

AXIS Device Manager Extend

User manual

AXIS Device Manager Extend

Table of Contents

About	3
About organizations	4
Solution overview	5
Prerequisites	9
Get started	11
Register a My Axis account	11
Install the client and activate your account	11
Create organization	11
Install the edge host	11
Claim the edge host	12
Manage devices	13
Add discovered devices to your edge host	13
Remove devices	14
Log in to your devices	14
Configuration	15
Activating remote access	15
Remove a site	15
Add users to your organization	15
About user roles	15
Elevate user role	16
Remove users	16
AXIS OS management	17
Manage AXIS OS versions based on model	17
Manage AXIS OS on an edge host	17
View ongoing and completed AXIS OS upgrades	17
Policies	18
Create and apply a security policy	18
Create and apply an app policy	18
Edit a policy	19
Delete a policy	19
Manage licenses	20
License your product	20
Troubleshooting	21
How to configure firewall settings	21

AXIS Device Manager Extend

About

About

AXIS Device Manager Extend solution provides system administrators with an interface for discovering, configuring, and operating Axis devices on their organization's networks.

The AXIS Device Manager Extend desktop app

The desktop app is a software utility program that can be used as an on-demand, or always available user interface for managing the system. It can be run on a dedicated machine together with a locally installed edge host, or separately from the edge host on a remotely connected laptop. The client presents the user with the overall status of the system and readily available management actions.

The edge host

The edge host component in AXIS Device Manager Extend is an always available, on-premise management service that is responsible for maintaining local devices, such as cameras. The AXIS Device Manager Extend edge host also acts as a link to the Axis remote management service, where the same API functionality supports remote administration of sites via the Axis service platform.

AXIS Device Manager Extend

About organizations

About organizations

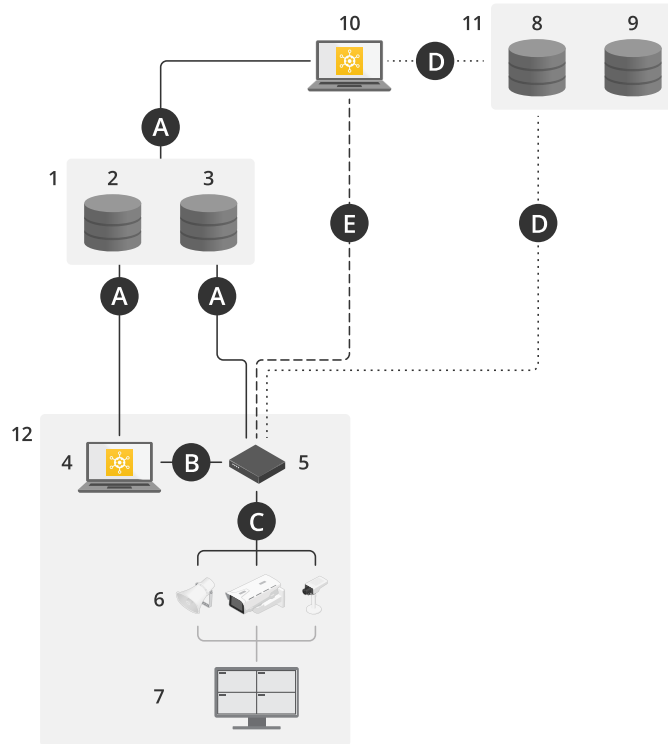
The organization is a virtual representation of your Axis system installations, and it's at the center of your cloud services. An organization hosts all of the devices and user accounts of a company in a hierarchy that regulates access and ensures maximum security. At the same time it allows for flexible user and device management for small businesses as well as large corporations.

- When you create a new organization, you become its owner. The organization connects your system to the users of Axis cloud service.
- You can invite users to the organization. See *Add users to your organization on page 15*.
- You can assign different roles to users.
- The organization contains a default folder where you can start building your organizational structure that fits your needs. You can structure the organization into folders and sub-folders. Typically, a folder represents a physical site or location of a system within an organization.
- Manage your licenses for your system within your organization.
- To create an organization, you need a My Axis account.

AXIS Device Manager Extend

Solution overview

Solution overview



AXIS Device Manager Extend with local and remote access

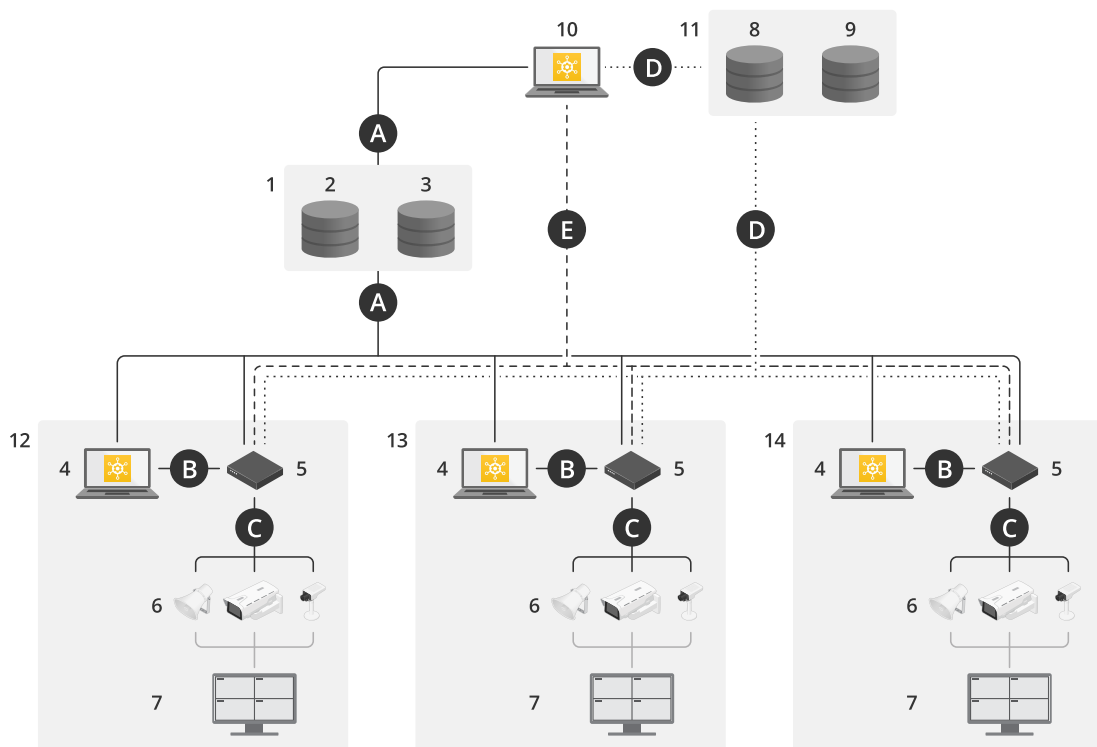
- 1 Axis
- 2 IAM (My Axis)
- 3 Organization data
- 4 Local client
- 5 Edge host
- 6 Devices
- 7 VMS
- 8 TURN
- 9 Signaling
- 10 Remote client
- 11 Remote Access WebRTC Servers
- 12 Site 1

Connection	URL and IP	Port	Protocol	Comment
A	prod.adm.connect.axis.com (52.224.128.152 or 40.127.155.231)	443	HTTPS	Required
B	HTTP Discovery (from client to edge hosts) Data transfer (between client and edge hosts) Multicast Discovery (from client to edge hosts) Multicast Discovery (from edge hosts to client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Needed to provision the site. Optional after provision.

AXIS Device Manager Extend

Solution overview

C	Data transfer (between edge host and devices) Unicast discovery Multicast discovery HTTP discovery	80 / custom port, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Required
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP and TCP)	Based on WebRTC standard Optional and set to off by default
E	Peer to Peer (P2P)	49152–65535	DTLS (UDP and TCP)	



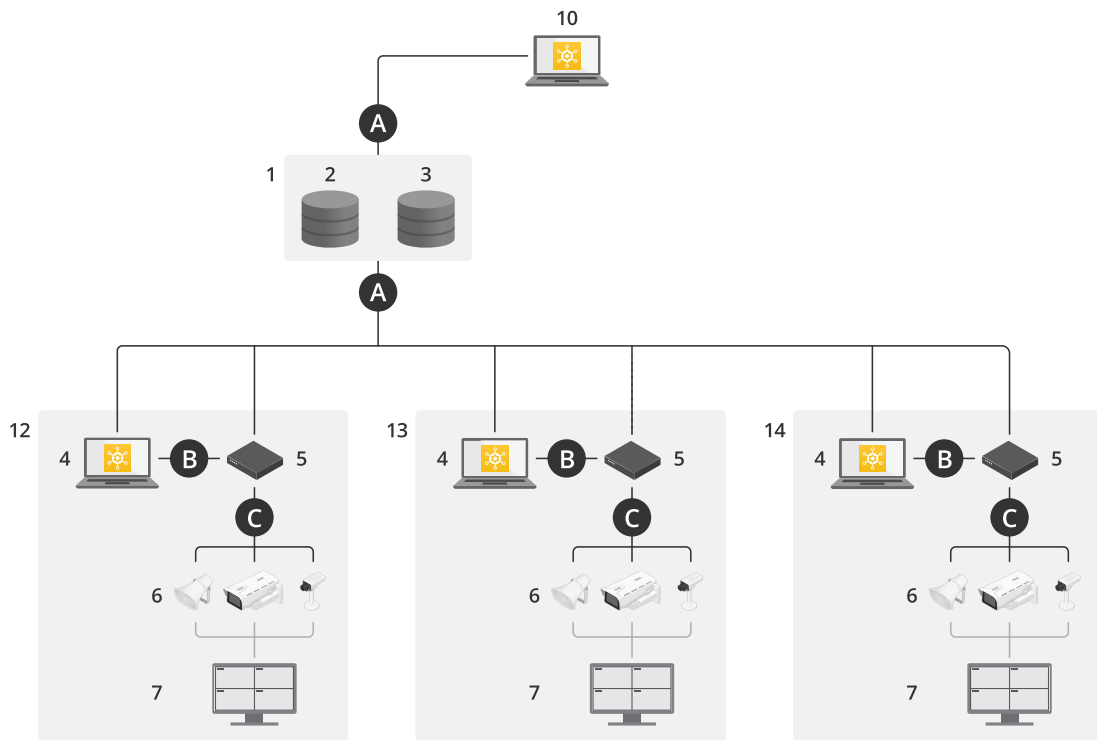
AXIS Device Manager Extend with a multi-site setup using local and remote access

- 1 Axis
- 2 IAM (My Axis)
- 3 Organization data
- 4 Local client
- 5 Edge host
- 6 Devices
- 7 VMS
- 8 TURN
- 9 Signaling
- 10 Remote client
- 11 Remote Access WebRTC Servers
- 12 Site 1
- 13 Site 2
- 14 Site 3

AXIS Device Manager Extend

Solution overview

Connection	URL and IP	Port	Protocol	Comment
A	prod.adm.connect.axis.com (52.224.128.152 or 40.127.155.231)	443	HTTPS	Required
B	HTTP Discovery (from client to edge hosts) Data transfer (between client and edge hosts) Multicast Discovery (from client to edge hosts) Multicast Discovery (from edge hosts to client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Needed to provision the site. Optional after provision.
C	Data transfer (between edge host and devices) Unicast discovery Multicast discovery HTTP discovery	80 / custom port, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Required
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP and TCP)	Based on WebRTC standard Optional and set to off by default
E	Peer to Peer (P2P)	49152–65535	DTLS (UDP and TCP)	



AXIS Device Manager Extend with local access and remote access using a VPN connection

- 1 Axis
- 2 IAM (My Axis)
- 3 Organization data
- 4 Local client
- 5 Edge host
- 6 Devices

AXIS Device Manager Extend

Solution overview

- 7 VMS
- 8 TURN
- 9 Signaling
- 10 Remote client
- 11 Remote Access WebRTC Servers
- 12 Site 1
- 13 Site 2
- 14 Site 3

Connection	URL and IP	Port	Protocol	Comment
A	prod.adm.connect.axis.com (52.224.128.152 or 40.127.155.231)	443	HTTPS	Required
B	HTTP Discovery (from client to edge hosts) Data transfer (between client and edge hosts) Multicast Discovery (from client to edge hosts) Multicast Discovery (from edge hosts to client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Needed to provision the site. Optional after provision.
C	Data transfer (between edge host and devices) Unicast discovery Multicast discovery HTTP discovery	80 / custom port, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Required
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP and TCP)	Based on WebRTC standard Optional and set to off by default
E	Peer to Peer (P2P)	49152–65535	DTLS (UDP and TCP)	

- An additional requirement is a Public DNS such as Google DNS: 8.8.8.8 / 8.8.4.4 or Cloudflare DNS: 1.1.1.1
- Both A and C connections are needed to support full functionality of the AXIS Device Manager Extend system.
- We are in ongoing development of the application, and we therefore advise you to allow firewall access to outgoing network connections for the AXIS Device Manager Extend desktop app and any edge host.

AXIS Device Manager Extend

Prerequisites

Prerequisites

Compatible operating systems:

- Windows 10 Pro and Enterprise
- Windows 11 Pro and Enterprise
- Windows Server 2016, 2019 and 2022 (x64-based system)
- System Administrator privilege required for installation and configuration changes.

Minimum system recommendation:

- CPU: Intel Core i5
- RAM: 4 GB
- Network: 100 Mbps

Internet connectivity

Note

The AXIS Device Manager Extend application requires internet connectivity to be provisioned with certificates identifying it as belonging to the organization created and associated with the My Axis account used in the installation. However, to benefit from certain features such as warranty information and multisite support you need an internet connection. In addition, the client and/or edge host only automatically updates in the online mode.

Synchronized time and date

Note

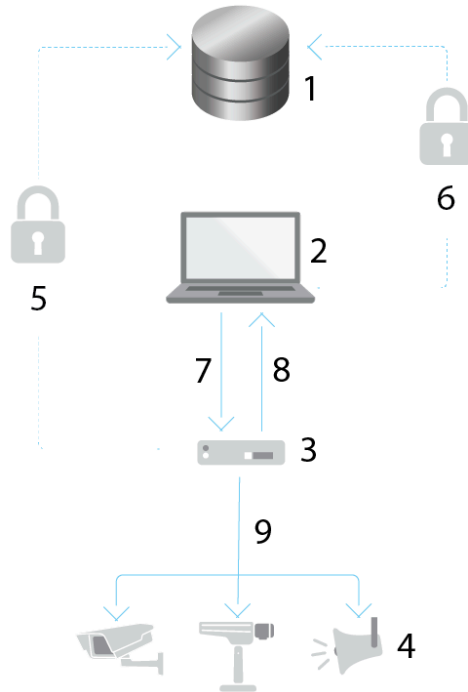
Ensure all the system components are synchronized, otherwise certificate authentication between the edge host and the client or back end could fail. It is recommended that all host machines are synchronized to a common Network Time Server to avoid any potential issues.

Open network ports:

For secure connections from the AXIS Device Manager Extend desktop app to the edge host, edge host discovery and Axis Remote Service.

AXIS Device Manager Extend

Prerequisites



- 1 Axis Service Platform
- 2 AXIS Device Manager Extend desktop app
- 3 Edge host
- 4 Devices
- 5 HTTPS (port 443)
- 6 HTTPS (port 443)
- 7 HTTPS (port 37443), UDP Multicast discovery (port 6801), HTTP discovery (port 37080)
- 8 UDP Multicast discovery (port 6801)
- 9 HTTPS and HTTP (port 443 and 80), Multicast discovery –SSDP (port 1900) – Bonjour (port 5353), Unicast discovery (port 1900), HTTP discovery (port 80 and 443)

Outgoing network access

We are in ongoing development of the application, and we therefore advise you to allow firewall access to outgoing network connections for the AXIS Device Manager Extend desktop app and any edge host.

AXIS Device Manager Extend

Get started


Get started

Register a My Axis account

Register a My Axis account at axis.com/my-axis/login.

To make your My Axis account more secure, activate multi-factor authentication (MFA). MFA is a security system that adds another layer of verification to ensure the user's identity.

To activate MFA:

1. Go to axis.com/my-axis/login.
2. Log in with your My Axis credentials.
3. Go to  and select **Account settings**.
4. Click **Security settings**
5. Click **Handle your 2-factor authentication**.
6. Enter your My Axis credentials.
7. Choose one of the authentication methods **Authenticator App (TOTP)** or **Email** and follow the on-screen instructions.

Install the client and activate your account

Go to the product page on axis.com and download the *AXIS Device Manager Extend desktop app installer*

1. Locate where you downloaded the application and click to install.
2. Select **client** and click **Install**.
3. Sign in to your My Axis account.
4. Confirm your e-mail address to complete the activation.
5. Create or join an existing organization.

Create organization

In order to add devices to your system, you need to be part of an organization. That is how you maintain and protect your devices in a secure way on one or more sites. If you're not already a member of an organization, a setup assistant will pop up and guide you through the process.

To create an organization:

1. Sign in to Axis Device Manager Extend using your My Axis account.
2. Follow the instructions of the setup assistant

To create additional organizations:

- Go to the drop-down menu with your organization's name.
- Select **+ Create new organization**
- Follow the instructions of the setup assistant.

AXIS Device Manager Extend

Get started

Install the edge host

The edge host and the desktop client are included in the AXIS Device Manager Extend installer. We recommend you install the edge host on a server as close to your devices as possible.

1. Choose a server where you want to install the edge host.
2. Run the installer on the server and only select to install the edge host.

Claim the edge host

To create a secure connection to your devices from the AXIS Device Manager Extend desktop app, you must first claim an edge host to your organization.

1. Click an edge host with the status **Unclaimed**
 - 1.1 Click **Add new edge host** if there is no edge host in the list
 - 1.2 Type the IP address of where the edge host is located
2. Type the name of your edge host
3. Add an optional description (recommended)
4. Click **Claim edge host**

AXIS Device Manager Extend

Manage devices

Manage devices

Add discovered devices to your edge host

1. Go to Edge hosts.
2. Select a claimed edge host in the list you want to add devices to.
3. Go to Devices > Discovered.
4. Select the devices you would like to add, or select all of the devices by checking the box at the top of the selection column.
5. Click Add devices to edge host .

The devices are now listed in the Managed tab, and their status can be reviewed in Edge host overview.

Add devices from IP addresses

Add devices that are not automatically discovered from subnets, individual IP addresses or an IP range.

Add devices from IP range

1. Go to an edge host claimed by your organization.
2. Go to Settings > Device discovery.
3. Click Add by IP
4. Select Manual entry
5. Type the IP range
6. Click Add IP addresses
7. Go to Devices > Discovered
8. Select the devices you would like to add, or select all of the devices by checking the box at the top of the selection column.
9. Click Add devices.

Add devices from a file

1. Go to a edge host claimed by your organization.
2. Go to Settings > Device discovery.
3. ClickAdd by IP
4. Select Import from file.
5. Select the comma separated (.CSV) file with the IP addresses
6. Click Import
7. Go to Devices > Discovered devices
8. Select the devices you would like to add, or select all of the devices by checking the box at the top of the selection column.
9. Click Add devices .

AXIS Device Manager Extend

Manage devices

Note

The file should have:
A header for the column of IP addresses.
A single column.
A maximum of 25,600 IP addresses.

Remove devices



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

help.axis.com/?&tid=63389&tsection=remove-devices

Remove devices from an edge host

1. Click **Edge host**
2. Select an edge host.
3. Go to **Devices**
4. Select the devices you would like to remove, or select all of the devices by checking the box at the top of the selection column.
5. Click the **Remove devices from edge host** icon in the action menu.
6. Click **Remove**.

The removed devices can be found in **Devices > Discovered**.

Log in to your devices

1. Click **Edge hosts**
2. Select an edge host.
3. Go to **Devices > Managed**
4. Select the devices you want to access, or select all of the devices by checking the box at the top of the selection column.
5. Click **Log in** to automatically log in to multiple devices.
6. Type the username and password.
7. Click **Log in**

Note

If the username and password are correct, the **Status** will show **Reachable**

AXIS Device Manager Extend

Configuration

Configuration

Activating remote access

If your firewall settings block outbound connections, you may have to enter a proxy connection to access the site remotely.

1. Select the edge host you want to activate remote access to.
2. Go to **Settings > Edge hosts connections**.
3. Activate **Allow remote access to edge host**.
4. If you need to enter a proxy address to access the internet, type an address under **Proxy address**.

You will be notified once the connection is active.

Note

To support the connection to edge hosts on other networks, you may have to add the following configuration to your corporate network firewall's "allow list": Endpoint Port Protocol signaling.prod.webrtc.connect.axis.com 443 HTTPS *.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn and P2P) 5349, 49152 - 65535 DTLS (UDP and TCP)

Remove a site

Before you remove an edge host from your organization, you need to *Remove devices on page 14* belonging to the edge host. The devices can then be found in **Devices > Discovered**.

1. Click **Edge hosts**.
2. Select the edge host with the arrow keys or hover over it with the mouse pointer.
3. Click **...** and select **Remove edge host** from the drop-down menu.
4. Check **I'm aware of the risks**.
5. Click **Remove**.

Add users to your organization

1. Select the organization where you would like configure user settings.
2. Go to the **My Systems** panel.
3. Go to **Organization > Users**.
4. Click **Invite users**.
5. Type the email address of the user you'd like to invite to your organization.
6. Select the role to assign to the users. Note that if you want another role for some users, you'll have to invite them in a separate invitation.
7. If you've selected **Operator** or **Viewer**, select which folders the users will have access to. Note that **Admin** roles have access to all of the folders in the organization.
8. Click **Invite user**.

Note

The user will receive an invitation email that they can use to sign in to My Systems. If the user doesn't have a My Axis account, the user must use that email to sign up in order to access the organization. Invites can be revoked while acceptance is pending.

AXIS Device Manager Extend

Configuration

About user roles

User roles determines how much access a user has to the systems in you organization. Available features vary depending on the role of the user.

Admin

Administrators have access to the entire system. That includes managing users, devices, licenses, videos and other content.

They can also onboard devices using AXIS Camera Station Pro and AXIS Installer. Administrators can manage AXIS Camera Station Pro Server Monitoring in My Systems.

Operator

Operators can monitor live video feeds, control devices, and access recordings for playback. They get an overview of the users of the organization and their respective roles. Operators can also manage AXIS Camera Station Pro Server Monitoring in My Systems.

Viewer

Viewers can monitor live video feeds, but can't control devices or access recordings. They get an overview of the users of the organization and their respective roles.

Elevate user role

1. Select the organization where you would like configure user settings.
2. Go to **Users**.
3. Go to **Role** of the user you'd like to elevate
4. Click the drop down menu to select the new role

Note

The role changes immediately once selected. For security reasons, invites are limited to the viewer role.

Remove users

1. Select the organization where you would like configure user settings.
2. Go to **Users**.
3. Hover the mouse pointer over the user you would like to remove to show a new options menu: ...
4. Click ... and select **Remove user** in the drop down menu.

AXIS Device Manager Extend

AXIS OS management

AXIS OS management

With AXIS Device Manager Extend you can manage the operating system of multiple devices in each organization.

For a list of AXIS OS updates that are available for every device in your organization grouped by model, go to Home > **AXIS OS inventory**. For a list of AXIS OS updates that are available on a specific edge host, select the edge host and go to **AXIS OS inventory**.

Manage AXIS OS versions based on model

To manage AXIS OS by model across your organization:

1. Go to Home > **AXIS OS versions**
2. Click on the recommended AXIS OS version link. That will open up the AXIS OS upgrade options.
3. Click on the **Upgrade** to drop-down menu to see what is available. The latest AXIS OS version will be preselected.
4. Click on **Upgrade**.

Manage AXIS OS on an edge host.

To manage AXIS OS on some or all of the devices added to an edge host:

1. Go to **Edge hosts**
2. Click on the edge host you want to access.
3. Go to **Devices**
4. Select all or just the devices you'd like to manage.
5. Click the **AXIS OS** icon in the action menu
6. Check all or some of the models in the list.
7. If you'd like to change the AXIS OS version, click on the suggested version to see what is available for each device. The latest AXIS OS version will be preselected.
8. Click **Upgrade**.

View ongoing and completed AXIS OS upgrades

To view ongoing software upgrades of devices connected to a specific edge host:

1. Click **Edge hosts**
2. Click on the edge host you want to access.
3. Go to **Log**

To see ongoing software upgrades:

4. Go to **Log > Ongoing tasks**

AXIS Device Manager Extend

Policies

Policies

Policies manage your devices automatically. Create policies to maintain cyber security across your site. You can also set a policy to automatically install and update apps on your devices.

Create and apply a security policy

In this example use case, we create and apply a basic security policy to a select number of devices connected to an edge host.

Create a basic security policy:

1. Go to **Edge hosts**
2. Click on the edge host you want to access.
3. Go to **Devices**
4. Click on + icon next to **Policies**
5. Select **Basic security** and click **Continue**
6. Name your policy
7. Select the settings that fits your security needs. For the recommended security level, keep the default settings.
 - To change the root password for selected devices, click **Device root password** and type the new root password.
8. Click **Create** .

Apply the policy:

1. Select the devices you would like the policy to be applied to.
2. Click the **Policy options** icon in the action menu.
3. Select the security policy and click **Save**.

Create and apply an app policy

In this example use case, we create and apply an app policy to a select number of devices connected to an edge host.

1. Go to **Edge hosts**
2. Click on the edge host you want to access.
3. Go to **Devices**
4. Click on + icon next to **Policies**
5. Select **Apps** and click **Continue**
6. Name your policy
7. Select the apps you want to be installed and updated on your devices.
8. Select the update window in the drop-down menu.
9. Click **Create** .

Apply the policy:

1. Select the devices you would like the policy to be applied to.

AXIS Device Manager Extend

Policies

2. Click the **Policy options** icon in the action menu.
3. Select the app policy you want to apply.
4. Click **Save**.

Note

The selected apps will be automatically reinstalled if removed.

Edit a policy

To edit an existing policy:

1. Go to **Edge hosts**
2. Click on the edge host you want to access.
3. Go to **Devices**
4. Click ... next to the policy you want to edit and select **Edit policy** from the drop-down menu.
5. Edit the policy settings to suit your needs.
6. Click **Save**

Delete a policy

To delete an existing policy:

- Go to **Edge hosts**
- Click on the edge host you want to access.
- Go to **Devices**
- Click ... next to the policy you want to edit and select **Delete policy** from the drop-down menu.
- Click **Delete**

Note

Any devices with that policy applied to them will keep the policy settings, but the settings will no longer be persistent.

AXIS Device Manager Extend

Manage licenses

Manage licenses

License your product

To license your product, go to *My Systems > Licenses*. To learn more about licenses for Axis products and services, see the *My Systems user manual*.

AXIS Device Manager Extend

Troubleshooting

Troubleshooting

How to configure firewall settings

AXIS Device Manager Extend client requires access to axis.com domain and any subdomain.

In order for AXIS Device Manager Extend edge host to communication with the Axis service the following IP addresses and ports should be added to the allow list of the organization's firewall:

- 40.127.155.231 (EU), port 443
- 52.224.128.152 and 40.127.155.231 (US), port 443
- A public DNS server IP, port 53

Alternatively, the domain prod.adm.connect.axis.com (which is a DNS A record pointing to the above IP addresses) could be used in the firewall settings.

AXIS Device Manager Extend edge host use the prod.adm.connect.axis.com domain name for all outbound requests.

For this to work, the network will need to use a public DNS server and allow traffic out to the DNS server IP address (and default port 53).

