AXIS Camera Station S1264 Rack Recording Server

User manual

AXIS Camera Station S1264 Rack Recording Server

Table of Contents

About your device 3
Get started 4
Install your device 5
Before installation 5
Configure your device 13
Initial Axis recorder setup 13
Configure AXIS Camera Station 13
License a system online 16
License a system offline 16
Manage Windows® user accounts 18
Create a user account 18
Create an administrator account 18
Create a local user group 18
Delete a user account 18
Change a user account's password 19
Create a password reset disk for a user account 19
Manage AXIS Camera Station user accounts 20
Configure user permissions 20
Add users or groups 20
User or group privileges 21
Manage your device 23
Update Windows® 23
Configure Windows update settings 23
Change the RAID 24
Add a hard drive 24
Configure iDRAC 27
Cybersecurity 28
Troubleshooting 30
Check the current BIOS version 30
Upgrade BIOS 30
Run diagnostics 30
Perform a system recovery 30
Export a SupportAssist collection 31
Troubleshoot the power supply unit 31
Troubleshoot memory errors 32
Troubleshoot AXIS Camera Station 32
Product overview 33
Front and rear sides 33
Specifications 33
Need more help? 37
Useful links 37
Contact support 37

AXIS Camera Station S1264 Rack Recording Server

About your device

About your device

AXIS Camera Station S12 Recorder series consist of out-of-the-box ready rack servers and workstations validated for reliable high-definition surveillance up to 4K. For quick and easy installation, the recorder series is preconfigured and preloaded with AXIS Camera Station video management software including licenses plus all necessary system software. The system configuration can easily be imported from AXIS Site Designer, and AXIS Camera Station lets you take full advantage of Axis wide range of video surveillance devices. With enterprise-grade hard disks, operating system stored on solid-state drive, the recorder series provides high-performance and reliability for your system.

Get started

Get started

Note

For systems with over 80 video channels or a recording bitrate over 750 Mbit/s, we recommend setting the size allocated for recording to 95%. All devices with AXIS Camera Station 5.56 or later has 95% as a default. See *Adjust storage capacity on page 14*.

The standard workflow to configure an AXIS Camera Station 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 13*.
4. Configure Windows. We recommend to:
   - Update Windows to the latest version. See *Update Windows® on page 23*.
   - Create a standard user account. See *Create a user account on page 18*.
5. Update AXIS Camera Station to the latest version.
   - If your system is online: open the AXIS Recorder Toolbox app and click **Update AXIS Camera Station**.
   - If your system is offline: go to *axis.com* and download the latest version.
6. *Configure AXIS Camera Station*
7. Register your AXIS Camera Station licenses.
   - *License a system online on page 16*
   - *License a system offline on page 16*
8. Connect your system to the AXIS Camera Station mobile viewing app. See *Connect to AXIS Camera Station server.*

To watch this video, go to the web version of this document.

help.axis.com/?&piaId=76450&section=about-your-device

Install your device

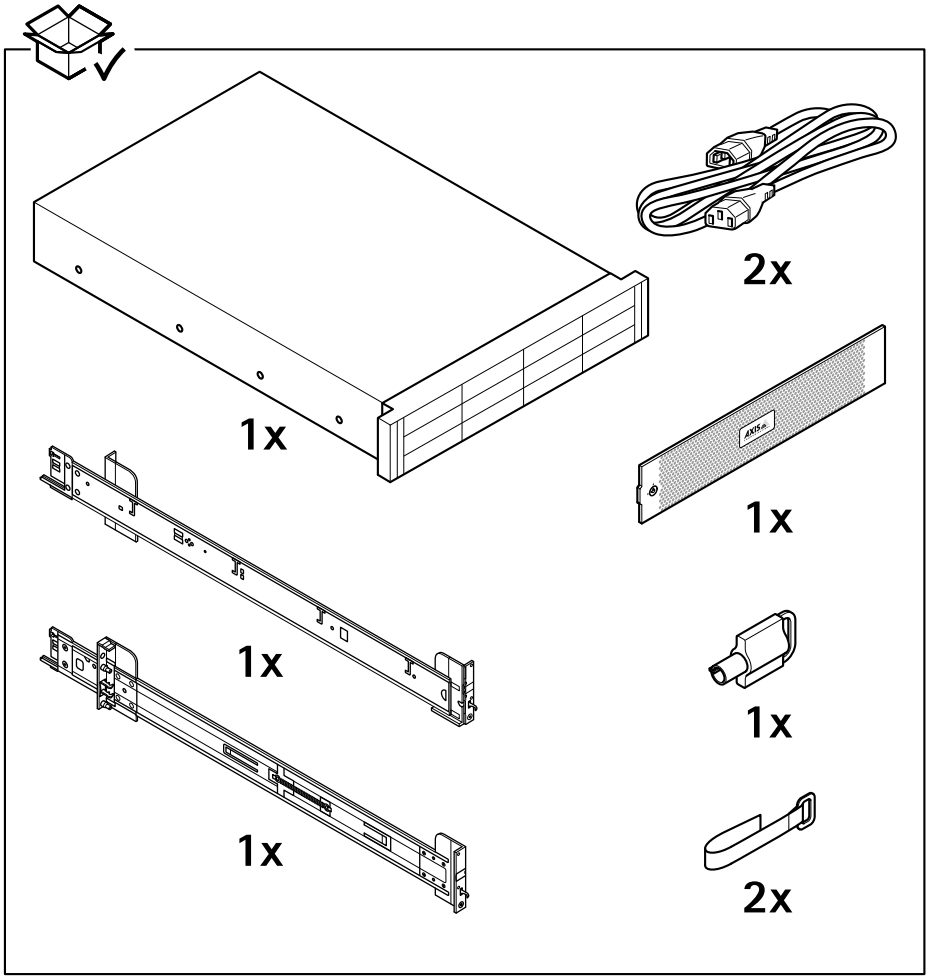
Before installation

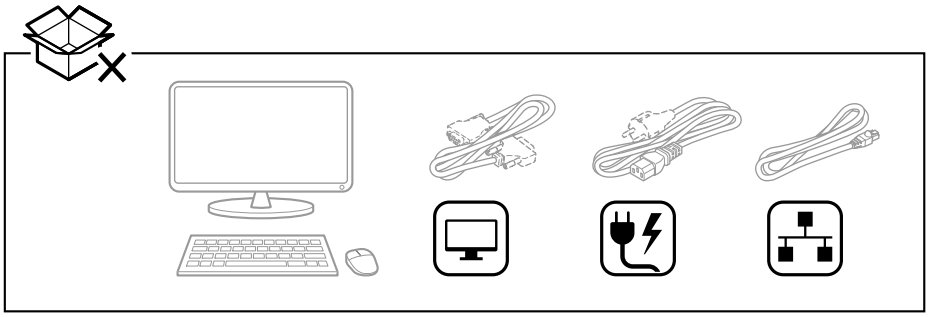
- Prepare additional accessories used for installation: monitor, mouse, keyboard and network cable.
- Note that the power cable to the wall is not included in the box.
- Understand the usage of different user accounts.

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

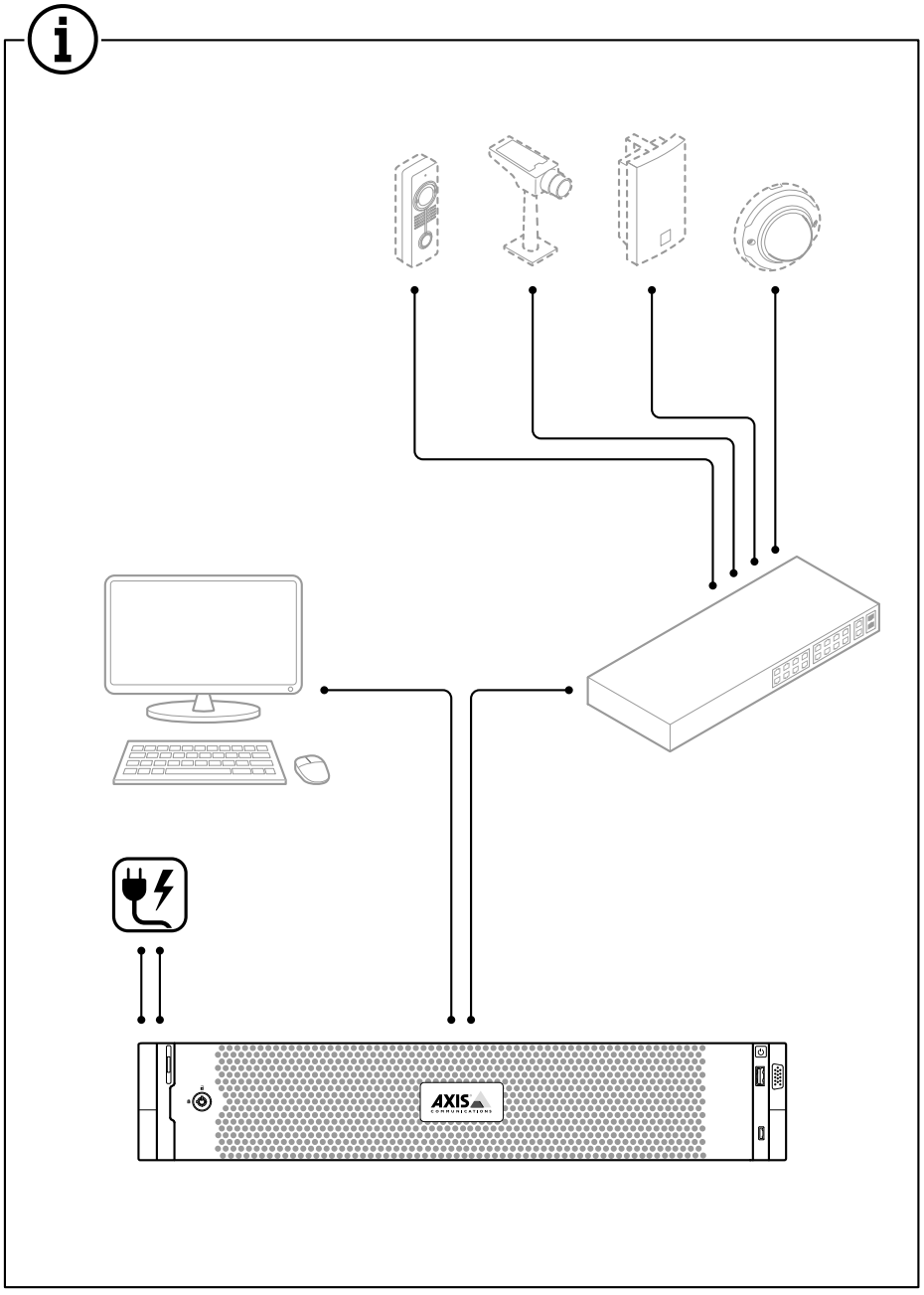
User account	Description	Note
MyAxis	Used to download the latest software, access the license system, Axis Secure Remote Access, and System Health Monitoring.	Registered from *my.axis.com*.
Windows®		
Windows administrator	Administrator privileges in Windows. We recommend you do not use it as AXIS Camera Station administrator.	Created during initial Windows setup.
Windows user with AXIS Camera Station administrator privileges	A Windows user granted with administrator privileges in AXIS Camera Station to be used by system integrator or system administrator for configuration or troubleshooting.	Created in Windows settings.
Windows user with AXIS Camera Station operator or viewer privileges	A Windows user granted with operator or viewer privileges in AXIS Camera Station.	Created in Windows settings.
Hardware management		
iDRAC	Used to access the iDRAC (Integrated Dell Remote Access Controller) tool.	Username: root Password: Printed on the back of the information tag.
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.

Install your device

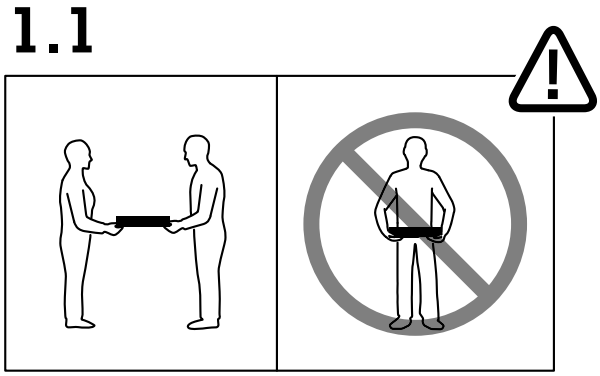


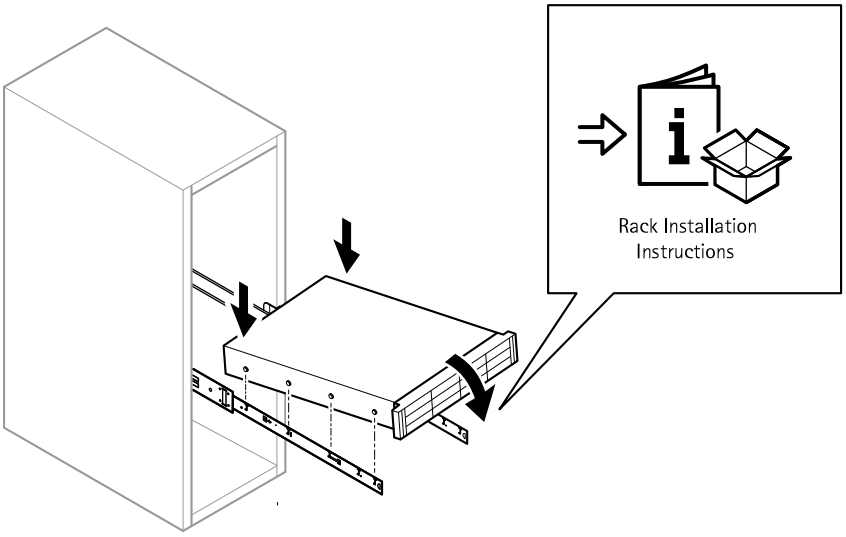


Install your device

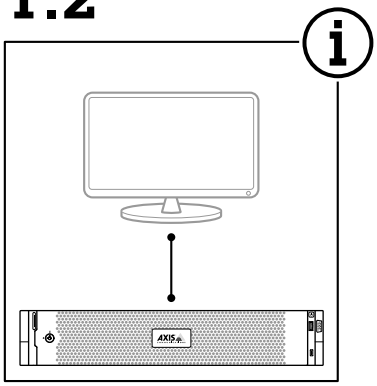


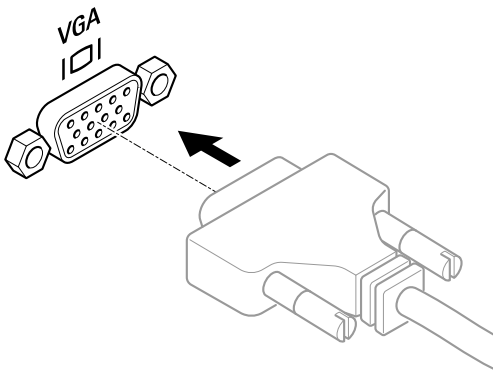
Install your device



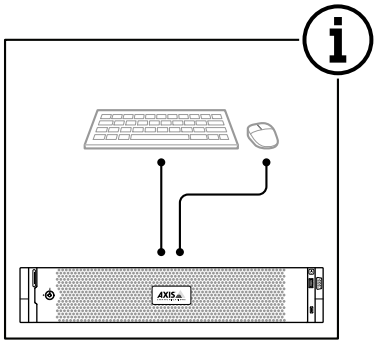


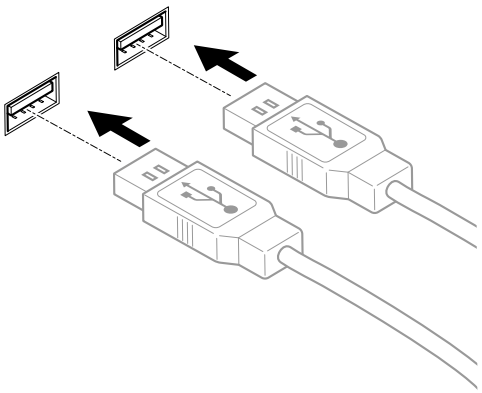
1.2



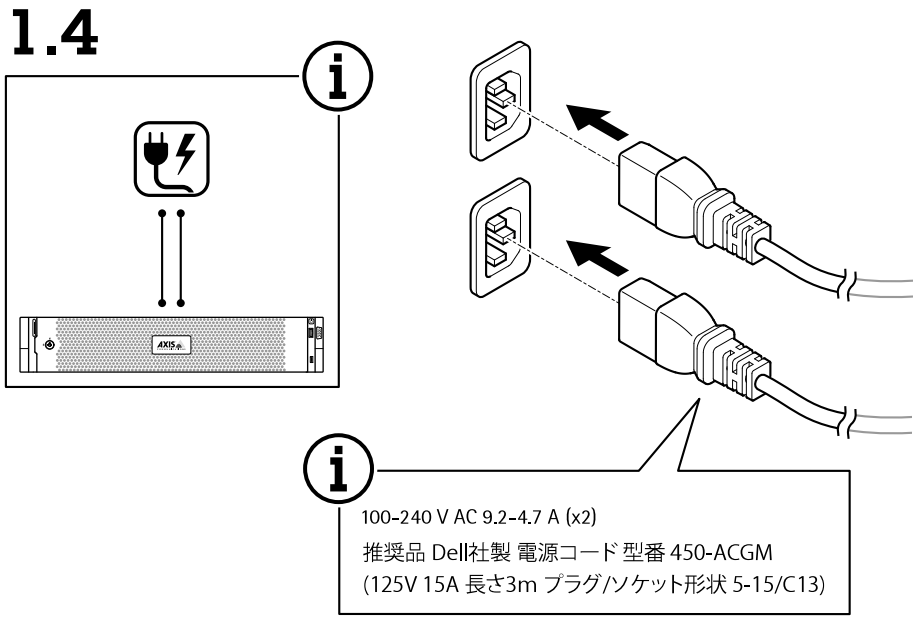


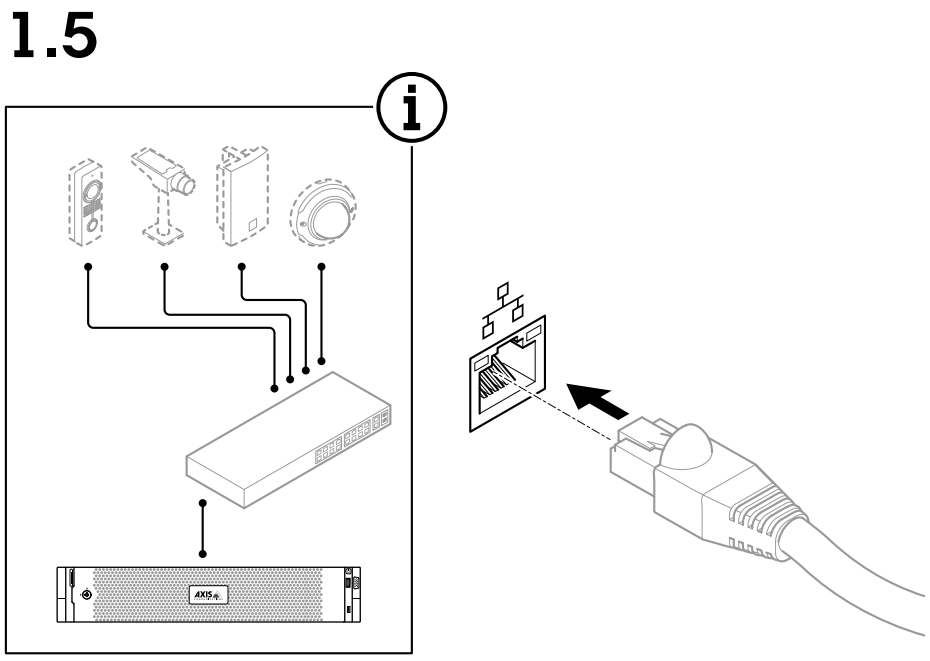
1.3



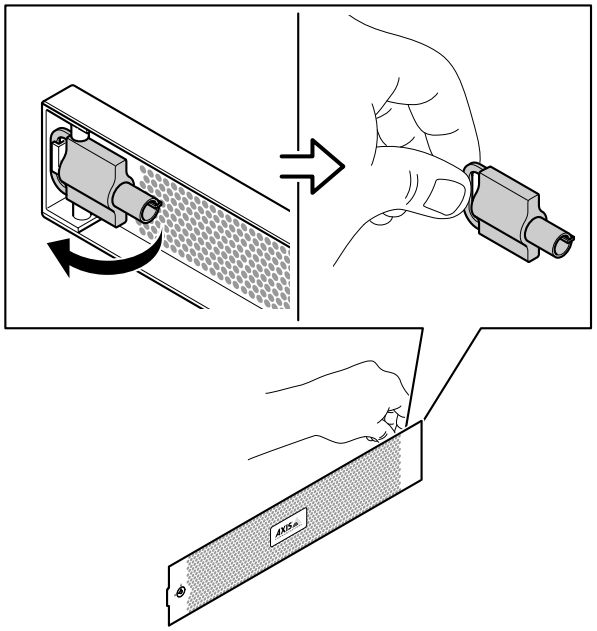


Install your device

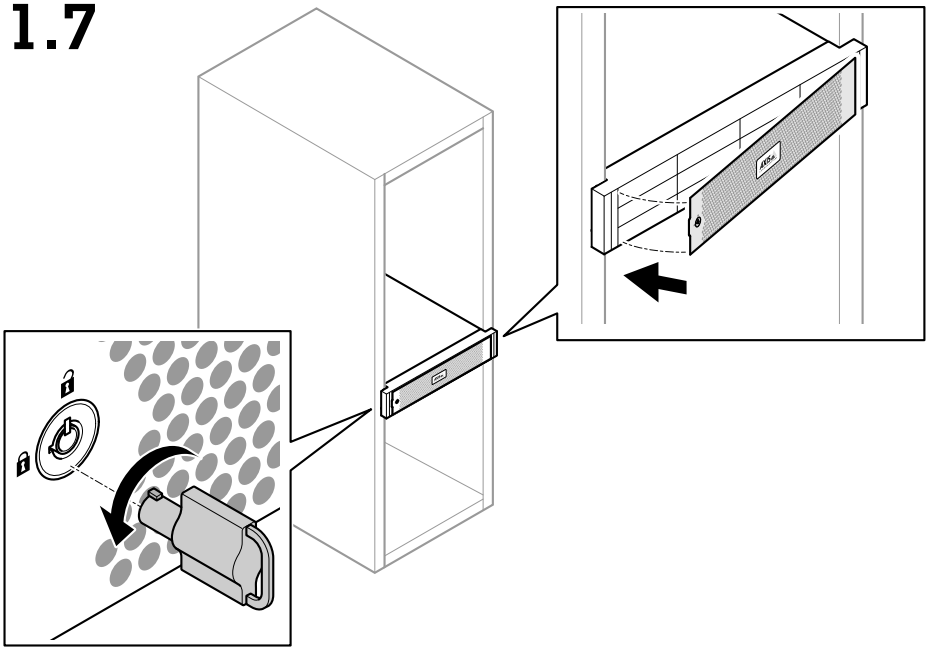




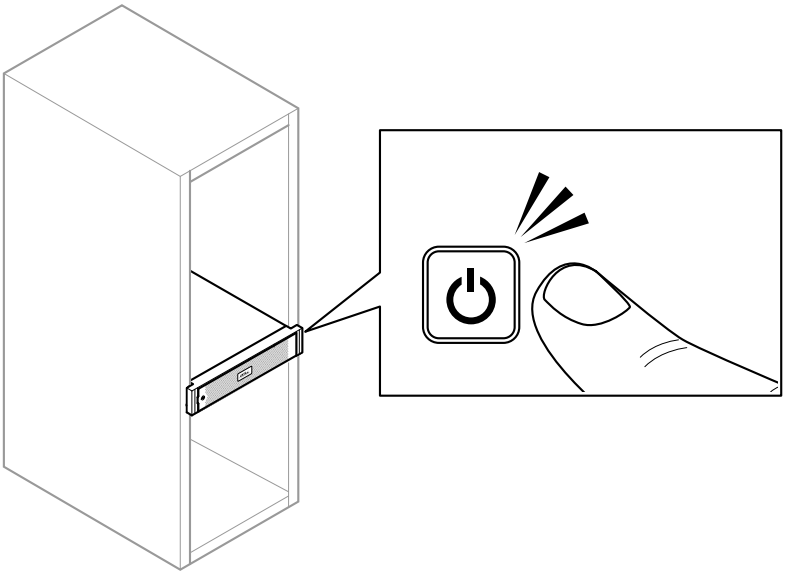
1.6

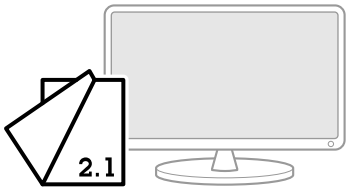


1.7



1.8





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

This Get started tutorial will walk you through the basic steps to make your system up and running.

Before you start, you may need to:

- 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:

1. *Start the video management system*
2. *Add devices*
3. *Configure recording method on page 14*
4. *View live video on page 14*
5. *View recordings on page 14*
6. *Add bookmarks on page 14*
7. *Export recordings on page 15*
8. *Play and verify recordings in AXIS File Player on page 15*

Configure your device

Start the video management system

Double-click the AXIS Camera Station 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 server installed on the same computer as the client.

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

Add devices

The Add devices page opens the first time you start AXIS Camera Station. AXIS Camera Station searches the network for connected devices and shows a list of devices found.

1. Select the cameras you want to add from the list. If you can't find your camera, click **Manual search**.
2. Click **Add**.
3. Select **Quick configuration** or **Site Designer configuration**. Click **Next**.
4. Use the default settings and ensure the recording method is **None**. Click **Install**.

Adjust storage capacity

Note

For systems with over 80 video channels or a recording bitrate over 750 Mbit/s, we recommend setting the size allocated for recording to 95%. All devices with AXIS Camera Station 5.56 or later has 95% as a default.

1. Go to **Configuration > Storage > Management** and select a local storage or shared network drive from the storage list.
2. Move the slide bar to set the maximum space to be used by AXIS Camera Station in the Overview section.
3. Click **Apply**.

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 of the camera, 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 in the description to make the bookmark easy to find and recognize.
5. Select **Prevent recording deletion** to lock the recording.

Note

It's not possible to delete a locked recording. To unlock the recording, clear the option 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**. The verification result page appears.

Note

Digital signature is different from Signed video. Signed video allows you to trace video back to the camera it came from, making it possible to verify that the recording wasn't tampered with. See *Signed video* and the camera's user manual for more information.

Network configuration

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

Client proxy settings

When a proxy server separates the client and the server, configure the client proxy settings.

1. Open the AXIS Camera Station client.
2. Click **Change client proxy settings**.
3. Change the client proxy settings.

4. Click **OK**.

Server proxy settings

When a proxy server separates the network devices and the server, configure the server proxy settings.

1. Open AXIS Camera Station Service Control.
2. Select **Modify settings**.
3. In the Proxy settings section, use the default **System account internet option** or select **Use manual proxy settings**.
4. Click **Save**.

NAT and Firewall

When a NAT, firewall, or similar separates the client and the server, configure the NAT or firewall to ensure that the HTTP port, TCP port, and streaming port specified in AXIS Camera Station Service Control can pass through the firewall or NAT. Contact the network administrator for instructions on configuring the NAT or firewall.

Server port configuration

For more information, see .

Security considerations

To prevent unauthorized access to cameras and recordings, keep the following in mind:

- Use strong passwords for all network devices (cameras, video encoders, and auxiliary devices).
- Install server, cameras, video encoders, and auxiliary devices on a secure network separate from the office network. You can install the client on a computer on another network, for example, a network with internet access.
- Make sure all users have strong passwords. Windows Active Directory provides a high level of security.

License a system online

Both the AXIS Camera Station client and the server must have internet connection.

1. Go to **Configuration > Licenses > Management**.
2. Make sure **Manage licenses online** turns on.
3. Sign in with your My Axis account.
4. The license key automatically generates and appears under **License keys**.
5. If you purchased license keys separately, enter your license key under **Add license key**.
6. Click **Add**.
7. In AXIS Camera Station client, make sure your license keys appear under **Configuration > Licenses > Keys**.

License a system offline

1. Go to **Configuration > Licenses > Management**.
2. Turn off **Manage licenses online**.
3. Click **Export system file**.
4. Save your system file to a USB flash drive.

Configure your device

5. Go to AXIS License Portal, *axis.com/licenses*,
6. Sign in with your My Axis account.
7. Click **Upload system file** to upload the system file from your USB flash drive.
8. The license key automatically generates and shows under **License keys**.
9. If you purchased license keys separately, enter your license key under **Add license key**.
10. Click **Add**.
11. Under **License keys**, click **Download license file** and save the file to a USB flash drive.
12. In AXIS Camera Station client, go to **Configuration > Licenses > Management**.
13. Click **Import license file** and select the license file on your USB flash drive.
14. Make sure your license keys appear under **Configuration > Licenses > Keys**.

Manage 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 people > Add someone else to this PC**.
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, got 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 placet. 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 user accounts

Configure user permissions

Go to **Configuration > Security > User permissions** to view the users and groups that exists in .

Note

Administrators of the computer that runs server are automatically given administrator privileges to . You can't change or remove the Administrators group's privileges.

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

When a user is part of a group, the user gets the highest role permission assigned to the individual or the group. The user also gets the access granted as an individual and receives the rights as part of a group. For example, a user has access to camera X as an individual. The user is also a member of a group that has access to cameras Y and Z. The user therefore has access to cameras X, Y, and Z.

	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 given to the user or group. Possible values: Administrator, Operator, and Viewer.
Details	Detailed user information as it appears in the local computer or 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 . To add a user to , you must add users or a group to Windows.

To add a user in Windows vary depending on which version of Windows you use. Follow the instructions on *Microsoft's site*. If you use an Active Directory domain network, consult your network administrator

Add users or groups

1. Go to **Configuration > Security > User permissions**.
2. Click **Add**.

   The list shows available users and groups.
3. Under **Scope**, select where to search for users and groups.
4. Under **Show**, select to show users or groups.

   The search result doesn't display if there are too many users or groups. Use the filter function.
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 servers, select a server from the **Selected server** drop-down menu.

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 dialogue, click **OK** to remove the user or group.

User or group privileges

There are three roles you can give 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 configure anything in the system.

Operator – Select cameras, views, and I/O ports to get access to live and recorded. An operator has full access to all functionality of 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 to start and stop recordings manually.
Mechanical PTZ	Allow access to mechanical PTZ controls. Only available 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. Only available for cameras with mechanical PTZ and 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 .
Edit	Allow to edit the views in .

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	Allow to view the state of the I/O port. The user can't change the port state.
Write	Allow to change the state of the I/O port.

System

You can't configure greyed out access privileges in the list. Privileges with check mark means the user or group have 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	Allow to take snapshots in the live view and recordings modes.
Export recordings	Allow to export recordings.
Generate incident report	Allow to generate incident reports.
Prevent access to recordings older than	Prevent access to recordings older than the specified number of minutes. When using search, the user doesn't find recordings older than the specified time.
Access alarms, tasks, and logs	Get alarm notifications and allow access to the **Alarms and tasks** bar and **Logs** 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.

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	Allow configuration of the system health monitoring system.
Access to system health monitoring	Allow access to the system health monitoring system.

Manage your device

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 > Update & Security > 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:

5. Open **Always automatically restart at the scheduled time** and select:
   5.1 **Enabled**
   5.2 **The restart timer will give users this much time to save their work (minutes)**: 15.
   5.3 Click **OK**.
6. Open **Configure Automatic Updates** and select:
   6.1 **Enabled**
   6.2 **Configure Automatic updates**: Auto download and schedule the install
   6.3 **Schedule Install day**: Every Sunday
   6.4 **Schedule Install time**: 00:00
   6.5 Click **OK**.
7. Open **Allow Automatic Updates immediate installation** and select:
   7.1 **Enabled**

7.2 Click **OK**.

Change the RAID

⚠CAUTION

Changing the RAID deletes all data from your disks.

1. Boot Lifecycle Controller:
   1.1 Power on your device.
   1.2 When you see the AXIS splash screen, press F10.
2. In the Lifecycle Controller, go to **Hardware Configuration > Configuration Wizards** and select **RAID Configuration**.
3. Select the **RAID Controller** on which you want to have the RAID created. Details of any virtual disk(s) available on the selected controller will be shown in the table displayed on the page below the controller list. *Foreign Configuration* will be displayed if there are any foreign or uninitialized HDD(s) available on the server.

Note

- Clear foreign configuration clears all the foreign HDDs available on the RAID controller selected.
- Ignore foreign Configuration ignores the foreign HDDs available on the RAID controller while creating the RAID.

4. Clear or ignore foreign HDDs and uninitialized HDDs.

   If you want, you can initialize the uninitialized disks:

   4.1 In the list of all non-RAID (uninitialized) HDDs, select the HDDs you want to convert to RAID capable (initialize) and click **Next** to initialize them.

   4.2 Select the corresponding option on the Configuration Wizards: RAID Configuration page.
5. Select a RAID level.
6. Select the physical disks from the table and click **Next**.

   If the you've selected **Ignore foreign configuration**, the foreign HDDs are not displayed in the table.
7. Enter the virtual disk attributes.
8. Click **Next**.
9. Review the settings and click **Finish**.
10. Lifecycle Controller displays a message to indicate that all the current data about the virtual disks available on the controller will be lost. Click **OK** to continue.
11. Click **OK** and **Finish**.
12. Exit the wizard and reboot the system.

Add a hard drive

The demand for storage can differ. Retention time of stored data or for storing high-resolution recordings often leads to the same: the need for installing more storage. This section explains how to expand your AXIS S12 series with more hard drives and how to add them to your RAID 5 configuration.

Note

The following instructions are to be used when adding additional storage to certain AXIS S12 series. These instructions are as is, and Axis Communications AB takes no responsibility for loss of data and/or misconfiguration during these steps. The standard precautions should be taken to backup data that is business critical. The following procedure of expanding storage will not be supported by Axis Technical Support.

Note

To avoid electrostatic discharge, it is recommended that you always use a static mat and static strap while working on components in the interior of the system.

Warranty

Detailed information about warranty is available at: *www.axis.com/support/warranty*.

Workflow

1. *Install a hot-swap hard drive on page 25*
    1.1 *Remove the bezel on page 25*
    1.2 *Remove the hard disk blank on page 25*
    1.3 *Install the hard drive on page 25*
2. *Create a new RAID array on page 26*
    2.1 *Enter the Dell PERC 11 Configuration Utility on page 26*
    2.2 *Create a RAID storage array on page 26*
    2.3 *Reconfigure a RAID storage array on page 26*
3. *Configure Microsoft Windows® on page 27*

Install a hot-swap hard drive

Remove the bezel

1. Locate the bezel key.
2. Unlock the bezel by using the key.
3. Slide the release latch up and pull the left end of the bezel.
4. Unhook the right end and remove the bezel.

Remove the hard disk blank

- Press the release button on the front of the blank and slide it out of the hard drive slot.

Install the hard drive

⚠CAUTION

- Use only hard drives that have been tested and approved for use with AXIS S12 series.
- When installing a hard drive, ensure that the adjacent drives are fully installed. Inserting a hard drive carrier and attempting to lock its handle next to a partially installed carrier can damage the partially installed carrier's shield spring and make it unusable.
- Combining SAS and SATA hard drives in the same RAID volume is not supported.

1. If a hard drive blank is installed in the hard drive slot, remove it.
2. Install a hard drive in the hard drive carrier.
3. Press the release button on the front of the hard drive carrier and open the hard drive carrier handle.
4. Insert the hard drive carrier into the hard drive slot until the carrier connects with the backplane.
5. Close the hard drive carrier handle to lock the hard drive in place.

Create a new RAID array

The Human Interface Infrastructure (HII) configuration utility is a storage management application integrated into the System BIOS. It is used to configure and manage the controllers, virtual disks, and physical disks. This utility is independent of the operating system.

Enter the Dell PERC 11 Configuration Utility

1. Turn on the system.
2. While the system startup, press F2 to enter System Setup.
3. Click **Device Settings** to view all the RAID controllers in the system.

Create a RAID storage array

1. *Enter the Dell PERC 11 Configuration Utility on page 26*.
2. Click **Main Menu > Configuration Management > Create Virtual Disk** and define the following virtual disk parameters.
   - **Select RAID Level**: Choose the RAID level.
   - **Select Physical Disks**: Select the physical disks from which the virtual disks are being created. This option is displayed if you select **Unconfigured Capacity** as your physical disk capacity.
   - **Configure Virtual Disk**: Configure the following virtual disk parameters.
   - **Virtual Disk Name**: Enter the name for the virtual disk.

     Allowed characters are A-Z, a-z, 0-9, underscore (_), and hyphen (-) only.
   - **Virtual Disk Size**: Set the capacity for the virtual disk.
3. Click **Create Virtual Disk**.

⚠CAUTION

There are more parameters available for modification. However, Axis Communications AB does not take responsibility for any misconfigurations that may happen when modifying those parameters. Always exercise caution when modifying parameters.

Reconfigure a RAID storage array

An online virtual disk can be reconfigured in ways that expands its capacity and changes its RAID level.

⚠CAUTION

- Spanned virtual disks such as RAID 50 and 60 can't be reconfigured.
- Reconfiguring virtual disks typically impacts disk performance until the reconfiguration operation is complete. Completion time can vary greatly up to several days. It is highly recommended to do the procedure during a maintenance window.
- Always create a validated backup of your data before starting any action.

1. *Enter the Dell PERC 11 Configuration Utility on page 26*.
2. Click **Main Menu > Virtual Disk Management**. All the virtual disks associated with the RAID controller are displayed.

3. To view the properties, click the virtual disk.
4. In the **Operations** drop-down, select **Reconfigure Virtual Disks** and press **GO**.
5. Select the **RAID Level** and press **Choose the Operation**.
6. Select the disks to be added to the virtual disk and press **Apply Changes**.
7. Confirm the operation and click **YES**.
8. Click **Start Operation**.
9. Click **OK**.

In the Virtual Disk Management page, you can see the status of the reconstruction on the modified Virtual Disk.

After the reconstruction starts, the system can be left in the Dell PERC 11 Configuration Utility until complete or the system can be rebooted into the operating system.

If the system is rebooted into the operating system, the system performance will be affected until the rebuild has completed.

You can also NOT extend the disk in Windows® until the rebuild is complete.

⚠CAUTION

The rebuilding time will vary between systems and can take up to several days.

Configure Microsoft Windows®

To configure a new volume:

1. Right-click the Start menu and select **Disk Management**.
2. Right-click an unallocated region on your hard disk, and select **New Simple Volume**.
3. In the **New Simple Volume Wizard**, click **Next**.
4. Enter the size of the volume you want to create in megabytes (MB) or accept the maximum default size, and click **Next**.
5. Accept the default drive letter or choose a different drive letter to identify the partition, and click **Next**.
6. In the Format Partition dialog:
   - If you don't want to format the volume right now, select **Do not format this volume**, and click **Next**.
   - To format the volume with the default settings, click **Next**.
7. Review your choices, and click **Finish**.

   Disk Management now shows the new volume. You can now close Disk Management and your system is ready to use the new volume.

To configure an existing volume:

1. Right-click the Start menu and select **Disk Management**.
2. Right-click the volume, and select **Extend Volume**.
3. In the **Extend Volume Wizard**, click **Next**.
4. Select the disk that has unused space and click **Next**. Normally this is selected by default.
5. Review your choices, and click **Finish**.

   Disk Management now shows the extended volume. You can now close Disk Management and your system is ready to use the new volume.

Configure iDRAC

The Integrated Dell Remote Access Controller 9 (iDRAC9) with Lifecycle Controller is designed to make system administrators more productive and improve the overall availability of Dell systems. iDRAC alerts administrators to system issues, help them perform remote system management and reduces the need for physical access to the system. You must configure the initial network settings based on your network infrastructure to enable the communication to and from iDRAC.

1. Press F10 during Power-on Self-test (POST).

Note

The Lifecycle Controller Initial Setup Wizard will be displayed only for the first time. Use the Initial Setup Wizard to select the language and keyboard, configure network settings, iDRAC network settings, credential configuration, and view the summary of the settings. To make configuration changes later, select **Settings** from the Lifecycle Controller home page.

2. Configure the language and keyboard, and click **Next**.
3. Check the product overview and click **Next**.
4. Configure Lifecycle Controller network settings:

   4.1 From the **NIC Card** drop-down list, select the NIC port to configure.

   4.2 From the **IPV4 Network Settings > IP Address Source** drop-down list, select one of the following options:

   - **DHCP:** indicates that the NIC must be configured by using an IP address from a DHCP server. DHCP is the default option and the DHCP IP address is displayed on the Network Settings page.
   - **Static IP :** indicates that the NIC must be configured by using a static IP. Type the IP address properties including **IP Address**, **Subnet Mask**, **Default Gateway**, and **DNS Address**. If you do not have this information, contact your network administrator.
   - **No Configuration:** indicates that the NIC must not be configured.

   4.4 If VLAN is used, click **Enabled** and type the **VLAN ID** and **Priority** under **Lifecycle Controller VLAN Settings** to configure the VLAN settings of a NIC.

   4.5 Click **Next**. If Lifecycle Controller settings are not correctly configured, an error message is displayed.

5. Configure iDRAC network and credentials:

   5.1 Go to **IPV4 Configuration > IP Address Source** and select one of the following options:

   - **Static:** indicates that the network must be configured by using a static IP. Type the IP address properties including **IP Address**, **Subnet Mask**, **Default Gateway**, **DNS Address Source** and **DNS Address**. If you do not have this information, contact your network administrator.
   - **DHCP:** indicates that the NIC must be configured by using an IP address from a DHCP server. DHCP is the default option and the DHCP IP address is displayed on the Network Settings page.

   5.3 Under **Credentials**, enter **Account Username** and **Password** to access iDRAC network.

   5.4 Click **Next**.

6. Verify the summary of the Lifecycle Controller and iDRAC network configuration and click **Finish**.

Cybersecurity

Secure boot

Secure boot is a feature that prevents malware and unsecure software to run on your system. The feature runs during start-up of your system and uses the digital signatures to verify the certificates of the software and OS. Only trusted software and OS can run on the system.

Trusted Platform Module (TPM)

The TPM is a component that provides cryptographic features to protect information from unauthorized access. It's active by default and we don't recommend that you turn this off.

Secure Component Verification (SCV)

When your device was made at the factory, a certificate was created to make sure that you get what you ordered and that no one tampered with the device after it left the factory. The factory signs the certificate and stores it in iDRAC. When you receive the device go to AXIS Recorder Toolbox to see if your device has SCV and verify the certificate. Upon verification, the system inventory either pass or mismatch. For more information about SCV, go to *dell.com*.

To learn more about the cybersecurity features in Axis devices, go to *axis.com/learning/white-papers* and search for cybersecurity.

Axis security notification service

Axis provides a notification service with information about vulnerability and other security related matters for Axis devices. To receive notifications, you can subscribe at *axis.com/security-notification-service*.

Vulnerability management

To minimize customers' risk of exposure, Axis, as a **Common Vulnerability and Exposures (CVE) numbering authority (CNA)**, follows industry standards to manage and respond to discovered vulnerabilities in our devices, software, and services. For more information about Axis vulnerability management policy, how to report vulnerabilities, already disclosed vulnerabilities, and corresponding security advisories, see *axis.com/vulnerability-management*.

Secure operation of Axis devices

Axis devices with factory default settings are pre-configured with secure default protection mechanisms. We recommend using more security configuration when installing the device. To find out more about Axis hardening guides and other cyber security related documentation, go to *axis.com/support/cybersecurity/resources*.

Troubleshooting

Check the current BIOS version

To check the current BIOS:

1. Power on the device.
2. Wait until you see the Axis splash screen. You'll see the version number above the splash screen.

Upgrade BIOS

You should upgrade the BIOS only when you are instructed by Axis technical support.

If you don't have access to Windows®: update package instructions for EFI

1. Go to the support pages on *dell.com* and enter your service tag. Go to **Drivers & Downloads** and download the .efi file.
2. Copy the file to a USB device.
3. Plug in the USB device and press F11 during POST to enter BIOS Boot Manager.
4. Go to **System Utilities menu > BIOS Update File Explorer**.
5. Select the USB device and navigate through the directory contents to find the executable (.efi).
6. Launch the executable and follow the instructions provided by the flash utility.

If you have access to Windows®: update package instructions for Windows® Dup

1. Browse to the location where you downloaded the file and double-click the new file.
2. Read over the release information in the dialog window.
3. Download and install any prerequisites identified in the dialog window before proceeding.
4. Install any necessary Embedded Systems Management firmware prior to this BIOS update.
5. Click **Install**.
6. Follow the onscreen instructions.

Run diagnostics

Running diagnostics help you to identify the cause for a system issue. The diagnostics test your system hardware without requiring additional equipment or risking data loss.

1. While the system is booting, press F10 to enter Lifecycle Controller.
2. Go to **Hardware Diagnostics** and click **Run Hardware Diagnostics**.
3. Note the error code and contact Axis technical support.

Perform a system 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 Recovery Kit, contact Axis technical support and supply the serial number of your device.

1. Download the AXIS Recovery Kit and AXIS ISO to USB Tool.

2. Insert a USB drive into your computer.
   - Use a USB drive with a minimum of 16 GB to 32 GB.
   - The USB drive will be formatted, and all existing data will be erased.
3. Run the AXIS ISO to USB Tool and follow the onscreen instructions.

   Writing data to the USB drive takes approximately 10 to 15 min. Don't remove the USB drive until the process is complete.
4. After the ISO to USB tool is complete, take the USB drive and plug it into your device.
5. Start your device.
6. When you see the AXIS splash screen, press F11.
7. Click **One-shot UEFI Boot Menu**.
8. Navigate to your USB drive and press ENTER. The system boots into the AXIS Recovery Kit.
9. Click **Reinstall Operating System**.

   The recovery takes roughly 10 to 15 min to complete. You find detailed instructions in the download for the recovery kit.

Export a SupportAssist collection

You can export the SupportAssist collection to a USB drive or a network share (CIFS/NFS). The collection includes the following data:

- Hardware
- RAID controller logs

To export the SupportAssist collection:

1. During Power-on-self-test (POST), press F10 to start Lifecycle Controller.
2. Go to **Hardware Diagnostics > Export SupportAssist collection**.
3. Read the terms and conditions and click **Next**.

   You must accept the terms and conditions to allow technical support to use the SupportAssist collection data.
4. Select the data options which you want to include in the SupportAssist collection and click **Next**.
5. Enter the required export settings information and click **Next**.
   - To export to a USB drive: select the USB drive option and then select the name of the USB Drive and enter the file path details to where the collection is to export.
   - To export to NFS: select the NFS option and enter the required information.
   - To export to CIFS: select the CIFS option and enter the required information.

     Click **Test Network Connection** to verify if the Lifecycle Controller can connect to the IP address that is provided. By default, it pings the Gateway IP, DNS Server IP, host IP and Proxy IP.
6. Verify your selection and click **Finish**.

   Lifecycle Controller retrieves the selected collection data and exports to the specified location. This can take a few minutes.

Troubleshooting

Troubleshoot the power supply unit

Note

After installing a power supply unit, allow several seconds for the system to recognize the power supply unit and determine if it the power supply works properly.

1. Ensure that no loose connections exist. For example, loose power cables.
2. Ensure that the power supply handle LED indicates that the power supply is working properly.
3. Check the status of the power indicator on the power supply unit. See *Specifications on page 33*.
4. If you have a redundant power supply configuration, ensure that both power supply units are of the same type and wattage.
5. Ensure that you use only power supply units with the Extended Power Performance (EPP) label on the back.
6. Reset the power supply unit.
7. If the problem persists, contact Axis technical support.

Troubleshoot memory errors

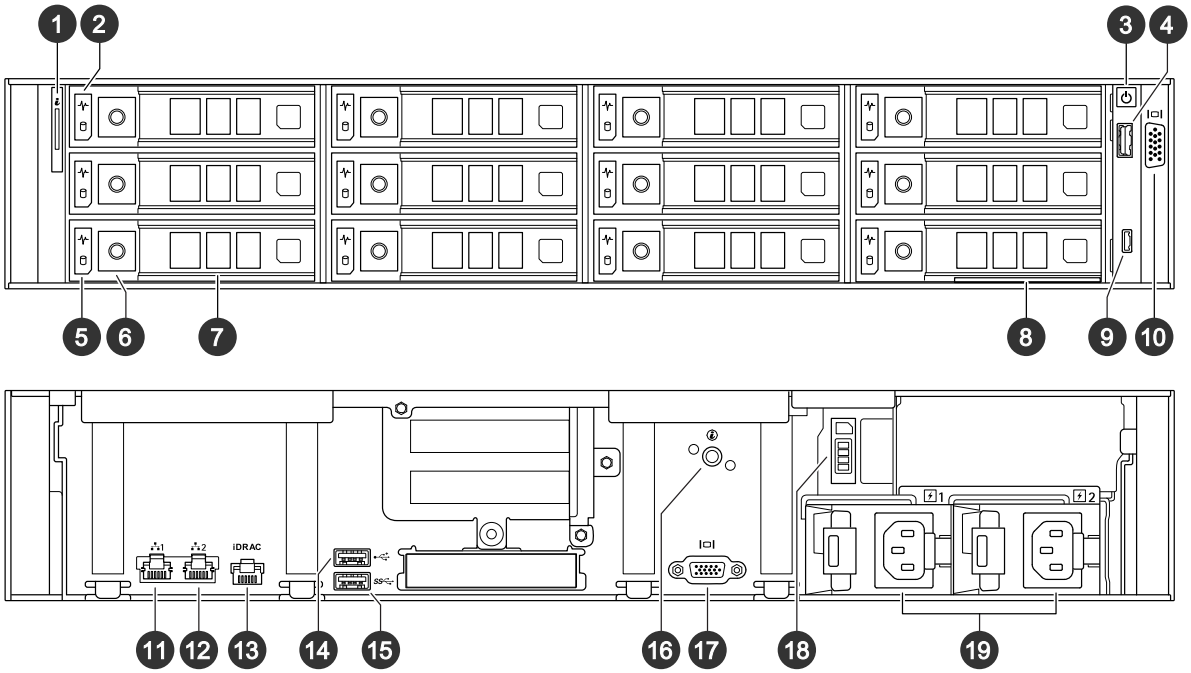
1. Upgrade the BIOS to the latest version.
2. If the errors persist, contact Axis technical support.

Troubleshoot AXIS Camera Station

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

Product overview

Front and rear sides



1 *System identification button and indicator*
2 *Hard drive status LED*
3 *Power button/power LED*
4 *USB 2.0 port*
5 *Hard drive activity LED*
6 *Hard drive tray release button*
7 *Hard drive tray*
8 *Information tag*
9 *iDRAC direct port*
10 *VGA port*
11 *1 GbE Ethernet port 1*
12 *1 GbE Ethernet port 2*
13 *iDRAC dedicated Ethernet port*
14 *USB 2.0 port*
15 *USB 3.0 port*
16 *System identification button and indicator*
17 *VGA port*
18 *Solid state drive tray*
19 *Power supply units*

Specifications

Status LED indicators

LED	Description	Action
Drive indicator	The indicator turns solid amber if there is a drive error.	Check the System Event Log to determine if the drive has an error.
Temperature indicator	The indicator turns solid amber if the system experiences a thermal error. For example, the ambient temperature is out of range or there is a fan failure.	Ensure that none of the following conditions exist: • A cooling fan has been removed or has failed. • System cover, air shrouds, or back filler bracket has been removed. • Ambient temperature is too high. • External airflow is obstructed.
Electrical indicator	The indicator turns solid amber if the system experiences an electrical error. For example, voltage out of range, or a failed power supply unit (PSU) or voltage regulator.	Check the System Event Log or system messages for the specific issue. If it is due to a problem with the PSU, check the LED on the PSU. Reseat the PSU.
Memory indicator	The indicator turns solid amber if a memory error occurs.	Check the System Event Log or system messages for the location of the failed memory. Reseat the memory module.
PCIe indicator	The indicator turns solid amber if a PCIe card experiences an error.	Restart the system. Update any required drivers for the PCIe card. Reinstall the card.

System health and ID indicators

LED	Description	Action
Solid blue	The system is powered on, is healthy, and system ID mode is not active.	Press the system health and system ID button to switch to system ID mode.
Blinking blue	The system ID mode is active.	Press the system health and system ID button to switch to system health mode.
Solid amber	The system is in fail-safe mode.	
Blinking amber	The system is experiencing a fault.	Check the system event log for the specific error message.

iDRAC direct LED indicators

LED	Description
Solid green for two seconds	The laptop or tablet is connected.
Blinking green (on for two seconds and off for two seconds)	The laptop or tablet connected is recognized.
Off	The laptop or tablet is unplugged.

NIC indicators

LED	Description
Link and activity indicators are off	The NIC is not connected to the network.
Link indicator is green and activity indicator is blinking green	The NIC is connected to a valid network at its maximum port speed and data is being sent or received.

Link indicator is amber and activity indicator is blinking green	The NIC is connected to a valid network at less than its maximum port speed and data is being sent or received.
Link indicator is green and activity indicator is off	The NIC is connected to a valid network at its maximum port speed and data is not being sent or received.
Link indicator is amber and activity indicator is off	The NIC is connected to a valid network at less that its maximum port speed and data is not being sent or received.

Power supply unit (PSU) indicators

LED	Description
Green	A valid power source is connected to the PSU and the PSU is operational.
Blinking amber	There is a problem with the PSU.
Not powered on	Power is not connected to the PSU.
Blinking green	The firmware of the PSU is being updated. **⚠CAUTION** Do not disconnect the power cord or unplug the PSU when updating firmware. If firmware update is interrupted, the PSUs will not function.
Blinking green and powers off	When hot-plugging a PSU, it blinks green five times at a rate of 4 Hz and powers off. This indicates a PSU mismatch due to efficiency, feature set, health status, or supported voltage. **⚠CAUTION** • If two PSUs are installed, both the PSUs must have the same type of label. For example, Extended Power Performance (EPP) label. Mixing PSUs from previous generations of PowerEdge servers is not supported, even if the PSUs have the same power rating. This results in a PSU mismatch condition or failure to power on the system. • If two PSUs are used, they must be of the same type and have the same maximum output power. • When correcting a PSU mismatch, replace the PSU with the blinking indicator. Swapping the PSU to make a matched pair can result in an error condition and an unexpected system shutdown. To change from a high output configuration to a low output configuration or vice versa, you must power off the system.

Drive indicators

LED	Description
Blinks green twice per second	The drive is being identified or preparing for removal.
Off	The drive is ready for removal. Note The drive status indicator remains off until all drives are initialized after the system is powered on. Drives are not ready for removal during this time.
Blinks green, amber, and then powers off	There is an unexpected drive failure.

Product overview

Blinks amber four times per second	The drive has failed.
Blinks green slowly	The drive is rebuilding.
Solid green	The drive is online.
Blinks green for three seconds, amber for three seconds, and then powers off after six seconds	The rebuild has stopped.

Need more help?

Need more help?

Useful links

- *AXIS Camera Station user manual*
- *Configure Axis Secure Remote Access*
- *What to include in an Antivirus allowlist for AXIS Camera Station*

Contact support

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

User manual
AXIS Camera Station S1264 Rack Recording Server
© Axis Communications AB, 2022 - 2024
Ver. M5.2
Date: February 2024
Part no. T10177845