP configuration > Settings**.
4. If you'd like to use a CSV-file, check that you allow the use of a CSV–file. Otherwise, go to 5.
   4.1. Click **Browse** and select the CSV–file you'd like to use.
   4.2. Click **Next**
   4.3. Choose how to name the columns of the CSV-file in the drop-down menu.
   4.4. Select either MAC-address, IPv4-address or host-address for one column in the CSV-file, and associate them with devices in the rows.
5. Click **Next**.
6. Select any of the following SIP and port settings:
   - **Enable SIP** - Enables SIP on the selected devices.
   - **Allow incoming SIP calls** - Allows incoming SIP calls to your devices.
   - **SIP port** - Assign a port number used for SIP calls.
   - **TLS port** - Assign a port number used for TLS encryption.
   - **RTP start port** - Assign a RTP port number for audio traffic.
7. Click **Next**.
8. Select any of the following audio and call settings:
   - **Audio direction** - Choose between **Send only**, **Receive only** or **Send and receive**.
   - **DTMF payload type** - Choose the type of DTMF Payload Type to carry DTMF digits, tones, and signals.

- **Calling timeout** - Choose the number of seconds to wait until a call is timed out.
- **Incoming call timeout** - Choose the number of seconds to wait until an incoming call is timed out.
- **End calls after** - Choose the number of seconds to wait until an incoming call is automatically ended. You can also choose to allow infinite call duration.

9. Click **Next**.
10. Select any of the following Network Address Translation (NAT) traversal parameters:
    - **ICE Enable** - Enables Interactive Connectivity Establishment (ICE) on the selected devices.
    - **TURN Enable** - Enables Traversal Using Relays around Network address translation (TURN).
    - **TURN server address** - Enter the address of the TURN server.
    - **TURN username** - Enter the TURN username.
    - **TURN password** - Enter the TURN password.
    - **STUN Enable** - Enables Session Traversal Utilities for Network address translation (STUN)
    - **STUN server address** - Enter the address of the STUN server.
11. Click **Next**.
12. Review the configuration of the listed devices.
13. If everything is in order, click **Finish**.

Manage SIP accounts

In Axis Device Manager Pro you can configure your SIP settings and add or remove SIP accounts.

Add SIP accounts

To add SIP accounts, you should specify them in a CSV-file. You can create a template in the setup assistant.

To generate a template:

1. Go to the **Device management** workspace.
2. Select the devices you want to configure.
3. Right-click and select **Configure devices > Advanced > SIP configuration > Add SIP accounts**.
4. Click **Generate template**
5. Select a place to save the CSV-file.
6. Add the accounts to the file. Use one row for each account you want to add to a device. You can add multiple accounts to a device.

The CSV-file has the following layout:

Column Name	Description	Mandatory/ Optional	Notes
deviceIdentifier	MAC address, IP-address or host-address	mandatory	This column specifies which device the account should be added to. It can be either MAC-address, IPv4-address or host-address.
active	Boolean	mandatory	
makeDefault	Boolean	mandatory	
answerAutomatically	Boolean	mandatory	
name	string	mandatory	
userId	string	mandatory	
domain	string	optional	In case this column is missing in the CSV file, all accounts will be set as Peer-to-peer. In case this column is present, the account will be Peer-to-peer if the cell is empty and Registered if it contains something.
password	string	mandatory	
authenticationId	string	mandatory	
callerId	string	mandatory	
registrar	string	optional	
transportMode	udp or tcp	mandatory	In MVP1, TLS is not supported.

To add the accounts to the selected devices:

- Go to the **Device management** workspace.
- Select the devices you want to configure.
- Right-click and select **Configure devices > Advanced > SIP configuration > Add SIP accounts**.
- Click **Browse**.
- Select the CSV-file you've added the accounts to.
- Click **Next**
- Review the configuration of the listed devices.
- If everything is in order, click **Finish**.

Remove SIP accounts

To remove all SIP accounts except the default account on selected devices:

1. Go to the **Device management** workspace.
2. Select the devices you want to configure.
3. Right-click and select **Configure devices > Advanced > SIP configuration > Remove accounts**.
4. In the setup assistant, check **Remove all accounts except the default account on the selected devices**.
5. Click **Finish**.

Enable metadata on devices

In this example use case we will enable metadata on multiple devices. Before you perform this task, we recommend that you try it on one device beforehand to avoid issues with multiple devices at once. To enable metadata on one or more devices:

1. Go to the **Device management** workspace.
2. Select the devices you want to enable metadata on.
3. Right-click and select **Configure devices > Advanced > Set configuration**.
4. Click OK
5. Select **Set NTP servers** in the drop-down menu.
6. In the **Uri** drop-down menu, make sure the method is **Post**.
7. In the address field, add this: **axis-cgi/analyticsmetadataconfig.cgi**
8. Add the following code in **Content**:

```
{ "apiVersion": "1.0", "context": "my context", "method": "setEnabledProducers", "params": { "producers": [ { "name": "objectanalytics", "videochannels": [ { "channel": 1, "enabled": true } ] } ] } }
```

9. Check that **Content-Type** is **application/json**
10. Click **Send**.

Note

Note that AXIS Device Manager Pro won't return a response when you use the method above. Always check the **Tasks** pane for errors. You can also use a dedicated software like POSTMAN to test the API with improved functionality. Some VMSs may have limitations that only allow a single producer at a time, so you may need to disable the extra producers using the API. mentioned above.

View warranty

To get device warranty information with AXIS Device Manager Pro, you need a connection to the internet and sign in with a valid My Axis account. Ensure that you have registered a My Axis account at *https://axis.com/my-axis/login*.

1. Go to **Configuration > Connected services > Device warranty**.
2. Click **Sign in**.

AXIS Device Manager Pro opens the default web browser of your system and fetches a sign in page, located at Axis.

3. Sign in with your MyAxis credentials.

The warranty expiration date will now appear in the device list in AXIS Device Manager Pro.

Update warranty information

If your device warranty information was incorrect and has been fixed by Axis customer services, you need to update the warranty information in AXIS Device Manager Pro to reflect the changes. Note that you have to be signed in to My Axis to be able to update the warranty information.

Export a list of your devices in a JSON file.

1. Go to the main menu.
2. Select **Import and export > Export devices**
3. Select a location for the file
4. Click **OK**

Note

The JSON file will have the data of your cameras in plain text, including usernames and passwords. Store it in a private folder and delete it after the procedure is completed.

Remove the devices with the wrong information.

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

Import the removed devices.

1. Go to the main menu.
2. Select **Import and export > Import devices**
3. The list will only show devices that aren't in the list already. To make the process easier, you can check the **Auto select** check box.
4. Click **Finish**.

Update the warranty info.

1. Go to the **Configuration** tab
2. Go to Device Warranty and click **Update**.
3. Check the progress of the update in the device list in the **Device Manager** tab

Note

The update can take a while if there are many devices. Do not close the client until the update is complete. If the client is closed before the process is complete, you need to repeat the last step in the process. If that doesn't resolve the issue, you need to remove the remaining devices, import them and update the information again.

Manage device software

AXIS OS upgrades

New AXIS OS versions can be obtained in two ways:

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

Note

We encourage you follow the AXIS OS recommended upgrade path. Read more about that here: *https://help.axis.com/axis-os#upgrade-path*

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 firmware**.
2. When informed that the devices will become inaccessible during the upgrade, click **Yes**.
3. To update the list of firmware versions available for download In the **Upgrade firmware** dialogue, click **Check for Updates**.
4. To browse for one or more AXIS OS version files stored on the local client, click the **Browse** button.
5. Select the devices and the AXIS OS versions that you want to upgrade.
6. 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.
7. Click **OK** to start upgrading the selected devices in the list.

Note

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

Automatic upgrades

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

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

AXIS OS upgrade order

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

- To upgrade 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

Software Bill Of Material

To get the Software Bill Of Materials (SBOM):

1. Go to *the product support page for AXIS Device Manager Pro* on axis.com.
2. Click on **SOFTWARE BILL OF MATERIALS**.

To read more about SBOM, go to the *AXIS OS Portal* on axis.com.

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 Pro Beta 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:

Additional information	
	• 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.
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.

Use command line to install AXIS Device Manager Pro

To deploy AXIS Device Manager Pro across multiple devices without user interaction, you can use command-line switches to run a silent installation.

Note

Limitations

The switches are part of the Inno Setup application and are not created by AXIS. The AXIS Support Helpdesk doesn't support silent installation.

Axis doesn't recommend bypassing the end user license agreement (EULA).

Before you start

Download the AXIS Device Manager Pro installation package from axis.com.

Download Inno setup, a freeware installer for Windows available from .

Install silently

1. Open a command prompt as an administrator.
2. Navigate to the folder where you saved the installation package.
3. Run the installer with the switches you need. For example:
   `ADM_installer.exe /VERYSILENT /SUPPRESSMSGBOXES /NORESTART`
4. To save a log of the installation, add **/LOG="C:\logs\adm_install.log"** to your command.

Customize the installation

You can add more switches to control the installation behavior:

- To specify an installation folder, add **/DIR="C:\your\path"**.
- To prevent the user from canceling, add **/NOCANCEL**.
- To save your settings for reuse, add **/SAVEINF="settings.inf"**. You can then load them later with **/LOADINF="settings.inf"**.

Switches that can be used for an AXIS Device Manager installation:

Switch	Description
/HELP or **/?**	Shows a summary of available switches.

/SP-	Disables the confirmation prompt at the beginning of setup.
/SILENT	Runs setup silently, hiding the wizard but showing the progress window.
/VERYSILENT	Runs setup silently, hiding both the wizard and the progress window.
/SUPPRESSMSGBOXES	Suppresses message boxes. Requires **/SILENT** or **/VERYSILENT**.
/ALLUSERS	Installs in administrative install mode.
/CURRENTUSER	Installs in non-administrative install mode.
/LOG	Creates a log file in the user's TEMP directory.
/LOG="filename"	Creates a log file at the specified path.
/NOCANCEL	Prevents the user from canceling the installation.
/NORESTART	Prevents the system from restarting after installation.
/RESTARTEXITCODE=exit code	Specifies a custom exit code when a restart is needed.
/CLOSEAPPLICATIONS	Closes applications that need to be updated during setup.
/NOCLOSEAPPLICATIONS	Prevents setup from closing applications.
/FORCECLOSEAPPLICATIONS	Forces applications to close during setup.
/NOFORCECLOSEAPPLICATIONS	Prevents setup from force-closing applications.
/LOGCLOSEAPPLICATIONS	Creates extra logging when closing applications.
/RESTARTAPPLICATIONS	Restarts applications after installation if possible.
/NORESTARTAPPLICATIONS	Prevents setup from restarting applications.
/LOADINF="filename"	Loads installation settings from a file.
/SAVEINF="filename"	Saves installation settings to a file.
/LANG=language	Specifies the language to use during installation.
/DIR="x:\dirname"	Overrides the default installation directory.
/GROUP="folder name"	Overrides the default Start Menu folder name.
/NOICONS	Prevents creation of a Start Menu folder.
/TYPE=type name	Overrides the default setup type.
/COMPONENTS="..."	Overrides the default component settings.
/EULA=ACCEPT	Bypasses the EULA. Not recommended by Axis.

For a complete list of switches, see the

T10250000

2026-11 (M3.2)

© 2026 Axis Communications AB