AXIS Camera Station S9002 Mk II Desktop Terminal

User manual

AXIS Camera Station S9002 Mk II Desktop Terminal

Table of Contents

About your device 3
Get started 4
Install your device 5
Configure your device 10
First-time configuration 10
Log in to the server 10
Configure AXIS Camera Station 11
Manage Windows® user accounts 15
Create a user account 15
Create an administrator account 15
Create a local user group 15
Delete a user account 15
Change a user account's password 16
Create a password reset disk for a user account 16
Manage AXIS Camera Station user accounts 17
Configure user permissions 17
Add users or groups 17
User or group privileges 18
Manage your device 21
Update Windows® 21
Configure Windows update settings 21
Troubleshooting 23
Check the current BIOS version 23
Perform a system recovery 23
Troubleshoot AXIS Camera Station 23
Product overview 24
Front and rear sides 24
Specifications 25
Need more help? 28
Useful links 28
Contact support 28

AXIS Camera Station S9002 Mk II Desktop Terminal

About your device

About your device

AXIS Camera Station S9002 Mk II Desktop Terminal is an easy-to-install desktop terminal for high-definition surveillance with support for four simultaneous 4K streams. The terminal is preloaded with AXIS Camera Station client and all necessary software and is preconfigured to minimize installation time. With its slim form factor, AXIS S9002 Mk II complements Axis rack servers to create a high-end surveillance workstation. The terminal has validated hardware components, such as graphic card and CPUs and supports four monitors for optimal system overview. AXIS S9002 Mk II includes three-year hardware warranty with on-site replacement service, a keyboard and computer mouse.

AXIS Camera Station S9002 Mk II Desktop Terminal

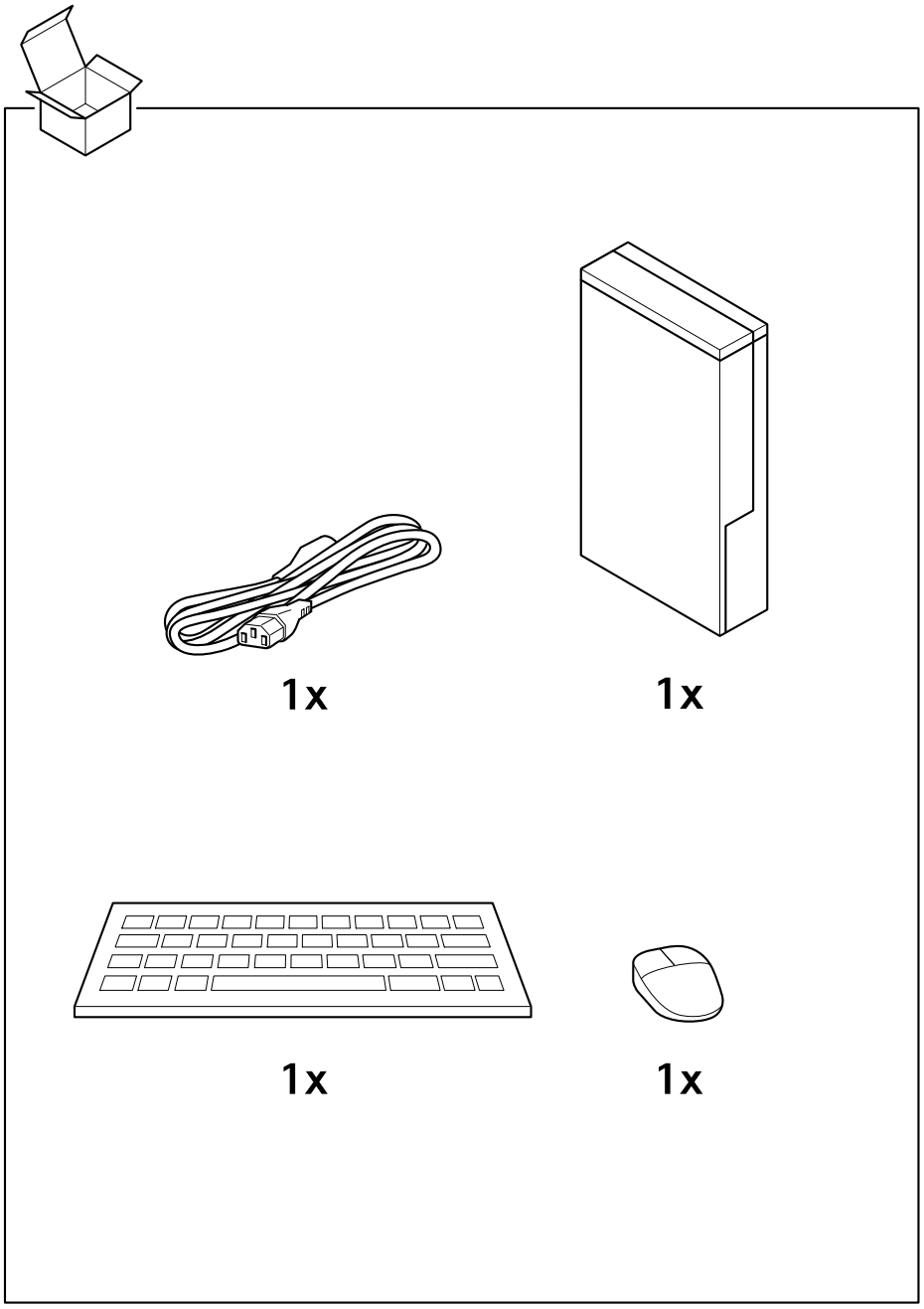
Get started

Get started

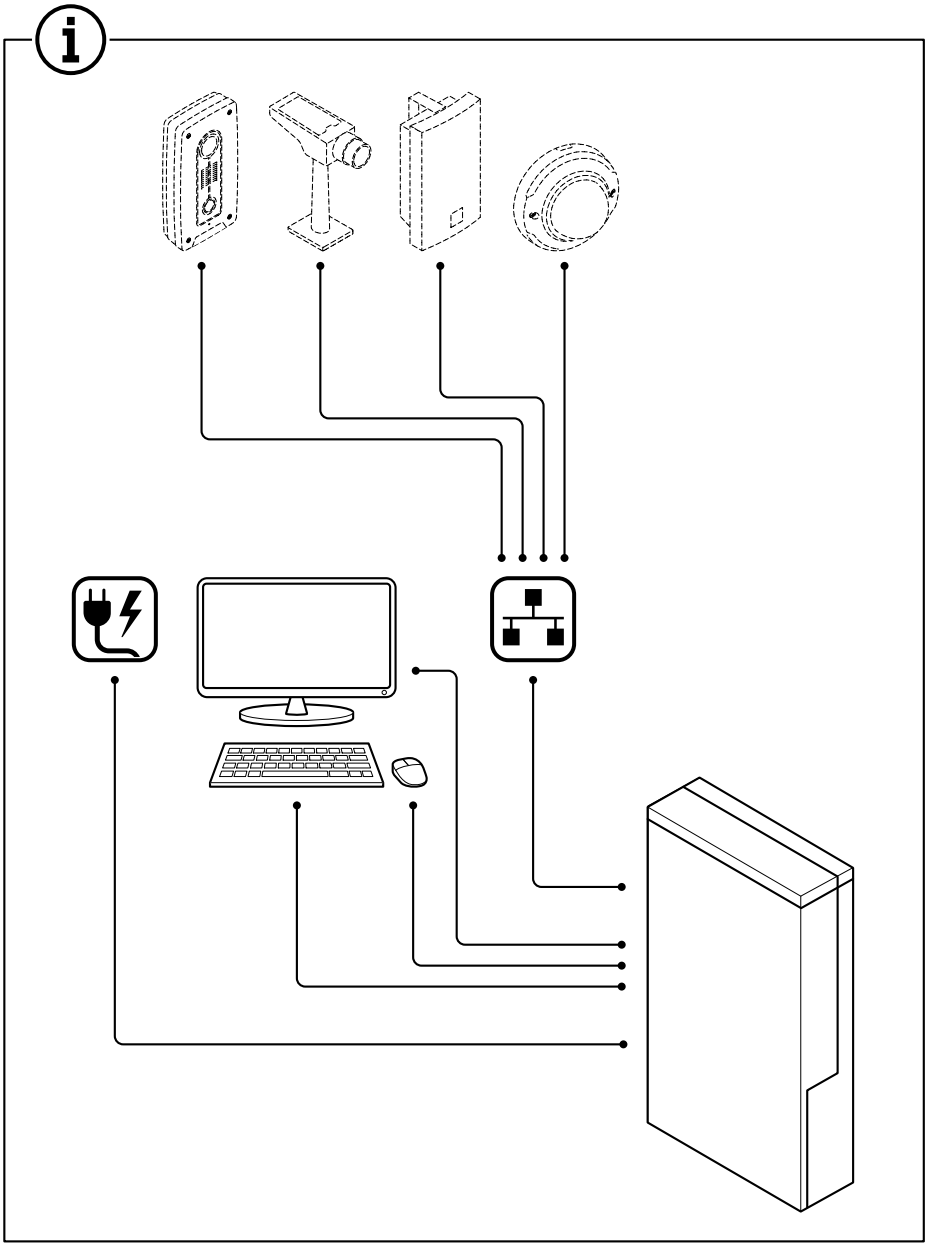
The standard workflow to configure an AXIS Camera Station desktop terminal is:

1.
2. Configure Windows®. We recommend to:
   - Update Windows® to the latest version. See
   - Create a standard user account. See
3.
4. 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.
5.

Install your device

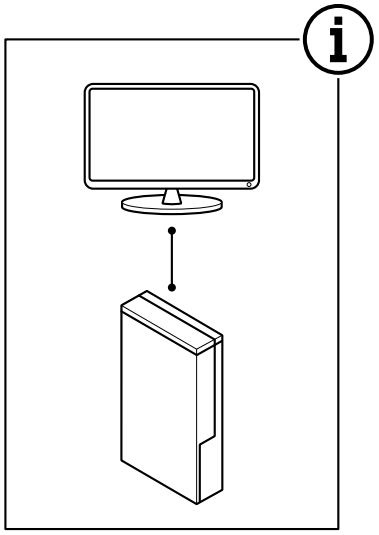


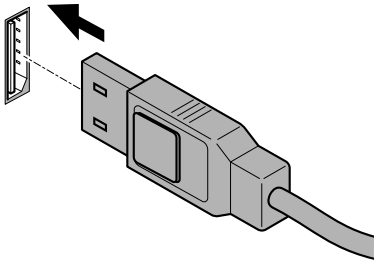
Install your device



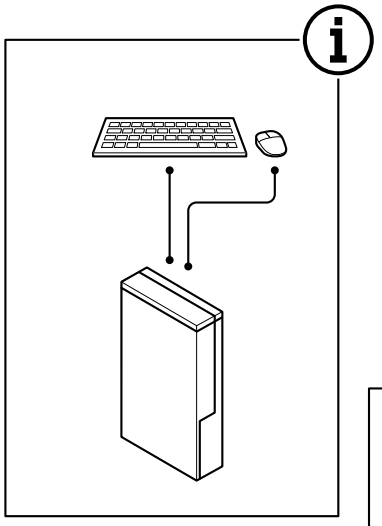
Install your device

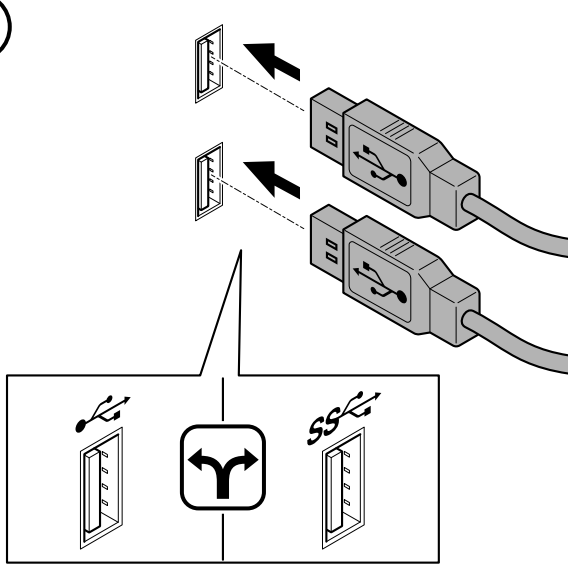
1.1

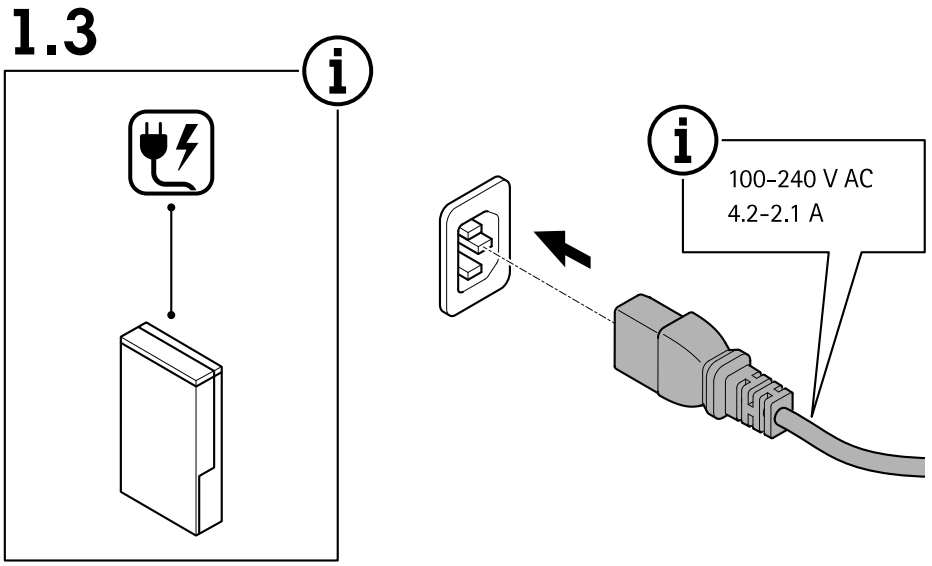


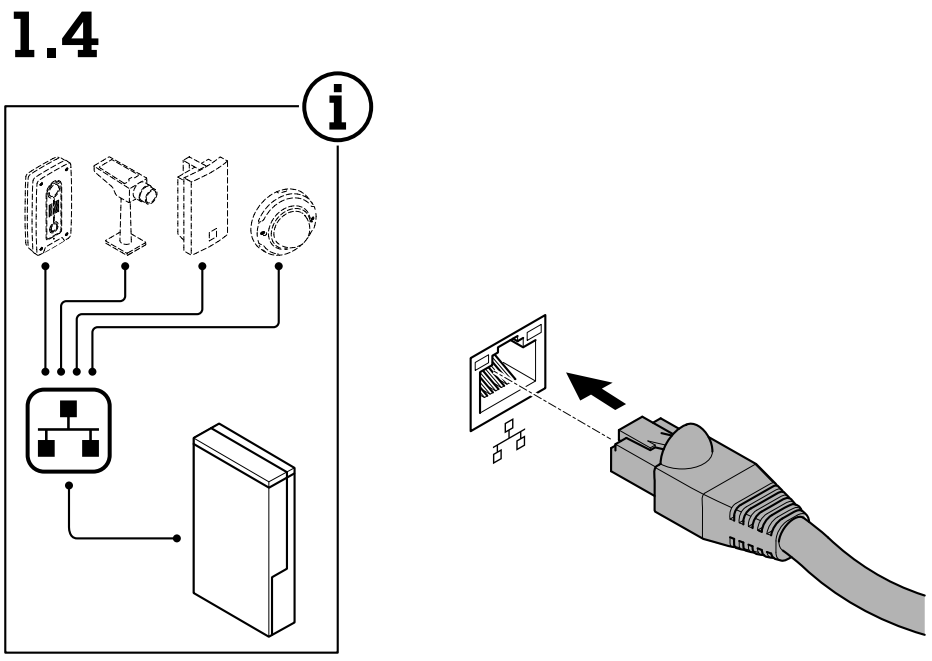


1.2

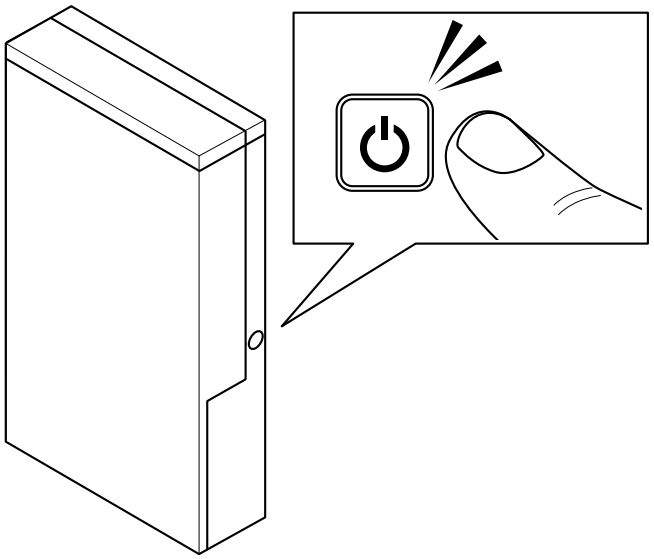




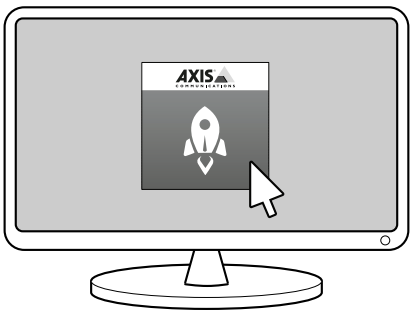

1.3
100–240 V AC
4.2–2.1 A


1.4

1.5



1.6



Configure your device

First-time configuration

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

help.axis.com/?&piaId=46529&section=first-time-configuration

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

1. Change the computer name if you want and click **Next**.
2. 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.
3. 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.
4. Under **Power settings**,
   - **Never put the computer to sleep** and **Never turn off the display** are selected by default.
   - We recommend that you keep both options selected to make the live view and recordings available all the time. You can always go to **Start > Settings > System > Power & sleep** to change the settings.
5. Click **Finish**. If you have changed the computer name, AXIS Recorder Toolbox will prompt you to restart the device.

Log in to the server

Using the AXIS Camera Station client, you can connect to multiple servers or a single server installed on the local computer or somewhere else on the network. You can connect to AXIS Camera Station servers in different ways:

Last used servers – Connect to the servers used in the previous session.

This computer – Connect to the server installed on the same computer as the client.

Configure your device

Remote server – See .

AXIS Secure Remote Access – See .

Note

When trying to connect to a server for the first time, the client checks the server certificate ID. To ensure that you're connecting to the correct server, manually verify the certificate ID with the one displayed in AXIS Camera Station Service Control.

Server list	To connect to servers from a server list, select a one from the **Server list** drop-down menu. Click to create or edit the server lists.
Import server list	To import a server list file exported from AXIS Camera Station, click **Import server list** and browse to an .msl file.
Delete saved passwords	To delete saved usernames and passwords all connected servers, click **Delete saved passwords**.
Change client proxy settings	You might need to change the client proxy settings to connect to a server, click **Change client proxy settings**.

Log in on a remote server

1. Select **Remote server**.
2. Select a server from the **Remote server** drop-down list or enter the IP or DNS address. If the server isn't listed, click to reload all the available remote servers. If the server is configured to accept clients on a different port than the default port number 55752, enter the IP address followed by the port number, for example, 192.168.0.5:46001.
3. You can:
   - Select **Log in as current user** to log in as the current Windows user.
   - Clear **Log in as current user** and click **Log in**. Select **Other user** and provide another username and password to log in with a different username and password.

Sign in to AXIS Secure Remote Access

Note

When trying to connect to a server using Axis Secure Remote Access, the server can't upgrade the client automatically.

1. Click the **Sign in to AXIS Secure Remote Access** link.
2. Enter your My Axis account credentials.
3. Click **Sign in**.
4. Click **Grant**.

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 .
- Configure your server ports if needed. See .

- Consider security issues. See .

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

1.
2.
3.
4.
5.
6.
7.
8.

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**.

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.

Configure your device

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

Configure your device

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

AXIS Camera Station 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, keep the following in mind:

- Use strong passwords for all network devices (cameras, video encoders, and auxiliary devices).
- Install AXIS Camera Station S9002 Mk II Desktop Terminal server, cameras, video encoders, and auxiliary devices on a secure network separate from the office network. You can install the AXIS Camera Station S9002 Mk II Desktop Terminal 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.

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 AXIS Camera Station S9002 Mk II Desktop Terminal.

Note

Administrators of the computer that runs AXIS Camera Station S9002 Mk II Desktop Terminal server are automatically given administrator privileges to AXIS Camera Station S9002 Mk II Desktop Terminal. 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 .

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 AXIS Camera Station S9002 Mk II Desktop Terminal. To add a user to AXIS Camera Station S9002 Mk II Desktop Terminal, 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**.

   You can see the available users and groups 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 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 AXIS Camera Station S9002 Mk II Desktop Terminal 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 .
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 give to a user or group. For how to define the role for a user or group, see .

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 AXIS Camera Station S9002 Mk II Desktop Terminal 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 AXIS Camera Station S9002 Mk II Desktop Terminal.
Edit	Allow to edit the views in AXIS Camera Station S9002 Mk II Desktop Terminal.

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 data search	Allow searching for data to track what happened at the time of an event.

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.

Manage AXIS Camera Station user accounts

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**.

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.

Perform a system recovery

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 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 and before the AXIS splash screen appears press F12. We recommend that you tap the F12 key repeatedly as the device boots fast.
6. Navigate to your USB drive and press ENTER. The system boots into the AXIS Recovery Kit.

   For example it should say UEFI: Sandisk.
7. Click **Reinstall Operating System**.

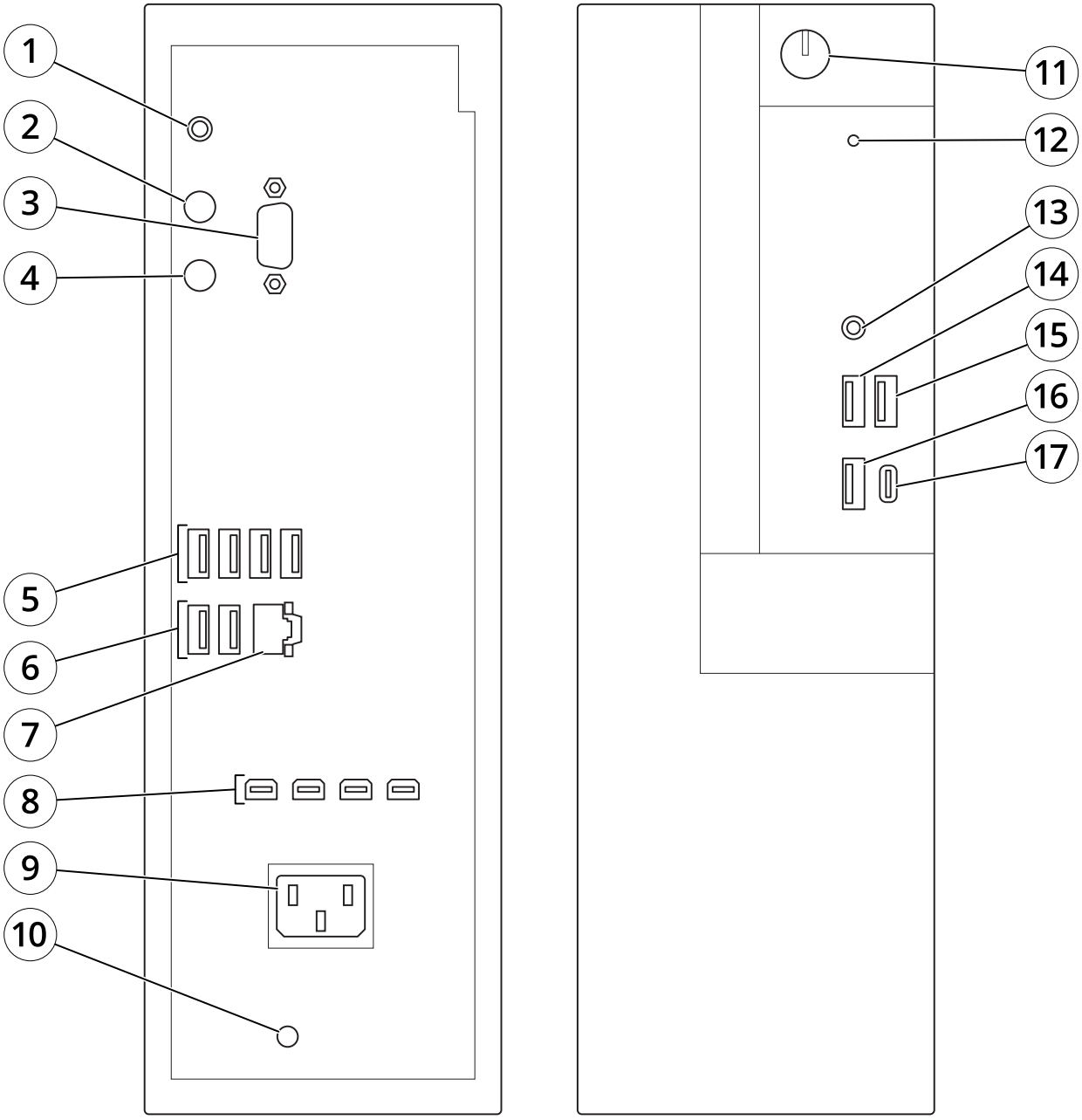
   The recovery takes roughly 10 to 15 min to complete. You find detailed instructions in the download for the recovery kit.

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 *Audio line out*
2 *PS2 keyboard port*
3 *Serial port*
4 *PS2 mouse port*
5 *USB 3.1*
6 *USB 2.0*

7 *Ethernet (RJ45) 1 GbE*
8 *Mini DisplayPort™*
9 *Power connector*
10 *System power LED*
11 *On/off button*
12 *Drive activity LED*
13 *Universal audio jack*
14 *USB 2.0*
15 *USB 2.0*
16 *USB 3.1*
17 *USB 3.1 Type-C*

Specifications

System health and ID indicators

LED	Description	Action
Blue solid	The system is turned on, system is healthy and system ID mode is not active.	Press the system health and system ID button to switch to system ID mode.
Blue blinking	The system ID mode is active.	Press the system health and system ID button to switch to system health mode.
Amber solid	The system is in fail-safe mode.	-
Amber blinking	The system is experiencing a fault.	Check the system event log for the specific error message.

IDRAC quick sync 2 indicator

LED	Description	Action
Off (default state)	The iDRAC Quick Sync 2 feature is turned off.	Press the iDRAC Quick Sync 2 button to turn on the iDRAC Quick Sync 2 feature.If the LED fails to turn on, reset the left control panel flex cable and check again.
White solid	The iDRAC Quick Sync 2 is ready to communicate.	Press the iDRAC Quick Sync 2 button to turn off.If the LED fails to turn off, restart the system.
Blinks white rapidly	Data transfer activity	-
Blinks white slowly	Firmware update is in progress.	-
Blinks white five times rapidly and then turns off	The iDRAC Quick Sync 2 feature is disabled.	Check if iDRAC Quick Sync 2 feature is configured to be disabled by iDRAC.
Amber solid	The system is in fail-safe mode.	Restart the system.
Amber blinking	The iDRAC Quick Sync 2 hardware is not responding properly.	Restart the system.

NIC indicators

LED	Description
Link and activity indicators are off	The NIC is not connected to the network.

Product overview

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
Link indicator is blinking green and activity is off	NIC identify is enabled through the NIC configuration utility.

Power supply unit indicators

LED	Description
Green	A valid power source is connected to the PSU and the PSU is operational.
Blinking amber	Indicates a problem with the PSU
Not illuminated	Power is not connected.
Blinking green	When the firmware of the PSU is being updated, the PSU handle blinks green. CAUTION: Do not disconnect the power cord or unplug the PSU when updating firmware. If firmware update is interrupted the PSUs do not function.
Blinking green and turns off	When hot-plugging a PSU, the PSU handle blinks green five times at a rate of 4Hz and turns off. This indicates a PSU mismatch with respect to efficiency, features 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 turn the system on. • When correcting a PSU mismatch, replace only the PSU with the blinking indicator. Swapping the PSU to make a matched pair can result in an error condition and unexpected system shutdown. To change from a high output configuration to a low output configuration or vice versa, you must turn off the system. • AC PSUs support both 240 V and 120 V input voltages with the exception of Titanium PSUs, which support only 240 V. When two identical PSUs receive different input voltages, they can output different wattages, and trigger a mismatch. • If two PSUs are used, they must be of the same type and have the same maximum output power. • Combining AC and DC PSUs is not supported and triggers a mismatch.

Product overview

Power indicators

LED	Description
Green	A valid power source is connected to the PSU and the PSU is operational.
Blinking amber	Indicates a problem with the PSU.
Not illuminated	Power is not connected.
Blinking green	When hot-plugging a PSU, the PSU indicator blinks green. This indicates that there is a PSU mismatch with respect to efficiency, feature set, health status, or supported voltage. **⚠CAUTION** • When correcting a PSU mismatch, replace only the PSU with the blinking indicator. Swapping the PSU to make a matched pair can result in an error condition and unexpected system shutdown. To change from a High Output configuration to a Low Output configuration or vice versa, you must turn off the system. • If two PSUs are used, they must be of the same type and have the same maximum output power. • Combining AC and DC PSUs is not supported and triggers a mismatch.

Hard drive indicators

LED	Description
Flashes green twice per second	Identifying drive or preparing for removal.
Off	Drive ready for insertion or removal. Note The drive status indicator remains off until all hard drives are initialized after the system is turned on. Drives are not ready for removal during this time.
Flashes green, amber and then turns off	Predicted drive failure.
Flashes amber four times per second	Drive has failed.
Flashes green slowly	Drive is rebuilding.
Steady green	Drive is online.
Flashes green for 3 s, amber for 3 s, and then turns off after 6 s	Rebuild 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 S9002 Mk II Desktop Terminal
© Axis Communications AB, 2018 - 2024
Ver. M6.2
Date: October 2024
Part no. T10130277