AXIS Device Manager Extend

User Manual

Table of Contents

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

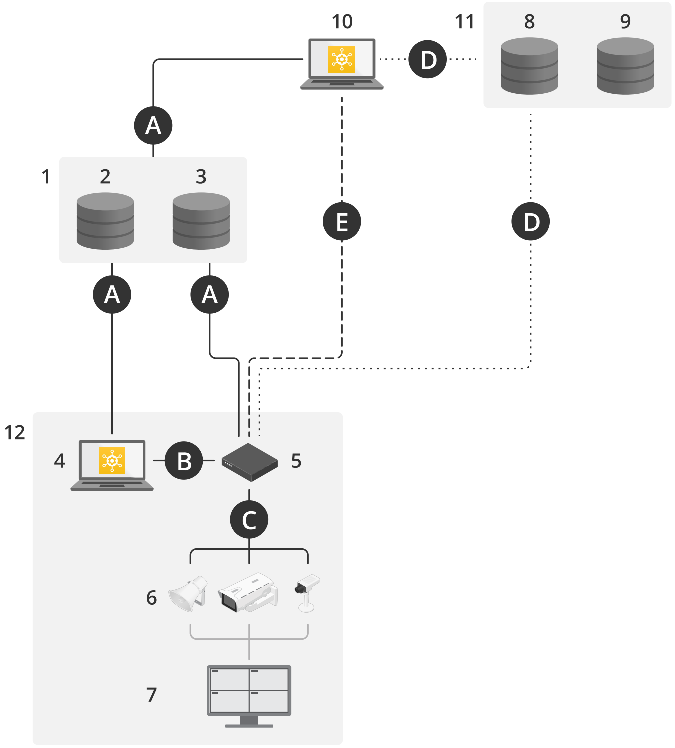
The desktop app is a software utility program that can be used as an on-demand, or always available user interface for managing the system. It can be run on a dedicated machine together with a locally installed site controller or separately from the site controller on a remotely connected laptop. The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

The site controller

The site controller component in ADM Extend is an always available, on-premise management service that is responsible for maintaining local devices, such as cameras. The ADM Extend site controller 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.

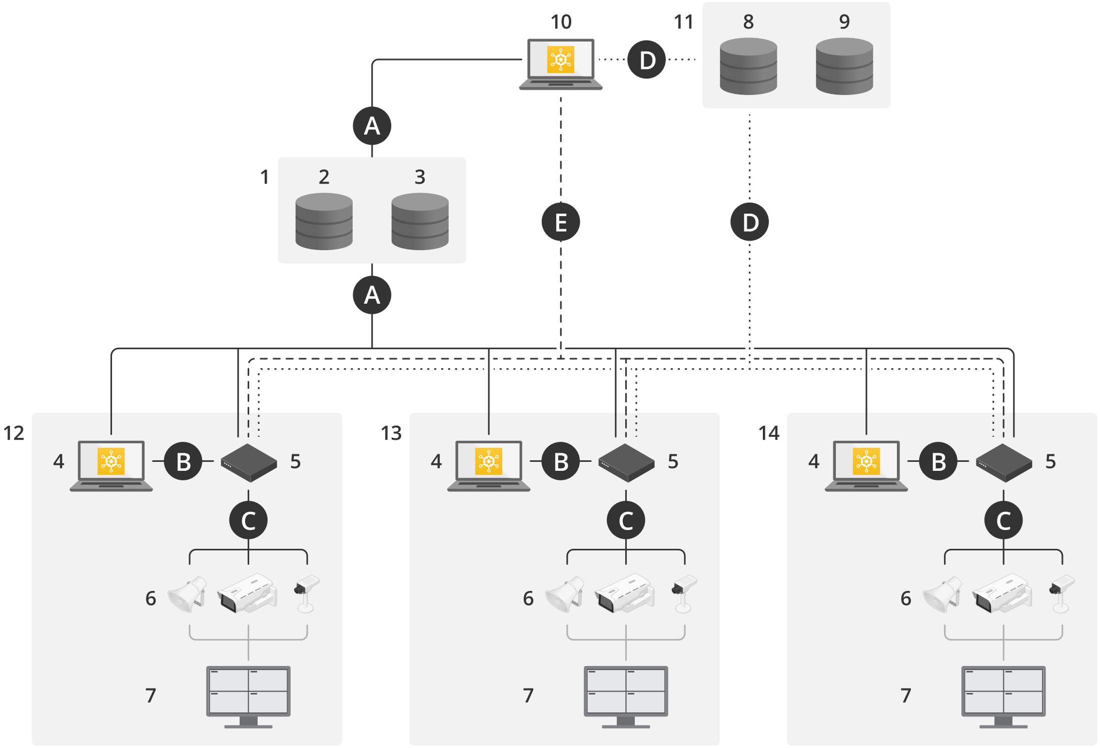
Solution overview

Solution overview



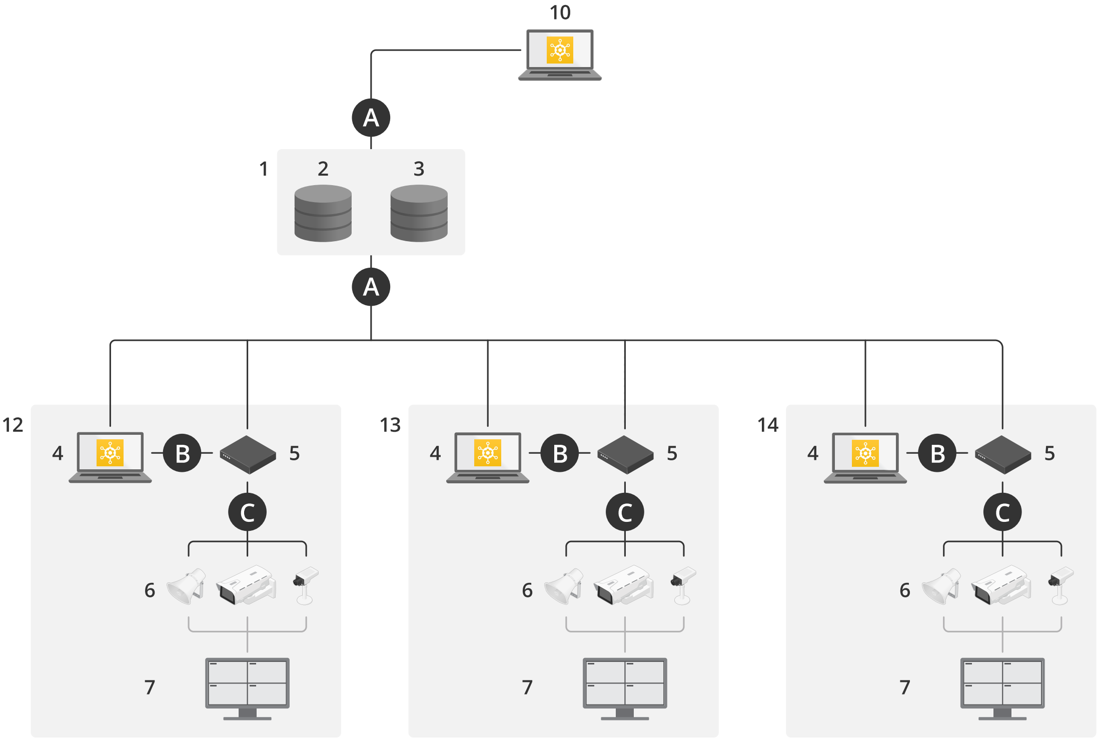
ADM Extend with local and remote access

Solution overview



ADM Extend with a multi-site setup using local and remote access

Solution overview



ADM Extend with local access and remote access using a VPN connection

1	*Axis*
2	*IAM (My Axis)*
3	*Organization data*
4	*Local client*
5	*Site controller*
6	*Devices*
7	*VMS*
8	*TURN*
9	*Signaling*
10	*Remote client*
11	*Remote Access WebCRT 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 Site Controllers) Data transfer (between client and site controller) Multicast Discovery (from client to site controllers) Multicast Discovery (from site controllers to client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Needed to provision the site. Optional after provision.

C	Data transfer (between site controller 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 (UDT and TCP)	Based on WebRTC standard Optional and set to off by default
E	Peer to Peer (P2P)	49152–65535	DTLS (UDT 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 ADM Extend desktop app and any site controller.

Prerequisites

Prerequisites

Compatible operating systems:

- Windows 10 Pro, Enterprise, Server 2016 and 2019 (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 MyAxis 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 site controller only automatically updates in the online mode.

Synchronized time and date

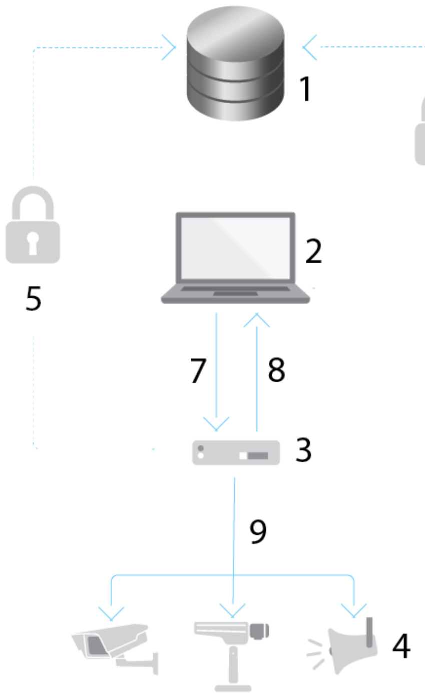
Note

Ensure all the system components are synchronized, otherwise certificate authentication between the site controller and the client or backend 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 ADM Extend desktop app to the site controller (SC), site controller discovery and Axis Remote Service.

Prerequisites



1 *Axis Service Platform*
2 *ADM Extend desktop app*
3 *Site controller*
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 ADM Extend desktop app and any site controller.

Get started

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

www.axis.com/products/online-manual/63389#t10156566

Install the software, create an organization and add devices

Register a MyAxis account

Register a **MyAxis** account at *axis.com/my-axis/login*.

You can make your MyAxis account more secure by activating multi-factor authentication (MFA). MFA is a security system that adds another layer of verification to ensure the user's identity.

Activate MFA:

1. Log in with your **MyAxis** credentials.
2. Go to **MyAxis** and select **Account settings** in the drop-down menu.
3. Turn on **2–Step verification**.

You are redirected to a login page.

4. Log in with your **MyAxis** credentials.

MFA is now active.

Log in when MFA is active:

1. Log in to your **MyAxis** account.

An email is sent to you.

2. Open the email and click **Authenticate**.

If you didn't receive an email, then check if it's in your spam folder. If it's not there, then contact IT support.

Install the site controller

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

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

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 the client and click **Install**.
3. Sign in to your MyAxis account.
4. Confirm your e-mail address to complete the activation.
5. Create or join an existing organization that the site belongs to.

Claim the site controller

To create a secure connection to your devices from the ADM Extend desktop app, you must first claim the site controller to your organization.

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

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

www.axis.com/products/online-manual/63389#t10156554

Add a site using IP address and activate Remote Access

Manage devices

Add discovered devices to your site

1. Click **Sites**
2. Go to **Devices** > **Discovered devices**
3. 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.
4. Click **Add devices** to site.

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

www.axis.com/products/online-manual/63389#t10156553

Add device to your site in AXIS Device Manager Extend

Add devices from IP addresses

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

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

www.axis.com/products/online-manual/63389#t10166268

Add undiscovered devices to your site

Add devices from IP range

1. Go to a site claimed by your organization.
2. Go to **Settings** > **Device discovery options**.
3. Click **Add subnet or IP address**
4. Select **Import from file**
5. Type the IP range
6. Click **Add IP addresses**

7. Go to **Sites**
8. Go to **Devices** > **Discovered devices**
9. 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.
10. Click **Add devices** to site.

Add devices from a file

1. Go to a site claimed by your organization.
2. Go to **Settings** > **Device discovery options**.
3. Click **Add subnet or IP address**
4. Select **Import from file**.
5. Select the comma separated (.CSV) file with the IP addresses
6. Click **Import**
7. Go to **Sites**
8. Go to **Devices** > **Discovered devices**
9. 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.
10. Click **Add devices** to site.

Note

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

Remove devices

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

www.axis.com/products/online-manual/63389#t10182209

Remove devices from your site

1. Click **Sites**
2. Select a site.
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 site** icon in the menu.
6. Click **Remove**.

Log in to your devices

1. Click **Sites**
2. Select a site.
3. Go to **Devices > Site devices**
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 **Add credentials** to automatically log in to multiple devices.
6. Type the username and password.
7. Click **Use**

Note

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

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 site you want to activate remote access.
2. Go to **Settings > Site controller connections**.
3. Activate **Allow remote access to site**.
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 site controllers 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 a site from your organization, you need to *Remove devices on page 13* belonging to the site. The devices can then be found in **Discovered devices**.

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

www.axis.com/products/online-manual/63389#t10182220

Remove a site

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

Add users to your organization

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

www.axis.com/products/online-manual/63389#t10166271

How to invite users and how they join.

1. Click you organization's name to access the organization drop down menu.
2. Select the organization where you would like configure user settings.
3. Go to **Organization** and click **Users**.
4. Click **Invite to organization**.
5. Type the email address of the user you'd like to invite to your organization.
6. Click **Send invite**.

Note

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

Elevate user role

1. Click you organization's name to access the organization drop down menu.
2. Select the organization where you would like configure user settings.
3. Go to **Organization** and click **Users**.
4. Go to **Role** of the user you'd like to elevate
5. 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. Click you organization's name to access the organization drop down menu.
2. Select the organization where you would like configure user settings.
3. Go to **Organization** and click **Users**.
4. Hovering the mouse pointer over the user bar of the user you would like to remove will show a new options menu: **...**
5. Click **...** and select **Remove member** in the drop down menu.

Firmware management

With AXIS Device Manager Extend you can manage firmware of multiple devices on the sites of each organization.

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

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

www.axis.com/products/online-manual/63389#t10175885

Upgrade Firmware in AXIS Device Manager Extend

Manage firmware based on device model

To manage firmware on a site by device model:

1. Go to **Sites**
2. Click on the site you want to access.
3. In the **Site overview**, go to **Firmware inventory**
4. Select the models you'd like to manage.
5. Click on the firmware in the **Recommended** column.
6. The latest firmware will be preselected. Check the devices in the list and click **Upgrade**. If you'd like to change the selected firmware, click on the suggested firmware to see what is available.

Manage device firmware on a site individually

To manage the firmware of some or all of the devices on a site:

1. Go to **Sites**
2. Click on the site you want to access.
3. Go to **Devices**
4. Select all or just the devices you'd like to manage.
5. Click the **Firmware upgrade options** icon in the action menu
6. The latest firmware will be preselected. Check all or some of the devices in the list and click **Upgrade**. If you'd like to change the selected firmware, click on the suggested firmware to see what is available for each device.

View ongoing and completed firmware upgrades

To see completed firmware upgrades:

Firmware management

1. Go to **Sites**.
2. Click on the site you want to access.
3. Go to **Tasks**

To see ongoing firmware upgrades:

4. Go to **Sites**.
5. Click on the site you want to access.
6. Go to **Tasks>Ongoing tasks**

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

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

www.axis.com/products/online-manual/63389#t10175884

1. Go to **Sites**
2. Click on the site you want to access.
3. Go to **Policies**
4. Select **Basic security** and click **Continue**
5. Name your policy
6. 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.
7. Click **Create** .
8. To apply the policy, go to **Devices**.
9. Select the devices you would like the policy to be applied to.
10. Go to **Policy options** in the action menu
11. Select the security policy and click **Save**

Create and apply an app policy

1. Go to **Sites**
2. Click on the site you want to access.
3. Go to **Policies**
4. Select **Apps** and click **Continue**
5. Name your policy
6. Select the apps you want to be installed and updated on your devices.

7. Select the update window in the drop-down menu.
8. Click **Create** .
9. To apply the policy, go to **Devices**.
10. Select the devices you would like the policy to be applied to.
11. Go to **Policy options** in the action menu
12. Select the app policy you want to apply.
13. Click **Save**.

Note

The selected apps will be automatically reinstalled if removed.

Edit a policy

To edit an existing policy:

- Go to **Sites**
- Click on the site you want to access.
- Go to **Policies**
- Click **...** next to the policy you want to edit and select **Edit policy** from the drop-down menu.
- Click **Save**

Delete a policy

To delete an existing policy:

- Go to **Sites**
- Click on the site you want to access.
- Go to **Policies**
- 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.

Troubleshooting

How to configure firewall settings

In order for AXIS Device Manager Extend client and site controller to communicate with the Axis service the following IP addresses and/or domain names should be added to the allowlist by the organization's firewall:

-
- 40.127.155.231 (EU)
- 52.224.128.152 or 40.127.155.231 (US)
- A public DNS IP

The URL is a simple A DNS entry which resolves to IP address 52.224.128.152 or 40.127.155.231. These IP addresses host a single application gateway that forwards the requests to the appropriate (depending on the incoming request path) backend host.

AXIS Device Manager Extend client and the site controller use the domain name for all requests.

For this to work, the network will need to use a public DNS (or for example cache the domain name in a local DNS). Therefore, in addition to the application gateway IP address, some public DNS server IP should also be added to the allowlist.

For example: Google's public DNS which is available at IPs: 8.8.8.8 and 8.8.4.4.

Provide feedback

Provide feedback

To send us feedback about the application:

1. Click **main menu icon** in the top right corner.
2. Select Provide feedback
3. Describe your experience and any thoughts on improvements
4. Enter your email address (optional)
5. Click **Send feedback**

Note

Local Axis customer representatives do not offer full support. We kindly refer you to *axis.com/support*.

User Manual
AXIS Device Manager Extend
© Axis Communications AB, 2020 - 2021

Ver. M13.2
Date: June 2022
Part No. T10153497