Technical support guide

FREQUENTLY ASKED QUESTIONS KNOWN ISSUES AND LIMITATIONS FIXES AND IMPROVEMENTS

AXIS Device Manager Extend

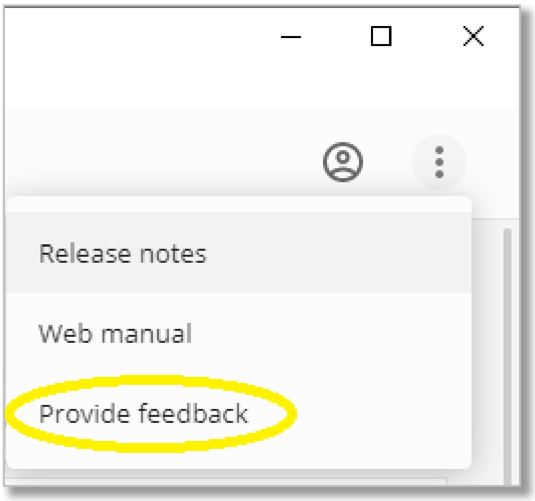
Version 1.51
Tuesday, 23 March 2021

Introduction

Axis is expanding its device management offering by launching AXIS Device Manager Extend. This tool is expected to be used in conjunction to the existing AXIS Device Manager in order to provide more focus on life cycle management and cybersecurity. The purpose of this document is to facilitate onboarding of users for this tool by covering:

- Frequently asked questions
- Known issues and limitations and
- Fixes and improvements

We encourage all people involved in testing ADM Extend to contact our dedicated project team if you cannot find the answer to your question here or if you need additional support. Please use the feedback option in the ADM Extend client available in the top right drop down menu:



NOTE:

- This document will be updated regularly

Frequently asked questions

Q: What is the main purpose of ADM Extend?

A: The purpose of ADM Extend is to broaden Axis' device management offering and contribute to the capabilities and peace-of-mind of system integrators as well as end users. We want to do this by offering a software-based tool with focus on device lifecycle management and cybersecurity. System management and security are tightly coupled since many security breaches start with poorly maintained and misconfigured systems. Furthermore, in today's complex IT environments, it is difficult to keep track of the security status of devices and make sure policies are enforced and maintained without appropriate tools. ADM Extend aspires to be such a tool for Axis devices.

Q: Why is ADM Extend tagged with 'Beta' label?

A: The program implementing ADM Extend is following the Agile software implementation philosophy. This means we aim to launch as soon as possible with the minimal functionality to support a viable product, but with commercial grade quality and then with frequent iterations, additional features will be made available in application updates. These updates are generally small and frequent, aiming to minimise disruption to the system while still keeping it up to date with the latest features and security patches. When the product has a more complete feature set and is considered more mature, we will remove the Beta tag. By using the product now and providing Axis with useful feedback via the client application, you get the opportunity to influence which features will be supported, and how they are implemented.

Q: What is the difference between ADM Extend and earlier versions of AXIS Device Manager?

A: ADM Extend should be seen as an extension to the existing ADM. ADM and ADM Extend complement each other can be used side-by-side or individually. ADM Extend focuses on lifecycle management of devices, while ADM provides more capabilities for once off configurations. ADM Extend's device management via policies supports that configurations are maintained over time and can be automatically applied to any new device as well. ADM Extend features a live dashboard which provides instant situational awareness of potential issues in the system, such as devices which are offline, out-of-warranty or sites that are not following optimal security settings and pre-set configurations. Compared to ADM, improved remote access and site health monitoring capabilities are planned for ADM Extend so that its users can concurrently manage many sites in the network from anywhere.

Q: Why an extension to the existing ADM?

A: The current ADM implementation has been around for some years now and with the intention to make the application less resource dependent and more OS independent in future, it was decided to move to a new implementation platform, so AXIS Device Manager Extend is not implemented on the .Net framework like AXIS Device Manager is.

Q: Which devices can I manage with ADM Extend?

A: Currently, you can manage Axis cameras running firmware versions 6.50 or later. Limited functionality is available for earlier firmware versions and other Axis devices (e.g. door stations). Other devices supported are:
Q-line: series 1xxx - 9xxx; P-line: series 1xxx - 9xxx; M line: series 1xxx - 8xxx; F Line: series 1xxx - 4xxx; FA Line: series FA5xxx; C line: series 1xxx - 8xxx; D line: series 1xxx - 4xxx; A line: series 8xxx only

Non-Axis ONVIF devices are currently not supported.

Q: Which components do I have to install to use ADM Extend?

A: In any ADM Extend system there are two components, the system requires at least one instance of each component, but can also support many instances of either or both components:

1. The ADM Extend client, which is preferably installed on the computer(s) intended to be used for management of the system, e.g. a roaming laptop belonging to the system administrator.

2. The site controller, which is a server application similar to and complementing the existing ADM server part. The site controller will be the entity that ensures 24/7 oversight and control of the on-premise device system. Because of this it should be installed locally on a 24/7 server machine and close to the devices to be managed. The site controller requires internet access and supports access through standard HTTP(S) proxies. Several site controllers can be installed in the network, e.g. one in every branch location, office or building. In this case, each site controller would be responsible for the devices in that location (site). But exactly how to partition the deployment would depend on the type of business, IT configuration, etc.

Q: Does ADM Extend need internet access to work?

A: Currently both the ADM Extend client and site controller components require internet access. This is to be able to auto update and to provide functionality like Warranty data, firmware updates and remote management functionality. If one component doesn’t have internet access, they will end up getting incompatible versions and will no longer be able to communicate with each other

Q: What Operating Systems are supported?

A: Currently, both the ADM Extend client and site controller components are built for Windows. Current support includes Windows 10 Professional/Enterprise, Windows Server 2019, Windows Server 2016. Mac and Linux support is planned to be available later.

Q: How do I update ADM Extend and keep my system up to date?

A: Both the ADM Extend client and the site controller(s) are Evergreen components, meaning both the ADM Extend client and site controller(s) need internet access in order to update themselves with the latest security patches and features. Your devices (e.g. cameras) will never be automatically updated as part of this process.

Q: How many devices can ADM Extend manage?

A: By default, there is a recommended limit of 1000 devices per site controller (This can be manually changed by editing the value set for ‘maxnbrofsitedevices’ in the sitecontroller.yml file to be found in ‘C:\ProgramData\site controller’). However, ADM Extend can support multiple Sites Controllers in a system, meaning that since both number of devices per site controller and number of site controllers per organisation is scalable, almost any size installation can be managed.

Q: Can I manage remote sites via ADM Extend?

A: Since client version **6.39 ADM Extend** provides full management of all Sites irrespective of the sites being local or remote to the ADM Extend client. However, it is required that the 'allow remote access to site' option be enabled in the Site Controller settings before you can connect to that particular site remotely.

Q: Do I need to register for a 'My Axis' account to use ADM Extend?

A: When using ADM Extend for the first time, the administrator is required to define their 'Organization' via their 'My Axis' account. The account used to create the 'Organization' will be what the ADM Extend system is based on. Be sure to use an appropriate account as the setup is not transferrable between MyAxis accounts.

Q: Will ADM Extend impact existing integrations, e.g. to my VMS?

A: Any pre-existing integrations will not be affected by the deployment of ADM Extend. Device configurations will not be changed by ADM Extend unless set by the system administrator. ADM Extend is designed with legacy systems in mind to make it possible to install and run the site controller side-by-side with other system components without risk of disruptions.

Q: Does ADM Extend support different types of user account?

A: Currently ADM Extend supports only one user account. This account is by default an administrator account. In a coming release to ADM Extend, additional user accounts will be possible, as will different types of user account where access levels will be restricted compared to the current admin account.

Q: Does ADM Extend require that my system uses a single NTP source?

A: It is possible to connect the ADM Extend components without using a Network Time Protocol source to synchronize the host machines time and date, however if there is any significant difference in time and date between the hosts and the Axis Service platform, issues can be encountered connecting the client and or site controllers.

Q: How does ADM Extend help administrators manage their devices?

A: The ADM Extend client provides the Administrator with a graphical overview of the aggregated system status, all in one place. Problem devices are easily accessed to address any issues.

Q: How does ADM Extend help manage the life cycle of my AXIS devices?

A: Once the system is set up, ADM Extend can display all devices information such as count of devices per model, Warranty expiration dates, discontinued date and end of support by AXIS customer service in one aggregated view, supporting easy inventory and budget planning for your security system.

Q: How does ADM Extend help raise the cybersecurity of the system?

A: ADM Extend provides an inventory of all devices in the system, along with their current status for a complete system overview. Additionally, by making use of the available policies, ADM Extend continually monitors the devices in the system to secure they are configured as specified by the system administrator.

Q: Can I update my devices firmware via ADM Extend?

A: Yes. By accessing each device individually through the AXIS Camera Assistant interface, you can manage the devices firmware. Bulk firmware management and scheduling of firmware updates is expected to be supported in a future release.

Q: Can ADM Extend help harden my network devices?

A: ADM Extend supports the configuration of some basic security options, either via the recommended defaults as specified in the AXIS Hardening Guide or as edited by the System Administrator. These security settings are applied and maintained by the site controller on the selected devices.

Q: What ACAPs are currently supported in ADM Extend?

A: Currently ADM Extend supports only the Guard Suite set of ACAPs. This means that at this time, Video Motion Detection, Motion Guard, Loitering Guard and Fence Guard can be set to be installed, maintained and updated on the system devices by ADM Extend. Additional ACAP support will be added in coming releases.

Q: Can I configure my ACAP via ADM Extend?

A: ADM Extend currently supports installation, updating and maintaining that the ACAP is active. However, any run time configuration is not supported via ADM Extend yet. This functionality together with license management is expected to be supported in a future release.

Q: What can I do about the site controller being identified as a Trojan by my AntiVirus scanner?

A: Axis has identified a minority of antivirus scanners (2/69) that may identify the site controller as a potential threat. Axis ensures the integrity of the site controller install, but to ensure ADM Extend operation, AXIS suggests to specify the following in the "allowed" list in the applicable antivirus suite:

C:\Program Files\site controller
C:\ProgramData\site controller
C:\Users\Administrator\AppData\Roaming\adm6-client
C:\Users\Administrator\AppData\Local\@adm6electron-updater
C:\Users\Administrator\AppData\Local\Programs\@adm6electron

Q: Is AXISREMOTEACCESSSERVICE.EXE malware?

A: No. This is a module included in AXIS Device Manager Extend which supports the remote connection between client and remote site controllers. This service should be added to any anti-virus allow list.
If you experience this issue, please report it to AXIS using the 'Provide Feedback' option in the 'more' menu top right of the ADM Extend client, or by mailing adm-extend@axis.com

Q: Is it possible to manage all my site controllers outgoing data?

A: Yes! Each site controller has the possibility to be configured to connect via a local proxy to secure all outgoing data can be managed from one internal access point.

Q. How can I tell if my device is being managed by ADM Extend?

A. If you check what users are configured on the device (settings > system > users), and there is a user called "AXISDeviceMgmt" for ADM Extend clients 6.39 and later or "scuser" (site controller user for clients pre version 6.39) then it is likely that the device is under management of ADM Extend.

Q. Why doesn’t the site controller find my devices?

A. 1. Check discovery options are enabled on the devices. 2 Check the site controller can ping the camera network. 3. Try adding the device subnet to the site controller specifically (Settings > subnet).

Q: My network is behind a corporate firewall, will ADM Extend still work?

A: Yes! ADM Extend directs all its outgoing connections used for remote management, warranty data, firmware images and device status information to be shown on the aggregated Dashboard via a unified endpoint.
This endpoint should be added as a trusted destination to your corporate firewall. The details of this connection are:

- prod.adm.connect.axis.com = 40.127.155.231 and 52.224.128.152
- Some public DNS IP

The URL prod.adm.connect.axis.com is a simple A DNS entry which resolves to IP address 40.127.155.231 or 52.224.128.152. These IP addresses hosts an Application Gateway forwarding the requests further to the appropriate (depending on the incoming request path) backend host.

Both the ADM Extend client and the site controller will use the domain name for all requests.

For this to work the network will need to use a public DNS (or e.g. 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 available (added to the allowlist).

For example: Google’s public DNS available at IPs: 8.8.8.8 and 8.8.4.4 or CloudFlare’s public DNS available at 1.1.1.1.

For Remote Access to site controllers on other subnets than where the client is running, additional firewall configuration is required:

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)

Q: Can you explain in more depth when and why internet access is required for ADM Extend?

A: The computer running the ADM Extend client requires internet access when you provision a new site controller into your organization, i.e. when creating a new site. The reason for this is to ensure system security and integrity. As part of the provisioning process, ADM Extend will download security certificates and install them in the site controller server. This will ensure the site controller will be part of the same security domain as the ADM Extend client, which is needed make sure data is not leaked outside of that domain as well as prevent the site controller for communicating with any entities not part of the same domain.

ADM Extend also needs internet access when you login to a site in order to be able to verify and renew the security certificates.

The site controller does not rely on internet access to maintain the local system 24/7. But some functionality will not be available in such a case, e.g. automatic download and storage of device firmware or ACAPs, download of device warranty and discontinuation information etc. The site controller has support for internet access though standard proxies, so it is possible to control and schedule access from there.

As mentioned, internet access is required for both client and server as part of the running field tests. As also mentioned, ADM Extend does not require devices, e.g. cameras, to be externally connected.

Q. What is the AXIS Device Management Service ACAP?

A. You may see some references to AXIS Device Management Service ACAP. This is an ACAP installed on devices being managed by a site controller. This ACAP provides additional functionality to devices that support those capabilities. You could see references to this ACAP in the site log, Axis Camera Assistant, or even in the Support ACAP for example.

Q. Why can’t I access my devices that have Anonymous Viewer enabled?

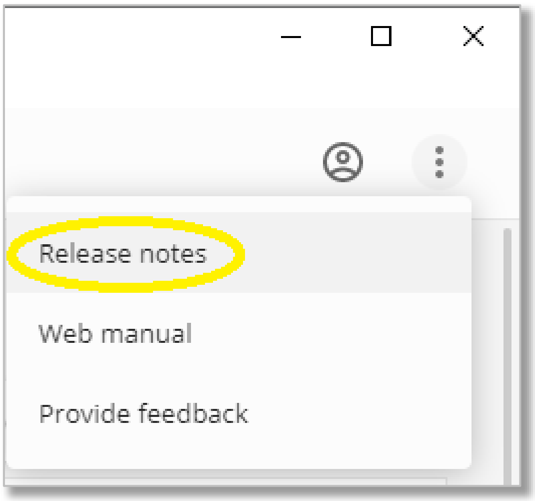
A When enabling the anonymous viewer option in the Axis device, the anonymous viewer is the default user expected to access the device. AXIS Device Manager Extend currently does not support opening the user interface directly for these devices. It is recommended to either disable anonymous viewer option (more secure as well) or manually open the user interface in a browser instead.

Known issues and limitations

Limitation	Description
Currently only one user available	Multi-user support in ADM Extend is under development and will be available soon (Q42020). There is also the intention of providing different user access levels. However, currently, one organization = one user credential set.
ONVIF devices	There is currently no support for ONVIF devices.
Maximum number of devices per site	Currently, the maximum number of devices per site is limited to 1000 on a Windows server.(can be adjusted, see FAQ)
Log in	The initial authentication or registration of a new MyAxis log in is not supported via Internet Explorer, Chrome is recommended instead.
Application access	Currently only the user installing the application gets access to it. Not all host users will be able to access the ADM Extend client.
Anonymous Viewer	Devices that have anonymous viewer enabled cannot open their user interface directly in the ADMX client but should be opened in a browser instead.

Fixes and improvements

See the Release Notes available in the application:


Release notes
Web manual
Provide feedback