

AXIS Camera Station S1216 Mk II Tower Recording Server

Get started

The standard workflow to configure an AXIS Camera Station Pro recording server is:

1. *Install your device.*
2. Initial Windows® setup: After installing your device, you are guided through a few steps to set up the region, language, keyboard layout, an administrator account and its password.
3. Initial Axis recorder setup: After the initial Windows® setup, AXIS Recorder Toolbox is opened and you are guided through a few steps to set up basic and necessary settings, for example, computer name, date and time, and network. See *Initial Axis recorder setup, on page 4*.
4. Configure Windows®. We recommend to:
 - Update Windows® to the latest version. See *Update Windows®, on page 16*.
 - Create a standard user account. See *Create a user account, on page 8*.
5. Update AXIS Camera Station Pro to the latest version.
 - If your system is online: open the AXIS Recorder Toolbox app and click **Update AXIS Camera Station Pro**.
 - If your system is offline: go to *axis.com* and download the latest version.
6. Start the AXIS Camera Station Pro client.
7. *Connect to AXIS Camera Station Pro server.*
8. *Configure AXIS Camera Station Pro, on page 4.*

Install your device

Before installation

- Prepare additional accessories used for installation: monitor, mouse, keyboard and network cable.
- Understand the usage of different user accounts.

The following table lists the user accounts that can be used for installation, configuration and operation of your Axis system.

User account	Description	Note
MyAxis	Used to download the latest software, access the license system, Axis Secure Remote Access, and System Health Monitoring.	Registered from <i>my.axis.com</i> .
Windows®		
Windows® administrator	Administrator privileges in Windows®. We recommend you do not use it as AXIS Camera Station Pro administrator.	Created during initial Windows® setup.
Windows® user with AXIS Camera Station Pro administrator privileges	A Windows® user granted with administrator privileges in AXIS Camera Station Pro to be used by system integrator or system administrator for configuration or troubleshooting.	Created in Windows® settings.
Windows® user with AXIS Camera Station Pro operator or viewer privileges	A Windows® user granted with operator or viewer privileges in AXIS Camera Station Pro.	Created in Windows® settings.
Device		
Device administrator	Used by the administrator to access the camera from the video management system or device webpage.	Created from the device webpage or when you add the device to AXIS Camera Station Pro.

Installation

For instructions on how to install the product, see the installation guide included in the box or on the product's support page on *axis.com*.

Configure your device

Initial Axis recorder setup

After you have configured Windows®, AXIS Recorder Toolbox is opened automatically and you are guided through the first-time configuration setup assistant. In this setup assistant, you can configure several basic and necessary settings before you manage your device in AXIS Recorder Toolbox.

1. Select **Light** or **Dark** theme and click **Next** (if it's available for your product).
2. Change the computer name if you want and click **Next**.
3. Under **Date and time**, configure the following settings and click **Next**.
 - Select a time zone.
 - To set up an NTP server, select **NTP server** and enter the NTP server address.
 - To set manually, select **Manual** and select a date and time.
4. Under **Network settings**, configure the following settings and click **Next**.
 - **Use automatic IP settings (DHCP)** and **Use automatic DNS settings** are turned on by default.
 - If your device is connected to a network with a DHCP server, the assigned IP address, subnet mask, gateway, and preferred DNS are automatically displayed.
 - If your device is not connected to a network or there is no DHCP server available, enter the IP address, subnet mask, gateway, and preferred DNS manually depending on the network requirements.
5. Click **Finish**. If you have changed the computer name, AXIS Recorder Toolbox will prompt you to restart the device.

Configure AXIS Camera Station Pro

Before you start:

- Configure your network depending on your installation. See *Network configuration*.
- Configure your server ports if needed. See *Server port configuration*.
- Consider security issues. See *Security considerations*.

After necessary configurations, you can start to work with AXIS Camera Station Pro:

1. *Start the video management system*
2. *Add devices*
3. *Configure recording method, on page 5*
4. *View live video, on page 5*
5. *View recordings, on page 5*
6. *Add bookmarks, on page 5*
7. *Export recordings, on page 5*
8. *Play and verify recordings in AXIS File Player, on page 6*

Start the video management system

Double-click the AXIS Camera Station Pro client icon to start the client. When you start the client for the first time, it attempts to log in to the AXIS Camera Station Pro server installed on the same computer as the client.

You can connect to multiple AXIS Camera Station Pro servers in different ways.

Add devices

The first time you start AXIS Camera Station S1216 Mk II Tower Recording Server, the **Add devices** page opens and searches the network for devices to add.

1. Select the devices you want to add from the list. If you can't find a device, click **Manual search** or type to filter.
2. Click **Add**.
3. Click **Close** to skip configuration and continue later. To continue with the configuration now:
 - 3.1. Choose **Quick configuration** or **Site Designer configuration**. See for more information.
 - 3.2. Select **Add image overlay for date, time, and text** to add overlays to any Axis cameras that don't already have one.
 - 3.3. Click **Next**.
 - 3.4. Select your **Recording method** preference.
 - 3.5. Click **Next**.
 - 3.6. Choose your **Retention time** and **Recording storage**, and click **Finish** to apply the configuration.

Configure recording method

1. Go to **Configuration > Recording and events > Recording method**.
2. Select a camera.
3. Turn on **Motion detection**, or **Continuous**, or both.
4. Click **Apply**.

View live video

1. Open a **Live view** tab.
2. Select a camera to view its live video.

View recordings

1. Open a **Recordings** tab.
2. Select the camera you want to view recordings from.

Add bookmarks

1. Go to the recording.
2. In the timeline, zoom in and out and move the timeline to put the marker at your desired position.
3. Click .
4. Enter the bookmark name and description. Use keywords to make the bookmark easy to find.
5. Select **Prevent recording deletion** to lock the recording.

Note

To unlock the recording, clear **Prevent recording deletion** or delete the bookmark.

6. Click **OK** to save the bookmark.

Export recordings

1. Open a **Recordings** tab.
2. Select the camera you want to export recordings from.

3. Click  to display the selection markers.
4. Drag the markers to include the recordings that you want to export.
5. Click  to open the **Export** tab.
6. Click **Export...**

Play and verify recordings in AXIS File Player

1. Go to the folder with the exported recordings.
2. Double-click **AXIS File Player**.
3. Click  to show the recording's notes.
4. To verify the digital signature:
 - 4.1. Go to **Tools > Verify digital signature**.
 - 4.2. Select **Validate with password** and enter your password.
 - 4.3. Click **Verify** to see the verification results.

Note

- A digital signature is different from signed video. Signed video lets you trace a recording back to the camera it came from, so you can verify it wasn't tampered with. See *Signed video* and the camera's user manual for more information.
- If stored files don't have any connection with an AXIS Camera Station database (non-indexed files), you need to convert them to make them playable in AXIS File Player. Contact Axis Technical support for help converting your files.

Network configuration

Configure proxy or firewall settings before using AXIS Camera Station S1216 Mk II Tower Recording Server if the client, server, and connected network devices are on different networks.

Client proxy settings

If a proxy server is between the client and the server, configure the proxy settings in Windows on the client computer. Contact Axis support for more information.

Server proxy settings

If the proxy server is between the network device and the server, you must configure the proxy settings in Windows on the server. Contact Axis support for more information.

NAT and Firewall

When a NAT or firewall separates the client and the server, configure it to ensure that the HTTP port, TCP port, and streaming port specified in AXIS Camera Station S1216 Mk II Tower Recording Server Service Control can pass through. Contact your network administrator for help.

Server port configuration

The AXIS Camera Station S1216 Mk II Tower Recording Server server uses ports 55752 (HTTP), 55754 (TCP), 55756 (mobile communication), and 55757 (mobile streaming) for communication between the server and the client. You can change the ports in AXIS Camera Station Service Control if required.

Security considerations

To prevent unauthorized access to cameras and recordings:

- Use strong passwords for all network devices (cameras, video encoders, and auxiliary devices).

- Install the AXIS Camera Station S1216 Mk II Tower Recording Server server, cameras, video encoders, and auxiliary devices on a secure network, separate from the office network. You can install the AXIS Camera Station S1216 Mk II Tower Recording Server client on a computer on another network, for example, a network with internet access.
- Make sure all users have strong passwords.

License a system online

To use automatic licensing, you must register your system and connect it to an organization.

1. Go to **Configuration > Licenses > Management**.
2. Make sure **Automatic licensing** is on.
3. Click **Register...**
4. Sign in using your My Axis account and follow the onscreen instructions.
5. Click **Go to AXIS License Manager** to manage your licenses. Read the *My Systems user manual on help.axis.com* for more information.

License a system that's offline

To license your system manually:

1. Go to **Configuration > Licenses > Management**.
2. Turn off **Automatic licensing**.
3. Click **Export system file...** and save the file to your computer.

Note

You must have an internet connection to access AXIS License Manager. If your client computer doesn't have internet, copy the system file to a computer that does.

4. Open *AXIS License Manager*.
5. In *AXIS License Manager*:
 - 5.1. Select the correct organization, or create one if you haven't already. Read the *My Systems user manual on help.axis.com* for more information.
 - 5.2. Go to **System setup**.
 - 5.3. Click **Upload system file**.
 - 5.4. Click **Upload system file** and select your system file.
 - 5.5. Click **Upload system file**.
 - 5.6. Click **Download license file**.
6. Go back to the AXIS Camera Station S1216 Mk II Tower Recording Server client.
7. Click **Import license file...** and select your license file.
8. Click **Go to AXIS License Manager** to manage your licenses.

Manage local Windows® user accounts

Create a user account

To help keep your personal data and information more secure, we recommend that you add a password for each local account.

Important

Once you create a password for a local account, don't forget it. There's no way to recover a lost password for local accounts.

1. Go to **Settings > Accounts > Other users > Add other user** and click **Add account**.
2. Click **I don't have this person's sign-in information**.
3. Click **Add a user without a Microsoft account**.
4. Enter a user name, password and password hint.
5. Click **Next** and follow the instructions.

Create an administrator account

1. Go to **Settings > Accounts > Other people**.
2. Go to the account you want to change and click **Change account type**.
3. Go to **Account type** and select **Administrator**.
4. Click **OK**.
5. Restart your device and sign in with the new administrator account.

Create a local user group

1. Go to **Computer Management**.
2. Go to **Local Users and Groups > Group**.
3. Right-click **Group** and select **New Group**.
4. Enter a group name and a description.
5. Add group members:
 - 5.1. Click **Add**.
 - 5.2. Click **Advanced**.
 - 5.3. Find the user account(s) you want to add to the group and click **OK**.
 - 5.4. Click **OK** again.
6. Click **Create**.

Delete a user account

Important

When you delete an account you remove the user account from the login screen. You also remove all files, settings and program data stored on the user account.

1. Go to **Settings > Accounts > Other people**.
2. Go to the account you want to remove and click **Remove**.

Change a user account's password

1. Log in with an administrator account.
2. Go to **User Accounts > User Accounts > Manage another account** in sequence.

You'll see a list with all user accounts on the device.

3. Select the user account whose password you would like to change.
4. Click **Change the password**.
5. Enter the new password and click **Change password**.

Create a password reset disk for a user account

We recommend to create a password reset disk on a USB flash drive. With this, you can reset the password. Without a password reset disk, you can't reset the password.

Note

If you're using Windows® 10, or later, you can add security questions to your local account in case you forget your password, so you don't need to create a password reset disk. To do this, go to **Start** and click **Settings > Sign-in options > Update your security questions**.

1. Sign in to your device with a local user account. You can't create a password reset disk for a connected account.
2. Plug an empty USB flash drive into your device.
3. From the Windows® search field, go to **Create a password reset disk**.
4. In the **Forgotten Password** setup assistant, click **Next**.
5. Select your USB flash drive and click **Next**.
6. Type your current password and click **Next**.
7. Follow the onscreen instructions.
8. Remove the USB flash drive and keep it in a safe place. You don't have to create a new disk when you change your password even if you change it several times.

Manage AXIS Camera Station Pro user accounts

User permissions

Go to **Configuration > Security > User permissions** to see the users and groups in AXIS Camera Station S1216 Mk II Tower Recording Server.

Note

Administrators of the computer that runs the AXIS Camera Station S1216 Mk II Tower Recording Server are automatically granted administrator privileges in AXIS Camera Station S1216 Mk II Tower Recording Server. You can't change or remove the Administrators group's privileges.

Before you can add a user or group, make sure they're registered on the local computer or have a Windows® Active Directory user account. To add users or groups, see *Add users or groups*.

When a user belongs to a group, they receive the highest role permission assigned to them individually or to the group. For example, a user with access to camera X who also belongs to a group with access to cameras Y and Z has access to all three cameras.

	Indicates the entry is a single user.
	Indicates the entry is a group.
Name	Username as it appears in the local computer or Active Directory.
Domain	The domain that the user or group belongs to.
Role	The access role assigned to the user or group. Possible values: Administrator, Operator, and Viewer.
Details	Detailed user information as it appears on the local computer or in Active Directory.
Server	The server that the user or group belongs to.

Add users or groups

Microsoft Windows® and Active Directory users and groups can access AXIS Camera Station S1216 Mk II Tower Recording Server. To add a user to AXIS Camera Station S1216 Mk II Tower Recording Server, you must add users or a group to Windows®.

To add a user in Windows® 10 and 11:

- Press the Windows key + X and select **Computer Management**.
- In the **Computer Management** window, navigate to **Local Users and Groups > Users**.
- Right-click **Users** and select **New User**.
- In the popup dialog, enter the new user's details and clear **User must change password at next login**.
- Click **Create**.

If you use an Active Directory domain, consult your network administrator.

Add users or groups

1. Go to **Configuration > Security > User permissions**.
2. Click **Add**. The available users and groups appear in the list.
3. Under **Scope**, select where to search for users and groups.
4. Under **Show**, select to show users or groups. The search results may not appear if there are too many users or groups. Use the filter to narrow the results.

5. Select the users or groups and click **Add**.

Scope	
Server	Select to search for users or groups on the local computer.
Domain	Select to search for Active Directory users or groups.
Selected server	When connected to multiple AXIS Camera Station S1216 Mk II Tower Recording Server servers, select a server to search for users or groups on that server.

Configure a user or group

1. Select a user or group in the list.
2. Under **Role**, select **Administrator**, **Operator**, or **Viewer**.
3. If you selected **Operator** or **Viewer**, you can configure the user or group privileges. See *User or group privileges*.
4. Click **Save**.

Remove a user or group

1. Select the user or group.
2. Click **Remove**.
3. In the pop-up dialog, click **OK** to remove the user or group.

User or group privileges

There are three roles you can assign to a user or group. For how to define the role for a user or group, see *Add users or groups*.

Administrator – Full access to the entire system, including access to live and recorded video of all cameras, all I/O ports, and views. This role is required to access system configuration.

Operator – Select cameras, views, and I/O ports to get access to live and recorded video. An operator has full access to all functionality of AXIS Camera Station S1216 Mk II Tower Recording Server except system configuration.

Viewer – Access to live video of selected cameras, I/O ports, and views. A viewer doesn't have access to recorded video or system configuration.

Cameras

The following access privileges are available for users or groups with the **Operator** or **Viewer** role.

Access	Allow access to the camera and all camera features.
Video	Allow access to live video from the camera.
Audio listen	Allow access to listen from the camera.
Audio speak	Allow access to speak to the camera.
Manual Recording	Allow starting and stopping recordings manually.

Mechanical PTZ	Allow access to mechanical PTZ controls. Available only for cameras with mechanical PTZ.
PTZ priority	Set the PTZ priority. A lower number means a higher priority. No assigned priority is set to 0. An administrator has the highest priority. When a role with higher priority operates a PTZ camera, others can't operate the same camera for 10 seconds by default. Available only for cameras with mechanical PTZ that have Mechanical PTZ selected.

Views

The following access privileges are available for users or groups with the **Operator** or **Viewer** role. You can select multiple views and set the access privileges.

Access	Allow access to the views in AXIS Camera Station S1216 Mk II Tower Recording Server.
Edit	Allows editing of views in AXIS Camera Station S1216 Mk II Tower Recording Server.

I/O

The following access privileges are available for users or groups with the **Operator** or **Viewer** role.

Access	Allow full access to the I/O port.
Read	Allows viewing the state of the I/O port without changing it.
Write	Allows changing the state of the I/O port.

System

You can't configure grayed-out access privileges in the list. A check mark means the user or group has this privilege by default.

The following access privileges are available for users or groups with the **Operator** role. **Take snapshots** is also available for the **Viewer** role.

Take snapshots	Allows taking snapshots in live view and recording mode.
Export recordings	Allow exporting recordings.
Generate incident report	Allow generating incident reports.
Prevent access to recordings older than	Prevent access to recordings older than the specified number of minutes. Users can't find these recordings when they search.
Access alarms, tasks, and logs	Get alarm notifications and allow access to the Alarms and tasks bar and Logs tab.
Access data search	Allow searching for data to track what happened at the time of an event.

Add categories to events	Allow adding categories to events in the Recordings tab.
Remove categories from event	Allow removing categories from events in the Recordings tab.

Access control

The following access privileges are available for users or groups with the **Operator** role. **Access Management** is also available for the **Viewer** role.

Access control configuration	Allow configuration of doors and zones, identification profiles, card formats, and PIN, encrypted communication, and multi-server.
Access management	Allow access management and access to the Active Directory settings.

The following access privileges are available for users or groups with the **Viewer** role.

System health monitoring

The following access privileges are available for users or groups with the **Operator** role. **Access to system health monitoring** is also available for the **Viewer** role.

Configuration of system health monitoring	Allows configuration of system health monitoring.
Access to system health monitoring	Allows access to system health monitoring.

Manage your device

Update Secure Boot certificates

Microsoft is retiring the 2011 Secure Boot certificates in June 2026 and replacing them with new 2023 certificates. To keep your recorder safe, install the 2023 certificates before then.

Installing the 2023 certificates requires Windows 10 LTSC (Long-Term Servicing Channel) or Windows 11 LTSC. If your device is within warranty but is running Windows 10 SAC (Semi-Annual Channel) instead of an LTSC version, contact Axis Technical Support. They can tell you if you can upgrade to an LTSC version before you update the BIOS or change any certificates.

Note

After June 2026, devices without the 2023 certificates will keep working as normal, but won't receive new security protections for the early boot process, including Windows Boot Manager updates and revocation lists for new vulnerabilities.

Check your certificate status

To verify that the 2023 certificates are installed and that the Windows bootloader has been updated, use one of the following methods:

Method 1:

1. Open Registry Editor.
2. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing.
3. Check the UEFICA2023Status value. If the value says **Updated**, the 2023 certificate is installed.

 (Default)	REG_SZ	(value not set)
 BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
 ConfidenceLevel	REG_SZ	No Data Observed - Action Required
 ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
 LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
 UEFICA2023Status	REG_SZ	Updated
 WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

Method 2:

1. Open Windows Security.
2. Go to Device security.
3. Under Secure boot, check the status message. If the certificate is up to date, the card shows: "Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed."

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

Note

Windows Security only shows certificate status if your device has the April 14, 2026 cumulative update or later installed. If you don't see a certificate status message, install the latest Windows update or use Method 1 instead.

Recommended actions

A BIOS update stores the 2023 certificates permanently in the firmware. This is the most reliable method, and we recommend it even if you've already installed the certificates through Windows Update.

Important

If you only install the certificates through Windows Update and then reset the BIOS Secure Boot keys to factory defaults, the certificates will be lost and the device won't start with Secure Boot turned on. Update the BIOS to make the certificates permanent before you reset Secure Boot keys.

Update certificate through the BIOS

For AXIS S12 and S93 series, get the BIOS update from Dell instead of Axis.com. See *Update the BIOS*, on page 15.

More information:

- *Dell: Microsoft 2011 Secure Boot Certificate Expiration.*
- *Dell: PowerEdge Server BIOS Update Guidelines for Secure Boot.*

Update certificate through Windows Update

If a BIOS update isn't available yet for your model, you can get the 2023 certificates through Windows Update instead.

Important

Certificates installed this way are stored in the current Secure Boot database, not in the firmware. If you reset the BIOS Secure Boot keys to factory defaults, you'll lose the certificates and the device may not be able to start with Secure Boot turned on. Install a BIOS update as soon as one is available for your model, even if you've already used this method.

To use this path:

1. Make sure your device runs Windows 10 LTSC or Windows 11 LTSC.
2. Install all Windows updates released April 14, 2026 or later.
3. Go to **Windows Security > Device security > Secure Boot** to check your certificate status.
4. If the certificate doesn't update after installing the latest updates, check the **UEFICA2023Status** registry value. If your device remains ineligible for the automatic update, update the BIOS or contact Axis Technical Support.

Important

Don't manually revoke the 2011 certificate until you've confirmed that all recovery media, boot environments, and drivers in your environment are signed with the 2023 certificate. Revoking the 2011 certificate too early will leave your device unable to start with Secure Boot turned on.

Check the current BIOS version

To check the current BIOS:

1. Power on the device and repeatedly press F2 until the Axis logo appears.
2. The version number is shown as first entry under **Overview**.

Update the BIOS

1. Go to *Dell support*.
2. In the **Service tag** field, enter the last 7 characters of your device's serial number. For example, HW030ABC1234.
3. Go to **Drivers & Downloads** and search for "BIOS".

4. If no newer version appears for your OEM product name (for example, "OEMR XL R760xs"), search again using the generic Dell platform name instead of the serial number (for example, "R760xs").
5. Download and install the latest BIOS version released after April 2026.

Update Windows®

Windows® periodically checks for updates. When an update is available, your device automatically downloads the update but you've to install it manually.

Note

Recording will be interrupted during a scheduled system restart.

To manually check for updates:

1. Go to **Settings > Windows Update**.
2. Click **Check for updates**.

Configure Windows® update settings

It is possible to change how and when Windows® do its updates to suit your needs.

Note

All ongoing recordings stop during a scheduled system restart.

1. Open the Run app.
 - Go to **Windows System > Run**, or
2. Type `gpedit.msc` and click **OK**. The Local Group Policy Editor opens.
3. Go to **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
4. Configure the settings as required, see example.

Example:

To automatically download and install updates without any user interaction and have the device restart, if necessary, at out of office hours, use the following configuration:

1. Open **Always automatically restart at the scheduled time** and select:
 - 1.1. **Enabled**
 - 1.2. **The restart timer will give users this much time to save their work (minutes): 15.**
 - 1.3. Click **OK**.
2. Open **Configure Automatic Updates** and select:
 - 2.1. **Enabled**
 - 2.2. **Configure Automatic updates: Auto download and schedule the install**
 - 2.3. **Schedule Install day: Every Sunday**
 - 2.4. **Schedule Install time: 00:00**
 - 2.5. Click **OK**.
3. Open **Allow Automatic Updates immediate installation** and select:
 - 3.1. **Enabled**
 - 3.2. Click **OK**.

Add a hard drive

1. Prepare the device:
 - 1.1. Shut down the system and disconnect the power cord.

- 1.2. Place the device on its side with the two thumb screws on the back facing upward.
- 1.3. Unscrew the two thumb screws on the back of the chassis.
- 1.4. Slide the cover off by gently pulling the handle on the side panel, then lift it off.
- 1.5. Unsnap the three hinges to remove the front panel.
2. **Attach the hard drive:**
 - 2.1. Lift the hard drive bracket upward to remove it.
 - 2.2. Unscrew the four blue rubber mounting screws from the primary hard drive bracket.
 - 2.3. Attach the four mounting screws to the sides of the new hard drive. Don't use the middle hole on each side.
 - 2.4. Insert the hard drive into the bracket with the SATA connectors facing outward, then push it gently until you hear a click.
 - 2.5. Reattach the bracket to the chassis, starting with the front-facing side.
 - 2.6. Connect the free SATA cables to the hard drive (both data and power).
3. **Close and restart:**
 - 3.1. Reattach the front panel.
 - 3.2. Reattach the side panel and tighten the thumb screws
 - 3.3. Reconnect the power cord and start the system.
4. **Next steps:**
 - If you want to use RAID, continue with *Create RAID volume, on page 17*.
 - If you don't want to use RAID, skip to *Add a new recording storage, on page 18*.

Create RAID volume

1. Make sure that the disks to be used in the RAID volume are detected.
 - 1.1. Turn on your device and instantly press F12 until the Axis logo appears.
 - 1.2. In the UEFI boot menu, select **Device Configuration** and press Enter.
 - 1.3. In the Intel® Rapid Storage Technology menu, make sure that the disks are correctly displayed under **Non-RAID Physical Disks**.

Note

Only RAID 0 and RAID 1 are available on devices that have physical space for just an additional single drive.

2. In the Intel Rapid Storage Technology menu, select **Create RAID Volume** and press Enter.
3. Type a name for the volume.
4. Choose the RAID level.
 - 4.1. Select **RAID Level** and press Enter.
 - 4.2. In the popup dialog, select the RAID level you want to use and press enter.
5. Include the disks to be used in the volume.
 - 5.1. Select a disk and press enter.
 - 5.2. Select **X** to include this disk in the volume.
 - 5.3. Repeat until you have selected all the disks you want to use.
6. Leave **Stripe Size** and **Capacity** to the default values, unless specified.
7. Select **Create Volume** and press enter.
8. In the Intel Rapid Storage Technology menu, the newly created RAID volume appears under **RAID Volumes**.
9. Press **Esc** and then press **Y** to save and exit to the UEFI menu.

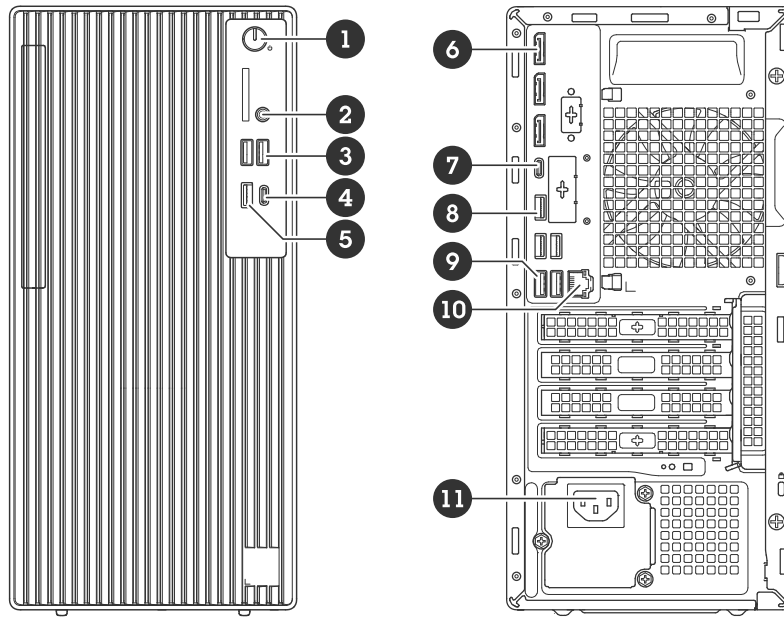
10. Press CTRL + ALT+ DELETE to restart your device.

Add a new recording storage

1. Create and format a new hard disk partition in Windows:
 - 1.1. Right-click the **Start menu** and select **Disk Management**.
 - 1.2. Click **OK** if the **Initialize Disk** popup appears. If it doesn't, right-click on the new hard drive and select **Initialize Disk**.
 - 1.3. Right-click on an unallocated region on the newly initialized disk and select **New Simple Volume**.
 - 1.4. Follow the wizard to set the volume size, assign a drive letter, and format the partition.
 - 1.5. Complete the wizard to create the new simple volume.
2. Add a new recording storage in AXIS Camera Station Pro:
 - 2.1. Open AXIS Camera Station Pro.
 - 2.2. Go to **Storage > Management**.
 - 2.3. Click **Add...**
 - 2.4. Select the newly added drive and click **OK**.
 - 2.5. Go to **Storage > Selection**.
 - 2.6. Select which devices you want to transfer recording data to the new drive.
 - 2.7. In the **Store to** drop-down list, select the new drive and click **Apply**.

For more information about storage management, see *AXIS Camera Station Pro – User manual*.

Product overview



- 1 Power button/power LED
- 2 Universal audio jack
- 3 USB 2.0 ports
- 4 USB 3.2 gen 2x2 USB-C port
- 5 USB 3.2 gen 2x1 port
- 6 DisplayPorts™
- 7 USB 3.2 gen 2x1 USB-C port
- 8 USB 3.2 gen 1x1 ports
- 9 USB 2.0 ports
- 10 1 GbE Ethernet port
- 11 Power connector

Troubleshooting

Perform a system recovery

Internal recovery

If the device has had a system failure, perform an internal recovery to restore the system.

1. Open **Windows Settings**.
2. Select **System**.
3. In the menu, select **Recovery**.
4. Under **Recovery options** select **Reset this PC**.
5. Select **Keep my files** or **Remove everything**.
 - **Keep my files** will keep all your personal files and user data, as well as all Axis installed software.
 - **Remove everything** will remove all your personal files and user data, but will keep all Axis installed software (factory default).
6. Follow the onscreen instructions.

Note

Before selecting **Reset**, you can view a list of apps that will be removed in the process. Axis apps will be restored after the recovery, but if you've installed other apps, they won't be restored.

Important

After a successful recovery, it's important that you log in to Windows with an Administrator account to finalize the recovery process.

External recovery

If the device has had a complete system failure, you must use a recovery image to recreate the Windows® system. To download the AXIS Network Video Recovery Kit, contact *AXIS Technical Support* and supply the serial number of your device.

Note

The AXIS Network Video Recorder Recovery Kit comes in two variants:

- **sb11** – for devices still using the 2011 certificate.
- **sb23** – for devices that have moved to the 2023 certificate.

Check your certificate status before you download the Recovery Kit, and select the matching variant. If you select the wrong variant, the installation won't produce a bootable result, and you'll need to start over with the correct image. This won't damage your device.

If your device already has the 2023 certificate installed, the sb11 variant is still safe to use, as long as the 2011 certificate hasn't been manually revoked. Once it's revoked, only sb23 will work.

1. Download the AXIS Network Video Recovery Kit and an ISO to USB writing tool of your choice.
2. Insert a USB drive into your computer.
 - Use a USB drive with a minimum of 16 GB.
 - The USB drive will be formatted, and all existing data will be erased.
3. Run the ISO to USB writing tool and follow the onscreen instructions.
 - Writing data to the USB drive takes approximately 10 to 15 minutes. Don't remove the USB drive until the process is complete.
4. After the ISO to USB tool is complete, remove the USB drive from your computer and plug it into your device.
5. Start your device. When you see the Axis splash screen, press **F12** to open the boot menu.

6. Select your USB drive and press **Enter**. The system boots into the AXIS Network Video Recorder Recovery Kit.
7. Click **Start** and follow the onscreen instructions.
 - The recovery takes roughly 10 to 15 minutes to complete.

Troubleshoot AXIS Camera Station Pro

For information about how to troubleshoot AXIS Camera Station Pro, go to the *AXIS Camera Station Pro user manual*.

Need more help?

Useful links

- *AXIS Camera Station Pro user manual*
- *Sign in to AXIS Secure Remote Access*
- *Sign in to AXIS Secure Remote Access v2*
- *What to include in an Antivirus allow list for AXIS Camera Station*

Contact support

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

T10231342

2026-07 (M2.4)

© 2025 – 2026 Axis Communications AB